VIRTUBLIC

II

THE CAPITAL OF THE DIGITAL ECONOMY

VIRTUBLIC

Axiomatic Theory of Cybernetic Republicanism

VOLUME II

THE CAPITAL OF THE DIGITAL ECONOMY

Critique of Blockchain, Cryptocurrencies, and Digital Democracy

---

The theoretical work was realized with the support of the Home Office (UK) under the Section 95 program.

PREFACE

Volume I established the diagnosis. It determined that the attention economy is not a side effect of technological development but a system of political domination that generates measurable destruction of subjecthood through mechanisms structurally inaccessible to individual or collective resistance from within the system itself. The diagnosis concluded with the only question that logically follows from it: does an institutional form exist that is capable of constraining this system from without?

The present volume answers that question through the deconstruction of the most technically sophisticated attempt at such an answer proposed over the past decade.

Blockchain ideology proclaimed itself an alternative to platform capitalism. Its declarative foundation appears compelling: decentralized consensus in place of platform control; transparent code in place of opaque algorithm; anonymity in place of predictive profiling; automatic execution of the smart contract in place of the arbitrary decision of the corporate operator. Had these declarations corresponded to architectural reality, blockchain would have constituted the sought answer, and the present volume would not have been necessary.

It became necessary because the declarations do not correspond to reality — and this non-correspondence is not an incidental defect of implementation but a structural consequence of architectural foundations. The seven theorems of the present volume (T11–T17) prove, in sequence, that blockchain reproduces the contradictions of digital capital on a new substrate. Decentralization relocates the concentration of power to the level of token stake rather than eliminating it. Governance through token voting is a self-legitimating mechanism without an external normative source. The anonymity of the address generates power without political accountability. The smart contract without a normative axiom optimizes efficiency while systematically destroying subjecthood. The verification of the uniqueness of the subject without a trusted center is a logically irresolvable problem. Critique that proposes no institutional alternative is absorbed by the system as a legitimation resource.

The present volume is, nonetheless, not a negation of blockchain. T17 — the synthetic theorem of the volume — establishes that blockchain as a technological substrate is a necessary condition of the constitutional architecture of Volume III: zero-knowledge proof makes technically possible the protection of the right to unpredictability; the smart contract makes possible the automatic execution of constitutional norms; formal verification through Coq makes possible the constitutional audit of algorithms. Without this technological substrate, Volume III (Formal Theory of the Digital Republic) would be a declarative text rather than an operational specification.

The analytical structure of the volume reproduces the logic of Volume I, inverting its direction: there, the diagnosis was constructed bottom-up — from ontology to normative

synthesis; here, the deconstruction is constructed top-down — from the declared foundations of blockchain ideology to their structural defects, and from the defects to the sole identified solution. The three parts of the volume correspond to three analytical layers: the ontology of blockchain as a system of accumulation, the anthropology of blockchain as a system of subjectivation, and the epistemology of blockchain as a system of self-reproduction of legitimacy.

The volume concludes with the only inference that logically follows from the totality of its results. Blockchain technology is necessary. Blockchain ideology is insufficient. Critique without an institutional alternative stabilizes the system. The sole realizable form remains a constitutional architecture that employs blockchain as an instrument and constrains it by the logic of NA0 as a constitutional limit.

That architecture is constructed in Volume III.

INTRODUCTION

The Originating Contradiction

Volume II begins where Volume I ends: the impossibility of the self-regulation of digital capital has been proven. Blockchain emerged as a technological response to these problems: decentralization against monopolies (T2, the temporal barrier); cryptography against surveillance (N1, the right to unpredictability); smart contracts against arbitrariness (the principle of code supremacy).

Yet Volume II proves: blockchain as ideology fails. Decentralization reproduces concentration at a new level (proof-of-stake plutocracy). Cryptocurrencies generate new forms of alienation (tokenization as universal equivalent). DAOs do not resolve governance without legitimacy. Code is law without a normative axiom optimizes efficiency at the expense of subjecthood.

However, blockchain as technology remains the necessary substrate for the constitutional solution (Volume III). Cryptography (zk-proof), smart contracts, formal verification — these are instruments without which Virtublic is impossible.

Volume II is a critical theory of blockchain: what it attempts to resolve, why it fails, what can be salvaged from it. But it is also a meta-critique: an analysis of how critical discourse itself becomes part of the system it critiques.

0.1. Context of Emergence

Blockchain emerged as a response to four crises of digital capital (Volume I).

(1) The crisis of monopolization (T2): dominant platforms possess the temporal barrier through the early history of data. Blockchain proposes decentralization — the elimination of a single center of control.

(2) The crisis of surveillance (T1, surplus attention): platforms extract predictive value without compensating the subject. Blockchain proposes cryptography — the protection of data through privacy.

(3) The crisis of legitimacy (T8, the sovereignty gap): predictive power (de facto) and political sovereignty (de jure) move in opposite directions. Blockchain proposes code is law — the automatic execution of rules without human arbiters.

(4) The crisis of governance (T9, systemic collapse): the state as a purchaser of predictions cannot be a neutral regulator (structural Regularity 12, Volume I). Blockchain proposes DAOs (Decentralized Autonomous Organizations) — governance without the state.

The central thesis of Volume II: each of these solutions generates a new contradiction that reproduces the logic of digital capital at a new level. Moreover, the critical discourse concerning blockchain (and digital capital in general) itself becomes part of the system through the absorption and monetization of critique.

0.2. Methodological Approach

Volume II continues the axiomatic structure of Volume I but analyzes a new object — blockchain as an attempted institutional response. Numbering continues without interruption: axioms A19–A36 (ontology, anthropology, epistemology of blockchain); structural regularities 14–27 (derived from axioms A19–A36 and regularities 1–13 of Volume I); theorems T11–T17 (logical inferences proving the contradictions of blockchain).

Each theorem concludes with an indication of the solution in Volume III (Virtublic). This creates continuity: Volume I proves the impossibility of digital capital, Volume II proves the insufficiency of blockchain and the absorption of critique, Volume III (Formal Theory of the Digital Republic) proposes the constitutional architecture that employs blockchain technologies but avoids its contradictions.

0.3. Objective and Structure

To prove that blockchain ideology (decentralization, anonymity, code is law, token voting) reproduces the contradictions of digital capital. To demonstrate that blockchain technology (cryptography, smart contracts, zk-proof) remains a necessary substrate for Virtublic. To derive seven theorems (T11–T17) proving the structural contradictions of the capital of the digital economy. To prove that critique without an institutional alternative is absorbed by the system and becomes its stabilizer (theorem T16). To formulate the theorem of the constitutional necessity of blockchain (T17).

0.4. Criterion of Success

Volume II is considered successful upon the fulfillment of four conditions: (1) each contradiction of blockchain is formally proven through axioms A19–A36 and theorems T11–T17; (2) the connection with Volume I is demonstrated: each theorem T11–T17 explains why blockchain fails to resolve a specific theorem of Volume I; (3) the connection with Volume III is demonstrated: each theorem indicates how Virtublic resolves the contradiction through specific principles P0–P18; (4) it is proven that critical discourse without an

institutional alternative is absorbed by the system (T16), and that Virtublic avoids this absorption through constitutional form.

0.5. Key Terms

Blockchain — a distributed database with cryptographic protection of integrity. Analyzed as ideology (decentralization as a sufficient condition) and as technology (cryptography as a necessary substrate).

Proof-of-Work (PoW) — a consensus mechanism through computational power. Criticized for energetic inviability.

Proof-of-Stake (PoS) — a consensus mechanism through token ownership. Criticized for plutocracy (theorem T11).

Cryptocurrency — a digital asset used as a medium of exchange on a blockchain. Analyzed as an attempt to create a universal equivalent without state issuance.

Tokenization — the conversion of rights, assets, or access into tokens on a blockchain. Analyzed as a new form of alienation (axiom A22).

DAO (Decentralized Autonomous Organization) — an organization governed through smart contracts and token voting. Analyzed as governance without legitimacy (theorem T12).

Code is law — the principle of automatic execution of smart contracts without the possibility of human intervention. Analyzed as the optimization of efficiency without the protection of subjecthood (theorem T14).

Sybil resistance — protection against the creation of multiple fictitious identities. Analyzed as a requirement of centralization (theorem T15).

Critique as commodity — the monetization of critical discourse within the same attention economy it critiques. Analyzed through Regularity 18 and theorem T16.

Civic Guard — a college of civilian juror-auditors, randomly selected through VRF for the verification of the uniqueness of citizens in the course of Digital Census v2 (principle P13, Volume III). The sole form resolving the contradiction of T15 without reproducing centralization.

0.6. Key Philosophical References

Marx (critique of the universal equivalent, Capital Vol. I), Foucault (power through technique, not through ideology), Habermas (communicative action versus systemic action), Lessig (code is law), Zuboff (instrumentarian power), Srnicek (platform capitalism, Volume I).

Blockchain theorists: Vitalik Buterin (Ethereum governance), Vlad Zamfir (against governance minimization), Primavera De Filippi (DAO governance). Critics of blockchain: Nicholas Weaver, David Golumbia, Evgeny Morozov.

Critique as stabilization: Volume II analyzes not only blockchain as an institutional form but also critical discourse about digital capital as a structural element of the system itself. Zuboff, Han, Stiegler, Morozov brilliantly diagnose the conversion of subject into object — but their solutions remain within the ontology of the system (regulation, spiritual resistance, educational reform). Not one of them poses the question of a constitutional architecture external to the logic of capital and the state. This is not accidental. Critique that does not transcend the diagnosis performs the function of channeling tension: the reader is outraged, feels enlightened — and remains within the system.

0.7. How to Read This Volume

Parts I–III (axioms A19–A36, regularities 14–27): for blockchain theorists, economists, and political philosophers. They describe the structural contradictions of blockchain and critical discourse.

Part IV (theorems T11–T17): formal proofs, logically self-contained. For those who wish to verify the rigor of the argumentation.

Part V (connection with Volumes I and III): demonstrates how Volume II continues the diagnosis of Volume I and why it necessitates the solution of Volume III.

Appendices A–H: technical details of protocols, formal proofs, simulations, bibliography.

ANALYTICAL SYNOPSIS

PART I. THE ONTOLOGY OF BLOCKCHAIN

The Objective Layer: What Blockchain Is as a Structure — The Thesis of Decentralization. Objective: To describe blockchain as an institutional attempt to resolve the contradictions of digital capital (Volume I) and demonstrate that its own axioms logically produce new contradictions.

Chapter 1. Decentralization as the Primary Principle

Axioms of the Ontology of Blockchain

A19. Axiom of Decentralization. Decentralization — the elimination of a single center of control — is declared a sufficient condition for overcoming monopolization, on the premise that distributing data and computation across nodes eliminates the temporal barrier (T2, Volume I). Critique: monopolization occurs through temporal advantage in data history, not through a technical single point of failure; decentralization distributes control but does not eliminate the structural advantage of early participants.

A20. Axiom of Consensus Mechanisms. Majority consensus among nodes — through computational power in proof-of-work or token ownership in proof-of-stake — replaces trust in a centralized arbiter without external verification. Critique: majority consensus is not a sufficient source of legitimacy; in PoS, the majority is of capital, not citizens, reproducing governance without legitimacy (T12).

A21. Axiom of Immutability. Cryptographic hash functions make the transaction history unalterable without majority consensus. Critique: immutability protects against arbitrary revision but renders errors permanently uncorrectable, conflicting with the legal principles of rectification and intent.

1.1. Axioms of Tokenization

A22. Axiom of the Token as Universal Equivalent. Any right, asset, or access may be represented as a blockchain token, eliminating intermediaries through direct exchange. Critique: reproduces Marx's critique of the universal equivalent — all concrete relations are reduced to an abstract form; political participation is reduced to capital ownership.

A23. Axiom of Liquidity. Liquidity — free market exchange — is the primary property of a token; an illiquid token is worthless. Critique: converts all governance instruments into speculative assets, placing control in the hands of those who can purchase most tokens rather than those who participate.

A24. Axiom of Programmability. Smart contracts automate economic relations without intermediaries, eliminating human arbitrariness. Critique: power is not eliminated but relocated to the level of code authorship — algorithmic power (Regularity 14).

1.2. Decentralization as Ideology and Its Limit

Blockchain ideology rests on a libertarian presupposition: power is localized in institutions and can be eliminated through technical decentralization. Volume I proved (Regularity 12) that power is distributed within the structure of accumulation, not in institutions. The temporal barrier (T2) is structural, not technical — decentralization cannot dissolve it. PoW reproduces concentration through the energy barrier; PoS reproduces it through the token barrier. Both instantiate a new form of Ω_0 rather than resolving the original.

1.3. Cryptocurrencies, NFTs, and Governance Tokens

Cryptocurrencies fail to fulfill the three functions of money (medium of exchange, measure of value, store of value) and add financial speculation without resolving digital capital (Volume I). NFTs do not create scarcity but create a speculative market for ownership records — the attention-token crystallizes into a tradeable status signal, reproducing T1. Governance tokens formally decentralize decision-making but reproduce plutocracy (T12): whoever holds more tokens controls governance, replacing predictive power with tokenomic power without resolving T8.

Chapter 2. Consensus as a Surrogate for Legitimacy

Structural Regularities of the Ontology of Blockchain

Regularity 14 (from A19 + A24). Algorithmic Power. Decentralization relocates power from institutions to algorithms; whoever writes the code determines the rules, constituting a new form of governance without democratic legitimacy. Formal expression: Power(institutions) → Power(code writers + early adopters).

Regularity 15 (from A20 + A22). Plutocratic Consensus. Proof-of-Stake consensus is structurally equivalent to one token, one vote — a plutocracy, not a democracy — reproducing T2 at the level of tokens. Formal expression: Influence(i) ∝ Stake(i).

Regularity 16 (from A21). Irreversibility Without Justice. Immutability protects against arbitrary revision but makes unjust past consensus uncorrectable without a hard fork, constituting a new form of Regularity 12: regulation from within is structurally foreclosed. Formal expression: Error(t) ∈ Blockchain → Correction requires Fork.

Regularity 17 (from A23). Liquidity Destroys Governance. Free market exchange of governance tokens structurally enables governance capture by those with sufficient capital to purchase a majority. Formal expression: Liquidity(token) ↑ → Governance capture ↑.

Chapter 3. The First Proto-Theorem of Ontology and the Crisis of Objectivity

Proto-theorem of the ontology of blockchain (from Regularities 14–17). The blockchain system reproduces the structural properties of digital capital (T1–T3, Volume I) on a new technological substrate without eliminating them, which structurally necessitates an anthropological layer of analysis.

Δ3 — CRISIS: THE LIMIT OF THE OBJECTIVITY OF BLOCKCHAIN

Regularities 14–17 describe blockchain capital movement but contain an implicit subject of consequences — the holder who bears the costs of plutocracy, the user excluded from governance, the developer who writes rules without democratic mandate. Without identifying these subjects, the ontology of blockchain is formally incomplete. Δ3 obliges transition to the anthropological layer.

PART II. THE ANTHROPOLOGY OF BLOCKCHAIN

The Subjective Layer: Who Lives Within Blockchain — The Antithesis. Objective: To identify blockchain subjects and demonstrate how they reproduce the alienation of digital capital (Volume I).

Chapter 4. The Class Morphology of Blockchain

Axioms of the Anthropology of Blockchain

A25. Axiom of Anonymity. The blockchain subject is a private key, not a physical person; identity is not required for participation. Critique: subjecthood defined as a key eliminates political accountability — if the subject is a key, no person bears responsibility for actions (T13).

A26. Axiom of Pseudonymity. All transactions are public but attached to addresses rather than persons, making blockchain pseudonymous rather than anonymous. Critique: pseudonymity creates surveillance without protection — address-person linkage established once exposes the full transaction history to state or corporate surveillance.

A27. Axiom of the Holder as Subject. The blockchain subject is a holder, not a user or a citizen; governance rights attach to token ownership. Critique: reduces subjecthood to capital ownership; the daily user without tokens bears consequences but holds no voice, reproducing T4 (accountability without power).

A28. Axiom of Key Privacy. The private key constitutes total asset control with no recovery mechanism, protecting against state confiscation. Critique: generates irreversible errors through key loss; does not protect against coercion since the state may compel disclosure under legal threat.

A29. Axiom of Anonymization Instruments. Privacy is enhanced through transaction-mixing services and privacy coins employing Ring Signatures and zk-SNARKs. Critique: anonymization instruments are economically penalized by the system — coins from mixers rejected by exchanges, privacy coins delisted — confirming T5: individual resistance is economically non-viable.

A30. Axiom of Staking as Economic Participation. Staking — locking tokens to obtain validator rights and rewards — is the primary form of economic contribution in PoS systems. Critique: conceals compound interest accumulation whereby wealthy stakers grow wealthier without creating new value, reproducing Regularity 15 at the level of economic participation.

4.1. Five Class Positions of Blockchain

Holders control governance through token voting but are motivated by token price appreciation, not system welfare. Stakers possess the infrastructure and capital for PoS validation, receiving rewards proportional to stake — structurally analogous to infrastructure operators of Volume I but with political power through governance tokens. Users employ the system daily but hold no governance tokens, bearing consequences without voice — reproducing T4. Developers write smart contracts and protocols, possessing algorithmic power (Regularity 14). Critics analyze contradictions but propose no institutional alternative external to the system's logic, extracting symbolic and economic capital from diagnosis without resolution — a structural position, not a personal failing: the system requires critique to legitimize itself as open to discussion.

4.2. The Reproduction of the Temporal Barrier at the Level of Tokens

Early holders possess a structural advantage across three vectors: governance control through majority token holdings; economic advantage through early low-price acquisition yielding appreciation without additional contribution; and network effects through value

extraction from growth they did not generate. This is the precise analogue of T2 (Volume I). Blockchain does not resolve the temporal barrier — it reproduces it at the token level.

Chapter 5. Anonymity, Pseudonymity, and Surveillance

5.1. Blockchain pseudonymity generates surveillance by design: address-person linkage through KYC exposes full transaction history to states and corporations, while on-chain public records enable social surveillance of wealth. Blockchain does not protect privacy (N1, Volume I) — it creates transparency without protection.

5.2. Anonymization instruments technically realize N1 but are economically penalized — rejected by exchanges, delisted from markets — confirming T5: individual resistance is economically non-viable. The system does not prohibit privacy; it renders its exercise financially ruinous.

Chapter 6. The Holder as Economic Subject

Structural Regularities of Holder Subjectivity

Regularity 18 (from A27 + class position of critics). Critique as Commodity. Critical discourse concerning digital capital is monetized within the same attention economy it critiques, converting critique into a system stabilizer rather than a threat, since any critique that proposes no institutional alternative is absorbed as a legitimation resource. Formal expression: Critique(system) → Monetization(critique) → System_stability ↑. Connection with Volume III: Virtublic does not critique digital capital — it constructs a constitutional alternative that crystallizes diagnosis into institutional architecture (P0–P18).

Regularity 19 (from A27 + A23). Speculative Motivation of Holders. Holder governance decisions structurally optimize token price rather than user welfare, since holder income depends on price appreciation rather than system health. Formal expression: Governance(decisions) → max(Token_price), not max(User_welfare).

Regularity 20 (from A29 + Regularity 17). Governance Capture Through the Market. Free exchange of governance tokens enables hostile capture through open-market purchase of a majority stake, which is technically legitimate under consensus logic but politically unjust and structurally irresistible by minority holders, reproducing T5. Formal expression: Capture_cost = Token_price × Tokens_for_majority.

Chapter 7. Stakers, Validators, and the Concentration of Infrastructure

Regularity 21 (from A20 + A30). Concentration Through Staking. PoS rewards proportional to stake produce compound wealth accumulation whereby wealthy stakers grow wealthier without creating new value, reproducing A6 (self-augmentation without saturation, Volume I). Formal expression: Wealth(t+1) = Wealth(t) × (1 + staking_reward_rate).

Regularity 22 (from A20 + A30). Centralization Through Staking Pools. Capital barriers to individual validation drive holders into staking pools, producing structural centralization of proof-of-stake, thereby refuting A19 and reproducing T2: early and wealthy participants dominate through pooled infrastructure.

Chapter 8. The Second Crisis: The Limit of the Anthropology of Blockchain

Regularities 18–22 establish that no blockchain subject — holder, staker, user, or critic — constitutes a genuine political subject: each is structurally motivated by economic accumulation, excluded from governance, or absorbed as a legitimation resource.

Δ4 — CRISIS: THE LIMIT OF THE SUBJECTIVITY OF BLOCKCHAIN

Individual resistance within blockchain is economically neutralized (T5). Critique is absorbed through monetization (Regularity 18). No collective subject can alter blockchain's structure because any collective action reproduces the plutocratic logic of token voting. This necessitates the epistemological layer: how does the system reproduce its own legitimacy despite evident contradictions?

PART III. THE EPISTEMOLOGY OF BLOCKCHAIN

The Synthetic Layer: How Blockchain Reproduces Itself as Truth. Objective: To demonstrate how blockchain constructs governance without legitimacy, code is law without a normative axiom, and Sybil resistance through centralization.

Chapter 9. Code Is Law and Its Limits

Synthetic Axioms of the Epistemology of Blockchain

ΣA31. Axiom of Code Is Law. Smart contracts execute automatically without human intervention; the rule encoded is the rule enforced, with no judges, appeals, or exceptions — rendering even exploit-based violations technically legitimate within this logic. Critique: arbitrariness is relocated to the level of code authorship (Regularity 14), and code is law without NA0 optimizes efficiency while systematically failing to protect subjecthood (T14).

ΣA32. Axiom of Irreversibility Without Correction. Deployed smart contracts cannot be altered; immutability protects rules from arbitrary revision but renders vulnerabilities permanently exploitable and unjust past consensus irreversible without a hard fork. Critique: produces systemic uncorrectable errors in direct conflict with the legal principles of intent and rectification.

ΣA33. Axiom of the Absorption of Critique. The system absorbs any critique that proposes no institutional alternative external to its logic, converting critique into a legitimation resource

demonstrating openness to discussion. Connection with Volume III: a constitution cannot be cited as evidence of openness — it can only be observed or violated.

ΣA34. Axiom of the DAO as Governance Without Legitimacy. DAOs governed through smart contracts and token voting eliminate traditional institutions but structurally reproduce plutocracy by design (Regularity 19), since token voting lacks any external source of legitimacy beyond self-referential code — circular legitimation. Critique: the elimination of institutions does not eliminate power; it relocates it to holders.

ΣA35. Axiom of Sybil Resistance as a Structural Problem. Blockchain's vulnerability to the creation of multiple fictitious identities for governance capture cannot be resolved without a mechanism for uniqueness verification, which is impossible without a trusted center — directly contradicting A19.

ΣA36. Axiom of Proof-of-Personhood and Its Limits. Proof-of-personhood mechanisms — biometric or social-graph verification — require centralized trusted authorities to function, contradicting decentralization and generating permanent privacy risks from biometric identifiers that cannot be changed if compromised.

9.1. NA0 (Volume I) established subjecthood as a politically protectable good. Smart contracts contain no NA0; they optimize a specified objective function without protecting subjecthood — the subject becomes an object of protocol optimization, reproducing the alienation of T1.

Chapter 10. Governance Without Legitimacy

10.1. DAOs reproduce T8 (the sovereignty gap): de jure, governance is formally decentralized; de facto, it is controlled by early holders, whales, and an active minority, with the majority of holders passive. Formal decentralization masks factual concentration.

10.2. Voter apathy is a structural regularity: DAO governance turnout typically falls below 10%, meaning decisions are made by an active minority of 5–10% of holders — not democracy, not even plutocracy, but an oligarchy of activists.

Chapter 11. Sybil Resistance as Centralization

Any mechanism of Sybil resistance requires compromise among three mutually incompatible requirements: centralized verification (contradicts A19); economic barrier through proof-of-stake (reproduces Regularity 15); computational barrier through proof-of-work (reproduces Regularity 22). No decentralized mechanism of Sybil resistance exists without sacrificing one of the three. This is theorem T15. Connection with Volume III: Virtublic acknowledges T15 honestly and resolves it through Digital Census v2 (P13) with the Civic Guard — a constitutionally responsible form of verification external to accumulated capital.

Chapter 12. Structural Regularities of the Epistemology of Blockchain

Regularity 23 (from ΣA31 + ΣA32). Code Bugs as Governance Crisis. Smart contract vulnerabilities generate governance crises requiring hard fork consensus that is difficult to achieve, producing network fragmentation.

Regularity 24 (from ΣA34). Governance by Active Minority. Low DAO turnout produces decision-making by 5–10% of holders — an oligarchy of activists, not a democratic form.

Regularity 25 (from ΣA35 + ΣA36). The Sybil Resistance Trilemma. Decentralization, Sybil resistance, and the absence of plutocracy cannot be simultaneously achieved; any solution sacrifices one of the three. Formal expression: Decentralization ⋀ Sybil_resistance ⋀ ¬Plutocracy = ⌀.

Regularity 26 (from A25 + ΣA31). Anonymity Without Accountability. Code is law combined with anonymous identity makes legal prosecution of contract exploits structurally impossible.

Regularity 27 (from all preceding regularities). Blockchain as an Insufficient Form. Blockchain resolves technical problems (Byzantine fault tolerance, double spending) but not political problems (legitimacy, accountability, justice) — necessary as technology, insufficient as institutional form.

PART IV. CONTRADICTIONS AND FAILURES

Theorems of Blockchain: Formal Proofs of Structural Contradictions. Objective: To construct a formal theorem for each blockchain contradiction and demonstrate connections with Volumes I and III.

Chapter 13. The Plutocracy of Proof-of-Stake

T11. Theorem of the Plutocratic Inevitability of PoS. Under proof-of-stake consensus, the system inevitably concentrates in the hands of early token holders, relocating the temporal barrier (T2, Volume I) to the token level without resolving it.

Proof: (1) PoS rewards are proportional to stake (Regularity 21). (2) Early holders acquired tokens at low price through ICOs, airdrops, and early mining. (3) Compound interest: Wealth(t+1) = Wealth(t) × (1 + r). (4) The wealth gap between early holders and late adopters grows exponentially. (5) Token voting means governance control is proportional to stake. (6) Conclusion: structural plutocracy is inevitable. Formal expression: Gini_coefficient(t+1) ≥ Gini_coefficient(t).

Connection with Volume I: T11 reproduces T2 — temporal advantage is not eliminated, only relocated. Connection with Volume III: Virtublic resolves T11 through dual sovereignty (P4): VIC⊥ (economic) is not convertible into EQU⊥ (political); Soulbound Identity (P3) distributes EQU⊥ equally among citizens.

Chapter 14. Governance Without Legitimacy

T12. Theorem of the DAO as Plutocracy by Design. Blockchain token voting has no external source of legitimacy; governance is controlled by capital (one token, one vote), not citizens (one person, one vote), reproducing T8 (sovereignty gap, Volume I) while replacing predictive power with tokenomic power.

Proof: (1) DAO governance is based on token voting (ΣA34). (2) One token, one vote — capital controls governance. (3) Tokens are freely exchanged (Regularity 17). (4) Governance may be captured: Capture_cost = Token_price × Tokens_for_majority. (5) Why is token voting legitimate? Because the code says so — written by developers without democratic mandate. (6) Circular legitimation. Formal expression: Legitimacy(DAO) = Code_says_so, not Legitimacy(DAO) = Democratic_mandate.

Connection with Volume I: T12 reproduces T8. Connection with Volume III: Virtublic resolves T12 through popular sovereignty (P0) and EQU⊥ (P4) — power belongs to citizens, not capital.

Chapter 15. Anonymity Destroys Accountability

T13. Theorem of Key Privacy Versus Political Accountability. Blockchain anonymity renders political accountability structurally impossible: if the subject is a key rather than a person, no one bears responsibility for actions, eliminating accountability altogether rather than realizing N1 (Volume I).

Proof: (1) The blockchain subject is a private key (A25). (2) Identity is not required for participation. (3) Smart contract exploitation by an anonymous attacker leaves no person to prosecute. (4) Legal accountability is architecturally foreclosed. (5) Privacy ↑ → Accountability ↓. Formal expression: Privacy ↑ → Accountability ↓.

Connection with Volume I: T13 is a new contradiction blockchain introduces rather than inheriting from digital capital. Connection with Volume III: Virtublic resolves T13 through Soulbound Identity (P3) plus zk-proof (P14) — anonymous participation with verifiable uniqueness, constitutionally establishing the balance between privacy and accountability.

Chapter 16. Code Is Law Without a Normative Axiom

T14. Theorem of Efficiency Versus Subjecthood. Blockchain implements code is law without NA0 (Volume I); code consequently optimizes efficiency while systematically failing to protect subjecthood, making exploitation not merely possible but architecturally constitutive.

Proof: (1) Smart contracts execute automatically (ΣA31). (2) The objective function is specified without NA0. (3) NA0 (Volume I): subjecthood is a politically protectable good; its

destruction is an evil regardless of efficiency. (4) Smart contracts do not contain NA0. (5) Conclusion: Optimize(efficiency) ∧ ¬Protect(subjecthood) → Exploitation.

Connection with Volume I: T14 reproduces the alienation of T1 — the subject becomes an object of protocol optimization. Connection with Volume III: Virtublic resolves T14 through code supremacy with a normative axiom (P2): the constitution is executable code that embeds NA0 through the formal verification of N1–N7.

Chapter 17. Sybil Resistance Through Centralization

T15. Theorem of Decentralization Versus Sybil Resistance. Any mechanism of Sybil resistance requires either a centralized trusted authority or an economic barrier (plutocracy), making decentralization + Sybil resistance + absence of plutocracy an impossible trilemma.

Proof: (1) Sybil attack = creation of fictitious identities (ΣA35). (2) Three solutions: (a) centralized verification — contradicts A19; (b) economic barrier (PoS) — reproduces T11; (c) computational barrier (PoW) — reproduces energy centralization. (3) No decentralized mechanism avoids all three compromises. Formal expression: Decentralization ∧ Sybil_resistance ∧ ¬Plutocracy = ∅.

Connection with Volume I: T15 is blockchain-specific — digital capital does not generate the Sybil problem in the same sense. Connection with Volume III: Virtublic resolves T15 through Digital Census v2 (P13) with the Civic Guard — a college of 21–99 civilian juror-auditors randomly selected through VRF, adopting decisions by a qualified 2/3 majority, taking on-chain oaths and rotating through VRF. Identities flagged as anomalous pass through the Dual Suspicion Protocol: stage 1 — automated behavioral Sybil-CAPTCHA; upon failure — stage 2, transmission to the college. This is not naïve decentralization but a constitutionally responsible temporary form of verification external to accumulated capital.

Chapter 18. The Absorption of Critique

T16. Theorem of Critique Without an Alternative as a System Stabilizer. Any critique of the system that proposes no institutional alternative external to the system's logic is absorbed by the system and becomes its stabilizer through monetization within the same attention economy the critique targets.

Proof: (1) The system monetizes critique through aggregation and self-augmentation (A5, A6, Volume I). (2) Critique is sold on the same market as system products. (3) The critic becomes a profile within the system she critiques, her reach determined by algorithm, her income by engagement. (4) Readers feel enlightened — a feeling that substitutes for political action. (5) Critique(system) ∧ ¬Alternative(institutional) → Absorption(critique) → Stability(system) ↑.

Connection with Volume I: T16 generalizes Regularity 11 — marginalization achieved through absorption rather than suppression. Connection with Volume III: Virtublic is not a critique but a constitutional architecture. A constitution cannot be cited as evidence of

openness — it can only be observed or violated. This is the sole form that the system cannot convert into a commodity.

Chapter 19. The Constitutional Necessity of Blockchain

T17. Theorem of Blockchain as a Necessary but Insufficient Substrate. Blockchain as technology (cryptography, zk-proof, smart contracts) is necessary for the constitutional solution of Volume III; blockchain as ideology (decentralization as sufficient condition, code is law, token voting) is insufficient; a constitutional architecture is required that employs blockchain technologies while adding popular sovereignty, republican form, and a normative axiom.

Proof by elimination: (1) Volume I proved: digital capital is not self-regulating; state regulation is structurally unreliable (T2, Regularity 12). (2) Volume II proved: blockchain ideology reproduces digital capital's contradictions at a new level (T11–T15); critique without an alternative is absorbed (T16). (3) The required form must employ blockchain technologies, avoid blockchain contradictions, add constitutional architecture, and be structurally absorption-resistant. (4) Virtublic (Volume III) = Blockchain(technology) + Constitution(P0–P18) $\wedge$ ¬Blockchain(ideology) $\wedge$ ¬Critique(absorbed).

What blockchain provides Virtublic: zk-proof realizes N1 and P13; smart contracts realize P2; cryptography realizes P3 (Soulbound Identity — non-transferable at protocol level); formal verification realizes P18. What Virtublic adds: popular sovereignty (P0) — power to citizens, not holders; dual sovereignty (P4) — EQU$\perp$ not convertible into VIC$\perp$, resolving T11; Soulbound Identity (P3) resolving T13; NA0 in code (P2) resolving T14; Civic Guard with Dual Suspicion Protocol (P13) resolving T15; constitutional form resolving T16.

PART V. CONNECTION WITH VOLUMES I AND III

Chapter 20. The Correspondence Matrix

T2 (Temporal Barrier, Volume I) → T11 (PoS Plutocracy, Volume II) → P4 (Dual Sovereignty) + P16 (Rockefeller Mode). Digital capital: platforms possess early data history. Blockchain: early holders dominate through PoS. Virtublic: VIC$\perp$ is not convertible into EQU$\perp$.

T8 (Sovereignty Gap, Volume I) → T12 (Governance Without Legitimacy, Volume II) → P0 (Popular Sovereignty) + P4 (EQU$\perp$) + Concordance Rule. Digital capital: predictive power and political sovereignty diverge. Blockchain: token voting controlled by capital. Virtublic: EQU$\perp$ = one person, one vote — legitimacy through popular sovereignty.

N1 (Right to Unpredictability, Volume I) → T13 (Anonymity Destroys Accountability, Volume II) → P3 (Soulbound Identity) + P14 (zk-proof). Digital capital: surveillance through profiling.

Blockchain: anonymity protects privacy but destroys accountability. Virtublic: anonymous participation with verifiable uniqueness.

NA0 (Subjecthood as a Protectable Good, Volume I) → T14 (Code Is Law Without NA0, Volume II) → P2 (Code Supremacy with Normative Axiom). Digital capital: algorithms optimize engagement. Blockchain: smart contracts optimize efficiency. Virtublic: the constitution is executable code embedding NA0 through formal verification of N1–N7.

Regularity 12 (Regulation from Within the System Is Unreliable, Volume I) → T15 (Sybil Resistance Requires Centralization, Volume II) → P6 + P13 (Digital Census v2 with Civic Guard and Dual Suspicion Protocol). Digital capital: the state cannot be a neutral regulator. Blockchain: decentralization + Sybil resistance = impossible without centralization. Virtublic: a temporary, rotating, constitutionally accountable Civic Guard ensures two-stage verification without a permanent centralized authority.

Regularity 11 (Marginalization of Opposition, Volume I) → T16 (Absorption of Critique, Volume II) → P17 + Volume III as constitutional form. Digital capital: critique is marginalized within the ranked environment. Blockchain: critique is absorbed through monetization. Virtublic: a constitution constrains the system from without and cannot be absorbed.

T10 (Constitutional Necessity, Volume I) → T17 (Constitutional Necessity of Blockchain, Volume II) → the entirety of Volume III. Digital capital: only a constitutional architecture resolves the contradiction. Blockchain: technology is necessary, ideology is insufficient, critique is absorbed. Virtublic: Blockchain(technology) + Constitution(P0–P18).

Chapter 21. Empirical Cases

Case 1 illustrates T12 and Regularity 14 (governance without legitimacy, algorithmic power) — resolved in Virtublic through P1 + P0. Case 2 illustrates T11 and Regularity 19 (PoS plutocracy, speculative motivation) — resolved through P4 (dual sovereignty: EQU⊥ for users, VIC⊥ for investors). Case 3 illustrates T14, Regularity 23, and Regularity 16 (code is law without NA0, bugs as governance crisis, irreversibility without justice) — resolved through P9 (Constitutional Convention) + P8 (Axiom-Break Condition), providing a constitutionally legitimate hard fork mechanism. Case 4 illustrates A22 and A23 (token as universal equivalent, liquidity as primary property) — resolved through P3 (Soulbound Identity): citizenship is non-transferable, speculation on citizenship is architecturally impossible. Case 5 illustrates T15 and ΣA36 (Sybil trilemma, proof-of-personhood limits) — resolved through P13: zk-proof of uniqueness without biometric disclosure, with the Civic Guard verifying procedure, not biometric data. Case 6 illustrates T16 and Regularity 18 (absorption of critique, critique as commodity) — resolved by the form of Volume III itself: one cannot listen to a constitution; one observes it or violates it.

CONCLUSION: BLOCKCHAIN AS AN INSUFFICIENT FORM

Volume II posed the question: can blockchain resolve the contradictions of digital capital? The answer is threefold: blockchain as ideology — no; blockchain as technology — necessary but insufficient; critique without an institutional alternative — absorbed.

Four concluding theses. First: blockchain ideology fails. T11 (PoS plutocracy) relocates rather than resolves the temporal barrier. T12 (governance without legitimacy) replaces democratic mandate with circular code-legitimation. T13 (anonymity destroys accountability) eliminates responsibility rather than realizing N1. T14 (code is law without NA0) optimizes efficiency at the expense of subjecthood. T15 (Sybil resistance requires centralization) makes full decentralization structurally impossible. T16 (absorption of critique) converts diagnosis into stabilization. T17 (constitutional necessity of blockchain) establishes that technology is necessary while ideology remains insufficient.

Second: blockchain technology remains necessary. T17 established that zk-proof enables N1 + P13; smart contracts enable P2; cryptography enables P3; formal verification enables P18. The substrate is indispensable — the ideology is not.

Third: Virtublic = blockchain technology + constitutional architecture. Volume III adds popular sovereignty (P0) in place of token voting; dual sovereignty (P4) in place of PoS plutocracy; Soulbound Identity (P3) in place of anonymity without accountability; NA0 in code (P2) in place of code is law without normative axiom; the Civic Guard with Dual Suspicion Protocol (P13) in place of naïve decentralization; constitutional form in place of absorbed critique.

Fourth: critique as stabilizer. T16 establishes a structural regularity extending beyond blockchain: critical discourse that proposes no institutional alternative channels tension, feels enlightening, and thereby substitutes for political action. Critique is monetized within the same attention economy it targets. This is not personal failure — it is a structural position. The system requires critique to legitimize itself as open to discussion.

Virtublic is not a critique. It is a constitutional architecture external to the logic of both digital capital and blockchain. The terminal contradiction: decentralization promises the elimination of power but relocates it to code, capital, and algorithms; critique promises accountability but becomes a commodity and stabilizer. The sole means of constraining this power is a constitutional architecture external to all three. Virtublic is not a blockchain project. It is a republic that employs blockchain. It is not a critique of the system. It is a constitution that constrains it.

APPENDICES

Appendix A. Technical Specifications of Blockchain Protocols

Proof-of-Work: mining algorithm, difficulty adjustment, energy expenditure. Proof-of-Stake: validator selection, slashing conditions, staking rewards. Smart contracts: Solidity specifications, EVM opcodes, gas costs. zk-SNARKs: cryptographic parameters, proof generation, verification. Civic Guard: VRF protocol, college formation, Dual Suspicion Protocol — the flagging algorithm, verification stages, and procedure for case transmission.

Appendix B. Formal Proofs of Theorems T11–T17

Complete mathematical proofs with formal expressions and empirical verification.

Appendix C. Empirical Data

Ethereum: ETH distribution, staking pool concentration, governance turnout. Bitcoin: mining pool concentration, energy consumption, address distribution. DeFi: TVL concentration, governance participation, liquidation events. NFTs: sales data, speculation patterns, wash trading. Critique as commodity: sales of books by Zuboff, Stiegler, and Morozov; speaking fees at blockchain conferences; research grants for the study of critique.

Appendix D. Comparative Analysis

Virtublic versus Ethereum governance. Virtublic versus Bitcoin mining. Virtublic versus DAO token voting. Virtublic versus critical discourse: why a constitution is not absorbed. Comparative analysis of Sybil resistance mechanisms: Worldcoin (biometrics), BrightID (social graph), the Virtublic Civic Guard (VRF + Dual Suspicion Protocol + constitutional accountability of jurors).

Appendix E. Glossary

A complete catalogue of axioms A19–A36, regularities 14–27, and theorems T11–T17 with definitions.

Appendix F. Bibliography

Blockchain theory: Satoshi Nakamoto (Bitcoin whitepaper), Vitalik Buterin (Ethereum), Vlad Zamfir (governance). Critique of blockchain: Nicholas Weaver, David Golumbia, Evgeny Morozov. Critique of digital capital: Shoshana Zuboff, Bernard Stiegler, Nick Srnicek. Cryptography: zk-SNARKs (Ben-Sasson et al.), formal verification (Coq, Lean). Political theory: Lessig, Rawls, Habermas, Arendt. Theory of the jury: Abramson (We, the Jury).

Appendix G. Correspondence Matrix: Volume I → Volume II → Volume III

Volume I / Volume II / Volume III

T2 (temporal barrier) / T11 (PoS plutocracy) / P4 + P16

T8 (sovereignty gap) / T12 (governance without legitimacy) / P0 + P4

N1 (right to unpredictability) / T13 (anonymity destroys accountability) / P3 + P14

NA0 / T14 (code is law without NA0) / P2

Regularity 12 (state capture) / T15 (Sybil trilemma) / P6 + P13 (Civic Guard + Dual Suspicion Protocol)

Regularity 11 (marginalization) / T16 (absorption of critique) / P17 + Volume III as constitutional form

T10 (constitutional necessity) / T17 (blockchain as necessary substrate) / the entirety of Volume III

VOLUME II — THE CAPITAL OF THE DIGITAL ECONOMY

Critique of Blockchain, Cryptocurrencies, and Digital Democracy 2026

PART I. THE ONTOLOGY OF BLOCKCHAIN

The objective layer establishes blockchain as a specific data architecture that emerged as an institutional response to the contradictions of digital capital described in Volume I. Blockchain lays claim to the role of an alternative order, replacing trust in a centralized intermediary with cryptographic verification and a distributed ledger. However, this layer contains internal axioms that, when deployed within the logic of speculation, generate new forms of alienation and concentration demanding systematic deconstruction.

Chapter 1. Decentralization as the Primary Principle

Volume I concluded with T10 — the theorem of constitutional necessity, proven by the method of exhaustion: internal market mechanisms, state regulation, and individual and informal collective action were each excluded as insufficient. What remains is the sole form — a constitutional architecture external to the logic of digital capital. Blockchain emerged historically as precisely a technological attempt to instantiate such externality: to eliminate a single center of control, to replace trust in an arbiter with cryptographic consensus, to codify rules in smart contracts unalterable without the consent of the majority of participants. This is an institutional project, not merely an engineering solution. Volume II analyzes this project as a structural response to the contradictions of Volume I — and proves that as ideology it fails, yet as a technological substrate it remains necessary.

Chapter 1 introduces the axioms of the ontological layer (A19–A24) and discloses their internal contradictions. The axioms of Volume II are not axioms in the sense of foundational truths — they are axioms in the sense of the implicit presuppositions of blockchain ideology, presuppositions accepted as sufficient that upon examination prove structurally insufficient.

Axioms of the Ontology of Blockchain

A19. Axiom of Decentralization. Decentralization — the elimination of a single center of control — is a sufficient condition for overcoming the monopolization of digital capital.

Justification: A19 is a direct response to the temporal barrier (T2, Volume I): if monopolization is generated by the concentration of data and computation in a single center,

then the distribution of data and computation among a plurality of independent nodes must eliminate that barrier.

Proof of the insufficiency of A19: T2 (Volume I) proved that monopolization occurs not through a technical center of control but through temporal advantage — the early history of data and accumulated network effects. The dominant platform possesses not merely a server — it possesses a history of behavioral data created years before the emergence of competitors. Decentralization distributes control over current operations but does not eliminate the advantage of early participants, who accumulated tokens, transaction history, and network connections prior to the joining of the majority. → Conclusion: A19 responds to an incorrectly posed question. It resolves the problem of a technical single point of control; T2 describes the problem of structural temporal advantage. The former is not a necessary condition of the latter.

Formal expression: Decentralization of control is not a sufficient condition for the elimination of the temporal barrier, given that the advantage of early participants is preserved through accumulated stake or data history.

Connection with Volume III: Virtublic acknowledges the insufficiency of A19 and responds to it through principle P3 (Soulbound Identity): citizenship is non-transferable, and consequently it cannot be accumulated as the structural advantage of early participants. EQU⊥ is not an object of accumulation.

A20. Axiom of Consensus Mechanisms. Consensus among nodes replaces trust in a centralized arbiter: in proof-of-work through computational power, in proof-of-stake through token ownership.

Justification: A20 is the technological response to the problem of legitimacy: if there is no central arbiter, there is no arbitral arbitrariness. The consensus of a majority of nodes is a sufficient source of the truthfulness of the state of the system.

Proof of the insufficiency of A20: The consensus of a majority is a sufficient source of legitimacy only on the condition that "majority" is defined by a criterion corresponding to the normative principles of the system. In proof-of-work, the majority is determined by computational power; in proof-of-stake, by token ownership. Neither of these criteria is equivalent to democratic majority (one person, one vote). It therefore follows that the "majority consensus" in existing blockchain systems is the consensus of a majority of capital or computational power, not a majority of participants. → Conclusion: A20 replaces the centralized arbiter — a single point of trust — with a plutocratic consensus that is legitimate in form but not in content in the normative sense of Regularity 10 (Volume I).

Connection with Volume III: Principle P0 (popular sovereignty) and principle P4 (EQU⊥/VIC⊥ orthogonality) in Virtublic extirpate the contradiction of A20 through the separation of economic consensus (VIC⊥ — proportional to contribution) and political consensus (EQU⊥ — equal per citizen). The conflation of these two types of consensus, which A20 does not distinguish, is the architectural source of plutocracy.

A21. Axiom of Immutability. The history of transactions is immutable: no one can alter past records without the consensus of the majority, and cryptographic protection through hash functions guarantees the integrity of the history.

Justification: A21 is a response to the problem of arbitrary retrospective alteration of rules — a central arbiter may alter history in its own interest. The immutability of blockchain eliminates this possibility.

Proof of the insufficiency of A21: Immutability protects against arbitrary alteration of history but generates the structural problem of errors without correction. If a transaction is recorded erroneously, or a smart contract vulnerability has led to the wrongful displacement of assets, the impossibility of correction without a hard fork is not a property of protection but a property of the irreversibility of injustice. The DAO case (2016) remains precedential: the smart contract was exploited through a reentrancy vulnerability to extract 3.6 million ETH; the community was compelled to execute a hard fork — that is, to violate A21 in order to correct an injustice. → Conclusion: A21 protects against censorship but generates the legal impossibility of correcting documented errors and injustices from within the system. Correction is possible only through a hard fork — that is, through a decision of the majority, which is not a neutral technical act but a political decision without a legitimate procedure.

Formal expression: Immutability and correctability stand in structural contradiction: the elimination of the first threat (arbitrary alteration) generates the second threat (irreversible errors and injustices).

Connection with Volume III: Principle P9 (Constitutional Convention) and principle P8 (Axiom-Break Condition) in Virtublic resolve the contradiction of A21 through a legitimate rule-modification mechanism: it exists but requires a qualified majority of citizens through EQU⊥, not a technical fork without a normative procedure.

1.1. Axioms of Tokenization

A22. Axiom of the Token as Universal Equivalent. Everything may be represented as a token: money, assets, rights, access — tokenization eliminates intermediaries and creates direct exchange between participants.

Justification: A22 is a generalization of blockchain logic beyond financial transactions. If any right or asset may be represented on a blockchain, then the predictive power of platforms (T1, Volume I) may be redistributed through the tokenization of data and governance.

Proof of the insufficiency of A22: A22 reproduces the logic that Marx described as the universal equivalent: an abstract form to which all concrete relations are reduced (Capital, Vol. I). The governance token reduces political participation to capital ownership — thereby eliminating the qualitative distinction between political sovereignty and economic power. The NFT reduces the cultural object to a speculative asset: the owner of an NFT associated with an image possesses not the right to the image itself but only the record in a blockchain to the effect that she "owns" a pointer to that image. The price fluctuation of an NFT is determined not by the cultural value of the object but by speculative demand for the token. This does not eliminate alienation (T1, Volume I) — it generates a new form of alienation: the attention-token crystallizes into an NFT, and the speculative market produces a new layer of

predictive value atop the original alienation. → Conclusion: tokenization is a neutral technology capable of representing any relation — but it does not alter the structure of the relation itself. Tokenized political participation under a one-token-one-vote mechanism remains plutocracy regardless of the technological substrate.

A23. Axiom of Liquidity. Tokens are freely exchanged on the market; liquidity is the primary property of the token.

Justification: A23 reflects an operational requirement: a token that cannot be exchanged does not perform the function of a medium of exchange and loses its economic value.

Proof of the insufficiency of A23 for governance: If governance tokens are freely exchanged (A23), then governance is controlled by those who can purchase the greatest number of tokens on the open market, not by those who use the system or possess the greatest competence in its administration. This is a direct consequence of structural Regularity 17 (governance capture through the market). → Conclusion: liquidity as the primary property of the token is a necessary condition for economic functions and simultaneously a structural condition for governance capture. These two requirements are incompatible within a unified token model.

Formal expression: The liquidity of a governance token is directly proportional to the vulnerability of governance to market capture.

Connection with Volume III: Principle P3 (Soulbound Identity) and principle P4 (EQU⊥/VIC⊥ orthogonality) in Virtublic resolve the contradiction of A22–A23 through the non-transferability of political participation. EQU⊥ is soulbound — it cannot be purchased, sold, or temporarily borrowed. VIC⊥ may be liquid; EQU⊥ may not. This is the architectural resolution of the contradiction between the requirements of liquidity and the requirements of the normative integrity of governance.

A24. Axiom of Programmability. Tokens are programmed through smart contracts that execute automatically without intermediaries, eliminating human arbitrariness.

Justification: A24 is the technological response to the arbitrariness of centralized arbiters: if rules are codified and execute automatically, there is no agent capable of violating them.

Proof of the insufficiency of A24: The automation of rule execution does not eliminate power — it relocates it to the level of code authorship. Whoever formulates the smart contract determines the rules; whoever controls protocol updates controls the normative environment of all participants. This is structural Regularity 14 (algorithmic power): Power(institutions) → Power(code writers + early adopters). The entailment is: code without a normative axiom (NA0, Volume I) optimizes the specified function without protecting subjecthood. A smart contract that automatically liquidates collateral upon the fall of price below a threshold (DeFi liquidation) executes correctly from the perspective of the code — and may simultaneously destroy the economic position of the subject as a result of a temporary market anomaly. The code was correct; the outcome was unjust. NA0 was absent from the code. → Conclusion: A24 eliminates the arbitrariness of the arbiter but generates the arbitrariness of the programmer — and this arbitrariness is less visible, since it is embedded in code as a neutral technical norm rather than as an explicit political decision.

Connection with Volume III: Principle P2 (code supremacy with the normative axiom NA0) in Virtublic resolves the contradiction of A24 through the embedding of NA0 in executable code at the level of formal verification. The constitution of Virtublic is a smart contract that contains NA0 as an ineliminable parameter of the optimization function.

1.2. Decentralization as Ideology and Its Limit

Axioms A19–A21 constitute the core of blockchain ideology, which may be formulated as a single proposition: the elimination of a single center is a sufficient condition for the elimination of power. This presupposition is libertarian in its provenance — it assumes that power is localized in institutions (the state, corporations) and can be eliminated through the technical distribution of control.

Volume I proved through Regularity 12 and T8 that power is not localized in institutions but distributed within the structure of accumulation: the temporal barrier (T2) is not a technical but a structural advantage, grounded in the early history of data and network effects. The decentralization of the protocol does not eliminate this structure — it reproduces it on a new technological substrate.

Proof-of-Work realizes decentralization at the protocol level: formally, any participant may become a miner without the permission of a central authority. This is a genuine achievement — there is no registration barrier, no license, no single point of failure. However, PoW reproduces concentration through a resource barrier: mining requires specialized hardware (ASICs), the availability of which is constrained by production chains, and enormous electricity expenditure with constantly declining marginal returns as difficulty grows. Consequently, the protocol is decentralized; block production is not. This is a structural reproduction of T2: not a formal barrier to entry, but a resource barrier that renders concentration structurally inevitable.

Proof-of-Stake is an energy-efficient response to PoW and eliminates the ASIC problem. However, PoS reproduces concentration through a direct capital barrier: staking rewards are proportional to the size of the stake, which determines that early holders accumulate stake faster than late participants — and this is the precise reproduction of the temporal barrier T2 at the level of tokens. The threshold for an independent Ethereum validator is 32 ETH; the majority of participants do not reach this threshold and are compelled to employ staking pools. Decentralization by protocol structure; concentration by capital structure.

Critical conclusion of subchapter 1.2: both consensus implementations reproduce the temporal barrier T2 — PoW through the resource barrier, PoS through the capital barrier. Blockchain ideology incorrectly identifies the source of power as technical centralization, whereas Volume I proved that the source of power is the structural advantage of early participants. Consequently, a technology that does not eliminate this advantage does not resolve the problem of power — it reformats it in new terminology.

The following subchapter 1.3 analyzes axioms A22–A24, which extend blockchain ideology beyond consensus to the tokenization of rights, assets, and governance, and proves that each of the three concrete applications of tokenization reproduces — rather than eliminates — the structural contradictions of digital capital.

1.3. Cryptocurrencies, NFTs, and Governance Tokens

Cryptocurrencies as an attempted money without a state. Bitcoin was conceptualized as peer-to-peer electronic cash — a medium of exchange without state issuance and a central bank. This is a direct response to Regularity 12 (Volume I): if the state is a structurally non-neutral regulator, then money without a state eliminates it as a source of monetary power.

Operational reality refutes this presupposition. The three functions of money as applied to BTC are not fulfilled by any of the relevant parameters. A medium of exchange requires price stability sufficient for the price of a good at the moment of agreement and the price at the moment of execution to be comparable; BTC's volatility renders it unsuitable for settlement in the majority of real-economy transactions. A measure of value requires a stable nominal for the comparison of values across time; price instability renders long-term pricing impossible. A store of value requires predictable preservation of purchasing power; BTC possesses deflationary architecture (an upper limit of 21 million coins), yet its price is determined predominantly by speculative demand rather than by the fundamental indicators of economic value — which renders its accumulative function structurally speculative. It therefore follows that BTC functions not as money but as a speculative asset — and in this capacity adds a new layer of financial instability to the problems described in Volume I rather than resolving them.

NFTs as the commodification of digital objects. The NFT (non-fungible token) was conceptualized as a solution to the problem of digital ownership: in digital space, any file may be copied without cost, which determines that no mechanism for establishing ownership of a digital object exists without a centralized registry. The NFT proposes a decentralized registry: a record in a blockchain confirms "ownership" of a token associated with a pointer to a digital object.

The structural problem: the NFT does not generate scarcity of the object itself — it generates scarcity of the record of "ownership" of the pointer. The image remains copyable; anyone may save it to her own filesystem. The owner of an NFT possesses not the image but the token — a blockchain record to the effect that she is the "owner" in the sense of this specific system. The value of an NFT is a function of speculative consensus, not of the value of the object. This is the precise reproduction of the logic of alienation T1 (Volume I): the attention of the subject is transformed into predictive value by the platform; the attention of the subject directed at an NFT is transformed into speculative value for the token. A new technological substrate — the same structure of alienation.

Governance tokens as the tokenization of political participation. The governance token is the most ambitious application of A22: if the rights to administer an organization may be represented as tokens, then governance becomes decentralized — no CEO, no board of directors, each holder participates in decision-making proportional to token holdings.

The structural problem of governance tokens is twofold. First, it reproduces plutocracy: one token, one vote means that influence over decisions is directly proportional to capital ownership, which determines that early holders and large investors dominate governance regardless of their competence or the interests of system users. This is operational confirmation of structural Regularity 15 (plutocratic consensus). Second, the liquidity of

governance tokens (A23) generates vulnerability to market capture: an attacker may temporarily acquire a majority of votes through a flash loan or accumulated open-market positions. Consequently, governance tokens do not resolve T8 (the sovereignty gap, Volume I) — they replace the predictive power of platforms with the tokenomic power of holders, preserving the same structure: formal decentralization with de facto concentration of power among early and wealthy participants.

Chapter Summary

Chapter 1 introduced six axioms of the ontological layer of blockchain (A19–A24) and deconstructed each of them through correspondence with the theorems and regularities of Volume I. A19 does not resolve the temporal barrier T2 — it distributes technical control without eliminating the structural advantage of early participants. A20 replaces the centralized arbiter with a plutocratic consensus — a majority of capital, not a majority of citizens. A21 eliminates the possibility of arbitrary alteration of history, thereby generating the structural impossibility of correcting injustices without a hard fork. A22–A24 reproduce the logic of alienation T1 on a new technological substrate through speculative token markets, liquidity as a governance vulnerability, and the algorithmic power of protocol developers. The three concrete applications of tokenization — cryptocurrencies, NFTs, governance tokens — were empirically verified through cases from 2020–2024 and demonstrated the reproduction, rather than the elimination, of the structural contradictions of Volume I.

Transition to Chapter 2

Chapter 1 described the axioms of blockchain as a technical system and their internal contradictions. However, the deconstruction of axioms is not yet the deconstruction of consensus as an institutional form. Chapter 2 proceeds to the analysis of how blockchain consensus mechanisms generate a surrogate for legitimacy — reproducing the problem of Regularity 10 (Volume I) in a new technological form — and why this necessitates transition to the anthropological layer of analysis.

Chapter 2. Consensus as a Surrogate for Legitimacy

Chapter 1 established the internal contradictions of the six axioms of the ontological layer of blockchain: A19–A24 describe a system that is decentralized in form and reproduces concentration in content. Chapter 2 completes the ontological layer through the synthesis of axioms A19–A24, introduces four structural regularities (14–17), and proves through the proto-theorem of ontology that blockchain as an objective structure necessitates an anthropological layer of analysis — the identification of the agents bearing the consequences of the structural regularities.

Synthesis of A19–A24

The six axioms of the ontological layer constitute a unified structure whose internal contradictions are not incidental defects of implementation but logical consequences of foundational presuppositions. A19 promises the elimination of the center through the decentralization of control — yet A20 demonstrates that consensus requires a qualified majority, defined by the criterion of capital or computational power. A21 protects history through immutability — yet renders documented errors and injustices uncorrectable without

a politically charged hard fork. A22–A24 generate new forms of alienation through tokenization: political participation is reduced to capital ownership (A22), liquidity converts governance into an object of market capture (A23), and the automation of execution relocates power from visible institutions to invisible protocol developers (A24).

The aggregate result of the synthesis of A19–A24: blockchain as an objective structure does not eliminate the structural contradictions of digital capital described in Volume I. It reformats them in new terminology. The temporal barrier T2 is reproduced at the level of tokens through the staking advantage of early holders. The sovereignty gap T8 is reproduced through the replacement of the predictive power of platforms with the tokenomic power of holders. The algorithmic consensus of Regularity 10 is reproduced through PoS and PoW as the consensus of capital, not of citizens. The absence of an external normative reference (Regularity 13) is reproduced through code is law without NA0.

This does not mean that blockchain is a useless technology. It means that blockchain as ideology — the set of presuppositions A19–A24 — is a structurally insufficient institutional form. Blockchain as a technological substrate (cryptography, smart contracts, zk-proof, formal verification) remains a necessary condition of the constitutional architecture of Volume III — on the condition that a normative layer absent from current implementations is added.

Structural Regularities of the Ontology of Blockchain

Regularity 14 (from A19 + A24). Algorithmic Power. Decentralization relocates power from visible institutions (the state, corporations) to invisible algorithms (protocols, smart contracts): whoever formulates the code determines the rules for all participants in the system.

Justification: A19 asserts that the elimination of a single center is a sufficient condition for the elimination of monopolization. A24 asserts that automation through smart contracts eliminates human arbitrariness. From the conjunction of these two axioms it follows not that power is eliminated but that it is displaced: the single center is eliminated, the arbitrariness of the arbiter is eliminated — yet power over the rules has passed to protocol developers and early participants who received tokens prior to the formation of an open market.

Proof: Power is defined as the capacity to establish rules that are binding on participants in the system and to modify them. In traditional institutions, this capacity belongs to formally identified agents (CEO, legislative body, regulator) with defined decision-making procedures and accountability mechanisms. In blockchain systems, this capacity belongs to the core developers of the protocol and the largest holders of governance tokens. Core developers formulate protocol changes; holders vote on their adoption proportional to stake. Consequently, algorithmic power is more concentrated than power in traditional institutions for one key reason: it is less visible. Traditional power is identifiable — its bearers are publicly known, their decisions formally documented. Algorithmic power is embedded in code as a neutral technical norm — and its bearers bear no political accountability for the consequences. → Conclusion: Power(institutions) → Power(code writers + early adopters) is not a neutral technical shift but a political displacement of power toward agents who possess no democratic legitimacy and bear no political accountability.

Connection with Volume I: Regularity 12 of Volume I established that regulation from within the system is structurally unreliable, since the regulator is a structurally interested participant. Regularity 14 extends this proposition: blockchain replaces the state as regulator with the protocol as regulator, but the protocol is written by participants without democratic legitimacy — consequently, the structural unreliability of regulation from within is reproduced in a new form.

Connection with Volume III: Principle P1 (republican form) in Virtublic requires that developers of constitutional code possess legitimacy through popular sovereignty (P0). Protocol modifications are subject to ratification through EQU⊥ — thereby constitutionally constraining the algorithmic power of developers.

Regularity 15 (from A20 + A22). Plutocratic Consensus. Proof-of-Stake consensus is the structural equivalent of one dollar, one vote rather than one person, one vote: a participant's influence on the state of the system is directly proportional to his stake.

Justification: A20 asserts that the consensus of the majority of nodes is a sufficient source of legitimacy. A22 asserts that rights may be represented as tokens exchangeable on the market. From the conjunction of these two axioms it follows that the majority determining consensus is the majority of tokens — that is, the majority of capital.

Proof: In proof-of-stake systems, the voting weight of a validator is determined by the size of his stake. Consequently, Influence(i) ∝ Stake(i): a participant's influence is directly proportional to his capital in the system. This is the precise definition of plutocracy in political theory — not as a normative description but as a structural property of the decision-making mechanism. Early holders of blockchain systems accumulated stake prior to the formation of an open market, at prices incommensurably below market rates — at the moment the majority of users joined. Consequently, the compound interest effect of staking rewards systematically increases the share of early holders relative to late participants: staking income is proportional to stake, which determines that a large holder accumulates new stake faster than a small holder in the same proportion by which his initial stake exceeds the small holder's. Through a sufficient number of iterations, initial advantage becomes ineliminable without an external redistributive mechanism. This is the reproduction of T2 (the temporal barrier, Volume I) at the level of tokens: the early history of data is replaced by early stake, but the structural logic is preserved. → Conclusion: plutocratic consensus is not an incidental defect of PoS implementation but a structural consequence of the conjunction of A20 and A22.

Formal expression: Influence(i) ∝ Stake(i). The staking advantage of early holders increases monotonically in the absence of an external redistributive mechanism.

Connection with Volume I: Regularity 15 reproduces T2 (the temporal barrier) at the level of tokens. Early holders dominate governance through a mechanism structurally analogous to the mechanism by which platforms dominate through the early history of data.

Connection with Volume III: Principle P4 (dual sovereignty) in Virtublic resolves the contradiction of Regularity 15 through the constitutional separation of VIC⊥ (economic sovereignty, proportional to contribution) and EQU⊥ (political sovereignty, equal per citizen). VIC⊥ may be proportional to stake — yet it is not convertible into the political power of

EQU⊥. Consequently, the staking advantage of early holders does not transform into political domination.

Regularity 16 (from A21). Irreversibility Without Justice. The immutability of the blockchain history protects against arbitrary alteration of the past but eliminates the possibility of correcting errors and injustices without a hard fork — a politically charged decision without a legitimate procedure.

Justification: A21 asserts that the immutability of history is a guarantee against censorship. From A21 follows a structural consequence: any transaction once recorded in a blockchain is permanent — including transactions grounded in code vulnerabilities, fraud, or technical error.

Proof: Legal systems in all jurisdictions contain a mechanism of rectification — the correction of documented errors and injustices. This mechanism is a foundational requirement of any system that lays claim to normative legitimacy: if an error is irreversible, the normative system possesses no mechanism of justice. Blockchain eliminates this mechanism structurally. Error(t) ∈ Blockchain → Correction requires Fork: correction is possible only through a hard fork — a protocol modification in which part of the participants accepts the modification and part refuses, with the result that the network divides. A hard fork is not a neutral technical act but a political decision: whoever possesses sufficient stake or hashrate to constitute the dominant branch determines which version of history is "correct." The Ethereum/Ethereum Classic split (2016) demonstrated that the question of the "correct" history was resolved not by a normative procedure but by market capitalization. → Conclusion: immutability is simultaneously a property protecting against censorship and a property protecting injustice from correction. This contradiction is not eliminable within the framework of A21: any weakening of immutability eliminates protection against censorship; the preservation of immutability eliminates the possibility of rectification.

Formal expression: Error(t) ∈ Blockchain → Correction requires Fork. The cost of correction is proportional to the political costs of coordinating a hard fork in the absence of a legitimate procedure.

Connection with Volume I: Regularity 16 is a new form of Regularity 12 of Volume I: regulation is impossible from within because history is immutable. Blockchain ideology rejects external correction mechanisms — thereby rejecting the possibility of rectification as such.

Connection with Volume III: Principle P9 (Constitutional Convention) in Virtublic resolves the contradiction of Regularity 16 through a legitimate rule-modification mechanism: the constitutional amendment procedure, requiring a qualified majority of EQU⊥ citizens, is an external correction mechanism — while constitutionally constrained so as not to become an instrument of arbitrary alteration of history.

Regularity 17 (from A23). Liquidity Destroys Governance. If governance tokens are freely exchanged on the market, governance is controlled by those who can purchase the greatest number of tokens, not by those who are participants of the system.

Justification: A23 asserts that liquidity is the primary property of the token — an illiquid token is worthless. The governance token is a token (A22) and consequently must be liquid. From the conjunction of A22 and A23 it follows that the governance token is a freely exchangeable voting right — which is equivalent to the sale of political participation on the open market.

Proof: If the governance token is a market asset, its price reflects the presumed value of the vote in forthcoming decisions. This generates two structural consequences. First: agents motivated by a specific governance decision have an incentive to temporarily accumulate the maximum number of tokens prior to the vote and to sell after it. This is not a violation of the rules of the system but the optimal strategy under conditions of A23. Second: even absent extreme attacks, the market liquidity of governance tokens means that the voting structure dynamically changes in response to market price fluctuations — consequently, governance at any given moment reflects the current capital structure rather than the long-term interests of users or citizens of the system. Liquidity(token) ↑ → Governance capture ↑: the higher the liquidity, the lower the cost of temporarily capturing a voting majority. → Conclusion: the requirement of liquidity (A23) and the requirement of governance integrity (A22 as applied to participation rights) are incompatible within a unified token model. This is a structural contradiction, not a problem of implementation.

Formal expression: The cost of governance capture is inversely proportional to token liquidity and directly proportional to the lock-up period required for voting.

Connection with Volume I: Regularity 17 reproduces T4 (accountability without power, Volume I) in a new form: the holder of a governance token bears economic risks from token price fluctuations but bears no political accountability for the consequences of governance decisions for system users. Users bear the consequences but do not control governance.

Connection with Volume III: Principle P3 (Soulbound Identity) in Virtublic resolves the contradiction of Regularity 17 through the non-transferability of EQU⊥: political participation is soulbound — it cannot be purchased, sold, pledged, or temporarily borrowed. A flash loan attack on governance is architecturally impossible, since EQU⊥ does not exist on the open market.

2.1. The Proto-Theorem of the Ontology of Blockchain

Regularities 14–17 complete the ontological layer. However, they contain an implicit agent of consequences: who bears the consequences of plutocratic consensus (Regularity 15)? Who bears the consequences of the liquidation of governance through market capture (Regularity 17)? Who bears the consequences of the algorithmic power of developers who possess no democratic mandate (Regularity 14)? The ontological layer describes the structure — yet does not identify the subjects whose subjecthood is destroyed by this structure.

Proto-theorem of the ontology of blockchain (from Regularities 14–17). Blockchain as an objective structure reproduces the structural properties of digital capital (T1–T3, Volume I) on a new technological substrate without eliminating them: algorithmic power reproduces the non-neutrality of the regulator (Regularity 12, Volume I), plutocratic consensus reproduces the temporal barrier (T2, Volume I), irreversibility without justice reproduces the impossibility of correction from within (Regularity 12, Volume I), and liquidity destroys governance —

reproducing accountability without power (T4, Volume I). This structural reproduction is not incidental — it is the logical consequence of axioms A19–A24.

Justification: Regularity 14 (algorithmic power) is a new form of Regularity 12 of Volume I. Regularity 15 (plutocratic consensus) is a reproduction of T2 at the level of tokens. Regularity 16 (irreversibility without justice) is a new form of Regularity 12 through immutability. Regularity 17 (liquidity destroys governance) is a reproduction of T4 in tokenomic form.

Proof: If each structural regularity of blockchain (14–17) is a structural reproduction of a regularity or theorem of Volume I, then blockchain ideology as the set of axioms A19–A24 is a system that reproduces the contradictions it declaratively claims to resolve. This does not prove the uselessness of blockchain as a technological substrate — it proves the insufficiency of blockchain as an autonomous institutional form. → Conclusion: blockchain necessitates supplementation by a normative layer external to its own logic — which is the requirement of Regularity 13 of Volume I as applied to the technological substrate. This supplementation is the subject of Volume III.

Logical requirement of transition: the proto-theorem of ontology identifies the structural reproduction of contradictions but does not identify the subjects bearing the consequences of this reproduction. Who occupies the position analogous to the "attention supplier" (class position 1, Chapter 4 of Volume I) in the blockchain economy? Who is the "forming subject" in the tokenomic system? Who occupies the position of the "algorithmic intermediary"? These questions necessitate the anthropological layer — Part II of the present volume.

Δ3 — CRISIS: THE LIMIT OF TECHNOLOGICAL DETERMINISM

Regularities 14–17 and the proto-theorem of the ontology of blockchain jointly prove: blockchain as an objective structure reproduces the structural contradictions of digital capital through algorithmic power, plutocratic consensus, irreversibility without justice, and the destruction of governance through liquidity. Blockchain ideology presupposes that the technological properties of the system (decentralization, immutability, programmability) are sufficient conditions for institutional goals (the elimination of monopoly, legitimate governance, justice). This technological determinism reaches its limit: technological properties are normatively neutral, and their application without a normative layer reproduces the same structural contradictions in a different technological form.

However, the ontological layer describes blockchain without agents — as an abstract structure of consensus, tokens, and code. The answer to the question of who bears the consequences of structural regularities 14–17 necessitates transition to the anthropological layer. Part II identifies the class positions of the blockchain economy and proves that the subjective layer reproduces the same logic of the extraction of subjecthood that Volume I established in digital capital.

Chapter Summary

Chapter 2 completed the ontological layer of blockchain through the synthesis of axioms A19–A24 and the introduction of four structural regularities (14–17). The synthesis of A19–A24 proved that each of the six foundational presuppositions of blockchain ideology contains a structural contradiction that is the logical consequence of the presupposition itself, not a defect of implementation. Regularity 14 established that algorithmic power is a less visible and less accountable form of power than the form blockchain replaces. Regularity 15 established that the plutocratic consensus of PoS reproduces the temporal barrier T2 of Volume I at the level of tokens. Regularity 16 established that the immutability of history is simultaneously a protection against censorship and a protection of injustice from correction. Regularity 17 established that the liquidity of governance tokens is the structural condition of their market capture. The proto-theorem of the ontology of blockchain formalized that each of the four regularities is a reproduction of a regularity or theorem of Volume I. Δ3 established the limit of technological determinism.

Transition to Part II

The ontological layer described blockchain without subjects — as an objective structure of consensus, tokenization, and automation. Part II proceeds to the anthropological layer: who precisely bears the consequences of structural regularities 14–17? What class positions does the blockchain economy constitute? In what manner do anonymity, pseudonymity, and holder-subjectivity reproduce — or transform — the forms of subjecthood described in Volume I? This is the logically obligatory next step: the proto-theorem of ontology contains implicit agents of consequences whose identification is the condition of the completeness of the analysis.

Chapter 3. The First Proto-Theorem of Ontology and the Crisis of Objectivity

Chapters 1 and 2 sequentially deconstructed the six axioms of blockchain ideology (A19–A24) and derived from them four structural regularities (14–17). Each of the regularities was verified as a reproduction of a contradiction already described in Volume I: algorithmic power (Regularity 14) reproduces the non-neutrality of the regulator (Regularity 12, Volume I), plutocratic consensus (Regularity 15) reproduces the temporal barrier (T2, Volume I), irreversibility without justice (Regularity 16) reproduces the impossibility of correction from within, and liquidity destroys governance (Regularity 17) — reproducing accountability without power (T4, Volume I). Chapter 3 formalizes this result into a proto-theorem, establishes the logical incompleteness of the ontological layer, and grounds the transition to the anthropological layer.

Proto-Theorems of the Ontological Layer

Proto-theorem of the ontology of blockchain (from Regularities 14–17). The blockchain system reproduces the structural properties of digital capital (T1–T3, Volume I) on a new technological substrate without eliminating them; this reproduction is not a defect of implementation but a logical consequence of axioms A19–A24, by virtue of which it necessitates an anthropological layer of analysis for its complete proof.

Justification (from Regularities 14–17 + T1–T3, Volume I): Regularity 14 established that algorithmic power is a less visible and less accountable form of power. Regularity 15 established that plutocratic consensus structurally reproduces the temporal barrier T2. Regularity 16 established that the immutability of history renders documented injustices irreversible. Regularity 17 established that the liquidity of a governance token is the structural condition of its market capture. From the conjunction of these four regularities it follows that blockchain as an objective structure contains no mechanism for eliminating any of the structural contradictions of Volume I.

Proof: It is required to prove that for each structural contradiction of Volume I (T1–T3, Regularities 12–13) there exists a structural regularity of Volume II (14–17) that is its formal equivalent on the blockchain substrate.

T1 (the alienation of attention) → Regularity 17: the liquidity of the governance token converts the right of participation into a market asset that the holder does not control following its sale — this is the precise reproduction of the structure of alienation in which the subject generates value (participation in governance) that the system extracts and realizes without his control. T2 (the temporal barrier) → Regularity 15: the staking advantage of early holders is the temporal barrier at the level of tokens — early entry into the system generates a structurally increasing advantage through the compound effect of staking rewards. T3 [structural platform dominance] → Regularity 14: the algorithmic power of protocol developers and early adopters is dominance without a democratic mandate, reproducing the structural dominance of platforms over users. Regularity 12 (regulation from within is structurally unreliable) → Regularities 14 + 16 jointly: algorithmic power renders regulation from within dependent on the mandate of developers rather than citizens; the irreversibility of history renders the correction of injustices technically impossible without a politically charged hard fork. Regularity 13 (the sole source of legitimacy is an external reference) → directly applicable to blockchain: a blockchain protocol without NA0 is a system without an external normative reference, and consequently it cannot legitimize itself through its own instruments (consensus hash, token vote) on the same grounds by which digital capital could not legitimize itself through virality (ΣA14, Volume I).

The conjunction of these five correspondences constitutes the formal proof: each structural contradiction of Volume I has an equivalent in the regularities of Volume II. It therefore follows that blockchain reproduces the contradictions it declaratively claims to eliminate — not as a result of errors in specific implementations, but as a result of the structural properties of axioms A19–A24. → Conclusion: the proto-theorem of ontology is proved. The technological substrate is necessary but insufficient. Sufficiency necessitates the addition of a normative layer (NA0 + the constitutional architecture of Volume III) and presupposes the identification of the agents of consequences — which is the task of the anthropological layer.

Logical incompleteness of the ontological layer: Regularities 14–17 contain an implicit agent of consequences not identified by ontological analysis. Regularity 15 (plutocratic consensus) implicitly contains the subject bearing the consequences of plutocracy — the holder with a small stake, systemically excluded from governance without awareness of the mechanism of his exclusion. Regularity 17 (liquidity destroys governance) implicitly contains the system user bearing the consequences of governance decisions adopted through market capture of tokens — without his participation and against his interests. Regularity 14 (algorithmic

power) implicitly contains the developer who determines the rules for all participants without a democratic mandate and without an accountability mechanism. Without the identification of these agents, the ontological layer describes structure in the abstract — as the movement of tokens and consensus mechanisms without subjects bearing their consequences. This is a formal incompleteness: structural analysis that does not identify the bearers of consequences is not operationally complete in the normative sense.

Connection with Volume III: The proto-theorem of ontology is the necessary precursor of the constitutional architecture of Volume III: it proves that the blockchain substrate necessitates the superposition of a normative layer. Principles P0 (popular sovereignty), P2 (code supremacy with NA0), P3 (Soulbound Identity), and P4 (dual sovereignty EQU⊥/VIC⊥) are the operational responses to each of the five proved correspondences of the proto-theorem. Without the proto-theorem, the constitutional architecture of Volume III could be read as a normative preference — with the proto-theorem, it is a structurally necessary conclusion.

Chapter Summary

Chapter 3 formalized the ontological layer of Volume II through a proto-theorem proved by the method of structural correspondence: each of the five key contradictions of Volume I (T1, T2, T3, Regularities 12 and 13) has a formal equivalent in the regularities of Volume II (14–17). This proof is not a normative critique of blockchain but a logical derivation: axioms A19–A24 structurally produce the reproduction of the contradictions that blockchain ideology declaratively claims to eliminate. Δ3 established the limit of objectivity: the ontological layer describes the structure without the subjects of its consequences — holder, user, developer — whose identification is the condition of the completeness of the analysis.

Transition to Part II

The ontological layer is complete. The proto-theorem of ontology contains three implicit agents of consequences that cannot be identified through structural analysis — they necessitate the anthropological layer. Part II introduces the class positions of the blockchain economy, proves that anonymity and pseudonymity do not eliminate structural subjecthood, and demonstrates how holder-subjectivity reproduces — in a specific form — the same logic of the extraction of subjecthood that Volume I established with respect to digital capital.

PART II. THE ANTHROPOLOGY OF BLOCKCHAIN

The subjective layer: who lives within blockchain — the antithesis

The ontological layer of Volume II established that blockchain as an objective structure reproduces the contradictions of digital capital on a new technological substrate. The proto-theorem of ontology contains implicit agents of consequences — holder, user, developer — whose identification is the condition of the completeness of the analysis. Part II fulfills this task: it identifies the subjects of blockchain, describes the class positions they constitute, and proves that the specific forms of blockchain subjectivity (anonymity,

holder-position, staking, critique) reproduce the logic of alienation established in Volume I within a new technological envelope.

Chapter 4. The Class Morphology of Blockchain

Part I described blockchain as a structure without subjects — as the movement of hashes, tokens, and consensus mechanisms. This description is necessary but logically incomplete: a structure generates consequences that are borne by concrete agents occupying concrete positions within that structure. Chapter 4 introduces the axioms of the anthropological layer (A25–A30), derives from them five class positions of the blockchain economy, and proves that the temporal barrier T2 of Volume I is reproduced at the level of tokens as a structural consequence of these positions.

Axioms of the Anthropology of Blockchain

A25. Axiom of Anonymity. The subject on blockchain is identified through a private key rather than a physical person: participation in the system does not necessitate the disclosure of identity.

Justification: A25 is a direct response to the structural surveillance described in Volume I. If the platform generates predictive value through the profiling of the subject (A3, Volume I), then the elimination of the link between address and identity must render profiling impossible — and consequently protect subjecthood from its alienation into a predictive product.

Proof of the structural limit of A25: A25 eliminates one type of identification — the link between address and identity through personal data. However, it does not eliminate identification through behavioral patterns: the sequence of transactions, amounts, temporal patterns, and the network connections of addresses constitute a behavioral profile functionally analogous to the profile of Volume I (A3). It therefore follows that anonymity in the sense of A25 is anonymity from direct identification, but not from structural profiling. Additionally: A25 eliminates political accountability alongside surveillance. If the subject is a key rather than a person, the bearer of the key bears no political accountability for actions: a governance decision adopted by an anonymous holder generates consequences for all participants in the system, yet its author remains unidentified. → Conclusion: A25 generates protection from surveillance at the cost of eliminating political accountability — this is a structural exchange, not a neutral technical property.

Connection with Volume III: Principle P3 (Soulbound Identity) in Virtublic resolves the contradiction of A25 through separation: political participation (EQU⊥) is bound to a verified identity through zk-proof — consequently, accountability is preserved without the direct disclosure of personal data. Anonymity in the sense of privacy from surveillance and accountability in the sense of responsibility for governance decisions are mutually compatible under the correct cryptographic architecture.

A26. Axiom of Pseudonymity. Blockchain is not an anonymous but a pseudonymous system: all transactions are public and attached to addresses; anyone may trace the movement of tokens between addresses without knowing the identities of their owners.

Justification: A26 is a specification of A25: the system does not conceal transactions, it conceals only the transaction-identity link. This presupposes a balance between the transparency of the system (transaction verification) and the privacy of the subject (protection from identification).

Proof of the structural limit of A26: Pseudonymity generates a structural contradiction invisible under superficial analysis. On one hand, the publicity of transactions is a necessary condition of verification: any participant may confirm that a transaction is valid, since she can view the entire history of the blockchain. On the other hand, the publicity of transactions is a necessary condition of de-anonymization: if an address is disclosed even once — through a KYC procedure on a centralized exchange, through a public announcement of an address for donations, or through forensic analysis — then the entire transaction history of that address becomes known retrospectively. This generates surveillance without protection in the sense of the right to erasure: the subject cannot delete the history of her transactions once it has been recorded (A21). → Conclusion: pseudonymity is not a compromise between privacy and transparency but a mechanism of deferred surveillance: the subject considers herself protected until the moment of the first address disclosure, after which her entire history becomes accessible without the possibility of its elimination.

Formal expression: Privacy(pseudonymous address) → 0 in the presence of a single point of de-anonymization and the immutability of transaction history (A21).

Connection with Volume III: Principle P14 (Proof-of-Offline) in Virtublic responds to the structural limit of A26 through the cryptographic architecture of zk-proof: the citizen verifies the fact of participation (voting, transaction) without disclosing the content of that participation. History is not public by default; verified aggregates are public. This resolves the contradiction of A26 at the level of protocol architecture.

A27. Axiom of the Holder as Subject. The subject of blockchain is defined through token ownership (holder) rather than through the use of the system (user) or civic status (citizen): governance is grounded in token voting, and consequently political subjecthood is identical to capital ownership.

Justification: A27 is a direct consequence of A22 (the token as universal equivalent) and Regularity 15 (plutocratic consensus): if the right to participate in governance is instantiated through the token, then the subject of governance is the token holder.

Proof of the structural limit of A27: A27 generates the fundamental separation between political subjecthood and economic participation that blockchain ideology declaratively claims to overcome yet in fact reproduces in a new form. The user who employs a DeFi protocol daily bears the consequences of all governance decisions: changes in interest rates, liquidation conditions, and security parameters. However, if the user is not a holder of governance tokens, she does not participate in the adoption of these decisions. This is the precise reproduction of T4 (accountability without power, Volume I): the subject bears the consequences of decisions in the adoption of which she does not participate. The inversion is that the holder is not necessarily a user of the system: a significant portion of governance tokens in major protocols belongs to venture capital funds that acquired them at the stage of pre-launch financing. These funds are governance holders but not users of DeFi protocols — they control the parameters of systems in which they do not participate as users.

Consequently, A27 generates a structural situation in which power over the system is concentrated among agents whose interests are investment-oriented (token price appreciation) rather than operational (system quality for users). → Conclusion: holder-subjectivity reproduces the alienation of T1 of Volume I in a specific form: political subjecthood is alienated from the users of the system and concentrated among capital holders who possess access to tokens at the pre-launch stage.

Connection with Volume III: Principle P4 (EQU⊥/VIC⊥ orthogonality) in Virtublic severs the identity declared by A27: civic status (EQU⊥) is the foundation of political subjecthood, not token ownership. VIC⊥ determines economic participation proportional to contribution — yet it does not convert into the political power of EQU⊥. A user without VIC⊥ possesses full political sovereignty through EQU⊥.

A28. Axiom of Key Privacy. The private key is the complete and sole proof of the right to assets: whoever knows the key owns the assets; loss of the key is equivalent to the irreversible loss of assets.

Justification: A28 is a consequence of A21 (immutability) and the technological principle of self-custody: if there is no centralized arbiter (A19), there is no key custodian to whom one may apply for their recovery. This eliminates dependence on third parties.

Proof of the structural limit of A28: A28 generates three structural problems, each of which is irreversible by definition. First: the key as the sole proof of the right to an asset eliminates the distinction between de facto and rightful ownership. Whoever obtained the key through fraud, coercion, or breach possesses de facto ownership of the assets with no mechanism of contestation (A21). Second: key privacy does not protect against coercion — it protects against technical breach. The state, employing legal or physical mechanisms of coercion, may compel the subject to disclose the key. The so-called wrench attack — coercion to disclose the key under threat of physical harm or legal prosecution — is documented in numerous cases and admits no technical solution within the framework of A28. Third: A28 generates the problem of inheritance without a legal framework: if the holder dies without transferring the key, the assets are irreversibly lost; if the holder transferred the key to an heir, the blockchain has no knowledge of the heir's right — it is his right solely because he knows the key. → Conclusion: A28 replaces the legal framework of ownership with the technical fact of key control. This is not the elimination of power but the elimination of the legal protection of the subject against the arbitrary seizure of assets.

Connection with Volume III: Principle P8 (Axiom-Break Condition) and principle P2 (code supremacy with NA0) in Virtublic require that constitutional code contain mechanisms for the correction of documented injustices. The complete replacement of the legal framework with the technical fact of key ownership is constitutionally impermissible, since it eliminates rectification — a necessary property of any normative system.

A29. Axiom of Anonymization Instruments. Anonymity is enhanced through technological instruments: mixers (transaction-blending services) and privacy coins (cryptocurrencies employing Ring Signatures and zk-SNARKs to conceal sender, recipient, and amount).

Justification: A29 is a response to the limit of A26 (pseudonymity does not protect against de-anonymization): if the publicity of transactions generates vulnerability, specialized anonymization instruments must eliminate that vulnerability.

Proof of the structural limit of A29: A29 generates a conflict between technical privacy and economic operability. Mixer-anonymized assets are de facto excluded from the liquid market — they exist in the system but cannot be realized through the primary points of conversion between fiat and crypto assets. Privacy coins have been delisted from major exchanges. Consequently, anonymity through privacy coins is technically accessible and economically penalized: the subject who chooses full anonymity bears significant liquidity costs. This is the precise reproduction of T5 of Volume I (structural neutralization): individual resistance — the use of anonymization instruments — is economically non-viable in a ranked (regulated) environment. → Conclusion: A29 proposes instruments of anonymity that function technically yet are destroyed economically through the regulatory environment. This is not incidental — the state, described in ΣA17 of Volume I as the structurally interested purchaser of predictions, possesses a direct incentive to eliminate instruments that disrupt its access to transactional data.

A30. Axiom of Staking as Economic Participation. Participation in a blockchain system through staking — the locking of tokens to obtain validator rights and staking rewards — is the primary form of economic contribution in PoS systems.

Justification: A30 reflects the operational logic of PoS: instead of electricity expenditure (PoW), the participant provides economic collateral through the locking of tokens, thereby generating an incentive to maintain honest consensus.

Proof of the structural limit of A30: A30 conceals the duality of staking through the neutral formulation of "economic contribution." Staking is simultaneously an infrastructural contribution (the validator maintains network operations) and an accumulation mechanism (staking rewards increase stake proportional to its initial size). The compound effect of staking rewards generates increasing stratification: the large staker receives more rewards in absolute terms, by virtue of which his stake grows faster, which increases his governance power (Regularity 15), which enables him to influence protocol parameters in his favor. Staking pools controlled more than 60% of all staked ETH in 2024. Consequently, staking is de facto oligopolistic: not every participant, but only those who reach the threshold (independently or through a pool), participate in consensus directly. → Conclusion: A30 neutralizes the political characterization of staking as a mechanism of governance power accumulation by representing it solely as an economic contribution. This is the ideological function of the axiom: the concealment of the political dimension of economic participation.

Connection with Volume III: Principle P4 (VIC⊥) in Virtublic preserves the economic function of staking (reward for infrastructural contribution) while eliminating its political dimension through the separation of VIC⊥ and EQU⊥. Staking rewards are a function of VIC⊥; governance is a function of EQU⊥. The compound effect of VIC⊥ accumulation does not convert into the growth of EQU⊥.

4.1. Five Class Positions of Blockchain

Axioms A25–A30 constitute five structural class positions of the blockchain economy. These positions are not normative categories — they are structurally defined positions within the system of production and distribution of predictive and governance power.

Holders (token holders) occupy the first and politically dominant class position (from A27 + Regularity 15). Holders control governance through token voting — consequently, they possess the power to determine system parameters: interest rates in DeFi protocols, liquidation conditions, treasury distribution, and smart contract upgrades. The motivational structure of holders is investment-oriented: their primary incentive is token price appreciation, not the operational quality of the system for users. The consequence of this structure is a systematic divergence between governance decisions optimal for holders (short-term price growth through buybacks, limitation of competing forks) and governance decisions optimal for users (security, accessibility, low fees). This divergence is not the result of malicious intent by specific holders — it is the structural consequence of the coincidence of governance subjectivity with investment interests.

Stakers (validators in PoS) occupy the second class position (from A30 + Regularity 15), which is a subspecies of holders with additional infrastructural rights and obligations. The staker locks tokens as collateral and receives validator rights — that is, the right to participate directly in block production and to receive block rewards. The staker is simultaneously an economic agent (receiving rewards) and a political agent (validating transactions, instantiating protocol norms). Staking pools concentrate staking power among infrastructure operators: Lido DAO controls more than 30% of staked ETH through liquid staking (stETH), thereby generating a systemic risk of consensus centralization within a formally decentralized system. This is the structural analogue of the algorithmic intermediaries of Volume I (class position 4, Chapter 4): the staking pool operator is a technically necessary intermediary possessing operational power without the direct political subjecthood of pool users.

Users occupy the third class position (from A27), which structurally reproduces the position of the "attention supplier" of Volume I. The user is the functional subject of the system — she employs DeFi protocols, trades NFTs, and interacts with smart contracts. The user generates transactional activity that creates value for holders (token price growth through utilization) and for stakers (transaction fees). However, the user is not a holder of governance tokens in the majority of cases — consequently, she bears all the consequences of governance decisions (changes in liquidation parameters, protocol security, operating conditions) without participating in their adoption. This is the precise reproduction of T4 of Volume I: the subject bears accountability (economic risks from governance decisions) without power (participation in governance). The gap between user and holder is not an incidental distribution of tokens — it is the structural consequence of the token distribution model at protocol launch: early investors and the development team receive a significant share of governance tokens prior to user onboarding, by virtue of which governance is controlled by a group that does not constitute the user base.

Developers occupy the fourth class position (from A24 + Regularity 14), which is the position of algorithmic power. The developer formulates smart contracts and protocol parameters, thereby determining the normative environment for all other participants. The algorithmic power of the developer is de facto political power (Regularity 14) — it determines which

transactions are possible, which parameters are fixed, and which governance mechanisms exist — without a democratic mandate and without a mechanism of political accountability. Core developers of Ethereum (Ethereum Foundation) possess influence over the development roadmap of the protocol disproportionate to their formal governance status: EIPs (Ethereum Improvement Proposals) are formulated by a limited circle of technical experts, while holders vote for or against without possessing the technical resources for independent assessment of consequences. This generates epistemic asymmetry: formally, holders possess governance power, yet factually they depend on the agenda-setting authority of developers.

Critics occupy the fifth class position, specific to the blockchain economy relative to the class morphology of Volume I. The critic is an intellectual agent who identifies the structural contradictions of the system and produces their analysis — without proposing an institutional alternative. This position is structurally necessary to the system for a reason that requires formal description. A system that declaratively asserts its openness to discussion and the elimination of censorship requires the presence of critics to verify its own declaration: the presence of visible critics constitutes proof of openness. Critics functioning within the information space of the blockchain economy (publications, conferences, podcasts, social media) receive from that same space symbolic and economic capital: media visibility, speaking fees, grants from protocol foundations, and book sales to an audience interested in the subject of the critique. Consequently, critics are participants in the system whose critique they produce — this does not eliminate the value of their analysis, but it generates a structural position in which radical institutional critique is economically non-viable for the critic himself. This is the reproduction of Regularity 11 of Volume I (the epistemological non-viability of internal critique) as applied to intellectual production: the critic who proposes the complete transcendence of blockchain logic (rather than its improvement) deprives himself of the audience and institutional resources upon which his capital depends.

4.2. The Reproduction of the Temporal Barrier at the Level of Tokens

The class morphology of blockchain is not static: positions are not determined once and for all but are reproduced through a mechanism analogous to the temporal barrier T2 of Volume I. T2 established that the early history of data generates a structural advantage that increases monotonically and is not self-correcting. In the blockchain economy, this mechanism is reproduced through three interrelated processes.

The first process is governance control. Early holders receive tokens at the pre-launch stage through three channels — ICO (initial coin offering), airdrop (token distribution to early users), and early mining (token extraction prior to the system reaching maturity). Through all three channels, tokens are acquired at prices incommensurably below subsequent market prices — which means the early holder possesses a disproportionately large quantity of tokens at far lower initial cost. Since governance power is proportional to stake (Regularity 15), early holders possess disproportionate governance power — not as a result of greater contribution to the system, but as a result of earlier entry into it.

The second process is economic advantage. Early token purchases at low prices generate economic profit proportional to the growth of market capitalization, which is in turn determined by the growth of the user base. Users joining later generate network value

(protocol utilization) that capitalizes into token price — that is, it is redistributed toward early holders. This is the structural mechanism of value extraction analogous to the extraction of predictive value by the platform from attention suppliers (T1, Volume I): late users generate value through utilization, early holders extract it through token appreciation.

The third process is network effects. The more users join the system, the more valuable the token — and consequently the more valuable the holder-position of early participants (Regularity 2, Volume I: network effects). Early holders do not generate the network value of user base growth, yet extract it entirely through token price appreciation. This is the reproduction of the mechanism through which dominant platforms extract value from network effects without proportional contribution: the platform does not generate the social connections of users, it generates the infrastructure, while value is produced by users through their interactions.

The conjunction of these three processes constitutes the precise analogue of T2 at the level of tokens. T2 asserted that the early history of data generates a structural advantage that increases monotonically. At the level of tokens: early entry into the system generates governance advantage (through token quantity), economic advantage (through low acquisition price), and network advantage (through token appreciation following user base growth). Each of the three advantages increases monotonically without a self-correction mechanism: the compound effect of staking rewards increases governance power; token price growth increases unrealized gains; user base growth increases appreciation. Consequently, the temporal barrier T2 is reproduced at the level of tokens not as an exception to the decentralized principle but as its logical consequence under axioms A27 and A30.

Antithesis: mechanisms exist for mitigating the influence of the temporal barrier in tokenomics — vesting schedules (the gradual unfreezing of team tokens over several years), retroactive airdrops (the post-factum distribution of tokens to actual users), and governance power decay (diminishing vote weight over time without active participation). Response: vesting schedules reduce the speed of realization of the early investors' advantage but do not eliminate the advantage itself — upon expiration of the vesting period, early investors possess the same disproportionate holdings. Retroactive airdrops were executed as one-time events and did not alter the long-term concentration of governance. Governance power decay is a rare mechanism not employed in the largest protocols. Consequently, the existing mechanisms for mitigating the temporal barrier are palliative rather than structural solutions.

Chapter Summary

Chapter 4 introduced six axioms of the anthropological layer of blockchain (A25–A30) and deconstructed each through correspondence with the theorems and regularities of Volume I and Volume II. Five class positions were identified: holders (governance control without operational accountability), stakers (infrastructural power through the concentration of staking), users (operational participation without governance power), developers (algorithmic power without democratic mandate), and critics (a structural position within the system whose critique they produce). Subchapter 4.2 proved that the temporal barrier T2 of Volume I is reproduced at the level of tokens through three interrelated processes — governance

control, economic advantage, and network effects — each increasing monotonically without a self-correction mechanism.

Transition to Chapter 5

The identification of five class positions is a necessary but not sufficient condition for proving that blockchain reproduces the alienation of subjecthood established in Volume I. It is necessary to prove the mechanism of this reproduction — the manner in which holder-subjectivity structurally supplants civic subjecthood and how this supplantation generates specific forms of injustice. Chapter 5 fulfills this task through theorems T11–T13.

Chapter 5. Anonymity, pseudonymity, and surveillance

The class morphology described in Chapter 4 constituted five structural positions of the blockchain subject. However, all five positions share a common condition of participation: the subject interacts with the system through a private key that generates a public transaction history. This condition is not a neutral technical fact but a normatively significant architectural choice: the publicity of transaction history creates a specific visibility configuration in which the subject is observable to the system without reciprocal observability of the system to the subject. Chapter 5 analyzes this configuration through two axioms A25–A26 and A29, expands them into structural regularities, and proves that blockchain generates surveillance by design and that the instruments for overcoming it are economically neutralized — which constitutes a reproduction of the mechanism of T5 of Volume I at the level of transactional privacy.

5.1. Pseudonymity as surveillance without protection

Blockchain ideology declares pseudonymity to be a compromise between the transparency of the system — necessary for the verification of transactions — and the privacy of the subject — necessary for protection from surveillance. A26 formulates this compromise as follows: the address is public, the identity behind the address is not; it therefore follows that the system is transparent and the subject is protected. This assumption is structurally untenable, because it ignores the asymmetry that pseudonymity produces between different classes of observers.

The three directions of surveillance constituted by pseudonymity are independent and function simultaneously, mutually reinforcing one another.

State surveillance. Pseudonymity protects against direct identification only up to the first point of disclosure of the address–identity link. After this point, the entire transaction history, including retrospective data, becomes known without additional technical effort. The point of disclosure is in the majority of cases not an exception but a structurally necessary condition of participation in the economy: centralized exchanges, which are the primary channels for conversion between cryptocurrency and fiat assets, are obliged to conduct KYC verification pursuant to the requirements of the Financial Action Task Force (FATF) in jurisdictions covering more than 90% of global GDP. It therefore follows that a subject seeking to realize assets through the fiat economy is structurally compelled to disclose the address–identity

link. Blockchain forensics companies — Chainalysis, Elliptic, CipherTrace — provide state bodies with instruments for the retrospective analysis of transactional patterns, enabling the reconstruction of the history of asset movements from the moment of the first token receipt. According to Chainalysis (2024), the DEA, FBI, IRS Criminal Investigation, and analogous agencies are the largest corporate clients of blockchain surveillance services. This constitutes the operational realization of the conflict of ΣA17 of Volume I as applied to blockchain: the state as a structurally interested purchaser of predictions invests in instruments that extirpate the subject's pseudonymous protection. Pseudonymity with respect to the state is accordingly not a protection but a deferral of identification.

Corporate surveillance. The publicity of transaction history creates a new type of behavioral data extractable without the subject's participation. On-chain activity — the sequence of interactions with DeFi protocols, patterns of NFT purchase and sale, staking history, participation in governance votes — is a publicly accessible behavioral profile structurally analogous to the profile generated by digital capital platforms (A3, Volume I). The essential distinction from Volume I consists in the fact that the data is not generated covertly by a platform — it is generated publicly by the subject. However, the structural function is identical: behavioral history permits the prediction of the subject's future behavior and the adaptation of service offerings, advertising, or attacks to it, including targeted phishing based on the on-chain portfolio. NFT analytics platforms — Nansen, Dune Analytics — produce the segmentation of addresses by behavioral patterns — smart money wallets, NFT whales, DeFi farmers — which constitutes an operational classification of subjects by their transactional profile. This reproduces T1 of Volume I (the alienation of behavioral data into predictive value) with one structural distinction: the subject personally and voluntarily publishes data, producing alienation without an intermediary platform-agent. The structure of alienation is identical; its visibility to the subject is paradoxically lower, because the subject perceives the publication of transactions as a personal act of transparency.

Social surveillance. The publicity of on-chain data creates a third type of observation — horizontal, effected not by the state or a corporation but by other participants in the system. Rich addresses — wallets with large positions — are publicly observable objects: their transactions are tracked through wallet-tracking services by thousands of participants who copy their trading decisions (copy trading) or use information about their movements to obtain a competitive advantage. This produces a specific form of compelled transparency: a subject with substantial holdings does not possess the right to unpredictability (N1, Volume I) — each of the subject's transactions is observable in real time. The absence of privacy with respect to wealth creates concrete security risks: documented cases of physical compulsion to disclose keys (wrench attacks) systematically correlate with the public identification of large holders. This is the paradoxical consequence of A21 (immutability) and A26 (pseudonymity): a system that declares the protection of the subject from state confiscation generates public wealth exposure that increases the risks of non-state compulsion.

The aggregate structural result of the three directions: pseudonymity is not a compromise between transparency and privacy — it is transparency with deferred identity disclosure. For the state, this deferral is operationally surmountable through the KYC obligations of exchanges. For corporations, it is immaterial, because the behavioral profile is accessible without personal identification. For horizontal social observation, identity is not necessary at all — the address functions as an observable subject independently of the identity of its

holder. Conclusion: blockchain does not generate privacy — it generates transparency without protection, in which the subject believes itself to be pseudonymously protected while remaining in fact observable across three independent directions simultaneously.

Formal expression: the effectiveness of pseudonymous protection is inversely proportional to the number of independent observation channels and directly proportional to the number of on-chain transactions generating a profilable history.

Connection to Volume I: the structure of surveillance generated by pseudonymity is a precise reproduction of the mechanism Capture → Prediction → Governance (ΣA15, Volume I) on a blockchain substrate. On-chain history is Capture; wallet analytics is Prediction; adapted offerings or attacks are Governance. The technological substrate has changed — the structural loop is reproduced.

Connection to Volume III: principle P14 (Proof-of-Offline) and principle P3 (Soulbound Identity with zk-proof) in Virtublic architecturally sever the mechanism of surveillance by design: the citizen verifies the fact and legitimacy of participation through a zk-proof without disclosing the content of participation. Transaction history is not public by default — aggregated verified results are public. This extirpates all three directions of surveillance while preserving the verifiability of the system.

5.2. Anonymization instruments and their economic limits (extension of A29)

A29 declares: anonymity is strengthened through technological instruments — mixers and privacy coins. This constitutes the technological response to the limit of pseudonymity described in section 5.1: if the publicity of transactions creates observability, specialized instruments for its neutralization must restore the subject's privacy. Chapter 4 recorded the limit of A29 briefly through an analogy with T5. Section 5.2 deploys the formal structure of this limit.

Regularity 18 (from A29 + T5, Volume I). Economic neutralization of privacy instruments. Technically accessible anonymization instruments are systemically neutralized by regulatory and market mechanisms, thereby reproducing T5 of Volume I (structural neutralization of individual resistance) at the level of transactional privacy.

Justification: A29 established that mixers and privacy coins are technically functional anonymization instruments. T5 of Volume I established that an individual strategy of resistance is economically unprofitable within a ranked environment. From the conjunction of these two elements it follows that a technically functional privacy instrument existing within a regulated economic environment is subject to the same neutralization mechanisms as individual resistance in Volume I.

Proof: Tornado Cash is the most significant documented case of the complete neutralization cycle. The protocol was a technically functional instrument for the anonymization of Ethereum transactions through cryptographic mixing. In August 2022, OFAC placed the Tornado Cash smart contracts on the SDN list (Specially Designated Nationals), establishing a precedent of sanctions against program code rather than against a legal entity. The immediate consequence was the blocking of all addresses that had interacted with the protocol on major centralized exchanges — including addresses that had used Tornado

Cash for legitimate purposes (for example, Ethereum Foundation developers who had accidentally received "dust" from mixer addresses). Alexei Pertsev, one of the developers, was convicted in the Netherlands in 2024 to 5 years and 4 months for money laundering — notwithstanding the court's acknowledgment that the code functioned without the developer's awareness of the specific unlawful transactions. This precedent establishes the criminal liability of the developer of a neutral instrument for its use by third parties for unlawful purposes. Consequence for blockchain development: the creation of privacy instruments is legally risky irrespective of the developer's intentions.

Privacy coins demonstrate the neutralization mechanism through delisting. Monero (XMR) uses Ring Signatures and stealth addresses to conceal the sender, recipient, and transaction amount. Zcash (ZEC) uses zk-SNARKs for optional shielded transactions. Both protocols are cryptographically mature and functionally superior to Bitcoin on privacy parameters. However: Binance delisted XMR in February 2024; Coinbase has never listed XMR; Kraken delisted XMR for EU users in 2023. ZEC is listed on a limited number of exchanges with low liquidity compared to BTC or ETH. Operational consequence: a subject using Monero to protect transactional privacy simultaneously incurs costs of several types. First, liquidity costs: the spread between XMR and fiat on available venues is substantially higher than for BTC or ETH. Second, conversion costs: the XMR → fiat pathway requires intermediate stages through P2P platforms or decentralized exchanges with limited volumes. Third, reputational costs: the very use of a privacy coin creates suspicion in a compliance context irrespective of the content of transactions.

The structural logic of neutralization is identical to the mechanism of T5 of Volume I. T5 proved that the algorithmic ranking function assigns lower reach to critical content, which renders the individual strategy of resistance economically unprofitable. As applied to privacy instruments: the regulatory and market environment assigns lower liquidity to assets that have passed through a mixer or privacy coin — which renders the individual strategy of privacy preservation economically costly. In both cases the instrument of resistance is technically accessible and economically penalized. The system does not prohibit privacy instruments — it renders their use prohibitively costly. This is a more effective neutralization mechanism than direct prohibition, because prohibition creates a legal basis for contestation, whereas market neutralization is the technically neutral consequence of the compliance requirements of exchanges. Conclusion: Regularity 18 is a reproduction of T5 at the level of transactional privacy. The right to unpredictability (N1, Volume I) is technically realizable and economically penalized in the existing blockchain economy.

Formal expression: the economic accessibility of a privacy instrument is inversely proportional to the degree of its conflict with the compliance requirements of the dominant exchange platforms.

Empirical verification: according to Chainalysis (Crypto Crime Report 2024), the share of transactions using privacy-enhancing tools in the total volume of on-chain transactions declined in 2022–2024 despite the technological improvement of the instruments. This constitutes a measurable confirmation of Regularity 18: the growth of technical privacy capabilities is accompanied by a decline in their actual use — under the influence of mounting economic costs.

Critique: why neutralization is structural rather than incidental. An objection obtains: state neutralization of privacy instruments is a political decision of specific governments, not a structural property of blockchain. Should regulatory policy change, privacy instruments may become economically accessible. Response: this objection is correct with respect to the political reversibility of specific regulatory decisions. However, the structural argumentation of Regularity 18 rests not on the immutability of specific regulatory decisions but on the structural conflict of interests of ΣA17 of Volume I: the state as a purchaser of transactional data through blockchain surveillance services — Chainalysis is a state contractor — possesses a structural incentive to neutralize instruments that extirpate this possibility. This conflict of interests is not an incidental political disposition — it is a consequence of the state's role as simultaneously a regulator and a consumer of surveillance products. It therefore follows that the neutralization of privacy instruments is structurally reproducible irrespective of changes in specific governments or regulators. Conclusion: the system does not neutralize privacy through an arbitrary political decision — it neutralizes it through the structural conflict of interests described in ΣA17 of Volume I and reproduced at the level of blockchain compliance economics.

Supplement to Regularity 18: the cognitive dimension. The economic neutralization of privacy instruments is not the sole barrier to their use. The second barrier is cognitive, analogous to T6 of Volume I (cognitive disarmament): the correct use of privacy instruments requires technical competences — an understanding of UTXO versus account-based models, correct management of seed phrases, and verification of smart contracts of mixer protocols. The majority of users do not possess these competences, which renders privacy instruments functionally inaccessible irrespective of their economic accessibility. A technically proficient user may use Monero through P2P exchange without centralized exchanges. However, this path requires technical knowledge, time expenditure, and readiness for liquidity losses — that is, resources systematically inaccessible to the majority of participants in the blockchain economy. It therefore follows that the double barrier — economic plus cognitive — reproduces the structure of T5 + T6 of Volume I at the level of transactional privacy: individual resistance to surveillance is economically costly and cognitively exhausting simultaneously.

Connection to Volume III: the Virtublic architecture resolves the contradiction of Regularity 18 not through the protection of privacy instruments as such but through the embedding of privacy into the protocol at the constitutional level. N7 (the right to cognitive autonomy) and N1 (the right to unpredictability) are constitutional norms, not optional instruments. The Virtublic citizen does not select a privacy instrument — privacy is the architectural property of participation by default through zk-proof verification. This extirpates the economic barrier — no choice between liquidity and privacy is required — and the cognitive barrier — no technical competences are required to use the built-in protocol mechanism.

Chapter Summary

Chapter 5 proved two interrelated theorems with respect to the privacy of the blockchain subject. Section 5.1 established that pseudonymity is not a compromise between transparency and privacy but transparency with deferred disclosure — producing surveillance across three independent directions (state, corporate, social) without real protection of the subject. The observability configuration is a structural consequence of A26,

not a defect in the implementation of specific platforms. Section 5.2 introduced Regularity 18 (economic neutralization of privacy instruments) and proved that technically accessible anonymization instruments are neutralized by a double barrier — economic (through the compliance requirements of exchanges and regulatory sanctions) and cognitive (through the technical requirements imposed on the user). This double barrier is a reproduction of T5 + T6 of Volume I at the level of transactional privacy and is structurally robust by virtue of the state's conflict of interests as a purchaser of surveillance products (ΣA17, Volume I).

Transition to Chapter 6

Chapters 4 and 5 identified the class positions of the blockchain subject and proved that the instruments protecting the subject's subjecthood — anonymity, pseudonymity, privacy tools — are structurally neutralizable. The next logically necessary step is the formalization of these results into theorems T11–T13, which complete the anthropological layer and prepare the transition to the epistemological one. T11 will prove PoS plutocracy as a structural theorem. T12 will prove the surrogate character of DAO legitimacy. T13 will prove the impossibility of accountability without identity. Their conjunction forms the anthropological limit of blockchain as an autonomous institutional form.

Chapter 6. The Holder as Economic Subject

Structural Regularities of Holder Subjecthood

The anthropological layer of Volume II has reached the point at which the following must be registered: if Chapter 4 established the class morphology of the blockchain as a structure of positions, and Chapter 5 analyzed the mechanics of anonymity and pseudonymity as the false sovereignty of privacy, then Chapter 6 proceeds to the analysis of the holder as a subject — not in the sense of his personal characteristics, but in the sense of the structural position that determines the horizon of possible motivations, decisions, and consequences. The holder exists not as an individual with preferences, but as a functional unit whose behavior is determined by three regularities: the logic of critique as commodity, the logic of speculative motivation, and the logic of governance capture through the market mechanism. Each of these regularities is not an incidental observation, but the necessary consequence of axioms A27 and A23, introduced in the preceding chapters.

Regularity 18. Critique as Commodity

Regularity 18 is derived from axiom A27 (the holder as subject) and the class position of critics identified in Chapter 4. Its formal expression: Critique(system) → Monetization(critique) → System_stability ↑.

The substantive meaning of this is as follows. Critical discourse concerning digital capital, the blockchain, and surveillance capitalism is invariably embedded in the very attention economy that it describes as its object of critique. A book about surveillance is sold through surveillance platforms. A lecture on attention manipulation is monetized through the same audience retention mechanisms that the lecture exposes. An article on the structural contradictions of proof-of-stake is published in media financed through venture capital that

has invested in proof-of-stake protocols. This is not hyperbole and not a particular case — it is the structural property of the system, following from axiom A6 of Volume I: the cycle Attention → Data → Model → Utility → ↑Attention has no internal point of saturation, and critique is not an exception to this cycle. It is a part of it.

The mechanism operates as follows. Critical analysis produces content with high engagement density: it offers cognitive contradiction, activates reflexivity, and generates in the consumer a sense of being informed. All of these are emotional and cognitive states that algorithmic platforms optimize for the retention of attention. Critique of the system is, consequently, structurally profitable content for the system: it produces engagement, channels tension, and prevents the conversion of cognitive discomfort into political action. The reader who has finished Zuboff's book feels enlightened — and precisely this feeling substitutes for action. Enlightenment without an institutional alternative is a form of stabilization of the system it describes.

Consider specific cases that demonstrate Regularity 18 as a systemic, rather than singular, phenomenon.

Shoshana Zuboff, in The Age of Surveillance Capitalism, produces what is arguably the most precise and detailed diagnosis of surveillance capitalism published in the academic genre. The book has been translated into twenty languages, has become a bestseller, and has brought the author significant symbolic and economic capital. The normative solution Zuboff proposes — "new rights" of the subject within liberal democracy, regulatory pressure on platforms — does not affect the structure of accumulation described in Volume I: it presupposes that the state is a neutral regulator, whereas Regularity 12 of Volume I demonstrated the structural conflict of interest of the state as a buyer of predictions. The result: Zuboff's book is cited by Google as evidence that the company "takes academic critique seriously." Critique becomes a legitimation resource for the very subject it critiques.

Bernard Stiegler developed the concept of an "economy of contribution" as a response to the pharmacology of digital technologies — the idea that the same instruments that produce psychic atrophy can be reoriented toward individuation. Morally, this position is attractive. Institutionally, it is vacuous: the economy of contribution possesses no operational definition that would permit its distinction from existing forms of participation in the platform economy. "Contribution" in Stiegler's conception is indistinguishable from "engagement" in the platform's conception — both denote the active participation of the subject in the production of value. The absence of institutional architecture means that the idea remains in the space of discourse, without passing into the space of structural change.

Evgeny Morozov systematically critiques technological solutionism — the illusion that technical solutions are capable of extirpating political contradictions. This is a precise diagnosis, applicable to the majority of blockchain projects. However, Morozov's positive program reduces to calls for state regulation. Regularity 12 of Volume I exhausts this answer: a state that systematically buys predictive data from the very platforms it is supposed to regulate cannot be a neutral regulator. Critique of technological solutionism that offers state regulatory solutionism as an alternative reproduces the same logic at the institutional level.

Critics of the blockchain — Nicholas Weaver, David Golumbia, Vlad Zamfir — accurately diagnose the plutocratic nature of proof-of-stake and the problem of governance without legitimacy. Zamfir publicly argues against "governance minimization" at conferences sponsored by the Ethereum Foundation. The Ethereum Foundation cites these arguments as evidence of openness to debate. The critique does not alter the architecture of the protocol — it legitimizes the Foundation as an institution tolerant of dissent. This is not the pathology of particular actors. It is the structural consequence of Regularity 18: any critique without an institutional alternative performs the function of channeling tension and legitimizing its object.

Formally, Regularity 18 registers the following mechanism. A system founded on the maximization of predictive power (A6, Volume I) extracts from critique the same type of value as from any other content with high engagement density: it monetizes the attention of the critique's audience, produces data on the cognitive patterns of critically disposed subjects, and uses the very fact of the existence of critique as a legitimation resource. The critic who publishes analysis within the existing media infrastructure is invariably a part of the cycle being analyzed. This does not render critique useless — it renders it insufficient. Critique without an institutional alternative is the necessary but not sufficient condition for change.

The connection to Volume III is determined by precisely this derivation. Virtublic does not produce critical discourse about digital capital. Virtublic produces constitutional architecture that is the institutional alternative. The diagnosis elaborated in Volumes I–II is not channeled into books and lectures — it crystallizes into the executable code of principles P0–P18. A constitution cannot be cited as evidence of openness. It can only be observed or violated. This is the sole form that the system is incapable of converting into a legitimation resource.

Regularity 19. Speculative Motivation of Holders

Regularity 19 is derived from axiom A27 (the holder as a subject defined by token ownership) and axiom A23 (liquidity as the fundamental property of a token). Its formal expression: Governance(decisions) → max(Token_price), not max(User_welfare).

The content of this regularity is as follows. Since the governance token is freely exchangeable on the market and possesses speculative value, the motivation of the holder is structurally directed toward the maximization of the token price, not toward the welfare of the system or its users. This is not a psychological assertion about the greed of particular actors. It is an institutional derivation: in a system where governance rights are expressed as a liquid token, the rational holder optimizes his token ownership as an investment. A governance decision that increases the token price is structurally preferable regardless of its consequences for user welfare.

The mechanism of realization of Regularity 19 unfolds through several causal chains. The first: revenue protocol → token buyback/burn → token price ↑ → holder wealth ↑. A DeFi protocol adopting a decision on high fees increases its own revenue. A portion of the revenue is directed toward the buyback and destruction of governance tokens (buyback/burn). The reduction of supply at constant demand increases the token price. The holder accumulates wealth. Users pay higher fees for using the protocol. The governance decision optimizes holder wealth at the expense of user welfare. This is not an aberration —

it is the rational realization of the objective function within the institutional architecture defined by A27 and A23.

The second chain: narrative → speculation → price ↑ → governance capture. A holder possessing a significant share of governance tokens is interested in the propagation of narratives that increase speculative interest in the protocol: roadmap announcements, partnership deals, technical updates with high PR effect. Governance decisions concerning such narratives are adopted not because they are technically optimal, but because they produce a favorable market signal. The ratio between the real technical value of a decision and its PR value shifts in favor of PR value as the share of speculative capital in the holder structure increases.

The third chain: governance paralysis in the event of conflicts of interest between holder groups. Large holders with differing portfolio positions may block governance decisions that do not correspond to their specific investment interests. This is not governance in the sense of collective administration — it is bargaining between concentrated positions. Voter apathy among small holders amplifies this effect: when the cost of participation in governance exceeds the expected influence of a single vote, the rational small holder does not participate. Governance is de facto in the hands of the active minority of large positions, which reproduces Regularity 15 (plutocratic consensus) at the operational level.

The connection to Volume I is discernible through theorem T1 (surplus attention). In the model of digital capital, users generate value through the alienation of attention, platforms extract value through the monetization of predictive data, and the subject receives no compensation commensurate with the value produced. In the model of blockchain governance, users generate value through the use of the protocol (liquidity, volume, fee generation), holders extract value through the growth of the token price, and users do not participate in governance. The structure of exploitation is preserved: the substrate has changed (attention-tokens → governance tokens), but the asymmetry of appropriation has remained isomorphic. The blockchain does not resolve T1 — it reproduces it in tokenomic form.

It is necessary to register that Regularity 19 does not mean the absence of holders motivated by the long-term development of the protocol. Such holders exist. However, their motivation within the existing institutional architecture structurally coincides with the motivation of a speculative holder over a sufficiently long time horizon: long-term development of the protocol also maximizes the token price. The absence of a distinction between governance directed at the welfare of the system and governance directed at the growth of the token price is not a defect of a particular implementation, but the systemic property of an architecture in which governance rights are expressed as a liquid asset.

Connection to Volume III: principle P4 (Dual Sovereignty) resolves Regularity 19 through the constitutional orthogonality of EQU⊥ and VIC⊥. EQU⊥ — political sovereignty — is distributed as soulbound identity, not as a liquid token. It cannot be bought, sold, or speculatively valued. Consequently, political decisions in Virtublic cannot be motivated by the growth of the price of a political token, since no such token exists. The economic motivation of VIC⊥ holders is preserved — but it is confined to technical decisions concerning infrastructure, not political decisions concerning norms. Principle P16 (Rockefeller Mode)

institutionalizes this separation: infrastructure operators extract economic value from VIC⊥ without obtaining access to EQU⊥ decisions.

Regularity 20. Governance Capture Through the Market

Regularity 20 is derived from axiom A29 (anonymization instruments and their economic limits) and Regularity 17 (liquidity destroys governance). Its formal expression: Capture_cost = Token_price × Tokens_for_majority.

The formulation is concise, but its consequences are fundamental to the understanding of the structural failure of the DAO as a form of governance. If governance tokens are freely exchangeable on the open market, then the right to administer the protocol is a purchasable asset. The cost of acquiring control over governance is the market value of the tokens necessary to form a majority. Given the known market capitalization of the protocol and the known distribution of tokens, Capture_cost is computable. This means that governance is vulnerable to hostile takeover in precisely the same degree that a joint-stock company is vulnerable to a hostile takeover — with the essential difference that traditional corporate law contains instruments of protection against hostile takeover (poison pills, staggered boards, supermajority requirements), whereas the majority of DAOs contain no analogous mechanisms, or contain them in insufficient form.

The mechanics of capture unfold as follows. The attacker accumulates governance tokens on the open market, acquiring a share sufficient to form a simple or qualified majority. The attacker introduces a governance proposal optimized for value extraction: withdrawal of treasury funds, modification of the fee structure in favor of large holders, modification of the smart contract to redirect the flow of funds. The proposal passes the vote, since the attacker controls the majority. Capture_cost is amortized by the extracted value. The attacker sells the tokens, whose price falls following the extraction event. Minority holders sustain losses.

This is not a hypothetical scenario. MakerDAO in 2020 faced the threat of governance capture through the open-market accumulation of MKR. Beanstalk Farms in April 2022 was subjected to a flash loan attack: the attacker used an instant credit to temporarily acquire a majority of governance tokens, adopted a proposal for the withdrawal of $182 million from the protocol, repaid the flash loan, and disappeared. Technically the operation was correct: the attacker used the governance mechanism in precise accordance with the code. Code is law operated against the governance system it was supposed to protect. This is not a vulnerability of the implementation — it is the logical consequence of an architecture in which the liquid token is the sole form of governance rights.

It is necessary to register that partial protection mechanisms exist: timelock (delay of proposal execution), quorum requirements, and veto rights for the core team. However, each of these mechanisms introduces an element of centralization that directly contradicts axiom A19 (decentralization as a sufficient condition). Timelock protects against flash loan attacks, but creates a window for counter-coordination and thereby presupposes the existence of a trusted coordinating center — a core team, foundation, or multisig committee. Quorum requirements are effective against low-turnout capture, but are vulnerable to the concentrated positions of large holders who participate in governance systematically (Regularity 24, to be introduced in Part III). Veto rights of the core team constitute de facto centralization of governance beyond the declared DAO architecture.

Regularity 20 reproduces theorem T5 of Volume I (structural neutralization of resistance) in the blockchain context. In the model of digital capital, any strategy of individual resistance is economically non-viable: the share of reach of an alternative position tends to zero as the predictive power M of the platform increases. In the DAO model, any strategy of a minority holder for resisting majority capture is structurally neutralized through the market mechanism: Capture_cost decreases as the token price falls, minority holders lose not only governance influence but their economic position simultaneously. The capital sufficient for a counter-takeover is structurally smaller among minority holders than among the attacker — otherwise they would not be minority holders. Resistance to capture from within the DAO system reproduces the same asymmetry as resistance to platform dominance from within the recommendation environment.

The following is of fundamental importance: Regularity 20 operates not only in the case of an explicit hostile takeover. It operates continuously as structural pressure on governance architecture. Every large holder knows that his governance influence is proportional to his share of tokens. Every governance decision that reduces the token price reduces his influence and simultaneously increases the relative share of positions that do not sell tokens on a price decline. This generates sustained pressure in favor of governance decisions that optimize the token price — regardless of whether this is a conscious strategy or the structural consequence of institutional logic. Regularity 20 thereby reinforces Regularity 19: the speculative motivation of holders and the possibility of capture through the market form a mutually reinforcing mechanism, in which governance is consistently displaced in the direction of the interests of large capital.

The connection to Volume I is also discernible through theorem T4 (responsibility without power): the holder bears the economic risks of the protocol (loss of token value in the event of systemic failure), but the user bears the political risks of governance decisions (loss of funds upon modification of the fee structure, liquidation upon modification of collateral requirements), without possessing commensurate influence over the decisions adopted. In a DAO, holder and user are intersecting but non-coincident sets. The intersection is incomplete precisely where it is most important: a large holder controlling governance may not be an active user of the protocol and thereby bears none of the operational risks of the decisions he adopts.

Connection to Volume III: principle P5 (limited influence) resolves Regularity 20 through the quadratic cost function of additional influence: $cost(n) = n^2$. With quadratic scaling, Capture_cost grows as the square of the required influence, not linearly with the required share of tokens. This does not extirpate the possibility of concentration of influence, but renders it structurally more costly through the non-linear growth of that cost. Principle P11 (Success Multiplier) supplements P5: a broad organic coalition of users receives institutional amplification proportional to the number of unique citizen-participants, which generates a structural advantage for distributed participation over concentrated capital. Together, P5 and P11 resolve what Regularity 20 identified as the systemic defect of the DAO: the absence of a mechanism by which the organic breadth of participation could exceed concentrated capital intensity.

Analytical Synthesis of Chapter 6

The three regularities introduced in this chapter constitute a closed analytical structure that must be registered before the transition to the following part.

Regularity 18 demonstrates that critique of the system without an institutional alternative is not a threat to the system, but its functional element: it produces engagement, channels tension, and legitimizes the object of critique as open to debate. This means that the position of critic in the class morphology of the blockchain (Chapter 4) is not external to the system, but structurally integrated into it.

Regularity 19 demonstrates that the holder as a subject is the bearer of a motivation directed toward the maximization of the token price, not user welfare. This follows directly from the institutional architecture that makes governance rights a liquid market asset. Governance, in such a structure, does not optimize the collective good, but the portfolio positions of the dominant holders.

Regularity 20 demonstrates that the liquidity of governance tokens renders the political administration of the protocol a purchasable asset with a computable cost. Capture through the market is structurally possible and periodically realized. Protection mechanisms introduced against capture introduce elements of centralization that contradict A19.

These three regularities together describe the holder as a subject who simultaneously bears the economic consequences of the protocol, determines its governance trajectory, and is vulnerable to displacement by concentrated capital. This position is structurally unstable: the small-scale holder bears risks without commensurate influence, the large-scale holder optimizes the system in the direction of his own benefit, and the critic reproduces the system through discourse without an alternative.

The conjunction of Regularities 18–20 exhausts the anthropological analysis of holder subjecthood. The next step is the transition to stakers, validators, and the concentration of infrastructure (Chapter 7), since staking as a form of participation is the operational mechanism through which Regularity 15 (plutocratic consensus) is realized in the form of concrete institutional practices of power accumulation.

Chapter Summary

The following has been deconstructed: the thesis concerning critical discourse as an instrument of systemic change (Regularity 18 demonstrates its function as a stabilizer); the thesis concerning holders as actors oriented toward the welfare of the protocol (Regularity 19 demonstrates the structural conditionedness of speculative motivation); the thesis concerning DAO governance as a protected form of collective administration (Regularity 20 demonstrates its vulnerability to market capture). Demonstrated: the holder as a subject is the product of an institutional architecture that produces these motivations and this vulnerability with the necessity following from axioms A23 and A27.

Transition to Chapter 7

If Chapter 6 registers the motivational structure of the holder as an economic subject, Chapter 7 proceeds to the analysis of the staker and validator as an infrastructural subject. This is logically necessary, since it is precisely through staking that the mechanism which

Regularity 15 described as plutocratic consensus is realized: the compound interest effect, concentration through staking pools, and the structural impossibility of a small participant competing with an institutional staker. Chapter 7 translates the analysis from the level of governance motivation to the level of infrastructural concentration — and thereby completes the anthropological layer before the transition to the epistemology of the blockchain.

Chapter 7. Stakers, validators, and the concentration of infrastructure

Structural regularities of staking

Where Chapter 6 established the motivational structure of the holder as a subject whose position is determined by the speculative logic of the liquid token, Chapter 7 proceeds to the level of infrastructural participation — to the staker and validator as subjects whose role in the protocol is conditioned not solely by token ownership but by control over the computational infrastructure that secures consensus. It is precisely here that the promise of decentralization encounters its most severe structural refutation: the mechanism intended to distribute consensus power among a plurality of participants generates concentration through two mutually reinforcing mechanisms — the compound interest effect and centralization through staking pools. Regularities 21 and 22 formalize this process as structurally inevitable rather than as an artifact of a specific implementation.

Regularity 21. Concentration through staking

Regularity 21 is derived from axiom A20 (consensus mechanisms and their logic) and axiom A30 (staking as economic participation). Its formal expression: Wealth(t+1) = Wealth(t) × (1 + staking_reward_rate).

This expression establishes a mechanism structurally identical to axiom A6 of Volume I (self-augmentation without saturation). There, the cycle was described as Attention → Data → Model → Utility → ↑Attention — a closed loop in which the accumulated resource generates additional resource without an organic point of saturation. In proof-of-stake, the logic is isomorphic: Stake → Validation rights → Staking rewards → ↑Stake. The base resource — tokens — generates the right to validation, which generates rewards denominated in those same tokens, thereby increasing the base resource. The loop is closed. No internal equalization mechanism exists.

Consider the quantitative dynamics at standard Ethereum parameters. The staking reward rate for the period 2023–2026 was approximately 4% per annum. At this value, a staker with a position of 1,000 ETH receives an annual reward of 40 ETH on the condition that the reward is reinvested in staking. A staker with a position of 10 ETH receives 0.4 ETH. The absolute gap per year is 39.6 ETH. Over ten years, under the condition of constant reinvestment, the position of the staker with an initial 1,000 ETH reaches approximately 1,480 ETH; the position of the staker with an initial 10 ETH reaches 14.8 ETH. The absolute gap grows from 990 ETH to 1,465.2 ETH. The relative gap is preserved: both positions grew by the same percentage. Yet this is precisely the property that Regularity 21 establishes as a structural defect: under proportional reward, inequality is measured in absolute units of governance influence — and in absolute units the gap only grows.

It is critically important to note that this mechanism does not constitute exploitation in the narrow sense — the extraction of a resource from one party in favor of another. It is the automatic consequence of an architectural choice: reward proportional to contribution. This choice is intuitively just — whoever contributes more to network security receives more reward. However, in conjunction with the fact that governance influence is also proportional to stake, it generates the progressive concentration of political power without any active act of extraction. The wealthy staker does not exploit the small staker — he simply participates in a mechanism that, by its architecture, produces increasing inequality as a byproduct of correct operation.

This reproduces axiom A6 of Volume I on a different substrate, yet with the same structural logic. There, the axiom described: "the loop is closed without an internal point of saturation or self-regulation." Here, the same obtains: Wealth(t+1) > Wealth(t) for any t; the loop has no internal point of saturation. The gap between large and small stakers grows monotonically for any non-zero staking_reward_rate. Reducing the reward rate slows the growth of the gap but does not eliminate it: at rate = 1%, the gap grows more slowly but remains an increasing function of time.

It is also essential to consider the interaction of Regularity 21 with the slashing mechanism — sanctions for incorrect validator behavior (downtime, double-signing). Slashing is applied either as an absolute value or as a percentage of stake. Under absolute slashing, the large staker incurs smaller relative losses than the small staker. Under percentage slashing, relative losses are equal, yet the large staker possesses a greater buffer for absorbing absolute losses without losing validator status. In both cases, slashing as a security mechanism generates asymmetric pressure: it is structurally more demanding for small participants, who possess a lower margin of resilience. This is not a constructive defect of slashing as a mechanism — it is a consequence of its application to participants with fundamentally different resource positions.

Connection with Volume I: Regularity 21 reproduces theorem T1 (surplus attention) on a new substrate. In digital capital, the asymmetry was expressed as the systematic excess of predictive value over the subject's zero compensation. In the PoS system, the asymmetry is expressed as the systematic increase of the gap between positions under a formally equal reward rate. T1 described the profile-index as the formal measure of predictive value at zero monetary reward. Staking reward is not zero compensation, yet it is proportional to position, which means it is itself a form of reproducing inequality through the correct operation of the mechanism.

Connection with Volume III: Principle P12 (Dual Reserve Market) addresses Regularity 21 through the severance between VIC⊥ (economic sovereignty) and EQU⊥ (political sovereignty). In Virtublic, staking rewards in the form of VIC⊥ remain proportional to contribution — the mechanism for rewarding infrastructure operators is preserved, since it is economically functional. However, VIC⊥ does not convert into EQU⊥. Consequently, the accumulation of VIC⊥ through staking rewards does not generate the accumulation of governance influence in the political dimension. The compound interest effect continues to operate in the economic space — yet it is constitutionally precluded from conversion into political domination through principle P4 (Dual Sovereignty).

Regularity 22. Centralization through staking pools

Regularity 22 is derived from the same axioms A20 and A30 as Regularity 21, yet establishes a different mechanism of concentration — not through the compound interest effect, but through the structural barrier to participation that compels small holders to delegate staking to centralized intermediaries.

The architectural fact from which the regularity is derived: the minimum stake for launching an independent validator on the Ethereum network is 32 ETH. At the ETH price range of $2,500–$3,000 characteristic of the period 2023–2026, this corresponds to an entry barrier of $80,000–$96,000. This barrier is not an incidental number but the result of a deliberate architectural choice: the threshold of 32 ETH was established as a compromise between a sufficient number of validators for distributed consensus and sufficient economic commitment to preclude Sybil attacks. This is a technically justified choice. Its structural consequence — the exclusion of the majority of holders from direct validation — is not intentional, yet is necessary.

A holder of 5 ETH, 10 ETH, or 25 ETH cannot independently launch a validator. The economically rational strategy for such a holder is to delegate stake through a liquid staking protocol or centralized exchange. Lido Finance, the largest liquid staking protocol, controlled more than 30% of all staked ETH by 2024–2026. Coinbase, Kraken, and Binance in aggregate controlled a further significant share. In this way, several entities de facto controlled validation rights for the greater part of the staked ETH of a network that declaratively identifies itself as decentralized.

This is the precise reproduction of the temporal barrier described in theorem T2 of Volume I — yet not through the early history of data, but through the minimum economic barrier to participation. T2 asserted: "past the point of no return, competition within a homogeneous modal layer is structurally impossible without external intervention." In the staking context: once Lido had accumulated a sufficient share of staked ETH, its competitive advantage — the liquid token stETH, deep integration with the DeFi ecosystem, reputation, and trust — became self-reproducing. A new liquid staking protocol cannot reproduce this history from a zero position. The barrier is not created technically but economically — through network effects and integration that reproduce the structure of T2 on a new substrate.

It is necessary to establish with precision the mechanism through which staking pools generate centralization. When a holder delegates ETH to Lido, she receives stETH — a liquid token representing her share of staked ETH. Lido accumulates ETH from multiple holders and distributes it among node operators — legal entities that have passed an onboarding procedure. The decision as to which operators to entrust with ETH is adopted by the governance of the Lido protocol, controlled through the LDO token. The loop is closed: the holder delegates ETH to the pool, the pool delegates validation rights to operators, operators generate staking rewards, the pool retains its commission, and the holder receives stETH with a yield. At each stage of this chain, a point of centralized control emerges, masked by the tokenomic wrapper of decentralization.

Consider the systemic risk generated by this architecture. If Lido controls more than 33% of staked ETH, it possesses the potential capacity to attack consensus finality (liveness attack). If control exceeds 51%, double-spending attacks become theoretically possible, though

economically irrational for a legitimate operator. The Ethereum community recognizes this risk: initiatives for staking diversification exist. However, the very necessity of these initiatives confirms Regularity 22: absent external correction, proof-of-stake generates concentration that necessitates external countermeasures. This constitutes direct evidence of theorem T3 of Volume I (the structural absence of correction) in the blockchain context: the system contains no internal mechanism for correcting concentration.

Axiom A19 (decentralization as a sufficient condition for overcoming monopolization) is refuted not through theoretical reasoning but through observable data: the most successful implementation of proof-of-stake produces a level of staking concentration at which several entities control more than half of all validation rights. This is not a critique of a failed implementation. It is a statement of structural consequence: minimum participation barrier + rationalization through liquid tokens = inevitable concentration through intermediary pools.

The connection to staking advantage as a concept requires separate formal establishment. Staking advantage in the context of this analysis denotes the aggregate advantage accruing to a subject capable of independently launching validators: direct control over validation rights without an intermediary, full staking reward without a pool commission (Lido retains 10% of rewards), voting in the protocol governance through direct ownership of validator keys, and the absence of counterparty risk of a staking pool. This multidimensional advantage is inaccessible to the holder with a position below 32 ETH. Staking advantage is a form of inequality generated by the architectural choice of a minimum participation barrier, not by market forces in a neutral sense.

The conjunction of Regularities 21 and 22 describes the following structural loop: the wealthy staker accumulates stake through compound interest (Regularity 21), obtains staking advantage through direct validation, controls governance through token voting, adopts decisions that optimize token price (Regularity 19), which additionally increases his position. The small holder delegates to a staking pool (Regularity 22), loses a portion of the reward as commission, does not control governance directly, and bears counterparty risk from the pool. Both participants are formally situated within a "decentralized" system. Factually, they occupy fundamentally different structural positions with incommensurable rights and risks.

Connection with Volume III: Principle P16 (Rockefeller Mode) and principle P12 (Dual Reserve Market) in conjunction address Regularity 22. Virtublic acknowledges that infrastructure operators are economically necessary and merit reward through VIC⊥. NodeFactory as an institution secures the technical participation of operators in the network. However, operators receive VIC⊥ without EQU⊥: their economic dominance in the infrastructural layer is constitutionally precluded from conversion into political dominance. This resolves the fundamental defect of staking pools — not their economic existence, but their political influence through governance tokens. In Virtublic, a staking pool may control 30% of the infrastructural layer and receive commensurate VIC⊥ reward — yet this has no bearing on the distribution of EQU⊥, which remains equal for each citizen through Soulbound Identity.

Analytical synthesis of Chapter 7

Regularities 21 and 22, considered jointly, establish the following. Proof-of-Stake as a decentralized consensus mechanism contains two embedded vectors of concentration: the

compound interest effect (Regularity 21), which generates an increasing gap between large and small stakers as the automatic consequence of proportional reward, and the minimum participation barrier (Regularity 22), which generates the delegation of small holders to centralized pools as a rationally compelled choice. Both mechanisms operate without malicious intent on the part of specific actors — they are structural consequences of architectural decisions adopted to secure the safety and efficiency of consensus.

This means the contradiction between the promise of decentralization and the practice of concentration in PoS systems is neither incidental nor eliminable through parameter adjustment. It is structural, following from axioms A20 and A30 with the same necessity by which theorem T2 of Volume I follows from Regularity 4. Reducing the minimum participation barrier mitigates Regularity 22 but intensifies Sybil vulnerability (T15). Raising the entry barrier strengthens security but intensifies Regularity 22. This is not a trilemma requiring the identification of an optimum — it is a structural contradiction admitting no solution within the logic of PoS.

Chapter 7 concludes the anthropological analysis of blockchain. Chapters 4–7 identified the subjects of blockchain: holders with their speculative motivation, stakers and validators with their infrastructural advantage, users without governance influence, developers with algorithmic power, critics as functional stabilizers of the system. Not one of these subjects is a genuine political subject in the sense of NA0 of Volume I: the holder optimizes token price, the staker extracts compound interest, the user bears consequences without influence, the developer writes rules without a democratic mandate, the critic channels tension without altering the structure.

Chapter Summary

The following has been deconstructed: the thesis of proof-of-stake as a mechanism of equal participation (Regularity 21 demonstrates the structural increase of inequality through compound interest); the thesis of decentralized consensus as the overcoming of the temporal barrier (Regularity 22 demonstrates its reproduction through concentration in staking pools); and the thesis of the staker as a functionally equal network participant (staking advantage is a structural property of the architecture inaccessible to the majority of holders). It is proved that proof-of-stake generates the concentration of infrastructural power with the same structural necessity by which digital capital generates the temporal barrier.

Transition to Chapter 8

Chapters 4–7 have exhausted the anthropological layer: all class positions of blockchain have been identified, motivational structures have been formalized, and mechanisms of concentration have been proved. Chapter 8 establishes the second Δ-crisis: not one of the identified subjects is a political subject in the constitutional sense, and not one of the described forms of participation generates legitimate governance. This necessitates transition to the epistemological layer — to the analysis of how blockchain reproduces its own legitimacy despite the evident structural contradictions established in Parts I and II.

Chapter 8. The second crisis: the limit of blockchain anthropology

Proto-theorems of the anthropological layer

The anthropological layer of Volume II fulfilled its analytical task to the extent determined by Δ3: to identify the subjects of blockchain and to demonstrate whether they bear the consequences of the structural contradictions recorded in Part I. The answer produced by the totality of Regularities 18–22 is unambiguous: they do — but not as political subjects, but as economic agents whose behavior is determined by the institutional architecture of the system. This distinction is fundamental and requires precise formalization before the anthropological layer can be closed.

Proto-theorems are not theorems in the full sense: they constitute intermediate conclusions that summarize the analytics of Parts I–II and formulate a requirement for the next layer. Their function is to record the limit attained by anthropological analysis and to demonstrate why this limit logically necessitates the transition to epistemology.

The first proto-theorem of blockchain anthropology is formulated as follows: none of the subjects identified in the class morphology of blockchain realizes political subjecthood within the meaning of axiom A7 — that is, none is a bearer of intentionality not reducible to the subject's economic position within the system. The holder is reduced to a portfolio position through Regularity 19. The staker is reduced to an infrastructure share through Regularity 21. The user is reduced to a protocol consumer without governance rights through T4. The developer is reduced to algorithmic authority through Regularity 14. The critic is reduced to a producer of legitimation resources through Regularity 18. Axiom A7 of Volume I asserted: "the subject exists as an immediate datum not reducible to the subject's profile on the platform." Blockchain generates a different form of the same reduction: the subject is not reduced to a digital profile but is reduced to a tokenomic position.

The second proto-theorem records the following: individual and collective resistance to the structural contradictions of blockchain is neutralized not through suppression but through the reproduction of the same mechanisms that resistance opposes. The individual holder seeking to resist governance capture may vote against a proposal — but the holder's influence is proportional to the holder's share, which by definition is smaller than the majority's share (Regularity 20). A coalition of small holders may coordinate, but coalition coordination reproduces the same logic of token voting that it seeks to neutralize: the coalition aggregates tokens, and the aggregate of tokens remains smaller than the position of the large staker under the preservation of the compound interest effect (Regularity 21). Critical discourse resisting the ideology of decentralization is monetized through the same attention economy that it criticizes (Regularity 18). At every level — individual, coalitional, discursive — resistance structurally generates the reproduction of that which it resists.

This is the precise blockchain analogue of theorem T5 of Volume I: "any strategy of individual resistance is economically unprofitable within a ranked environment." In the blockchain context: any strategy of resistance to plutocratic logic is economically unprofitable within a system in which governance influence is proportional to capital position.

The third proto-theorem records the logical necessity of transition: the anthropological layer describes subjects who bear the consequences of structural contradictions but are incapable of altering them either individually or collectively. However, the system itself continues to function, to attract participants, and to reproduce the narrative of its own legitimacy. This

means that there exists an epistemological mechanism through which the system constructs legitimacy without possessing an external democratic foundation for it. This mechanism is the subject of Part III.

Δ4 — CRISIS: THE LIMIT OF BLOCKCHAIN SUBJECTIVITY

Regularities 18–22, considered in their totality, produce a conclusion that the anthropological layer cannot resolve by its own means.

The holder is motivated by token price appreciation, not by the good of the system; governance decisions optimize the portfolio position (Regularity 19). The staker accumulates infrastructural power through the compound interest effect without generating new value (Regularity 21) and concentrates validation rights through staking pools, reproducing the temporal barrier T2 of Volume I in the tokenomic substrate (Regularity 22). The user bears the operational risks of the protocol without commensurate governance influence (T4). The developer determines the rules through algorithmic authority without a democratic mandate (Regularity 14). The critic is absorbed by the system through the monetization of diagnosis, thereby stabilizing what the critic diagnoses (Regularity 18).

None of these subjects is a political subject within the meaning of NA0 of Volume I. No form of their participation generates governance grounded in popular sovereign authority. Blockchain ideology declared: the elimination of centralized control is a sufficient condition for the emergence of genuine self-governance. The anthropological analysis refutes this declaration not through theoretical reasoning but through the exhaustive typology of subject positions: in each of them the subject proves to be an agent of economic logic rather than a bearer of political will.

Regularities 18–22 together reproduce Δ2 of Volume I on a blockchain substrate. There the limit of anthropology was formulated through theorems T5 and T6: individual resistance is neutralized economically and cognitively. Here the limit is formulated through Regularities 19–22: individual and collective resistance is neutralized through the reproduction of the same plutocratic logic that resistance opposes. In Volume I the conclusion necessitated the transition to the epistemological layer for analysis of how the system reproduces its own legitimacy. Here — the same conclusion, the same structural necessity of transition.

The question that the anthropological layer cannot answer — and which defines the agenda of Part III — is formulated as follows: by what means does a system structurally devoid of a democratic foundation for governance, containing no mechanism of equal participation, and generating the concentration of infrastructural power as a necessary consequence of its own architecture — nonetheless reproduce the narrative of its own legitimacy? How does "code is law" function as a source of normative authority in the absence of a normative axiom? How does DAO token voting reproduce the appearance of democratic participation under the structural dominance of capital? How is Sybil resistance constructed as a technical problem when its solutions inevitably require centralization? Part III answers these questions through the epistemological analysis of the legitimation mechanisms of blockchain.

Chapter Summary

The following is recorded: the three proto-theorems of the anthropological layer summarize the reduction of all subject positions of blockchain to economic agency, the insufficiency of individual and collective resistance as strategies for altering the structure, and the logical necessity of transition to epistemological analysis. Δ4 formally closes the anthropological layer, recording that the limit of blockchain subjectivity consists in the fact that the system does not generate a political subject — it generates an economic agent whose subjecthood is exhausted by tokenomic position.

Transition to Part III

The anthropological question "who bears the consequences" is exhausted: all subjects have been identified, all mechanisms of resistance neutralization have been formalized. The epistemological question "how the system reproduces its legitimacy" is the sole remaining undisclosed one. Part III opens with the analysis of "code is law" as the primary mechanism for the construction of normative authority without a normative axiom — and it is precisely with this that Chapter 9 begins.

PART III. THE EPISTEMOLOGY OF THE BLOCKCHAIN

The synthetic layer of analysis begins where the ontological and anthropological layers exhaust themselves. Parts I and II established: the blockchain reproduces the temporal barrier at the level of tokens (T11), plutocracy through staking advantage (T12), and speculative logic that excludes operational subjecthood (T13). The epistemological layer poses a more fundamental question: by what means does the blockchain construct its legitimacy, reproduce itself as truth, and absorb critique while producing none of the conditions necessary for the protection of subjecthood in the sense of NA0? The answer unfolds through three mechanisms: code is law as the optimization of efficiency without a normative axiom, DAO governance as circular legitimation through token voting, and Sybil resistance as a structural contradiction that requires precisely the centralized trust that blockchain ideology declares extirpated.

Chapter 9. Code is law and its limits

Synthetic axioms of the epistemology of the blockchain

The six synthetic axioms of the epistemological layer (ΣA31–ΣA36) do not describe new empirical phenomena — they register the logical structures that blockchain ideology accepts as the axiomatic foundations of its legitimacy. The analysis of each axiom demonstrates that it either contains an internal contradiction or reproduces the structural defects that the blockchain declares extirpated.

ΣA31 (code is law) registers the foundational principle: smart contracts are executed automatically, without the possibility of human intervention; there are no violations, since any action correct from the standpoint of the code is a legitimate action. Automation extirpates the arbitrariness of execution. The critique of ΣA31 consists not in the assertion that automation is undesirable, but in the demonstration that it displaces arbitrariness to an

earlier and less visible level — the level of writing the code (Regularity 14). He who writes the code effectuates a normative choice; however, this choice is concealed behind the appearance of technical neutrality. Moreover: if an exploit is the correct use of the code, it is technically legitimate within the framework of ΣA31 — which produces the paradox in which a theft effectuated through a correct function call is simultaneously a violation of intent and compliance with the law.

ΣA32 (irreversibility without correction) registers that the immutability of code protects against the arbitrary modification of rules. However, the consequence is the symmetric impossibility of correcting errors without deploying a new contract and leaving the old one vulnerable. If the consensus of the past was unjust, its reversal requires a hard fork — that is, a political decision disguised as a technical instrument. ΣA32 generates a conflict with the legal principle of rectification: law traditionally contains mechanisms for the correction of unjust decisions; blockchain ideology structurally excludes this mechanism in the name of predictability.

ΣA33 (absorption of critique) is the epistemologically most significant axiom of the layer. Critique that does not propose an institutional alternative external to the logic of the system becomes a stabilizer of that system — it demonstrates its openness without altering its structure. This is precisely why the Ethereum Foundation cites Zamfir and Weaver as evidence of the maturity of the ecosystem: critique has been absorbed and reprocessed into a legitimation resource. Volume III (Formal Theory of the Digital Republic) is the answer to ΣA33: Virtublic is not a critique of the blockchain and cannot be absorbed as such. A constitution cannot be cited as evidence of openness — it can only be observed or violated.

ΣA34 (DAO as governance without legitimacy) and ΣA35–ΣA36 (Sybil resistance and proof-of-personhood) are elaborated in sections 9.3 and 9.4 respectively. What must be registered here is their common logic: all six axioms of the epistemological layer describe mechanisms that the blockchain accepts as solutions to the problems of decentralized coordination, whereas analysis demonstrates that each of them reproduces a structural defect in a new form or generates a new defect that requires a solution the blockchain is structurally incapable of providing.

9.1. Code is law as the optimization of efficiency without subjecthood

Theorem T14 of the present volume is formulated as follows: a smart contract that optimizes an objective function without a normative axiom equivalent to NA0 produces efficient execution concurrent with the systematic destruction of the subjecthood of its participants. This is not a defect of a particular implementation — it is the structural property of the principle of code is law in its current form.

The proof of T14 is constructed through comparative analysis of two systems for the regulation of relations between the subject and the financial system. Traditional financial law contains a margin call mechanism — a notification to the subject of approach to a threshold value, together with the provision of a grace period for the deposit of additional collateral. This mechanism reflects a normative judgment: the subject is not the object of protocol optimization; he is a party to a relation possessing the right to notification and the possibility of action. DeFi protocols implementing algorithmic lending with position liquidation (Aave, Compound, MakerDAO) contain no grace period in their architecture: when the collateral

ratio falls below the liquidation threshold, the position is liquidated automatically, frequently under conditions of short-term volatility produced by the market itself, not by a fundamental change in the value of the collateral.

The efficiency of this mechanism from the standpoint of the protocol is indisputable: bad debt is extirpated immediately, systemic risk is minimized. However, from the standpoint of NA0, this mechanism produces the destruction of subjecthood in a concrete operational form: the subject who has deposited collateral is converted into the object of algorithmic optimization, which at no moment takes into account his intention, circumstances, or right to correction. The subject signed the code — he did not renounce his subjecthood — but the code contains no distinction between these two acts.

This reproduces T1 of Volume I on a new substrate: there, the subject produces predictive value without compensation and without a mechanism for restitution; here, the subject provides collateral that the optimizing protocol may seize at any moment without appeal. In both cases the structural defect is one: the system processes the subject as a resource of optimization, not as an agent with dignity and the right to correction.

A critic will observe: the subject voluntarily enters the DeFi protocol and accepts its conditions. The answer through A10 of Volume I: consent is valid only in the presence of informational competence and structural alternativity. The liquidation smart contract is publicly accessible on the blockchain; however, its operational consequences are cognitively inaccessible to the majority of participants without specialized technical preparation. This reproduces the informational asymmetry of T8 of Volume I on a new substrate: the code is public, but not transparent in the sense of cognitive accessibility.

An additional aspect of T14 concerns the bug as legitimate execution. ΣA31 asserts that the correct use of code is legitimate. Consequently, an exploit — the use of an unforeseen execution path of code — is technically legitimate within the framework of code is law, even as it violates the intent of the authors. The history of DeFi contains systematic confirmations of this principle: The DAO hack (2016, 60 million dollars), Ronin Network exploit (2022, 625 million dollars), Poly Network exploit (2021, 611 million dollars). In each case the attacker did not violate the code — he used the code in accordance with its formal logic. These are not anomalies of the ecosystem; they are the structural consequences of ΣA31.

The resolution of The DAO hack through a hard fork (Ethereum Classic being the entity that refused the hard fork) demonstrated that the principle of code is law is not absolute even for the blockchain ecosystem itself: when the damage is sufficiently large, the community resorts to a political decision disguised as a technical instrument. This means that the normative axiom exists de facto — it is simply not explicitly registered and is applied retroactively, which is a more arbitrary form of normative judgment than the explicitly introduced NA0.

Result of section 9.1: T14 is demonstrated. Code is law without NA0 optimizes efficiency concurrent with the systematic destruction of subjecthood. A normative axiom exists de facto in the ecosystem (as The DAO hard fork demonstrates), but it is applied retroactively and without procedural guarantees, which produces a more arbitrary form of normative judgment than constitutionally entrenched NA0. Connection to Volume III: P2 (code supremacy with

normative axiom) is the direct answer to T14: code is executed automatically, but contains NA0 as a constitutional limit, beyond which code may not be deployed.

9.2. The smart contract as norm: the limits of the automation of law

The principle of code is law implicitly presupposes that the smart contract is a sufficient form of normative regulation — that code can substitute for law. This thesis is subject to deconstruction through four arguments, each of which identifies a structural limit of the automation of law.

The first argument concerns the incompleteness of the contract. The theory of incomplete contracts (Grossman, Hart, Moore) establishes that any contract is incomplete in the sense that it cannot anticipate all possible states of the world. Traditional law resolves this problem through mechanisms of interpretation — courts interpret the intention of the parties and apply principles of good faith and reasonableness to fill lacunae. The smart contract has no mechanism of interpretation: it executes what is written, regardless of intention. The more complex the relation, the higher the probability that the code did not anticipate an essential state — and the more destructive the consequences of the automatic execution of incomplete code.

The second argument concerns the ineliminability of human judgment. Any smart contract interacting with real-world data (prices, identities, events) requires an oracle — an external data source. An oracle is a trusted intermediary whose existence contradicts the principle of trustlessness: if the oracle is controlled by a single agent, the entire smart contract is controlled. Attacks on oracles (Mango Markets, 2022, 117 million dollars; Cream Finance, 2021) demonstrate that this is not a theoretical vulnerability. The automation of execution under dependence on an external data source displaces the point of human judgment to the level of the oracle without extirpating it.

The third argument concerns the conflict between immutability and the legal principle of rectification. Law contains a mechanism for the reversal of unjust decisions: appeal, review, and the nullification of contracts. These mechanisms reflect the normative judgment that predictability is not the sole value of a legal system and that the correction of injustice may require retroactive intervention. The immutability of the smart contract structurally excludes rectification. The sole form of correction is a hard fork, which is a political act without an established procedure, without criteria of application, and without a legitimation mechanism — that is, a more arbitrary form of intervention than a judicial system with its procedural guarantees.

The fourth argument concerns the problem of the bug as legitimate execution, elaborated in detail in section 9.1. It suffices to register here its legal dimension: the legal system contains the principle of volenti non fit injuria — consent to the risk limits the claim. However, this is a principle applied by a court in light of specific circumstances; it is not an absolute rule of automatic execution. DeFi reproduces the form of this principle (the user signed the contract, consequently he consented) without its content (consent is valid only in the presence of informational competence and the absence of deception concerning key risks).

Regularity 14 of Volume II is formulated on the basis of these four arguments: the automation of the execution of a norm displaces the normative choice to the level of writing

the code, rendering this choice less visible and less contestable than traditional norm-creation, while preserving all of its structural significance. Automation does not extirpate the normative choice; it conceals it.

Connection to Volume III: P2 realizes the principle of code supremacy with an explicitly introduced NA0 and the Coq verification mechanism. Coq verification establishes the formal correctness of code relative to a given specification — it does not extirpate the normative choice (the specification contains NA0 and N1–N7 as obligatory parameters), but renders it explicit, verifiable, and ineliminable without modification of the constitutional norm.

9.3. DAO governance: circular legitimation and the structural defect of token voting

ΣA34 registers the DAO as an organizational form in which governance is fully automated through smart contracts and token voting. Analysis of this form through the axiomatics of Volume I and the theorems of Volume II demonstrates that the DAO reproduces the structural defect of the concentration of power in a new form, without providing a source of legitimacy for its decisions.

The problem of the legitimacy of token voting is logically prior to the problem of its concentration. Why is one token, one vote a legitimate principle for the organization of political power? The answer of blockchain ideology: because it is so written in the smart contract. This is circular legitimation: the legitimacy of the rule concerning token voting is established through the application of that same rule. Traditional democratic theory avoids this circle through appeal to an external source of legitimacy — popular sovereignty, natural law, a constitutional constituent act. The DAO possesses no such source: the legitimacy of its governance is entirely self-referential.

The consequence of circular legitimation is that any voting result is legitimate by definition if it is produced in accordance with the protocol. There is no external criterion by which the result can be contested as illegitimate. This produces a structural defect symmetric to the defect of digital capital described in Volume I: there, the algorithm determines what is politically visible without an external normative criterion; here, token voting determines what constitutes a governance decision without an external normative criterion. In both cases, power is closed upon itself.

The concentration of tokens in DAOs reproduces T2 (temporal barrier) and T11 (PoS plutocracy) in the form of governance plutocracy. Data for the largest DAOs in the ecosystem confirm this structure with a high degree of regularity. In Uniswap DAO, the top 10 addresses control more than 40% of voting power; in MakerDAO, the analogous indicator exceeds 55%; in Compound, the top 5 addresses control more than 35%. Voter turnout in the majority of large DAOs is 5–15% of the total number of tokens, which means that actual decisions are adopted by an even more concentrated group. This is not an accident of distribution; it is the structural consequence of T11: early participants who accumulated tokens at a low price possess disproportionate governance power, which intensifies with the growth of the token value and the complexity of participation for late participants.

Regularity 19 of Volume II: in a DAO without an external source of legitimacy, governance power is concentrated among early token holders by virtue of the same temporal mechanism described in Regularity 4 of Volume I as applied to predictive capital. The barrier to entry into

governance is the token equivalent of the temporal barrier of predictive capital: a structurally identical mechanism on a new substrate.

An additional aspect of ΣA34 concerns low voter turnout as a structural, not incidental, phenomenon. A critic of blockchain analysis will observe: low turnout is a design problem, resolvable through delegation mechanisms, quadratic voting, or other innovations. The answer: low turnout is the structural consequence of T9 of Volume I (epistemological asymmetry) applied to governance — participation in voting requires an understanding of the technical parameters of a proposal, which presupposes a competence that the majority of token holders do not possess. Delegation reproduces representative democracy, but without its legitimation mechanism (elections with established procedures and the right of recall); quadratic voting resolves the problem of concentration, but not the problem of circular legitimation. Neither of these mechanisms provides the external source of legitimacy that is the structural necessity of governance without NA0.

Connection to Volume III: P4 (Dual Sovereignty) is the direct answer to ΣA34. The separation into EQU⊥ (political sovereign) and VIC⊥ (economic participant) ruptures circular legitimation: EQU⊥ derives its legitimacy from P0 (popular sovereignty as constitutional foundation), not from the fact of token ownership. The Concordance Rule requires the agreement of both spaces for constitutionally significant decisions, which structurally precludes the adoption of decisions by an economic majority without the participation of the political sovereign.

9.4. Sybil resistance: the fundamental contradiction of decentralization

ΣA35 and ΣA36 describe the problem that is the most fundamental contradiction of blockchain ideology — not a defect of implementation, but a logical contradiction at the foundations. Decentralization requires the absence of a trusted center for the verification of identities. Sybil resistance — protection against the creation of multiple fictitious identities — requires a mechanism for the verification of uniqueness. The verification of uniqueness without a trusted center is a logically irresolvable problem in an open network without attachment to physical reality.

Proof-of-Work resolves Sybil resistance through economic costs: the creation of multiple identities requires proportional computational resources, which renders the attack costly. This is not verification of uniqueness — it is an economic barrier that a wealthy attacker overcomes through sufficient investment. PoW produces Sybil resistance through the concentration of economic power (T12), not through the verification of subjecthood.

Proof-of-Stake resolves Sybil resistance through the staking requirement: the creation of multiple validating identities requires proportional capital. This reproduces the same mechanism in a more energy-efficient form: Sybil resistance is achieved through economic concentration, not through the verification of uniqueness.

Proof-of-personhood is an attempt at genuine verification of uniqueness — the verification that an address belongs to a unique human being, not to multiple addresses of a single person or to algorithmically generated fictitious identities. ΣA36 registers three main approaches: biometric verification (Worldcoin), social graph verification (BrightID, Proof of Humanity), and government ID verification (various KYC providers).

Worldcoin implements biometric verification through iris scanning using a specialized device (Orb). Analysis of this approach through the axiomatics of Volume I reveals three structural defects. First: the iris is a permanent identifier — unlike a password or key, the subject cannot alter his iris in the event of database compromise. This produces a permanent privacy risk, ineliminable by any technical measures. Second: verification is effectuated by the Worldcoin Foundation, which is a trusted center; the principle of trustlessness is violated at the level of the verification of uniqueness itself. Third: the iris scan generates a biometric database with global coverage, which reproduces precisely the type of predictive profiling (A5 of Volume I) that blockchain ideology declares an alternative to the platform economy. Worldcoin is not an alternative to surveillance capitalism — it is surveillance capitalism with a cryptographic wrapper.

BrightID and analogous social graph approaches delegate the verification of uniqueness to the social connections of the subject: uniqueness is confirmed by a network of trust in which other subjects vouch for the individual. This reproduces social capital inequality: subjects with larger social networks have easier access to verification, whereas socially isolated subjects — including persons without fixed abode, migrants without established social connections, subjects with social anxiety — are structurally excluded or possess restricted access. This produces digital inequality structurally identical to the social inequality that blockchain ideology declares superseded through the open protocol.

Government ID verification is the most evident renunciation of the principle of decentralization: the verification of uniqueness is effectuated through a state institution. Furthermore, it reproduces ΣA17 of Volume I: the state that verifies identity possesses access to data concerning the subject's participation in blockchain governance, which produces precisely the type of state surveillance over political participation that N5 (Volume I) qualifies as a violation of NA0.

Regularity 20 of Volume II: any mechanism of Sybil resistance in an open network either requires a trusted center (violating the principle of decentralization), or produces Sybil resistance through economic concentration (reproducing T11–T12), or excludes socially vulnerable groups of subjects (violating NA0). These three paths are exhaustive within the framework of existing technical approaches. Sybil resistance without a trusted center and without discrimination on economic or social grounds is an unresolved problem of blockchain architecture.

Connection to Volume III: P3 (Soulbound Identity) is the constitutional answer to Regularity 20 — however, not through the extirpation of the trusted center, but through the constitutional limitation of the functions of the verification center. P3 does not claim trustlessness in the sense of blockchain ideology: it establishes that the verification of uniqueness is effectuated by a constitutionally constrained body with a prohibition on the use of verification data for purposes exceeding the constitutional mandate. This is a normative, not technical, solution to the problem of Sybil resistance.

9.5. Theorem T14: code is law without NA0 produces efficiency concurrent with the destruction of subjecthood

Formulation of T14: a smart contract as a normative mechanism in the absence of constitutionally entrenched normative axiom NA0 optimizes a given objective function

concurrent with the systematic destruction of the subjecthood of participants, measurable through the indicators PI, CHS, and structural alternativity (Appendix I of Volume I).

The proof of T14 is constructed through three independent arguments established in sections 9.1–9.4, each of which is sufficient individually.

The first argument (from section 9.1): DeFi liquidation produces the destruction of subjecthood through the absence of a grace period and an appeal mechanism. The subject is the object of protocol optimization at the moment of liquidation: his intention, circumstances, and right to correction are algorithmically irrelevant. This is structurally identical to T4 of Volume I (responsibility without power): the subject bears the consequences of the system's functioning without possessing instruments for influencing its parameters.

The second argument (from section 9.2): the bug as legitimate execution establishes that an exploit is technically legitimate within the framework of ΣA31, which produces the systematic transfer of value from subjects to attackers without a normative correction mechanism. The aggregate losses from DeFi exploits exceeded 3 billion dollars in 2022 (Chainalysis, 2023) — not as an anomaly, but as the structural consequence of the principle of code is law.

The third argument (from section 9.3): DAO governance without an external source of legitimacy produces governance power concentrated among early token holders, without a mechanism for contesting results on the basis of a normative criterion external to the protocol. This reproduces T10 of Volume I at the level of individual organizations: any decision of a DAO is legitimate by definition if it is produced in accordance with the protocol, which renders the protocol the sole arbiter of its own legitimacy.

T14 establishes that these are not three separate problems — they are three manifestations of a single structural defect: the absence of NA0 in the architecture of the smart contract. Upon the introduction of NA0 as a constitutional limit (Volume III, P2), all three manifestations receive an architectural answer: liquidation requires a grace period and an appeal mechanism (realization of N7); an exploit requires a rectification mechanism (realization of the principle of intent through Coq verification); DAO governance requires an external source of legitimacy (realization of P0 and P4). T14 is the bridge between the deconstruction of blockchain ideology (Parts I–III of the present volume) and the constitutional architecture of Volume III.

Chapter Summary

The assertion that code is law constitutes a sufficient normative form for the regulation of relations between subjects has been deconstructed. Established: the automation of execution displaces the normative choice to the level of writing the code without extirpating it; a smart contract without NA0 optimizes efficiency concurrent with the systematic destruction of subjecthood; DAO governance is circular legitimation without an external source; Sybil resistance without a trusted center and without discrimination is an unresolved technical problem. Theorem T14 formalizes these results as a single structural derivation.

Transition to the following chapter

T14 establishes that NA0 is the necessary condition for a constitutionally legitimate smart contract. However, this generates the following question: by what means can NA0 be introduced into a technological system without producing a new form of centralization — in this case, the centralization of normative authority? Chapter 10 analyzes the mechanisms of formal verification (Coq, zk-SNARK) as the technological substrate for constitutional code, and establishes the conditions under which constitutional code is distinguished from code is law in its current form.

Chapter 10. Governance without legitimacy

10.1. DAOs as the reproduction of T8 (the sovereignty gap)

Theorem T8 of Volume I established that predictive power (de facto) and political sovereignty (de jure) move in opposite directions, and that this gap is not self-correcting. In the model of digital capital, de jure sovereignty was expressed in the formal rights of the subject — the right to consent, the right to refusal, the right to data deletion. De facto power belonged to the predictive infrastructure of platforms, which had accumulated sufficient model depth to anticipate the subject in his own decisions. The gap between these two dimensions of power generated a situation in which the subject possessed formal sovereignty while his autonomy was factually extracted.

The DAO reproduces this gap with a precision that warrants its characterization as structural isomorphism rather than incidental resemblance. De jure, in the architecture of a DAO, every holder of governance tokens possesses the right to vote on any proposal. Governance is declared decentralized: there is no CEO, no board of directors, no single decision-making center. The smart contract executes the result of the vote automatically, without the possibility of veto by any centralized agent. This is the formal structure, declared a sufficient condition for democratic self-governance.

De facto, governance is controlled by the intersection of three sets: early holders who accumulated tokens during the ICO, airdrop, or early mining period at prices inaccessible to late participants; whales who accumulated positions of sufficient size to determine the outcome of votes at low turnout; and an active minority who systematically participate in governance while the majority of holders are passive. The intersection of these three sets constitutes a de facto ruling coalition whose control over governance outcomes is not the consequence of manipulation or malicious intent, but the structural consequence of the architectural properties of token voting.

This structure reproduces T8 through the following mechanism. In digital capital, the de jure/de facto gap was generated through the asymmetry of information and predictive power: the platform knew more about the subject than the subject knew about himself, and used this knowledge to constitute the Set(options) presented to the subject at the subsequent moment in time. In the DAO, the gap is generated through the asymmetry of resources and motivation: the large holder knows more about the protocol, possesses incentives for active participation, and has the resources to monitor governance, whereas the small holder is rationally passive — the cost of his participation exceeds the expected influence of a single vote given the existing token distribution.

It is necessary to establish precisely in what manner the blockchain variant of T8 differs from its original. In Volume I, the de jure/de facto gap was generated in the absence of formal mechanisms of participation available to the subject: the subject could not vote against the recommendation algorithm. In the DAO, the subject may formally vote — the mechanism of participation exists. The gap is generated through the structural non-viability of this participation for the majority of holders: the formal mechanism exists, yet its exercise is economically irrational at a small share. This does not eliminate T8 but modifies it: the de jure/de facto gap exists not because a mechanism of participation is absent, but because it exists in a form that renders participation rational only for those whose share is sufficient to influence the outcome. This is a more refined form of the same gap.

Let us establish the empirical confirmation of this thesis through specific cases, without recourse to generalizations that might be contested as unobservable.

Uniswap DAO is one of the largest decentralized protocols by TVL. Governance is exercised through the UNI token. According to on-chain data available for the period 2021–2024, the Uniswap Labs team and early investors controlled a significant share of UNI — sufficient to determine the outcome of the majority of votes at typical turnout below 5–8%. A number of governance proposals passed with the participation of fewer than 3% of the total UNI supply. Formally, every one of the millions of UNI holders possessed voting rights. Factually, outcomes were determined by institutional holders with concentrated positions who rationally monitored governance activity.

MakerDAO, the protocol governing the DAI stablecoin, repeatedly passed governance decisions with turnout below 10% of MKR. MKR is concentrated: early participants and funds hold disproportionately large shares relative to the total number of MKR holders. Foundational decisions regarding the monetary policy of DAI — the stability rate, collateral parameters — were adopted with the participation of a minority of holders, while the consequences of these decisions were borne by the broad population of DAI users who were not MKR holders and possessed no voting rights whatsoever.

Compound, Aave, Curve — across all major DeFi protocols with governance tokens, the same structure is observed: formal decentralization with de facto control by an active minority of large holders. This is not a coincidence of implementations — it is a structural property of the token voting architecture.

The following conclusion is determinative: the DAO does not resolve T8 but reproduces it on a new substrate with a modified mechanism. In digital capital, the gap was generated in the absence of formal mechanisms of participation. In the DAO, the gap is generated through formal mechanisms of participation that are structurally non-viable for the majority. The second variant is more stable: it preserves the appearance of democratic legitimacy — every holder could have voted but chose not to — whereas the first did not generate this appearance. It is precisely this property that renders the blockchain variant of T8 epistemologically more significant: the system reproduces the sovereignty gap while simultaneously producing the narrative of its overcoming.

10.2. Voter apathy as a structural regularity

Voter apathy in the context of DAO governance is not a psychological phenomenon of passivity on the part of specific individuals but a structural regularity following with necessity from the institutional architecture of token voting. Its analysis necessitates a distinction between two conceptually distinct states that empirically yield the same observable result — low turnout — yet possess fundamentally different natures.

The first state is rational passivity. A holder with a small share of governance tokens possesses an expected influence on the outcome of a vote that tends toward zero given a large number of participants and the concentrated positions of large holders. The cost of active participation — the time required to study the proposal, understand its technical and economic consequences, form a position, and execute an on-chain voting transaction — is finite and measurable. At expected influence approaching zero, the rational holder does not participate. This is not apathy in the sense of indifference — it is the correct calculation of the relationship between cost and expected outcome.

This state is a direct consequence of axiom A27 (the holder as subject defined by token ownership) and Regularity 19 (the speculative motivation of holders). If the holder regards the token as an investment asset, his participation in governance is an additional activity not incorporated into his primary investment logic. Governance participation constitutes a negative-NPV activity for him at a small share. Structurally, this is identical to the problem of the rational voter in classical political theory: given a large number of participants and small individual influence, non-participation is the rational choice. Blockchain does not resolve this problem — it reproduces it with additional intensification through the speculative motivation of holders.

The second state is informational asymmetry. A significant portion of governance proposals in DeFi protocols are technically complex: modification of smart contract parameters, alteration of the liquidation algorithm, addition of a new collateral type. Assessing the consequences of such proposals requires technical expertise inaccessible to the majority of holders. A holder who lacks the requisite expertise faces a choice: vote blindly, delegate the vote to an expert (if such a function is supported by the protocol), or abstain. Delegation reproduces the structure of centralization: if holders delegate votes to a limited number of experts, de facto control over governance falls into the hands of those experts regardless of their formal token share. Non-participation is the most prevalent choice, as confirmed by empirical data on turnout.

Informational asymmetry is compounded by the fact that the developers and core team who draft proposals possess considerably greater information about the consequences of their own proposals than external holders. This is a structural conflict of interest: those who propose modifications possess an informational advantage over those who must approve them. In traditional corporate law, this conflict is regulated through disclosure requirements and fiduciary duties. In DAO governance, it remains unregulated, since blockchain ideology consistently rejects traditional legal mechanisms as a form of centralization.

The third state, fundamentally distinct from the first two, is the strategic passivity of large holders. A whale holder controlling a sufficient share to determine the outcome of a vote may rationally refrain from openly participating in the early stages of proposal discussion, observe the formation of positions among other participants, and vote at the last moment with

determining weight. This is a strategically dominant behavior: the holder maximizes informational advantage while preserving anonymity of intention until the moment of voting. On-chain data demonstrate that large holders systematically vote later within the voting window than small holders — this is not a random distribution but a pattern corresponding to strategic logic.

The conjunction of these three states generates the following structure of de facto governance in the majority of DAOs. An active minority of 5–10% of holders adopts decisions. This minority is not random: it comprises early holders with historical staking advantage, institutional investors with resources for monitoring and participation, core developers with informational advantage, and whale holders with sufficient share to determine outcomes. The remaining 90–95% of holders are de jure participants in governance and de facto objects of its consequences, without influence over their production.

This structure admits formal characterization. It is not democracy in the sense of one person, one vote: token voting is not bound to physical subjects. It is not plutocracy in the pure sense of one dollar, one vote: although influence is proportional to token share, the fact of the structural non-participation of the majority of holders means that de facto governance is determined not by all capital but by active capital. It is an oligarchy of activists: a small group of participants who combine a sufficient token share with the motivation and resources for active participation de facto controls the protocol. The characterization "oligarchy of activists" is more precise than "plutocracy" because it captures the dual nature of de facto power in a DAO: it is determined not only by the size of position (the plutocratic component) but also by systematic participation (the activist component).

This conclusion has a direct consequence for the assessment of the legitimacy of DAO governance. If the majority of holders rationally does not participate in governance, then decisions adopted by the active minority possess neither democratic legitimacy (they do not reflect the will of the majority of citizens), nor plutocratic legitimacy in the pure sense (they do not reflect the weighted will of all capital), nor technocratic legitimacy (they are not adopted exclusively by experts). They reflect the will of a small coalition whose power is the consequence of the intersection of capital position, informational advantage, and investment of time — but not of a democratic mandate.

Regularity 24 (governance by active minority, introduced in the structure of Volume II) formalizes this conclusion: at typical turnout below 10%, decisions are adopted by an active minority of 5–10% of holders, which does not constitute democracy in any formally rigorous sense. This regularity is a direct consequence of the conjunction of axiom ΣA34 (the DAO as governance without legitimacy) and A27 (the holder as subject defined by token ownership).

Let us now consider the attempts to resolve the problem of voter apathy undertaken within blockchain ideology, and their structural limits.

The first attempt is delegation mechanisms. Compound introduced a delegation system enabling holders to delegate their votes to chosen delegates. This solution technically reproduces the logic of representative democracy: voters delegate authority to representatives. However, it generates the following structural problem: who are the delegates and how are they selected? In traditional representative democracy, delegates are

selected through elections with territorial representation, secret ballot, and regulatorily protected candidacies. In DAO delegation mechanisms, delegates are selected through an on-chain delegation transaction that may be executed arbitrarily. There is no mechanism for ensuring delegate competence, no mechanism for their recall upon incorrect behavior, and no protection against the capture of delegation through the purchase of delegation transactions. Delegation without a normative architecture reproduces the structure of token voting at a new level: delegated votes concentrate among those delegates who are most effectively marketed or affiliated with large holders.

The second attempt is quadratic voting in DAOs. A number of protocols experimented with quadratic voting as a mechanism for reducing plutocratic concentration of influence. Quadratic voting genuinely reduces the marginal influence of large holders — cost(n) = n² renders each additional vote exponentially more costly. However, it does not resolve the Sybil problem: if a holder can create multiple pseudonymous addresses and distribute tokens among them, she instantiates quadratic voting at the price of linear voting. Sybil resistance in the context of quadratic voting necessitates the verification of the uniqueness of physical subjects — that is, precisely the mechanism that DAOs reject as centralization. Quadratic voting in a DAO without Sybil resistance is technically untenable: it improves the formal distribution of influence without altering the de facto distribution, since large holders can circumvent quadratic scaling through identity fragmentation.

The third attempt is incentivized governance participation. Certain protocols introduced token rewards for participation in governance voting — an economic incentive for active engagement. This solution has a predictable defect: it incentivizes voting but not the quality of governance decisions. A holder motivated by receipt of governance reward votes irrespective of proposal quality — voting becomes an economic activity detached from its content. At a sufficiently high governance reward, it is rational to vote on all proposals in favor of any option while minimizing the time devoted to assessment. This generates not higher-quality governance but higher turnout at reduced quality of individual decisions — which constitutes an additional channel for whale manipulation: at high turnout composed of superficial votes, the influence of concentrated, informed positions increases rather than decreases.

All three attempts share a common property: they attempt to resolve the problem of voter apathy within the architecture of token voting without altering its foundational axioms. This is the precise reproduction of Regularity 18 at the architectural level: the system absorbs improvement attempts without altering its structure. Quadratic voting without Sybil resistance, delegation without a normative architecture, incentivized voting without quality control — each of these mechanisms is an attempt to improve a defective form from within that same form. This is structural Regularity 23 (code bugs as governance crisis) as applied to governance architecture bugs: an architectural bug is not eliminated by an architectural patch without modification of its foundations.

The conjunction of subchapters 10.1 and 10.2 establishes the following. The DAO reproduces T8 (the sovereignty gap) through formal decentralization with de facto concentration in an active minority. Voter apathy is a structural regularity following from the rational calculation of holders under conditions of resource and informational asymmetry, not a psychological phenomenon. The de facto governance of a DAO is an oligarchy of activists,

possessing neither democratic, nor plutocratic, nor technocratic legitimacy in any formally rigorous sense. Attempts to correct voter apathy from within the architecture of token voting are structurally insufficient.

From these conclusions there follows the sole possible normative conclusion: governance without an external source of legitimacy — without popular sovereignty as a constitutional foundation — cannot be corrected by technical means. This constitutes the evidentiary basis for theorem T12 (Governance without legitimacy), which will be formally proved in Part IV.

Connection with Volume III is determined through two principles. Principle P4 (Dual Sovereignty) constitutionally establishes EQU⊥ as a soulbound identity — political sovereignty not reducible to tokenomic position. This eliminates voter apathy as a structural regularity in the political dimension: each citizen possesses exactly one EQU⊥ irrespective of her economic position, and the cost of her participation does not depend on the size of her share. Principle P10 (Madison Mode) and principle P11 (Success Multiplier) in conjunction generate an institutional incentive for participation through quadratic weighting and a coalition multiplier — yet on the basis of Soulbound Identity, which forecloses the Sybil vulnerability of quadratic voting identified in this chapter. Principle P13 (Digital Census v2) with the Civic Guard and Dual Suspicion Protocol secures the verification of subject uniqueness without a centralized biometric authority — precisely what is absent from DAO implementations of quadratic voting.

Chapter Summary

The following has been deconstructed: the thesis of the DAO as a form of democratic self-governance (the analysis of subchapter 10.1 demonstrates the reproduction of T8 through formal decentralization with de facto concentration in an active minority); the thesis of voter apathy as a temporary, eliminable defect (the analysis of subchapter 10.2 demonstrates its structural nature, following from the rational calculation of holders); and the thesis of technical solutions to voter apathy as sufficient (the analysis demonstrates that delegation, quadratic voting, and incentivized participation reproduce the defect at a new level). It is proved that DAO governance is an oligarchy of activists, possessing neither democratic, nor plutocratic, nor technocratic legitimacy in any formally rigorous sense. This constitutes the evidentiary basis for theorem T12, which will be proved in Part IV.

Transition to Chapter 11

Where Chapter 10 established that DAO governance is devoid of democratic legitimacy through voter apathy and concentration in an active minority, Chapter 11 proceeds to the analysis of Sybil resistance as a problem in which blockchain ideology confronts its most acute internal contradiction: protection against fictitious identities necessitates the verification of subject uniqueness, which is impossible without a trusted center — that is, without precisely the centralization that blockchain declaratively claims to have overcome.

Chapter 11. Sybil resistance as centralization

11.1. The Sybil resistance triad

A Sybil attack — the creation of multiple pseudonymous identities by a single subject with the aim of obtaining disproportionate influence in a distributed system — is a fundamental threat to any decentralized architecture that distributes rights or resources on the basis of the number of participants. The problem was formally described by John Douceur in 2002 in the context of peer-to-peer networks, but its significance for blockchain governance increased manifold as DAO token voting and mechanisms of on-chain participation acquired financial and political dimensions. Sybil resistance — the capacity of a system to resist the creation of fictitious identities — is not an optional property of decentralized consensus but its necessary condition: without it, any mechanism of equal participation degenerates into a mechanism controlled by whoever is capable of generating the largest number of pseudonymous addresses.

Blockchain ideology declared: decentralization is a sufficient condition for overcoming monopolization (A19). The analysis of Sybil resistance reveals that precisely where decentralization is most consistently realized — in the absence of a trusted center for personal identity verification — the most acute structural contradiction emerges: protection against fictitious identities requires verification of the uniqueness of real subjects, which is impossible without a trusted center. This is not a technical defect of a specific implementation — it is a logical consequence of the axiomatics of decentralization applied to a domain in which participants are human beings rather than computational nodes.

The present chapter establishes that every known mechanism of Sybil resistance requires a compromise among three incompatible requirements, and that this compromise constitutes a structural trilemma not resolvable within the logic of blockchain ideology. The three vertices of the trilemma — centralized verification, the economic participation barrier, and the computational barrier — each reproduces in its own manner the structural contradictions that blockchain declared to have overcome.

First vertex: centralized verification. The most direct solution to the Sybil problem is the verification of the uniqueness of physical subjects through a trusted body. If each participant in the system can be unambiguously matched to a real physical person, multiple identities of a single subject are detected through contradiction with the verification data. Blockchain projects implemented this approach in two principal forms: biometric verification and verification through social graphs.

Worldcoin is the most technologically ambitious implementation of biometric verification. The system uses iris scan — scanning of the iris — as the biometric identifier of uniqueness. The subject visits a physical device (the Orb), which produces a scan, generates a cryptographic hash of the biometric data, and verifies uniqueness through comparison with the database of previously registered hashes. The result is a World ID — a proof of personhood confirming uniqueness without disclosing specific biometric data through zero-knowledge technology.

The technical elegance of this architecture is evident: the zk-proof permits verification of uniqueness without establishing a central biometric database in explicit form. However, structural analysis reveals two irremediable defects. The first: who controls the Orb devices and the verification algorithm? The Worldcoin Foundation — a centralized subject that makes decisions about which biometric data are sufficient for verification, which patterns are classified as anomalies, and what the rules of exclusion from the system are. The declared

decentralization of World ID does not extirpate the dependence on a trusted hardware manufacturer and a trusted developer of the verification algorithm. This is a precise reproduction of Regularity 14: algorithmic authority is transferred not to an ownerless protocol but to the subject controlling the key infrastructure.

The second defect is more fundamental from the perspective of the normative principles of Volume I. The iris scan is a permanent identifier: the iris does not change over the course of the subject's lifetime and cannot be replaced in the event of data compromise. If the database of iris hashes is compromised, the subject loses the ability to alter the biometric identifier — unlike a password or cryptographic key. This creates a privacy risk of a fundamentally different order than traditional forms of identification: the compromise is irreversible. Axiom A4 of Volume I described the irreversibility of the crystallization of attention into data as a structural property of digital capital. Worldcoin reproduces the same irreversibility at the level of biometric identification: biometric data, once recorded by the verification system, cannot be "returned" to the subject in the sense of extirpating their predictive value for potential future purchasers of these data.

BrightID implements verification through a social graph: the uniqueness of the subject is verified through a network of mutual confirmation (web of trust). Participants verify one another through video calls, creating a graph of social connections in which fictitious identities are more difficult to establish without a real social base. The structural defect of this approach consists in the following: trust in a social graph is transitive only at sufficient connection density. Subjects not included in existing social networks — geographic, linguistic, professional — have a structurally lower verifiability, not because they are Sybil, but because the web of trust algorithm produces exclusion through social marginality. This reproduces the regularity identified in Volume I (Part II, axiom A8): the limitedness of the subject — informational, cognitive, social — is a condition of structural vulnerability. In BrightID, the socially isolated subject is vulnerable to exclusion from verification not through malicious intent but through the architecture of the algorithm.

Both mechanisms of centralized verification — biometric and social — share a common property: they require a trusted verification body that contradicts axiom A19. Worldcoin requires trust in the Foundation and the Orb manufacturer. BrightID requires trust in the web of trust algorithm and in those who control it. This is the first vertex of the trilemma: Sybil resistance through centralized verification requires centralization structurally incompatible with the declared decentralization.

Second vertex: the economic barrier. Proof-of-Stake uses capital as a barrier against Sybil: the creation of multiple validator identities requires a corresponding quantity of tokens for each identity. With a minimum stake of 32 ETH for an Ethereum validator, the creation of one thousand fictitious validators requires 32,000 ETH — a sum rendering such an attack economically irrational at sufficient token value. The economic barrier is accordingly a functionally effective mechanism of Sybil resistance in the context of validation rights: it makes the attack costly.

However, the economic barrier as a mechanism of Sybil resistance is indistinguishable from the mechanism of plutocratic consensus described in Regularity 15. If each identity in the system must be backed by capital, then the distribution of identities with governance rights

reproduces the distribution of capital. One token, one vote in proof-of-stake governance is simultaneously a mechanism of Sybil resistance — costly for the creation of fictitious identities — and a mechanism of plutocracy — conferring influence proportional to capital. These are not two separate properties of the system but a single property described from two analytically distinct positions.

The consequence is fundamental: the economic barrier as Sybil resistance cannot be reduced without simultaneously reducing resilience to Sybil attack. If the minimum stake is reduced — Sybil becomes cheaper. If the minimum stake is increased — Sybil becomes more costly, but the participation barrier for legitimate subjects rises, reinforcing Regularity 22 (centralization through staking pools). The choice of the level of the economic barrier is accordingly a choice of a point on the trade-off curve between Sybil resistance and participant inclusivity — and any point on this curve reproduces plutocratic logic to a greater or lesser degree.

This mechanism has an additional consequence for governance of equal rights. If a governance system purports to realize one person, one vote — that is, the political equality of subjects as physical persons — the economic barrier is fundamentally incompatible with this claim. Verification of uniqueness through capital means that the right to political participation is mediated by the subject's economic position. This constitutes a formal violation of normative principle N1 of Volume I (the right to unpredictability) to the extent that the subject's political participation is a condition of the subject's unpredictability to the system: a subject deprived of governance rights through an economic barrier is an object of the system's decisions rather than a participant in them.

Third vertex: the computational barrier. Proof-of-Work implements Sybil resistance through a computational barrier: the creation of fictitious network nodes requires computational resources proportional to their number. Bitcoin PoW is the most large-scale implementation of this approach: a 51% attack requires control over the majority of the network's hashrate, which at the current scale is prohibitively costly. The computational barrier, like the economic one, renders the Sybil attack irrational at sufficient network scale.

The structural defect of the computational barrier was examined in detail with respect to Regularity 22: proof-of-work generates centralization in mining pools through economies of scale. It is necessary here to establish the precise connection between this defect and the problem of Sybil resistance. PoW protects against Sybil attack at the level of block production: the creation of an alternative chain requires hashrate that the attacker does not possess. However, PoW does not protect against Sybil at the level of governance: in PoW systems with on-chain governance, voting rights are determined not by hashrate but by token ownership. It therefore follows that the computational barrier is a mechanism of Sybil resistance with respect to consensus but not with respect to governance. The disjuncture between the two levels is structural: protection of consensus from Sybil does not ensure protection of governance from Sybil, because governance rights and consensus rights rest on distinct mechanisms.

When an attempt is made to use hashrate as the basis for governance rights — which was implemented in a number of Bitcoin Improvement Proposal discussions — a symmetric defect emerges: governance influence is concentrated among the largest mining pools,

reproducing the same oligarchic structure as PoS but with the additional dimension of energy expenditure. The energy unsustainability of PoW is not only an ecological problem but also a structural entry barrier: mining with competitive hashrate requires infrastructure and access to cheap electricity, which on a global scale means geographic concentration of mining in jurisdictions with specific energy conditions. This is a particular form of the temporal barrier described in T2 of Volume I: geographically and infrastructurally privileged participants obtain a structural advantage not reproducible by new participants without analogous access to resources.

Theorem T15: Decentralization ∧ Sybil_resistance ∧ ¬Plutocracy = ∅

Formulation. It is impossible to simultaneously achieve decentralization within the meaning of axiom A19, reliable Sybil resistance, and the absence of plutocratic consensus. Any solution realizing two of the three requirements structurally violates the third.

Justification. The three vertices of the trilemma are established above. Centralized verification ensures Sybil resistance without plutocracy but violates decentralization (A19). The economic barrier ensures Sybil resistance without a centralized body but generates plutocratic consensus (Regularity 15). The computational barrier ensures Sybil resistance in the consensus space without a permanent trusted body but generates centralization in mining pools (Regularity 22) and does not resolve governance Sybil.

Proof by exhaustion. Let system S purport to simultaneously realize all three requirements: D (decentralization), SR (Sybil resistance), NP (absence of plutocracy). Sybil resistance requires verification of the uniqueness of subjects. Verification of uniqueness is realizable through: (a) a trusted centralized body — which violates D; (b) an economic barrier — which violates NP through Regularity 15; (c) a computational barrier — which violates D through Regularity 22 in the long run, or violates NP through governance not bound to hashrate. No fourth variant exists in the space of known mechanisms. It therefore follows that SR ∧ D ∧ NP = ∅ in the space of realizable mechanisms.

A qualification must be entered regarding the status of this theorem: it is a theorem about the space of known mechanisms, not an absolute theorem about all conceivable mechanisms. The possibility of a fundamentally new mechanism of Sybil resistance not falling within any of the three categories is not logically precluded. However, no such mechanism was proposed within the framework of blockchain ideology over the period 2008–2026. T15 is a theorem about the structural sufficiency of existing solutions, not an absolute proof of impossibility.

Connection to Volume I: T15 is a new contradiction specific to blockchain and not present in the analysis of digital capital in Volume I. Digital capital does not have a Sybil problem in the same sense: platforms employ centralized identification — real name, email, phone — as a standard verification mechanism while not declaring decentralization. Blockchain creates the Sybil problem precisely through the attempt to realize A19: the elimination of a trusted center eliminates the standard mechanism for verifying uniqueness. T15 is accordingly a theorem about the price of declared decentralization: it generates an irremediable Sybil vulnerability as a structural consequence.

Connection to Volume III: principle P6 (verifiable census) and principle P13 (Digital Census v2) together realize an honest acknowledgment of T15 through a constitutionally accountable form that is neither naive decentralization nor a reproduction of the biometric centralization of Worldcoin. The Virtublic solution is fundamentally distinct from all three vertices of the trilemma on the following ground.

Digital Census v2 uses zk-proof for uniqueness verification: local verification on the subject's device, the proof is transmitted to the system, and personal data remain on the device. This extirpates the permanent centralized biometric database. However, for cases of anomalies — identities flagged as Sybil by statistical indicators — the Dual Suspicion Protocol transfers the decision to the Civic Guard: a panel of civilian juror-auditors randomly selected from active network nodes through VRF. The Civic Guard is temporary and rotational: each panel exists for a specific Census cycle, takes a constitutional oath on-chain, bears verifiable accountability for its decisions, and is replaced by the next panel through VRF. This is fundamentally distinct from the Worldcoin Foundation: there is no permanent body with accumulated authority, no biometric database, and no subject with an economic incentive to expand its own powers.

The political significance of this solution is as follows. Virtublic does not declare full decentralization within the meaning of A19 — it honestly acknowledges that the verification of the uniqueness of human subjects requires an element of human judgment not reducible to an algorithm. The Civic Guard is this element — but constitutionally bounded, temporary, rotational, and accountable. This is not a compromise with centralization but a constitutional acknowledgment that the verification of subjecthood is a political act, not a technical one, and that it requires a political form — a jury — rather than a technical form — a permanent biometric body.

Structural consequences of T15 for blockchain ideology

T15 reveals that axiom A19 (decentralization as a sufficient condition) is incompatible with the requirement of Sybil resistance in systems with equal participation. This means: if a blockchain system purports to realize equal rights of participation — one person, one vote or any form of equal weight voting — it cannot achieve reliable Sybil resistance without violating A19. It therefore follows that blockchain ideology confronts a choice among three strategically incompatible positions.

The first position: abandonment of the claim to equal participation, acceptance of token voting (one token, one vote). This constitutes an honest acknowledgment of the plutocratic nature of the system but contradicts the declared objectives of democratic self-governance. The majority of DAOs in fact occupy this position without openly acknowledging it.

The second position: acceptance of centralized verification as a necessary element, while declaring minimization of centralization through technical means — zk-proof, biometric hashing. Worldcoin occupies this position. It is more candid than the first but generates a permanent centralized body with accumulated authority and creates irreversible privacy risks through a permanent biometric identifier.

The third position: abandonment of Sybil resistance as a requirement, restriction of governance mechanisms to those that do not require verification of uniqueness — for

example, pure token voting without pretension to democraticness. This is a reduction to the first position with explicit abandonment of democratic pretensions.

None of the three positions resolves the trilemma. This constitutes evidence that the trilemma is structural rather than technical: it follows from the incompatibility of A19 with the requirement for verification of the uniqueness of physical subjects, and this incompatibility is not extirpated by technical improvements within the same ideological framework.

This conclusion completes the formation of the epistemological layer of Volume II. Chapters 9, 10, and 11 together established: "code is law" without NA0 generates optimization without subjecthood (Chapter 9), DAO token voting reproduces the sovereignty disjuncture through voter apathy and the oligarchy of activists (Chapter 10), and Sybil resistance in decentralized systems requires a compromise not resolvable within the framework of blockchain ideology (Chapter 11). These three analytical results in their totality justify the structural Regularities 23–27, which will be formally introduced in Chapter 12.

Chapter Summary

The following has been deconstructed: the thesis concerning the possibility of decentralized Sybil resistance without plutocracy (T15 proves the structural trilemma: decentralization, Sybil resistance, and the absence of plutocracy are simultaneously incompatible); the thesis concerning biometric verification as a sufficient technical solution (analysis of Worldcoin demonstrates the reproduction of centralization through the Foundation and the irreversible privacy risks of a permanent biometric identifier); the thesis concerning the social graph as a decentralized proof-of-personhood (BrightID generates exclusion through the social marginality of subjects outside existing networks). Proved: blockchain ideology contains no mechanism of Sybil resistance that simultaneously satisfies the requirements of decentralization, equal participation, and protection against fictitious identities. This is a structural, not an implementation, defect.

Transition to Chapter 12

Chapters 9–11 have exhausted the epistemological analysis of the three central claims of blockchain: "code is law," governance through DAO, and Sybil resistance. Chapter 12 proceeds to the formal introduction of the structural regularities of blockchain epistemology (23–27), which summarize the analytics of Part III in the form of formally rigorous regularities necessary for the subsequent proof of theorems T11–T17 in Part IV.

Chapter 12. Structural regularities of the epistemology of the blockchain

The epistemological layer of Volume II performs the same function as the epistemological layer of Volume I: to demonstrate how the system reproduces its own legitimacy without possessing an external democratic foundation for it. If in Volume I this mechanism was described through axioms ΣA13–ΣA18 and Regularities 10–13, then in Volume II the analogous task is resolved as applied to the blockchain: it is necessary to establish how code is law, DAO governance, and Sybil resistance collectively produce the appearance of legitimacy in the structural absence of its foundations. Chapters 9–11 produced the

analytical material for this derivation. Chapter 12 crystallizes it into five regularities that summarize the epistemology of the blockchain as a completed analytical structure.

Regularity 23. Code bugs as governance crisis

Regularity 23 is derived from axiom ΣA31 (code is law as the principle of automatic smart contract execution) and axiom ΣA32 (irreversibility without correction). Its content is as follows: a vulnerability in a smart contract deployed on the blockchain is not a technical incident resolvable through standard error-correction procedures, but a governance crisis requiring the achievement of consensus on the violation of the principle of code is law.

The mechanism unfolds as follows. A smart contract is deployed on the blockchain as immutable code: axiom ΣA32 declares that the transaction history is unalterable and that the contract is executed in exact accordance with the code. If the code contains a vulnerability — logical, arithmetic, or architectural — the exploitation of that vulnerability is the technically correct execution of the code. This is not a paradox — it is the direct consequence of the principle of code is law: everything the code permits is legitimate within the architecture of the blockchain. An attacker who exploits a reentrancy vulnerability does not violate the rules of the blockchain — he uses them with maximal precision.

When such exploitation produces significant financial losses for participants in the system, the community confronts a choice that is not technical: is the correct execution of defective code a legitimate outcome, or does the priority of the developers' intention and the protection of affected users require the violation of the principle of immutability through a hard fork? This is a political choice in the full sense of the word — a choice between competing normative positions — but it is produced within a system that declares the absence of politics through its substitution by code.

The most documented case is The DAO hack of 2016. The attacker used a reentrancy vulnerability in the smart contract of The DAO — at that time the largest decentralized fund on Ethereum — to extract approximately 3.6 million ETH (approximately $50 million at the then-prevailing exchange rate). The operation was technically correct: the code permitted repeated invocation of the withdrawal function prior to the updating of the balance. The Ethereum community faced a choice: recognize the result as legitimate (code is law) or conduct a hard fork for the return of funds (priority of intention and justice). Consensus on this question was not achieved: the majority of the community supported the hard fork, a minority refused. The result was the division of the network into Ethereum and Ethereum Classic — two independent blockchains with an incompatible transaction history following the point of divergence.

This case has several analytically significant consequences for Regularity 23. First: the principle of code is law is not absolute, but conditional. It is applied up to the point at which the community proves incapable of accepting its consequences — and at this point a political decision concerning the hard fork is produced, violating immutability. The declared principle is nullified by the concrete community when the stakes are sufficiently high. This means that code is law is not a constitutional norm, but an operational rule that operates until a political crisis.

Second consequence: a hard fork as the resolution of a governance crisis produces fragmentation of the network — that is, the forfeiture of the network effects that are the principal source of the blockchain's value. Fragmentation is not merely a technical problem — it is evidence that the community does not possess a mechanism for achieving consensus on normative questions analogous to the mechanism for achieving technical consensus through the protocol. Technical consensus is automated through Byzantine fault tolerance. Normative consensus — concerning justice, intention, and the rights of the affected — is not automatable through code and requires political institutions that blockchain ideology rejects.

Third consequence: following the hard fork, both blockchains continue to exist as competing narratives concerning the rightful history of the network. Ethereum presents the hard fork as the restoration of justice. Ethereum Classic presents the refusal of the hard fork as fidelity to the principle of code is law. This is an epistemological rupture irresolvable through technical means: two communities possess incompatible normative positions and two incompatible transaction histories. The blockchain, which declared the creation of a single indisputable truth, produced two competing narratives about truth.

Regularity 23 in analytical synthesis: a code vulnerability in a system founded on the principle of code is law is not a technical incident, but a normative crisis revealing the system's absence of a constitutional mechanism for resolving the conflict between formal rule and normative justice. This is the structural consequence of ΣA31 and ΣA32 in their conjunction: immutability protects the history from arbitrary modification, but renders legitimate correction through the system's internal mechanisms impossible.

Connection to Volume III: principle P18 (Conflict-Resolution Core) addresses Regularity 23 through four formally defined types of conflicts, including Sovereignty conflict. In the case of a technical conflict — differing interpretations of the protocol — the Formal Verification Protocol in Coq produces automatic proof. In the case of a semantic conflict — differing interpretations of the intent of a rule — the system refers to the historical patterns of the sovereign's votes. In the case of a fundamental conflict of values — the analogue of The DAO hack — a referendum through EQU⊥ is activated. Principle P9 (Constitutional Convention) with the conditions of Axiom-Break (P8) provides a legitimate mechanism for the revision of foundations during a systemic crisis: a hard fork in Virtublic is impossible without a constitutionally defined procedure that requires the achievement of a verifiable supermajority, not the splitting of the community along a normative fault line.

Regularity 24. Governance by active minority

Regularity 24 is derived from axiom ΣA34 (DAO as governance without legitimacy). Its formal content: at ordinary turnout below 10% in DAO governance, decisions are adopted by an active minority of 5–10% of holders, which is not democracy in any formally rigorous sense, but is the oligarchy of activists.

Chapter 10 produced a detailed analysis of voter apathy as a structural regularity. The task of the present section is to register Regularity 24 as a formal derivation from this analysis and to establish its precise place in the epistemology of the blockchain: not as an observation about the behavior of particular participants, but as a structural property of the architecture of token voting.

Governance by active minority is a regularity and not an anomaly on the following grounds. The architecture of token voting contains no mechanism ensuring broad participation: participation is voluntary, the cost of participation is non-zero, and the expected influence of a small holder tends to zero. Under these conditions, the rational holder with a small share is structurally disposed toward non-participation. It therefore follows that the active minority is not an incidental deviation from the norm of broad participation — it is the predictable equilibrium state of the system under the given institutional parameters.

The term "oligarchy of activists" requires precise definition to preclude ambiguity. Oligarchy — the power of the few — in this context is a de facto, not a juridical, description: juridically every holder possesses the right to vote. Activists — subjects who participate systematically in governance — constitute a particular subset of holders, distinguished by three parameters: a sufficient share for participation to be economically rational; informational resources for the evaluation of proposals; and motivation not confined to speculative interest in the token price. The intersection of these three characteristics produces a small group that de facto determines governance outcomes in the context of the mass passivity of the remaining holders.

The epistemological significance of Regularity 24 consists in the following. The DAO system produces a narrative about its own legitimacy through the declaration of openness: anyone can participate, governance is transparent, proposals are public. This narrative is formally correct — the possibility of participation is genuinely open. However, it conceals the structural regularity whereby openness is formal while being de facto closed: governance is determined by those for whom participation is economically rational, that is, large holders. The declared openness functions as a legitimation resource without altering the de facto structure of power. This is the precise blockchain analogue of the mechanism described in ΣA14 of Volume I (the axiom of the consensus surrogate): virality and reach have become surrogates for truth in the digital public sphere. In the DAO: declared openness has become a surrogate for democratic legitimacy in governance.

Connection to Volume III: principle P4 (Dual Sovereignty) resolves Regularity 24 through the constitutional entrenchment of EQU⊥ as a soulbound identity, not proportional to the token share. This extirpates the rational passivity of the small holder in the political dimension: his influence through EQU⊥ is fixed and equal to the influence of any other citizen regardless of his economic position. The cost of participation remains non-zero — this is an ineliminable property of any governance — but the expected influence of a single vote does not tend to zero, since EQU⊥ does not compete with the concentrated positions of large holders. Principle P10 (Madison Mode) further reduces the incentives for the concentration of influence through the quadratic cost of additional votes.

Regularity 25. The Sybil resistance trilemma

Regularity 25 is derived from axioms ΣA35 (Sybil attack as a structural problem) and ΣA36 (proof-of-personhood and its limits). Its content is the direct consequence of the analysis conducted in Chapter 11 and may be formulated as follows: it is impossible simultaneously to achieve decentralization in the sense of A19, reliable Sybil resistance, and the absence of plutocratic consensus. Any solution satisfying two of the three requirements structurally violates the third.

The necessity of a separate formalization of this derivation as Regularity 25 — notwithstanding the fact that the analysis was conducted in Chapter 11 — is determined by the following. Theorem T15 is the formal proof of the trilemma as applied to specific known mechanisms. Regularity 25 is the structural regularity of the epistemological layer: it registers that the trilemma is not a technical problem awaiting an engineering solution, but an epistemological property of a system that produces a narrative about decentralized equality of participation.

The epistemological significance of Regularity 25 consists in the following. Blockchain ideology declares simultaneously: decentralization (A19), equality of participation (one person, one vote or its equivalents), and the absence of plutocratic capture. Regularity 25 establishes that all three declarations cannot be true simultaneously — not because a particular implementation is imperfect, but because they are logically incompatible under any known mechanism of Sybil resistance. It therefore follows that a narrative declaring all three properties simultaneously is a narrative that produces a false consensus about the nature of the system. This is the blockchain analogue of Regularity 10 of Volume I (algorithmic consensus is structurally distinct from democratic consensus): DAO governance is structurally distinct from democratic governance — not only in the sense of procedures, but in the sense of basic capabilities.

Regularity 25 in the epistemological layer functions as a constraint on assertions: any assertion about a DAO that simultaneously declares decentralization, equal participation, and Sybil resistance is an assertion that is structurally inconsistent with realizable mechanisms. This constraint is not a normative judgment, but an analytical result.

Connection to Volume III: Virtublic openly acknowledges Regularity 25 through a constitutional solution that does not declare full decentralization. The civic watch in Digital Census v2 (P13) is an element of human judgment necessary for the verification of the uniqueness of subjects — and this is constitutionally acknowledged through principle P6. Virtublic does not attempt to resolve the trilemma through a technical mechanism that does not extirpate it, but constitutionally defines the form of the compromise: a temporary, rotating, accountable collegium of citizens is the institutionally acceptable form of the element of centralization necessary for Sybil resistance.

Regularity 26. Anonymity without accountability

Regularity 26 is derived from axiom A25 (anonymity as a property of the blockchain subject) and axiom ΣA31 (code is law). Its formal content: the combination of code is law with the anonymity of the subject produces the impossibility of legal accountability for actions within the system. Formal expression: Privacy ↑ → Accountability ↓, which is the direct consequence of the structural incompatibility of A25 with the requirement of prosecution in the event of a legal violation.

The mechanism of Regularity 26 unfolds through the following causal chain. A smart contract is executed automatically upon the satisfaction of the code's conditions. An attacker, identified only through a private key (A25), exploits a contract vulnerability. Code is law (ΣA31) means that the exploitation is a technically legitimate operation within the protocol. The attacker transfers the extracted funds through a chain of transactions, using mixers or privacy coins to sever the on-chain trail. The identification of the physical person behind the

attacking address is the task of blockchain forensic analysis, which does not guarantee a result at a sufficient level of anonymization. It therefore follows that prosecution is structurally impeded or impossible when the attacker is anonymous.

Empirical cases verify this regularity. The DAO hack of 2016: the attacker is anonymous; the community could not prosecute a physical person; the sole available response was a hard fork (the extirpation of the vulnerability through the violation of immutability, not the prosecution of the violator). The Ronin bridge hack of 2022: approximately $600 million was stolen from the Axie Infinity bridge; the attack was attributed to Lazarus Group — a state structure of the DPRK — through subsequent on-chain analysis, but prosecution proved impossible in the jurisdictional sense. The Poly Network hack of 2021: $611 million was stolen; the funds were subsequently returned by the attacker voluntarily — which is not a legal outcome, but an incidental result dependent on the motivation of a particular actor, not on the existence of an accountability mechanism.

Regularity 26 has a fundamental consequence for normative analysis. The absence of an accountability mechanism in a system that produces significant financial and political consequences for participants is not a neutral property, but a normative defect following from NA0 of Volume I. If subjecthood is a politically protected good (NA0), then a system that structurally deprives the subject of the possibility of demanding accountability for inflicted harm produces the destruction of subjecthood through the extirpation of one of its necessary conditions — legal protection.

It is necessary to register the precise relation between Regularity 26 and theorem T13 (anonymity destroys accountability), which will be formally demonstrated in Part IV. Regularity 26 is a structural observation about a property of the system. T13 is a theorem demonstrating that this property is structurally ineliminable while A25 is preserved. The relation between regularity and theorem here is the same as in Volume I: the regularity registers the pattern; the theorem demonstrates its necessity.

Simultaneously, it is necessary to register that Regularity 26 does not mean the denial of the value of privacy as such. The right to unpredictability (N1, Volume I) is normatively justified — the subject possesses the right to protection from surveillance. The problem consists not in the fact that privacy is of no value, but in the fact that its realization through complete anonymity without an accountability mechanism produces the structural impossibility of legal protection for affected subjects. Regularity 26 registers this contradiction as structural — not as an incidental balance of competing values, but as the consequence of specific architectural choices.

Connection to Volume III: principle P3 (Soulbound Identity) and principle P14 (zk-proof + Proof-of-Offline) jointly resolve Regularity 26 through the constitutional balance between privacy and accountability. Citizens of Virtublic participate through pseudonymous addresses protected by zk-proof — no one can determine how a specific citizen voted. However, Soulbound Identity is verifiable through Digital Census v2: when the establishment of accountability for a specific action is necessary, there exists a constitutionally defined procedure requiring a decision by P18 (Conflict-Resolution Core) and a qualified majority through EQU⊥. This is a constitutionally regulated balance, not a structural contradiction:

privacy operates as the default; accountability operates as a constitutionally defined exception.

Regularity 27. The blockchain as an insufficient form

Regularity 27 is derived from the conjunction of all preceding regularities of the epistemological layer (23–26) and is their synthetic result. Its formulation: the blockchain resolves the technical problems of Byzantine fault tolerance and double spending, but does not resolve the political problems of legitimacy, accountability, and justice. It therefore follows that the blockchain is necessary as a technological substrate, but insufficient as an institutional form.

Two elements of this regularity require separate analysis: the thesis concerning technical sufficiency and the thesis concerning institutional insufficiency.

The thesis concerning technical sufficiency is correct and is confirmed both by theoretical analysis and by empirical data for the period 2008–2026. Byzantine fault tolerance — the capacity of a distributed system to achieve consensus in the presence of incorrectly operating nodes — is realized in Bitcoin and Ethereum with sufficient reliability: neither of these networks has been subjected to a successful 51%-attack under the conditions of their current scale. Double spending — the problem of the repeated expenditure of the same digital asset — has been resolved through the cryptographically verifiable transaction history. These technical problems existed prior to the blockchain and were not resolved through other mechanisms with comparable effectiveness. The blockchain as a technological substrate is a necessary component of any system claiming decentralized administration of digital assets.

The thesis concerning institutional insufficiency is the central conclusion of Part III and is summarized as follows. Regularity 23 demonstrated: a technical crisis (code bug) produces a political crisis (governance crisis) that the system cannot resolve without violating its own principles. Regularity 24 demonstrated: governance by active minority is the structural equilibrium state of token voting, ineliminable through technical improvements. Regularity 25 demonstrated: the Sybil resistance trilemma is irresolvable within the space of known mechanisms under the simultaneous requirement of decentralization and the absence of plutocracy. Regularity 26 demonstrated: anonymity without accountability is the structural consequence of the architectural choices A25 + ΣA31, incompatible with the normative protection of subjecthood.

The conjunction of Regularities 23–26 produces the sole possible derivation: political problems — legitimacy, accountability, justice — are not technical problems and are not resolved through technical means. Legitimacy requires an external democratic foundation — popular sovereignty — which is not produced through code. Accountability requires a mechanism of legal responsibility, which is not produced through anonymity. Justice requires a normative axiom (NA0, Volume I), which is not derivable from an optimization algorithm.

The blockchain as ideology consistently presupposed that technical solutions are sufficient for political problems. This presupposition is the operational definition of technological solutionism — a concept introduced by Morozov, although, as Regularity 18 demonstrated, his own critique of this solutionism proved to be a part of the same structure that it critiqued.

Regularity 27 is the formal refutation of technological solutionism as applied to the blockchain: not through a normative judgment about the undesirability of such an approach, but through the exhaustive structural analysis of which problems it resolves and which it does not.

Connection to Volume I: Regularity 27 is the blockchain analogue of theorem T3 of Volume I (structural absence of correction). T3 asserted: the system of digital capital contains no internal mechanism for the correction of concentration. Regularity 27 asserts: the system of the blockchain contains no internal mechanisms for resolving the political problems of legitimacy, accountability, and justice. In both cases the derivation is identical: an institutional response external to the logic of the system is required.

Connection to Volume III: theorem T17 (the constitutional necessity of the blockchain) is the formal theoretical derivation from Regularity 27. If the blockchain is necessary as a technology but insufficient as an institutional form, then an institutional form that employs the blockchain as a technological substrate while adding constitutional architecture is not an arbitrary choice, but a structurally necessary solution. Virtublic = blockchain technology (zk-proof, smart contracts, formal verification, cryptography) + constitutional architecture (P0–P18, popular sovereignty, dual sovereignty, normative axiom in code). This is the resolution of Regularity 27 not through the negation of the blockchain, but through its constitutional embedding in a form that produces the missing elements.

Analytical synthesis of Chapter 12

The five regularities (23–27) jointly describe the epistemology of the blockchain as a system that produces a narrative about its own legitimacy through three declarations: technical sufficiency (code resolves problems), institutional neutrality (no power, only rules), and democratic openness (anyone can participate). Each of these declarations contains a formally correct element that renders the narrative plausible. Regularity 23 demonstrates: the technical sufficiency of code is insufficient in normative crises. Regularities 24 and 25 demonstrate: institutional neutrality is a narrative concealing the oligarchy of activists and the Sybil trilemma. Regularity 26 demonstrates: democratic openness does not ensure accountability when subjects are anonymous. Regularity 27 summarizes: the blockchain is technologically necessary and institutionally insufficient.

The conjunction of Regularities 23–27 completes the epistemological layer of Volume II and creates the complete justification for Part IV, in which the regularities of the three analytical layers (ontological, anthropological, epistemological) will be crystallized into seven formal theorems (T11–T17).

Chapter Summary

The following has been deconstructed: the thesis concerning the resolvability of normative crises through technical means (Regularity 23 demonstrates that a code bug produces a governance crisis irresolvable without the violation of the principle of code is law); the thesis concerning the democratic nature of the DAO (Regularity 24 demonstrates the oligarchy of activists as a structural equilibrium); the thesis concerning the technical resolvability of the Sybil trilemma (Regularity 25 demonstrates its structural character); the thesis concerning the compatibility of privacy and accountability (Regularity 26 demonstrates their structural

incompatibility under A25 + ΣA31); the thesis concerning the blockchain as a sufficient institutional form (Regularity 27 demonstrates its technical sufficiency concurrent with institutional insufficiency). Demonstrated: the blockchain produces a narrative about its own legitimacy through declarations each of which contains a structural defect revealed upon analytical exhaustion.

Transition to Part IV

The three analytical layers — ontology (Chapters 1–3), anthropology (Chapters 4–8), epistemology (Chapters 9–12) — have produced the complete diagnosis of the blockchain as an institutional form. Part IV proceeds to the formal demonstration of seven theorems (T11–T17) crystallizing this diagnosis into logically rigorous conclusions. Each theorem is demonstrated by the method of exhaustion through the axioms and regularities introduced in Parts I–III, and identifies the specific principle of Volume III that resolves the corresponding contradiction.

Δ5 — CRISIS: THE LIMIT OF THE IDEOLOGY OF DECENTRALIZATION

The epistemological layer of Volume II is exhausted. Chapters 9–12 demonstrated: the blockchain reproduces its own legitimacy through narratives that structurally contain a defect upon analytical exhaustion.

Code is law without a normative axiom optimizes efficiency without protecting subjecthood (Chapter 9). Governance through the DAO reproduces the sovereignty rupture of T8 through voter apathy and the oligarchy of activists (Chapter 10). Sybil resistance requires a compromise irresolvable within the framework of the declared decentralization (Chapter 11). Five regularities (23–27) summarize these results: the blockchain is technologically necessary and institutionally insufficient (Regularity 27).

Δ5 registers the limit of the ideology of decentralization as an analytical program. The ideology declared: the extirpation of centralized control is the sufficient condition for the emergence of equal self-governance. The three analytical layers refuted this declaration through the exhaustive analysis of the structural consequences of its realization. Decentralization produces concentration in staking pools (Regularity 22). The absence of a normative axiom produces the exploitation of subjects by smart contracts (Chapter 9). Token voting produces the oligarchy of activists, not democracy (Regularity 24). Sybil resistance requires centralization, reproducing that from which the ideology fled (Regularity 25). Anonymity produces the impossibility of accountability (Regularity 26).

Δ5 thereby formulates the requirement upon Part IV: not an additional analytical layer, but the formal demonstration of theorems T11–T17 summarizing the diagnosis in a logically rigorous form suitable for the subsequent construction of the constitutional answer in Volume III.

PART IV. CONTRADICTIONS AND FAILURES

Parts I–III produced a complete analytical diagnosis of blockchain across three layers: the ontological (what blockchain is as a structure), the anthropological (who bears the consequences of this structure), and the epistemological (how the structure reproduces its own legitimacy). The five regularities of the epistemological layer (23–27) concluded the diagnosis with the formulation of Regularity 27: blockchain is technologically necessary and institutionally insufficient. Part IV proceeds from diagnosis to proof: each contradiction identified in Parts I–III is formalized as a theorem with a precise structure — formulation, justification, proof, empirical verification, connection with Volumes I and III. Theorems T11–T17 do not generate new analytical observations — they crystallize observations already produced into a logically rigorous form suitable for subsequent constructive application in Volume III.

Chapter 13. The plutocracy of proof-of-stake

T11. Theorem of the plutocratic inevitability of PoS

Formulation. Under proof-of-stake consensus, the system inevitably concentrates in the hands of early token holders. This does not resolve the temporal barrier established by theorem T2 of Volume I — it relocates it to the level of tokenomic architecture.

Justification

T11 is derived from the conjunction of three analytical results produced in Parts I–III of the present volume: Regularity 15 (plutocratic consensus), Regularity 21 (concentration through staking), and Regularity 22 (centralization through staking pools). Each of these is a necessary but individually insufficient condition of the theorem — their joint operation generates the inevitability that T11 formalizes.

The connection with T2 of Volume I is determinative for understanding the theorem. T2 asserted: "past the point of no return, competition within a homogeneous modal layer is structurally impossible without external intervention." The temporal barrier in the model of digital capital was generated through the early history of data: the platform that first accumulated a sufficient volume of user behavioral data acquired predictive power not reproducible by a competitor within the same modal layer without an equivalent history. T11 asserts that proof-of-stake reproduces the identical mechanism with a substitution of substrate: the early history of data is replaced by the early accumulation of tokens. The mechanism of temporal advantage remains isomorphic; what changes is solely the resource through which this advantage is instantiated.

The axioms upon which the proof is constructed were introduced in Part I of the present volume: A20 (consensus mechanisms — proof-of-stake rewards are proportional to stake), A22 (the token as universal equivalent), A23 (liquidity as the fundamental property of the token), A30 (staking as economic participation). The conjunction of these axioms describes an architecture in which participation in validation and in governance is determined by token ownership, and reward for participation is paid in those same tokens. From this architecture,

the conclusion of concentration follows with logical necessity, requiring no additional empirical assumptions.

Proof

The proof is constructed through the sequential establishment of six logical steps, each of which is a necessary link in the causal chain.

The first step. Proof-of-stake rewards are proportional to stake (Regularity 21, axiom A20). This is an architectural choice, not an incidental property: proportionality provides the economic incentive for participation in validation and simultaneously generates a structural barrier against participants with a small share. At staking reward rate $r \neq 0$, the increment of position over period t is: $\Delta\text{Wealth}(t) = \text{Wealth}(t) \times r$. Consequently, the absolute increment is proportional to the initial position: the larger staker receives a greater absolute reward over the same period of time at an identical reward rate.

The second step. Early holders acquired tokens at prices not reproducible by late participants. This is a direct consequence of the temporal structure of token distribution at the launch of any PoS protocol. An ICO (Initial Coin Offering) places tokens at a price established prior to the formation of market demand — consequently, at a price below the equilibrium price that forms after launch. An airdrop transfers tokens at no cost to certain categories of early participants. Early mining in hybrid systems enables token acquisition through computational resources prior to the formation of a competitive mining market. Not one of these channels is accessible after the moment of launch at the same scale: after the formation of a liquid market, tokens are acquired at market price, which upon the protocol's success systematically exceeds the early placement price. The price advantage of early holders is not incidental but is the structurally necessary consequence of the temporal sequence of events at the launch of any protocol with limited issuance.

The third step. The compound interest effect generates an increasing gap between large and small positions. Formal expression: $\text{Wealth}(t+1) = \text{Wealth}(t) \times (1 + r)$. At constant r, this is a geometric progression with base $(1 + r)$. The gap between two positions $W_1 > W_2$ after n periods: $\text{Gap}(n) = W_1(1 + r)^n - W_2(1 + r)^n = (W_1 - W_2)(1 + r)^n$. The gap grows exponentially at any $r > 0$. This mathematical result is the consequence not of the malicious intent of specific actors but of the architectural choice of proportional reward — a choice logically necessary for securing validator incentives in PoS.

The fourth step. Governance control in proof-of-stake systems is proportional to stake. This follows from axiom ΣA34 (the DAO as governance without legitimacy) in conjunction with the architecture of token voting: each token provides one vote, the number of votes is proportional to the number of tokens, and influence over governance outcomes is determined by the share of tokens relative to total supply. Consequently, the growth of position through staking rewards automatically generates the growth of governance influence without any additional action by holders: the compound interest effect operating in the economic dimension produces an analogous effect in the political dimension through the mechanism of token voting.

The fifth step. The conjunction of steps 1–4 generates the following structure: early holders with large positions accumulate stake through compound interest (steps 1–3), which

produces an increasing gap relative to late participants. This gap is simultaneously economic (the gap in position value) and political (the gap in governance influence). Since governance decisions optimize token price (Regularity 19) rather than user welfare, early large holders adopt decisions in a direction that further reinforces their own position. This is a self-augmenting cycle: Stake → Governance control → Governance decisions favouring token price → ↑Token price → ↑Relative value of stake → ↑Governance control. The cycle is closed without an internal point of saturation — this is the precise blockchain analogue of axiom A6 of Volume I (self-augmentation without saturation).

The sixth step. Concentration through staking pools (Regularity 22) intensifies the mechanism described: small holders who do not reach the minimum barrier for independent validation delegate stake to centralized pools. Large pools accumulate staking rewards, retain a commission, and vote in governance on behalf of the accumulated position. This generates an additional level of concentration: governance influence is concentrated not only among early holders with large individual positions but also among staking pool operators who accumulate the voting rights of a delegated mass of tokens.

From the six steps the following conclusion obtains: the system inevitably concentrates in the hands of early holders and operators of large staking pools. This concentration is not an artifact of a failed implementation but the structural consequence of architectural axioms A20, A23, A30, and ΣA34 in their conjunction. Modification of individual parameters (reward rate, minimum stake) slows or accelerates the dynamics but does not alter the direction — at any non-zero values of these parameters, concentration is a monotonically increasing function of time.

Formal expression

$$\text{Gini\_coefficient}(t+1) \geq \text{Gini\_coefficient}(t).$$

This expression establishes the direction of change of the inequality of token distribution over time at any non-zero staking reward rate. The Gini coefficient is the standard measure of distributional inequality: at 0, absolute equality; at 1, absolute inequality. The assertion of the monotonic increase of Gini_coefficient means that the inequality of the distribution of governance influence in a PoS system does not decrease over time while the architectural parameters of the system are preserved.

It is necessary to establish the precise meaning of this formal expression. It is not a strict proof through formal mathematics but a structural assertion about the direction of change. Empirical data verify this assertion for the period 2015–2026 with respect to Ethereum and analogous PoS systems: the coefficient of inequality in ETH distribution exhibited no sustained downward tendency in any of the periods under examination. This is a necessary but not sufficient condition for the verification of T11: the theorem asserts structural necessity, not exclusively an empirical regularity.

Empirical verification

Data for Ethereum over the period 2023–2026 show the following. The top 100 addresses control more than 40% of the total ETH supply. This includes both institutional holders (Ethereum Foundation, large investment funds, early contributors) and custodial addresses

of centralized exchanges and staking pools. If custodial addresses representing the aggregated positions of multiple individual holders are excluded, the concentration in the hands of genuinely autonomous subjects proves even higher.

For Bitcoin, the data are yet more indicative for purposes of verifying T11, though Bitcoin is not a proof-of-stake system. The top 2% of addresses control approximately 95% of BTC supply. This is a consequence of Bitcoin's early epoch, when mining was accessible on ordinary consumer hardware — which constitutes in pure form a verification of the temporal barrier T2: early participants acquired the asset at zero or minimal cost, late participants pay the market price. PoS reproduces the same structure with the substitution of the computational barrier by a financial one.

With respect to governance rather than simple token distribution: analysis of on-chain data for Uniswap, MakerDAO, and Compound over the period 2020–2024 shows that in each of these protocols the top 10 addresses by volume of governance tokens controlled more than 50% of effective voting power accounting for delegation. This means that governance outcomes were de facto determined by ten subjects in each case — with formally open participation available to millions of holders.

The Ethereum Foundation and affiliated early contributors controlled, at the time of The Merge (Ethereum's transition to PoS in 2022), a share of ETH sufficient to determine the outcome of any on-chain vote at typical turnout. This is not an accusation of intentional manipulation — it is a verification of the structural assertion of T11: a PoS system launched under an existing token distribution inherits that distribution as its initial condition and contains no internal mechanisms for its correction.

Connection with Volume I

T11 is the direct continuation of T2 (the theorem of the temporal barrier) in the blockchain substrate. T2 asserted that the early history of data generates predictive power not reproducible by a competitor without an analogous history. T11 asserts that the early accumulation of tokens generates governance power not reproducible by late participants without an analogous ownership history. In both cases, the structural mechanism is identical: temporal advantage crystallizes into a resource (predictive data / tokens) that self-augments through a mechanism that has no internal point of correction.

Additionally, T11 reproduces T1 (the theorem of surplus attention) in a modified form. T1 described the asymmetry between the predictive value generated by the subject through the alienation of attention and the subject's zero compensation. T11 describes the asymmetry between the governance influence generated by users through protocol utilization (liquidity generation, fee generation, network effects) and the absence of commensurate governance rights for users who are not holders. The structure of the asymmetry is isomorphic: value is generated by one set of subjects and extracted by another — the mechanism differs (attention-tokens versus protocol usage), yet the asymmetry of appropriation is preserved.

Connection with Volume III

Virtublic resolves T11 through two constitutional principles in their conjunction. Principle P4 (Dual Sovereignty) is the primary instrument: VIC⊥ (economic sovereignty) and EQU⊥

(political sovereignty) are orthogonal and non-convertible. The symbol ⊥ establishes precisely this property: the two sovereignties exist in non-commingling spaces. Early contributors receive VIC⊥ for their genuine contribution to infrastructure through the Dual Reserve Market (principle P12) — this is the recognition of the economic value of their participation. However, VIC⊥ does not convert into EQU⊥: the accumulation of economic position does not generate the accumulation of political power. The compound interest effect continues to operate in the economic dimension of VIC⊥, yet is constitutionally precluded from the political dimension of EQU⊥.

Principle P3 (Soulbound Identity) secures the technical realization of this separation: EQU⊥ is distributed as a soulbound identity bound to a physical subject through zero-knowledge proof. It is non-transferable, non-delegable, and non-accumulative: each citizen possesses exactly one EQU⊥ irrespective of his economic position, his history of participation, and his volume of VIC⊥. This is the constitutional instantiation of the principle of one person, one vote in a space where token voting systematically violates it.

Principle P16 (Rockefeller Mode) additionally secures that infrastructure operators — including staking pool operators — receive VIC⊥ for genuine contribution to infrastructure yet receive no EQU⊥ and cannot participate in governance through the political dimension. NodeFactory as an institution separates economic participation from political dominance, which in PoS systems are structurally fused through token voting.

The conjunction of P4 + P3 + P16 yields the following result with respect to T11: the structural mechanism of concentration described in the theorem continues to operate in the economic space of VIC⊥ — Virtublic does not liquidate economic inequality and does not declare such a goal. However, it constitutionally blocks the conversion of economic inequality into political dominance. Gini_coefficient(VIC⊥)(t+1) ≥ Gini_coefficient(VIC⊥)(t) remains formally true in Virtublic. Yet Gini_coefficient(EQU⊥) = 0 at any t — since EQU⊥ is distributed in absolute equality through Soulbound Identity. The separation of these two coefficients is constitutionally protected and cannot be violated without the direct violation of principle P4, which is precluded by the Formal Verification Protocol (principle P2).

Chapter Summary

The following has been proved: T11 (the theorem of the plutocratic inevitability of PoS) is a rigorous consequence of axioms A20, A23, A30, and ΣA34 in their conjunction with Regularities 15, 21, and 22. Blockchain does not resolve the temporal barrier T2 of Volume I — it reproduces it through the substitution of substrate from predictive data to tokenomic position. The compound interest effect generates a monotonically increasing concentration of governance influence among early holders. Empirical data for Ethereum (top 100 addresses — more than 40% of supply) and Bitcoin (top 2% of addresses — 95% of supply) verify the structural assertion of the theorem. Virtublic resolves T11 through the constitutional separation of VIC⊥ and EQU⊥ with the absolute equality of the latter through Soulbound Identity.

Transition to Chapter 14

Where T11 established that economic inequality in PoS systems is structurally converted into political dominance, Chapter 14 proceeds to the analysis of why governance in a DAO is

devoid of an external source of legitimacy — irrespective of whether tokens are evenly or unevenly distributed. T12 (the theorem of the DAO as plutocracy by design) proves that the problem is not exhausted by concentration — it consists in circular legitimation: the power of holders is legitimized through code written by those same holders without a democratic mandate.

Chapter 14. Governance without legitimacy

T12. Theorem of DAO as plutocracy by design

Formulation. Blockchain token voting has no external source of legitimacy. Governance is controlled by capital (one token, one vote), not by citizens (one person, one vote). This does not resolve the sovereignty disjuncture established by theorem T8 of Volume I — but replaces the predictive authority of platforms with the tokenomic authority of holders, reproducing the structure of the disjuncture upon a change of substrate.

Justification

T12 is derived from axiom ΣA34 (DAO as governance without legitimacy), Regularity 17 (liquidity destroys governance), and Regularity 20 (governance capture through the market). Its central concept — circular legitimation — requires precise definition before the proof can be constructed.

Circular legitimation is a structure in which a system justifies its own normative validity through appeal to itself: the rule is legitimate because it is contained in the code; the code is valid because the community accepted it; the community is empowered because it participates through the code. This circle has no external point of reference — there is no source of legitimacy independent of the system. In democratic theory, that external point is popular sovereign authority: power is legitimate because it has been delegated by the people through procedures external to the specific institutions it establishes. In DAO, this point is structurally absent, not absent by virtue of a specific implementation.

T12 is constructed as a formal proof of this structural absence through six sequential steps, each of which is a necessary link in the causal chain leading to the conclusion of circular legitimation.

The connection to T8 of Volume I is fundamental for understanding the theorem within the general analytical architecture of the trilogy. T8 asserted: predictive authority (de facto) and political sovereignty (de jure) move in opposite directions under digital capitalism, and this disjuncture does not self-correct. In the platform capital model, de jure sovereignty was expressed in the subject's formal rights — the right to consent, the right to withdraw data, the right to contest decisions — while de facto authority belonged to the predictive infrastructure that preceded the subject in the subject's own decisions. T12 establishes that DAO reproduces this disjuncture through a substitution of substrate: de jure sovereignty is now expressed in the formal right of each holder to vote, while de facto authority belongs to those who control a sufficient share of governance tokens to determine the outcomes of votes. The form of the disjuncture has changed; its structural nature has not.

Proof

First step. DAO governance is based on token voting (axiom ΣA34). This is an architectural choice that within blockchain ideology required no additional justification: token voting appeared to be the natural consequence of decentralized consensus — if there is no central body, then the rule of decision-making must be expressed in code, and the most technically straightforward implementation is to assign voting rights to tokens. No democratic theory underlies this choice. None of the foundational documents of major DAOs — the Ethereum whitepaper, the Uniswap governance framework, the MakerDAO blue paper — contains a justification of why token voting specifically constitutes a legitimate form of governance. This is the first link in the chain of circular legitimation: the architectural choice is accepted as a given rather than as a decision requiring normative justification.

Second step. Token voting realizes the principle of one token, one vote. This means that governance influence is proportional to the quantity of tokens rather than to the number of physical subjects participating in the system. Political theory recognizes two fundamentally distinct bases for the distribution of governance rights: one person, one vote — democracy grounded in the political equality of subjects as citizens — and one dollar, one vote — plutocracy grounded in the proportionality of influence to capital. Token voting is a realization of the second principle: governance rights are distributed proportionally to capital expressed in tokens. To designate this system "decentralized democracy" constitutes a terminological inaccuracy: decentralization describes an architectural property of the system — the absence of a single center — but not its normative foundation — whose interests, and in what proportion, the system represents. DAO is a decentralized plutocracy, not a decentralized democracy.

Third step. Governance tokens are freely exchangeable on the market (Regularity 17, axiom A23). This property is intentional: the liquidity of tokens is one of the declared advantages of blockchain systems — the capacity to enter and exit a position without the authorization of a central body. However, the liquidity of governance tokens means that governance rights are a purchasable asset. This is fundamentally distinct from political rights in constitutional democracies: the right to vote is not saleable — it belongs to the citizen as a physical subject and cannot be transferred, delegated for payment, or acquired by third parties. In DAO, this constraint is structurally absent: governance rights are purchased on the open market. Consequently, governance is a market asset rather than a constitutional right.

Fourth step. From the third step it immediately follows that governance may be captured through the purchase of tokens on the open market. Formal expression: Capture_cost = Token_price × Tokens_for_majority. Given the known market capitalization of a protocol and the known distribution of tokens, the cost of acquiring a controlling share is computable. This means that governance is vulnerable to hostile acquisition to precisely the same degree that corporate governance is vulnerable to a hostile takeover — with the significant difference that corporate law contains protective instruments (poison pills, supermajority requirements for critical decisions, fiduciary duties of directors), whereas the majority of DAOs contain no analogous constitutional protections, or contain them in a form that reproduces the logic of centralization contradictory to A19. Capture through the market is not a theoretical possibility

but a documented phenomenon, as was demonstrated in the analysis of Beanstalk Farms in Chapter 6.

Fifth step is central to the proof of circular legitimation. Why is one token, one vote a legitimate form of governance? The answer produced by DAO ideology is as follows: because it is written in the smart contract. Why is the smart contract containing this rule valid? Because it is deployed on the blockchain and the community accepted it. Why is the community empowered to make such decisions? Because it is the set of governance token holders who, under the rules of the smart contract, have the right to make decisions. The circle is closed: the legitimacy of the rule is produced through the rule whose legitimacy is produced through the same rule. No external source of legitimacy — popular sovereign authority, a constitutional constituent act, a democratically legitimate founding procedure — exists.

It is of fundamental importance to record that this problem is not a problem of the design of a specific DAO but a structural problem of the concept itself. Any DAO based on token voting reproduces it: democratic legitimacy cannot be obtained through a procedure that is not itself democratically legitimated. This is a precise reproduction of the classical problem of constituent power in constitutional theory: who has the right to adopt a constitution? The answer of traditional constitutional theory — the people through a constituent assembly — is an answer that DAO is structurally incapable of reproducing: the "people" in the DAO sense is the set of governance token holders whose legitimacy is determined by the same code that they institute.

Sixth step. From the five preceding steps the conclusion follows: DAO governance is plutocracy by design in two interrelated senses. By architectural design: token voting is an architectural choice to distribute governance rights proportionally to capital rather than to subjects. By normative design: the absence of an external source of legitimacy is structural rather than incidental — no DAO can obtain democratic legitimacy without an external constituent act grounded in popular sovereign authority, because such an act presupposes the identification and verification of physical citizen-subjects, which requires precisely those mechanisms of Sybil resistance that T15 showed to be incompatible with A19 without compromise.

Formal expression

Legitimacy(DAO) = Code_says_so, not Legitimacy(DAO) = Democratic_mandate.

This expression records the structural distinction between two sources of normative authority. Legitimacy(DAO) = Code_says_so describes a system in which the normative validity of a rule is determined by its content in code. Legitimacy(DAO) = Democratic_mandate describes a system in which the normative validity of a rule is determined by its derivation from a democratically legitimated procedure. These two sources are not interchangeable: technically correct code is not a democratically legitimated rule, and a democratically legitimated rule is not technically optimal code. DAO systematically conflates these two sources, generating a narrative of democratic legitimacy through appeal to the technical execution of code.

The precise analytical function of this expression must be recorded. It is not an assertion that Code_says_so is a useless source of normative authority. In the domain of technical rules — Byzantine fault tolerance, double spending prevention — Code_says_so constitutes a sufficient justification. Regularity 27 (blockchain as an insufficient form) established that blockchain is technologically sufficient. The formal expression of T12 records that its technical sufficiency does not generate political legitimacy: this is a distinction in the substrate of application of normative authority, not its negation in general.

Empirical verification

Uniswap DAO provides a documented case of the first class of circular legitimation. At the launch of Uniswap v3 in 2021, the Uniswap Labs team and affiliated early investors — Andreessen Horowitz, Paradigm, Union Square Ventures — received significant shares of the UNI governance token through the initial distribution and airdrop. On-chain analysis for the period 2021–2024 shows that these subjects collectively controlled a share of UNI sufficient to determine the outcome of the majority of governance proposals at typical turnout below 5–8%. Uniswap governance is de jure open: any UNI holder may submit proposals and vote. De facto governance is determined by the team and early investors — the same subjects who wrote the code defining the rules of governance. This is circular legitimation in its pure form: those who wrote the rules control the vote on those rules, which renders the rules convenient for themselves.

MakerDAO provides a documented case of the second class — capture through the market. In November 2023, a large MKR holder, identifiable only through a blockchain address, accumulated a position sufficient to pass a governance proposal to transfer a significant share of treasury funds. The proposal passed at low turnout among the remaining MKR holders. This is a realization of Regularity 20 in practice: Capture_cost was computable, and the attacker executed the operation in strict conformity with the token voting mechanism. Technically the operation was correct. Normatively — it constituted an undemocratic extraction of funds from the totality of protocol users and small holders without their real participation in the decision.

Compound DAO provides a third documented case — governance paralysis through the conflict of interests of large holders. In 2022–2023, a number of proposals to alter the interest rate model in Compound failed to obtain sufficient quorum despite the evident technical necessity of the changes — because large holders with various positions in the DeFi ecosystem had mutually incompatible incentives and preferred the status quo to the uncertain outcome of changes. Governance paralysis is no less indicative a case of structural defect than governance capture: the system is not only vulnerable to capture but incapable of adopting necessary decisions in the presence of a conflict of interests among large holders.

Connection to Volume I

T12 reproduces T8 (the sovereignty disjuncture) with a precision that permits the establishment of a structural isomorphism rather than merely an analogy. T8 asserted: under digital capitalism, the subject's de jure sovereignty and the platform's de facto predictive authority move in opposite directions — the subject accumulates formal rights while actual autonomy declines. In DAO: de jure governance is open (each holder may vote), while de

facto governance is controlled by capital positions not corresponding to the set of physical participant-subjects. The mechanism of the disjuncture in T8 was predictive asymmetry — the platform knows more about the subject than the subject knows about the platform. The mechanism of the disjuncture in T12 is capital asymmetry — a holder with a large position has structurally greater influence that neutralizes the influence of the multitude of small holders. The form of asymmetry differs; the structure of the de jure / de facto disjuncture is identical.

T12 additionally reproduces the mechanism of T9 of Volume I (constitutional necessity): to precisely the extent that neither market forces nor technical innovations correct the structural contradictions of digital capital, constitutional intervention is necessary. T9 asserted: constitutional architecture is the sole mechanism of correction that does not reproduce the logic of the system it regulates. T12 produces an analogous conclusion for blockchain: DAO governance does not self-correct through market mechanisms — Capture_cost declines during market downturns — is not corrected through technical improvements — improvement of voting mechanisms does not extirpate circular legitimation — and it therefore follows that external constitutional architecture is required.

Connection to Volume III

Virtublic resolves T12 through two principles that in their conjunction extirpate each link of circular legitimation.

Principle P0 (the Preamble) is the response to the central problem of T12 — the absence of an external source of legitimacy. P0 establishes popular sovereign authority as the absolute and inalienable foundation of the constitutional architecture. This is not a declaratory assertion but an operational principle: P0 is the sole principle not subject to alteration even through the Axiom-Break procedure. No economic position, no technical expertise, no accumulation of VIC⊥ may alter P0 — popular sovereign authority precedes all other principles and is their condition rather than their consequence. This structurally distinguishes Virtublic from DAO: in Virtublic the source of legitimacy is external to the code — it is the constitutionally entrenched popular sovereign authority, which the code only realizes technically but does not institute normatively.

Principle P4 (Dual Sovereignty) is the response to the architectural defect of token voting. EQU⊥ — political sovereignty — is distributed as a soulbound identity: one physical subject corresponds to exactly one unit of EQU⊥, independent of the subject's economic position. This realizes the principle of one person, one vote in a domain technically secured by Soulbound Identity (P3) and Digital Census v2 (P13). It therefore follows that Legitimacy(Virtublic) = Democratic_mandate: political decisions are adopted through EQU⊥ distributed by the principle of popular sovereign authority, not through tokens distributed by the principle of capital. Capture_cost as applied to the political governance of Virtublic is fundamentally non-computable: EQU⊥ is non-transferable and has no market value, which extirpates the very mechanism of capture through the market described in the fourth step of the proof of T12.

It must be recorded that Virtublic preserves VIC⊥ as economic sovereignty with market properties — it is transferable within certain limits and bears economic value. For VIC⊥ the formal expression of T12 remains partially applicable: Legitimacy(VIC⊥-decisions) contains

an element of Code_says_so to the extent that infrastructural decisions are determined by the technical rules of the protocol. However, this is a constitutionally bounded domain of application, not political governance: VIC⊥-decisions concern exclusively the technical infrastructure and may not affect the political decisions adopted through EQU⊥. This separation, constitutionally entrenched in P4 and technically secured in P2 (Formal Verification Protocol in Coq), is the structural response to the circular legitimation of DAO.

Analytical synthesis of T12

Theorem T12 in its totality establishes the following. DAO governance is plutocracy by design in two independent senses: architectural (token voting = one token, one vote) and normative (circular legitimation through appeal to code without an external democratic foundation). Both aspects are structural consequences of the axiomatics of blockchain ideology, not artifacts of specific implementations. Correcting the design of individual DAOs does not extirpate the problem: any DAO based on token voting without an external constitutional foundation reproduces circular legitimation. The sole structural solution is constitutional architecture with an external source of legitimacy — popular sovereign authority — which is precisely what Virtublic realizes through P0 + P3 + P4.

Chapter Summary

The following has been proved. T12 (the theorem of DAO as plutocracy by design) is a rigorous consequence of axiom ΣA34 and Regularities 17 and 20 in their totality. DAO governance is plutocracy in the architectural sense (one token, one vote) and reproduces the sovereignty disjuncture of T8 through capital asymmetry under the preservation of declared openness. Circular legitimation is a structural property of any system based on token voting without an external democratic foundation: Legitimacy(DAO) = Code_says_so is not democratic legitimacy. Empirical verification through Uniswap, MakerDAO, and Compound demonstrates three distinct manifestations of a single structural defect: control by the team and early investors, capture through the market, and governance paralysis through the conflict of capital interests. Virtublic resolves T12 through P0 (popular sovereign authority as the inalienable foundation) and P4 (EQU⊥ = one person, one vote through Soulbound Identity).

Transition to Chapter 15

T11 established the economic concentration in PoS as a structural necessity. T12 established the normative insufficiency of token voting as a source of political legitimacy. Chapter 15 proceeds to the third dimension of the structural contradictions of blockchain — to anonymity as the mechanism that destroys accountability. If T12 showed that governance lacks a democratic foundation, then T13 will show that it is additionally deprived of legal accountability: anonymous subjects making governance decisions with consequences for thousands of users bear no verifiable accountability for the outcomes of those decisions. This is the third necessary element of the complete deconstruction of blockchain as an institutional form.

Chapter 16. Code is law without the normative axiom

T14. Theorem of efficiency versus subjecthood

Formulation. Blockchain instantiates the principle of code is law without the normative axiom NA0 established in Volume I. Consequently, the smart contract as a norm optimizes efficiency — the target function of the protocol — yet does not protect subjecthood. A smart contract may be simultaneously technically efficient and structurally exploitative: efficiency and the protection of subjecthood are independent variables, not obligated to coincide in their direction of optimization.

Justification

T14 is the logical continuation of T13 at the systemic level. Where T13 demonstrated that the subject of action in blockchain is indeterminable — there is no person bearing accountability — T14 demonstrates that the action itself is normatively unjustified in the absence of NA0: the rule is executed not because it is just in relation to the subjects upon whom it operates, but because the code is written thus. Together, T13 and T14 produce the complete deconstruction of the normative dimension of blockchain: neither the subject of action nor the action itself possesses a normative foundation in the existing architecture.

T14 is derived from axiom ΣA31 (code is law as the principle of automatic smart contract execution), axiom ΣA32 (irreversibility without correction), and normative axiom NA0 of Volume I (subjecthood as a politically protectable good, the systematic destruction of which is a political evil independent of its economic efficiency). The interaction of these three foundations generates the following analytical structure: the smart contract is executed automatically (ΣA31), its consequences are irreversible (ΣA32), and it contains no NA0 — that is, it has no embedded mechanism of suspension for the case in which efficient execution generates the destruction of the subjecthood of participants.

The concept of normative axiom NA0 in the context of T14 requires precise reproduction. NA0 of Volume I asserted: "subjecthood is a politically protectable good; its systematic destruction is a political evil independent of the economic efficiency of the destroying mechanism." The determinative element is the final qualification: independent of economic efficiency. This means that NA0 is not a criterion of efficiency — it is an external constraint upon the optimization function. A system that optimizes efficiency without NA0 is not a system with an incorrect efficiency function — it is a system without the constraint that would prohibit achieving efficiency through the destruction of subjecthood. This distinction is determinative for understanding T14: the theorem does not assert that blockchain is inefficient — it asserts that its efficiency is not normatively sufficient.

The connection of T14 with the preceding theorems of Part IV is as follows. T11 demonstrated that PoS generates economic concentration as the structural consequence of architecture. T12 demonstrated that token voting generates governance without democratic legitimacy. T13 demonstrated that anonymity generates accountability = 0. T14 completes this series by demonstrating that all three preceding defects are instantiated through one common mechanism: code is executed without a normative constraint prohibiting efficient optimization at the expense of the subjecthood of participants. T14 is therefore not the fourth isolated contradiction but the common foundation from which T11–T13 are particular consequences.

Proof

The first step. Smart contracts are executed automatically upon satisfaction of code conditions (axiom ΣA31). This is a deliberate architectural choice, not a technical limitation: automatic execution is the central advantage of smart contracts over traditional legal instruments. A traditional contract requires judicial interpretation, depends on the good faith of parties for performance, and admits contestation in the event of changed circumstances. A smart contract does not depend on interpretation, does not require good faith, and cannot be contested through changed circumstances: the conditions of execution are defined by code, and the code executes upon their occurrence. It is precisely this property — reliability of execution independent of the will of parties — that is the declared advantage. Yet this same property is the source of the defect of T14: the reliable execution of code that contains no normative constraint is the reliable production of consequences without a normative filter.

The second step. The target function of a smart contract is determined by code, not by a normative axiom. The smart contract optimizes the function embedded within it: maximize protocol revenue, minimize counterparty risk, liquidate undercollateralized positions upon reaching a threshold. These functions are technically correct formulations of optimization tasks. Not one of them contains a constraint of the form "do not destroy the subjecthood of the participant" or "suspend if the consequences of execution violate NA0." This is not an oversight on the part of developers of specific protocols — it is the structural property of the approach: within the framework of code is law, normative value is external to code and cannot be embedded without altering the architectural foundations of the system.

The third step. NA0 of Volume I establishes that subjecthood is a politically protectable good and that its systematic destruction is a political evil independent of the economic efficiency of the destroying mechanism. This is not an assertion about the psychology or morality of specific actors but a structural normative principle: a system that generates the destruction of subjecthood as a byproduct of its efficient operation is politically untenable independent of the technical correctness of its operations.

Subjecthood in the sense of NA0 encompasses: the capacity of the subject to form intentions not fully determined by the algorithmic decisions of the system (axiom A7, Volume I); the existence of a space of choice sufficient for the realization of those intentions (normative principle N2, Volume I); and protection from mechanisms that systematically transform the subject into an object of optimization (NA0). A smart contract that automatically liquidates the subject's position upon reaching a threshold, without the possibility of contestation, appeal, or deferral, is a mechanism that generates precisely such a transformation: the subject, from an agent with a position, becomes the object of a liquidation algorithm.

The fourth step. Smart contracts do not contain NA0 as an embedded constraint. This is not an incidental omission but the structural consequence of code is law as a principle: if law is code and code is the neutral inscription of an algorithm, then the inclusion of a normative constraint of the type "do not destroy subjecthood" necessitates an operational definition of subjecthood in a form suitable for encoding. This is precisely the task that Virtublic resolves through the Formal Verification Protocol (P2) — yet which blockchain ideology does not

structurally pose, since it presupposes the existence of a normative axiom external to the algorithm.

The operational definition of subjecthood requires: first, the identification of the physical subject (which is precluded by A25 — subject = key); second, a normative judgment as to whether a given consequence constitutes the destruction of subjecthood (which necessitates a political determination, not an algorithmic function); and third, a mechanism for suspending code upon the occurrence of such a consequence (which contradicts ΣA31 — code executes automatically). Consequently, the inclusion of NA0 in a smart contract is impossible without modification of three architectural axioms: A25, ΣA31, and the absence of an external normative foundation. This is not a technical task but a constitutional one: what is required is not better code but a constitutional architecture external to the code.

The fifth step. The case of DeFi liquidation upon a collateral price decline is an operational demonstration of T14, not merely an empirical illustration. In MakerDAO and analogous protocols, the user provides collateral (for example, ETH) to obtain a loan in a stable coin (DAI). When the value of the collateral falls below an established threshold (collateralization ratio), the smart contract automatically initiates liquidation: the collateral is sold at auction to extinguish the debt, and a portion of the collateral is extracted as a liquidation penalty. This mechanism is technically efficient from the perspective of the protocol's target function: it secures debt coverage and minimizes the risk of protocol insolvency. Simultaneously, it generates the destruction of the subject's economic position under conditions the subject could not fully foresee or control: the decline in collateral value is a market event not amenable to individual management, yet it entails individually catastrophic consequences through the automatic execution of code.

The subject whose position is liquidated is an object of the protocol's optimization: his collateral is employed to resolve the task of protocol solvency. His interests — preservation of position, allocation of time to provide additional collateral, appeal to the circumstances of a market crisis — are structurally unrepresented in the smart contract code. This is precisely the transformation of subject into object that NA0 characterizes as a political evil. Optimize(efficiency) ∧ ¬Protect(subjecthood) → Exploitation is not a normative judgment about the intentions of developers but an analytical conclusion about the structural consequences of the architecture.

The sixth step. From the five preceding steps the conclusion follows with logical necessity: a system that optimizes efficiency without NA0 generates the exploitation of subjects as the structural consequence of its correct operation. This is the definition of political evil in the sense of NA0: not the deliberate infliction of harm, but the systematic production of damage through a mechanism that contains no constraint against such production. The formal expression Optimize(efficiency) ∧ ¬Protect(subjecthood) → Exploitation establishes not a particular case but a necessary consequence under any optimization mechanism not constrained by NA0.

Formal expression

Optimize(efficiency) ∧ ¬Protect(subjecthood) → Exploitation.

This expression is a logical proposition establishing the structural consequence of two joint conditions: the presence of efficiency optimization and the absence of the protection of subjecthood. Under the simultaneous satisfaction of these conditions, exploitation is a necessary consequence — not a probable outcome but a logically inevitable result. Exploitation in this context is not a moral category but an operational term: the systematic use of the subject as a means for achieving the target function without a constraint prohibiting such use.

It is necessary to establish the precise status of this expression in relation to the technical correctness of blockchain. The expression does not assert that smart contracts are technically incorrect. It asserts that technical correctness and normative sufficiency are independent properties: a system may be simultaneously technically correct and normatively untenable. This distinction is central to understanding T14 in its relation to Regularity 27 (blockchain as an insufficient form): the insufficiency is not technical but normative.

Empirical verification

Black Thursday — March 12, 2020 — is the most documented and analytically clean case for the verification of T14. Over the course of several hours, the value of ETH fell by approximately 30% against the backdrop of global market panic associated with the onset of the COVID-19 pandemic. MakerDAO smart contracts responded in strict conformity with code: thousands of positions with ETH collateral crossed the liquidation threshold and were automatically placed at auction. A confluence of circumstances — network congestion on Ethereum (gas prices rose exponentially), technical failures with the keeper bots responsible for auction participation — resulted in a portion of liquidations proceeding at zero price: keeper bots won auctions without any competing bid, obtaining collateral at no cost. Users whose positions were liquidated in this manner lost all collateral without extinguishment of debt.

MakerDAO governance following Black Thursday adopted a series of modifications: an increase in the liquidation execution delay, the introduction of a new liquidation module (Liquidations 2.0), and a compensation fund for a portion of affected users. All of these modifications constitute a verification of T14 through the inverse argument: the community acknowledged that code which had executed correctly according to its target function had produced consequences violating the interests of subjects. The response confirms that NA0 had not been embedded in the code — which is precisely why post-factum correction was required. The correction does not eliminate the structural defect: it is its acknowledgment.

The determinative analytical aspect of Black Thursday is the following. Not one of the MakerDAO smart contracts functioned incorrectly: each contract executed precisely what had been written within it. The liquidation threshold was reached — liquidation was executed. The auction proceeded in accordance with code. Keeper bots won according to the auction rules. Optimize(efficiency) was achieved: protocol solvency was preserved. ¬Protect(subjecthood) was instantiated: thousands of users lost assets without the possibility of appeal, contestation, or compensation through a mechanism embedded in the code. Exploitation followed as the necessary consequence. This is the verification of T14 in its maximally pure form: not a hack, not a vulnerability, not an abuse, but the normal functioning of code without a normative constraint.

The Compound Protocol black swan of 2020 provides an additional documented case exhibiting the same structure. Upon a significant rise in the price of DAI relative to USD, a number of positions in Compound crossed the liquidation threshold due to peg deviation rather than any change in the value of collateral. Users whose positions were liquidated had performed no actions ordinarily associated with elevated risk: their collateral had not fallen, their leverage had not increased. They were liquidated solely because a market oracle registered a peg deviation that the code interpreted as a violation of the collateralization ratio. The code executed correctly. The subjecthood of users who had violated no conditions of the system was destroyed through the correct execution of code.

It is necessary to address the counterargument that blockchain ideology advances against such cases: users voluntarily accepted risk, since the conditions of liquidation were publicly known upon entry into the protocol. This is a partially correct assertion: the conditions of liquidation are indeed public and ought to be known to the participant. However, T14 responds to this argument as follows. First, informed consent is not a sufficient foundation for the elimination of NA0: even if the subject voluntarily accepted the conditions, a system that generates the destruction of subjecthood as its normal mode of operation violates NA0 structurally, not contingently. Second, informed consent under conditions of the high technical complexity of DeFi protocols is doubtful: the majority of users are incapable of independently verifying the smart contract code they are accepting. Acceptance of terms of use without the ability to verify code does not constitute informed consent in any normatively significant sense. Third, consent does not nullify the structural absence of NA0 in the code — it is a separate argument concerning the distribution of responsibility, not the nature of the mechanism.

The Euler Finance hack of March 2023 provides a third documented case with an additional dimension. The attacker exploited a vulnerability in the Euler Finance flash loan mechanism, obtaining the ability to self-liquidate at a loss to the protocol. Approximately $197 million was thereby extracted from the protocol. Notably, the attacker subsequently entered into negotiations with the Euler Finance team and returned the majority of funds — through the same smart contract mechanism employed for the attack. Code as an instrument of attack and code as an instrument of the return of funds are identical in nature: both execute a target function without a normative filter. The Euler case verifies T14 through the following aspect: code cannot distinguish "legitimate" from "illegitimate" use — it executes any function that is technically correct. NA0 is not embedded — consequently, "legitimate" and "exploitative" use are indistinguishable from the perspective of code.

Connection with Volume I

T14 is the deepest connection between Volume I and Volume II in Part IV: it does not reproduce a specific contradiction of Volume I but reproduces its central normative conclusion on a new substrate. Volume I proved that digital capital generates the alienation of subjecthood through the transformation of the subject into a data source: the subject ceases to be an agent and becomes a resource for the construction of predictive models. This was described through T1 (surplus attention), T5 (the neutralization of resistance), and T6 (cognitive disarmament). In each case, the mechanism was structurally identical: the system optimizes efficiency (predictive power, engagement, retention) without a constraint prohibiting such optimization at the expense of subjecthood.

T14 establishes that blockchain reproduces the same structure of alienation with a substitution of mechanism: there, alienation was produced through the algorithmic processing of behavioral data; here, through the automatic execution of a smart contract. The subject in both cases is an object of optimization: there — of the optimization of predictive power; here — of the optimization of protocol efficiency. The absence of NA0 is the common structural property of both mechanisms: neither the recommendation algorithm nor the liquidation contract contains a constraint prohibiting the production of the destruction of subjecthood as a byproduct of correct operation.

This means that blockchain is not a resolution of the contradiction established by NA0 in Volume I. It is its reproduction on a different substrate. The subject transitioning from the environment of platform capitalism into the environment of DeFi is not protected from the alienation of subjecthood — he is protected from the specific mechanism (predictive data) yet remains vulnerable to an analogous mechanism (liquidation algorithm). NA0 is violated in both spaces on the same ground: the absence of a constitutionally embedded normative constraint.

Theorem T4 of Volume I (accountability without power) is also reproduced in T14 with precise isomorphism. T4 asserted that the subject bears the cognitive and economic risks of decisions adopted by an algorithmic system he does not control. In the DeFi context: the user bears the economic risks of liquidation executed by a smart contract over whose architecture he had no influence and against whose decisions he may not appeal. The form of T4 is preserved: accountability for consequences (economic losses upon liquidation) is borne by the subject who does not possess power over the mechanism (the smart contract). This is an additional verification of the systemic isomorphism between Volumes I and II.

Connection with Volume III

Virtublic resolves T14 through principle P2 (Code Supremacy with NA0), which is the most technically specific principle of the constitutional architecture. P2 formulates the following provision: the constitution of Virtublic is executable code, yet the code embeds NA0 through the formal verification of normative principles N1–N7 by means of Coq.

This resolution requires precise understanding to preclude its interpretation as the simple addition of an "ethical check" to a smart contract. P2 is a fundamentally different architectural approach. The Formal Verification Protocol in Coq is a mathematical proof that executable code conforms to the formal specification of normative principles N1–N7. This means: prior to the execution of any code in the constitutional architecture of Virtublic, a mathematically verifiable proof is produced demonstrating that the given code does not violate the formal expression of NA0. This is not a check of the developer's intentions and is not a heuristic assessment of consequences — it is a mathematical proof that the code, under any admissible input data, produces output data that does not violate the formally defined normative constraints.

The operational realization of this principle with respect to T14 unfolds as follows. The liquidation mechanism in Virtublic — where it exists for VIC⊥ operations — is subject to formally verified constraints deriving from N2 (the right to a space of choice) and N3 (protection against irreversible harm without procedural guarantees). This means: automatic liquidation without notification, without a deferral period, and without a contestation

mechanism is code that does not pass Formal Verification — it shall be rejected as violating the formal specification of N2. A liquidation satisfying Formal Verification must contain: a notification period for the subject (instantiating N2 through the provision of a space of choice), a contestation mechanism through P18 (Conflict-Resolution Core) where grounds exist (instantiating NA0 through the possibility of the protection of subjecthood), and proportionality of consequences relative to the violation of conditions (instantiating N3).

This distinguishes Virtublic in principle from two extreme positions. The first extreme: traditional law, in which the normative protection of subjecthood is instantiated through judicial procedures post-factum — that is, after the harm has already been inflicted. In Virtublic, normative verification is antecedent: code that violates NA0 cannot be deployed. The second extreme: blockchain architecture, in which code executes without a normative filter and the correction of consequences is a post-factum voluntary act of governance (as in the case of MakerDAO following Black Thursday). In Virtublic, the violation of NA0 is constitutionally precluded at the level of Formal Verification rather than corrected after the fact.

Principle P18 (Conflict-Resolution Core) complements P2 in the resolution of T14: upon the emergence of a dispute as to whether a specific smart contract execution violates NA0, a constitutionally defined resolution procedure exists. This is the analogue of a judicial contestation mechanism in traditional law, yet instantiated constitutionally: four types of conflict with formally defined resolution procedures, the Civic Guard for semantic conflicts, and referendum through EQU⊥ for fundamental conflicts of values. The conjunction of P2 + P18 generates a system in which Optimize(efficiency) ∧ Protect(subjecthood) is an achievable state — not through the limitation of efficiency, but through the constitutional embedding of a normative constraint into the optimization function itself.

Analytical synthesis of T14

Theorem T14 is the culmination of the normative deconstruction of blockchain in Part IV. T11–T13 identified three specific structural defects: economic concentration, the absence of democratic legitimacy, and the impossibility of accountability. T14 demonstrates that all three defects are particular consequences of one common foundation: code is law without NA0 generates optimization without a normative constraint protecting subjecthood. The elimination of T14 is therefore a necessary condition for the elimination of T11–T13: absent embedded NA0, any technical improvements generate more efficient mechanisms without a normative filter, rather than mechanisms with the constitutional protection of subjecthood.

The synthetic conclusion of T14 with respect to blockchain as a technological substrate is the following. Blockchain is technologically necessary (Regularity 27) yet normatively insufficient. Normative insufficiency is not an incidental property of specific implementations but the structural consequence of the absence of NA0 in the architectural foundations. Consequently, the resolution of T14 is not a better blockchain protocol, a better smart contract, or a better governance procedure — the resolution is a constitutional architecture that embeds NA0 into executable code through formal verification. This is precisely what Virtublic instantiates through P2.

Chapter Summary

The following has been proved. T14 (the theorem of efficiency versus subjecthood) is a rigorous consequence of axioms ΣA31, ΣA32, and normative axiom NA0 of Volume I in their conjunction. The smart contract as a norm optimizes the target function of the protocol without a normative constraint prohibiting the destruction of subjecthood through correct operation. Optimize(efficiency) ∧ ¬Protect(subjecthood) → Exploitation is the necessary consequence of this architecture, not a particular case. Black Thursday (MakerDAO, 2020), the Compound peg deviation (2020), and the Euler Finance hack (2023) verify this assertion through three distinct mechanisms of instantiation. T14 reproduces the central normative conclusion of Volume I — the alienation of subjecthood through optimization without NA0 — in the blockchain substrate, demonstrating the structural isomorphism between platform capitalism and DeFi exploitation. Virtublic resolves T14 through P2 (Formal Verification with NA0 in Coq) and P18 (Conflict-Resolution Core), embedding the normative constraint in the antecedent verification of code rather than the post-factum correction of consequences.

Transition to Chapter 17

T11–T14 in their conjunction have deconstructed blockchain across four dimensions: economic concentration, the absence of legitimacy, the impossibility of accountability, and the absence of the normative axiom. Chapter 17 proceeds to T15 (Sybil trilemma), which concludes the analytics of Part IV through the proof of the most technically specific contradiction: the impossibility of simultaneously achieving decentralization, Sybil resistance, and the absence of plutocracy within the space of known mechanisms. T15 is a theorem concerning architectural limits rather than normative defects — and in this sense it is the necessary complement to T14: there, the normative constraint is absent from the code; here, the technical mechanism necessary for equal participation is structurally untenable without a constitutional resolution.

Chapter 17. Sybil resistance as centralization

T15. Theorem of decentralization versus Sybil resistance

Formulation. Every known mechanism for protection against Sybil attack requires either a centralized trusted verification body or an economic participation barrier that reproduces plutocracy. It therefore follows that the simultaneous achievement of decentralization, reliable Sybil resistance, and the absence of plutocracy is impossible in the space of realizable mechanisms. This is not a technical problem awaiting an engineering solution but a structural trilemma following from the incompatibility of axiom A19 with the requirement of verification of the uniqueness of physical subjects.

Justification

T15 completes the analytics of Part IV as a theorem about architectural limits — as distinct from T11–T14, which were theorems about normative defects. This distinction is fundamental. T11 asserted: PoS generates economic concentration because rewards are proportional to position — this is a normative defect, because it violates the principle of political equality. T12 asserted: token voting generates circular legitimation — this is a normative defect, because it violates the principle of popular sovereign authority. T13

asserted: anonymity generates the impossibility of accountability — this is a normative defect, because it violates the protection of the subjecthood of those harmed. T14 asserted: "code is law" without NA0 generates exploitation — this is a normative defect by the definition of NA0. T15 is different in nature: it asserts that three technical requirements simultaneously declared by blockchain ideology are logically incompatible. This is not a normative defect of a specific implementation — it is the logical incoherence of the original declaration.

T15 is derived from axiom ΣA35 (Sybil attack as a structural threat to systems with equal participation), axiom ΣA36 (proof-of-personhood and its architectural limits), axiom A19 (decentralization as a sufficient condition for overcoming monopolization), and theorem T11 (the plutocratic inevitability of PoS). The totality of these grounds produces the following analytical structure: Sybil resistance requires verification of the uniqueness of subjects (ΣA35), verification of uniqueness is realizable only through three classes of mechanisms (ΣA36), and each of these classes violates one of the declared requirements (A19, T11, or both).

It is necessary to record precisely why Sybil resistance is not a technical supplement but a necessary condition of any system with equal participation. If a system distributes rights or resources on the basis of the number of participants — one person, one vote, quadratic voting, airdrop by number of unique addresses — then a subject who has created n fictitious identities obtains an n-fold advantage. This renders the mechanism of equal participation structurally untenable: it distributes rights not equally among subjects but equally among identities, whose number is not bounded. It therefore follows that Sybil resistance is not an optional property but a necessary condition for the realization of equal participation. Any system that purports to democratic self-governance must resolve the Sybil problem. T15 proves that within the framework of blockchain ideology this resolution is impossible without a compromise that violates one of the three declared properties.

Proof

The proof is constructed through the method of exhaustion: the demonstration that all three known classes of solutions to the Sybil problem violate one of the three requirements, and that no fourth class of solutions exists in the space of realizable mechanisms.

First step. Definition of the three requirements constituting the trilemma. Requirement D (decentralization): the system must not depend on a trusted centralized body whose decisions may be arbitrary or captured (A19). Requirement SR (Sybil resistance): the system must verify the uniqueness of participants with sufficient reliability to preclude Sybil attack (ΣA35). Requirement NP (absence of plutocracy): governance influence must not be proportional to capital, because this violates the principle of political equality of subjects. Blockchain ideology declares the simultaneous satisfaction of all three requirements. T15 proves: $D \wedge SR \wedge NP = \varnothing$.

Second step. First class of solutions: centralized verification. This class realizes SR through the establishment of a trusted body that verifies the uniqueness of physical subjects: biometric identification, state registries, institutional KYC. It realizes NP, because verification of uniqueness does not depend on the subject's capital position. However, it violates D: the trusted verification body is a centralized subject with accumulated authority, making

decisions about the inclusion and exclusion of participants. This is a precise contradiction of A19.

Worldcoin is the most developed implementation of this class and demonstrates its structural limit with maximum clarity. The Worldcoin Foundation is a centralized subject controlling the iris verification algorithm. It makes decisions about which biometric patterns are sufficient for verification, which anomalies lead to rejection, and what the rules are for revoking a World ID. The declared decentralization through zk-proof — local processing of biometric data without transmission to a central database — does not extirpate the centralization of control over the verification algorithm and over the production of Orb devices. The Foundation remains the sole trusted hardware manufacturer and the sole developer of the verification algorithm. The replacement of a central database with zk-hashes is a technical innovation, not a structural change: authority over the rules of verification remains centralized.

The additional structural defect of biometric centralized verification was recorded in Chapter 11: the iris scan is a permanent identifier — the biometric key is not replaceable upon compromise. This constitutes an irreversible violation of N1 of Volume I (the right to unpredictability) in the sense that compromised biometric data cannot be "revoked" by the subject — they remain predictively accessible to any subject who gains access to them. Unlike a password or a cryptographic key, the biometric identifier is an immutable property of the subject's physical body. It therefore follows that centralized biometric verification violates not only D but also normative principle N1, generating irreversible privacy risk as a structural consequence.

BrightID implements a less technically aggressive form of centralized verification through a social graph: uniqueness is verified through a network of mutual confirmation. This approach generates a different form of centralization — not through a trusted body but through social privilege: subjects included in dense social networks are readily verifiable; socially marginal subjects are structurally vulnerable to exclusion from verification not through malicious intent but through the algorithm. It therefore follows that BrightID violates requirement NP in its extended interpretation: equal participation is not possible if access to the verification mechanism is structurally dependent on the subject's social capital.

First class of solutions, summary: SR $\wedge$ NP, but $\neg$D. The decentralization requirement is violated through the centralization of the verification body or through the reproduction of social inequality as a participation barrier.

Third step. Second class of solutions: the economic participation barrier. Proof-of-Stake realizes Sybil resistance through an economic barrier: the creation of n fictitious validators requires n × minimum_stake tokens. With a minimum stake of 32 ETH, creating one thousand fictitious validators requires 32,000 ETH — a sum rendering Sybil attack economically irrational at sufficient token value. SR is realized: the economic barrier is a functionally effective mechanism for precluding fictitious identities in the space of validation rights. D is realized in the declared sense: there is no trusted verification body; the rules are defined by code. However, NP is violated: the economic barrier is a mechanism of plutocracy by definition — it renders access to validation rights proportional to capital.

This is the precise content of T11, proved in Chapter 13: Gini_coefficient(t+1) ≥ Gini_coefficient(t) is a structural consequence of PoS. The second class of solutions is not

an alternative solution to T11 — it is its source. T11 and T15 are connected through the second class of solutions: PoS as Sybil resistance is simultaneously a mechanism of plutocratic concentration. The attempt to reduce the economic barrier to increase participant inclusivity simultaneously reduces Sybil resistance: as minimum_stake → 0, Sybil attack becomes costless. It therefore follows that NP and SR are in an inverse relationship under the second class of solutions: increasing one reduces the other, and no point on the trade-off curve exists at which both requirements are satisfied simultaneously.

Second class of solutions, summary: SR ∧ D, but ¬NP. The requirement of the absence of plutocracy is violated through the proportionality of Sybil resistance to the economic barrier.

Fourth step. Third class of solutions: the computational barrier. Proof-of-Work realizes Sybil resistance through a computational barrier: the creation of fictitious mining nodes requires computational resources proportional to their number. At sufficient network scale, a 51% attack is economically irrational. The mechanism is historically verified: Bitcoin PoW ensured consensus security without a successful 51% attack for more than fifteen years.

However, PoW generates two mutually reinforcing defects. The first: centralization in mining pools through economies of scale (Regularity 22). Mining with competitive hashrate requires specialized ASIC equipment and access to cheap electricity — resources creating an entry barrier that reproduces the temporal barrier of T2 of Volume I in the geographic and infrastructural dimension. The consequence is concentration of hashrate in a small number of large mining pools: during the periods 2018–2024, the five largest Bitcoin mining pools systematically controlled more than 65% of total hashrate. This violates D through de facto centralization: there is no formal centralized body, but de facto hashrate is concentrated among a limited number of subjects with a share sufficient for a theoretical consensus attack.

The second defect: PoW ensures Sybil resistance in the consensus space but not in the governance space. As was established in Chapter 11, in PoW systems with on-chain governance, voting is determined not by hashrate but by token ownership. It therefore follows that the computational barrier is an SR mechanism with respect to the production of blocks but not with respect to governance rights. The disjuncture between the two levels is structural: protection of consensus from Sybil does not ensure protection of governance from Sybil, because governance rights and consensus rights rest on distinct mechanisms in PoW systems with token voting. When an attempt is made to use hashrate as the basis for governance influence — that is, to eliminate this disjuncture — an additional violation of NP arises: governance is concentrated among the largest mining pools, reproducing the same plutocratic structure as PoS with the additional dimension of energy expenditure.

Third class of solutions, summary: SR with partial D and partial NP, violating both requirements through distinct mechanisms. Centralization in mining pools violates D de facto. Governance Sybil resistance is not ensured by the computational barrier under token voting. The attempt to eliminate governance Sybil through hashrate reproduces ¬NP.

Fifth step. The method of exhaustion is complete. All three known classes of solutions have been examined: each violates one or more of the three requirements. The possibility of a fourth class must be separately considered. A fourth class formally exists as a logical possibility: some mechanism not belonging to any of the three classes and simultaneously

realizing D ⋀ SR ⋀ NP. No such mechanism was proposed and implemented in the blockchain ecosystem during the period 2008–2026 — despite the significant resources directed toward research in proof-of-personhood. It therefore follows that T15 is a theorem about the space of realizable mechanisms, not an absolute theorem about all logically conceivable mechanisms. This limitation is a necessary qualification that does not diminish the practical force of the theorem: a fundamentally new class of Sybil resistance realizing all three requirements is a logical possibility, but not a realized actuality.

Sixth step. From the five preceding steps the conclusion follows: Decentralization ⋀ Sybil_resistance ⋀ ¬Plutocracy = ∅ in the space of realized and theoretically grounded mechanisms over the period 2008–2026. This is not an assertion about future impossibility but an assertion about the current incoherence of blockchain ideology's declaration of the simultaneous realization of all three requirements.

Formal expression

Decentralization ⋀ Sybil_resistance ⋀ ¬Plutocracy = ∅.

This expression records the structural incompatibility of the three requirements in the space of known mechanisms. The symbol ∅ (empty set) signifies that the intersection of systems simultaneously realizing all three requirements is empty: no such system exists. Each of the three classes of solutions realizes at most two of the three requirements.

It is necessary to record the precise relationship of this expression to the concept of the trilemma in blockchain theory. Vitalik Buterin's blockchain trilemma — security, scalability, decentralization — is a technical assertion about computational resources. T15 is a normative-architectural assertion about political requirements. Both are trilemmas, but in fundamentally distinct spaces: T15 is not a consequence of Buterin's trilemma and is not reducible to it. T15 is specific to the space of governance with equal participation — precisely where blockchain declares its greatest normative advantages, the trilemma is most acute.

Empirical verification

Worldcoin verifies T15 through the first class of solutions. As of 2024–2025, the Worldcoin Foundation registered several tens of millions of World IDs through a network of Orb devices in more than 35 countries. SR is realized: Sybil attack through the creation of multiple biometric identities is practically impossible under iris scan verification. NP is partially realized: verification does not depend on the subject's capital position. D is violated: the Worldcoin Foundation remains the sole trusted Orb manufacturer and the sole developer of the verification algorithm. Additionally: a number of states have imposed restrictions on Worldcoin's activities within their territories — Kenya, Germany, Hong Kong — which constitutes verification of the thesis that a centralized biometric verification body is a point of state regulation, that is, a point through which a decentralized system becomes dependent on its jurisdictional context.

Ethereum PoS verifies T15 through the second class of solutions. The minimum stake of 32 ETH at market price creates an entry barrier of $80,000–$100,000 for independent validation. Lido Finance controls more than 30% of staked ETH. SR is realized through the

economic barrier: a 51% attack on Ethereum PoS is economically irrational at existing market capitalization. D is formally realized: there is no trusted body. NP is violated: the Gini_coefficient of staking positions is increasing (T11). This constitutes verification of the second vertex of the trilemma: SR ∧ D, but ¬NP.

Bitcoin PoW verifies T15 through the third class of solutions. SR is realized for consensus: Bitcoin PoW has not been subjected to a successful 51% attack. D is violated de facto: the five largest mining pools systematically controlled more than 65% of hashrate. NP is violated in governance: the distribution of BTC remains highly concentrated — top 2% of addresses hold 95% of BTC — and governance influence de facto belongs to large holders and mining pools. This constitutes verification of the third vertex of the trilemma: SR partially realized, D violated de facto, NP violated.

The totality of the three cases empirically confirms that none of the mechanisms of Sybil resistance implemented in practice achieves all three requirements of T15 simultaneously. This is a necessary but not sufficient condition for the empirical verification of the theorem: the theorem asserts structural necessity, with empirical cases confirmed as realized consequences of the structural constraint.

Connection to Volume I

T15 is a theorem specific to blockchain and has no direct analogue in Volume I — analogously to T13. Digital capital does not have a Sybil problem in the same sense: platforms employ centralized identification as a standard mechanism while not declaring decentralization. The Sybil problem is a product of the attempt to eliminate centralized identification, that is, a product of blockchain's declared advantage over platform capitalism.

This produces the following analytical paradox meriting precise formulation. Platform capitalism violates N1 (the right to unpredictability) through surveillance: centralized identification is the precondition for constructing predictive models of the subject. Blockchain attempts to eliminate surveillance through decentralization and anonymity. But in the governance space with equal participation, decentralization and anonymity generate Sybil vulnerability, the elimination of which requires verification of uniqueness not achievable without an element of centralization. It therefore follows that blockchain faces a choice between two forms of violation of subjecthood: surveillance through centralization — the problem of Volume I — or Sybil vulnerability through decentralization — the problem of T15. This is not a situation of choosing the lesser of two evils but a proof that the technological elimination of one problem generates a structurally symmetrical problem in the adjacent space. This is the most fundamental evidence of Regularity 27 (blockchain as an insufficient form): the technological substrate cannot by itself resolve the contradiction between privacy and equal participation — this contradiction is political and requires a constitutional resolution.

Connection to Volume III

Virtublic resolves T15 through honest acknowledgment of the structural constraint and a constitutionally legitimate form of compromise — as distinct from blockchain architecture, which either denies the trilemma or selects one vertex while concealing the violation of the other two.

Principle P6 (Verifiable Census) establishes: verification of the uniqueness of citizens is a constitutionally recognized element of the architecture, realized through Digital Census v2 (principle P13). This constitutes an honest acknowledgment of T15: Virtublic does not declare full decentralization within the meaning of A19 with respect to uniqueness verification. The constitutional recognition of an element of centralization is a normatively more correct position than the declaration of decentralization while in fact implementing a centralized biometric body.

Principle P13 (Digital Census v2) implements the constitutionally accountable form of verification through the following architecture. In ordinary operation, each citizen undergoes verification through a zk-proof on the citizen's own device: local processing of biometric data generates a zero-knowledge proof of uniqueness without transmission of data to a central database. This extirpates the permanent biometric database as a point of centralization and as a source of irreversible privacy risk. The distinction from Worldcoin here is fundamental: the zk-proof in Virtublic does not require a centralized Orb device and does not generate iris-hashes stored by an external subject.

For identities flagged with an anomaly — statistical patterns corresponding to Sybil behavior — the Dual Suspicion Protocol is activated. Stage 1: automated behavioral Sybil-CAPTCHA tests verifying uniqueness through behavioral patterns not reproducible through automated means at scale. Upon success — the identity is confirmed. Upon failure — Stage 2: transfer to the Civic Guard.

The Civic Guard is the key element of the resolution of T15 and requires a precise description of its constitutional properties. The panel is constituted from 21 to 99 citizens proportionally to the total number of active citizens in the network — this range ensures scalability while preserving representativeness. Selection is effected through VRF (Verifiable Random Function): randomness is verifiable on-chain, and manipulation of panel composition is cryptographically impossible. Each panel member takes a constitutional oath on-chain, which is a verifiable public act: breach of oath is recorded in the immutable history of the blockchain. The panel adopts decisions by a qualified majority of 2/3, which requires substantial consensus within the panel and reduces the probability of arbitrary decisions. The panel is temporary: it is constituted for a specific Census cycle and is not a permanent body with accumulated authority. Rotation through VRF ensures that no group of citizens obtains systematic control over Sybil verification through repeated inclusion in the panel.

The structural distinction between the Civic Guard and the Worldcoin Foundation is as follows. The Foundation is a permanent body with accumulated powers, economic incentives to expand its role — through the WLD token — and without a rotation mechanism. The Civic Guard is temporary, rotational, randomly constituted, and constitutionally bounded in its powers: it adopts decisions only regarding identities that have passed Stage 1 of the Dual Suspicion Protocol and failed automatic verification. These are fundamentally distinct institutional forms for structurally similar tasks: both presuppose an element of human judgment in the verification of uniqueness, but one crystallizes authority in a permanent body while the other distributes it through random rotation of citizens with constitutional accountability.

The conjunction of P6 + P13 produces the following result with respect to T15. Virtublic realizes SR: Digital Census v2 with the Dual Suspicion Protocol ensures verification of uniqueness at two levels — automatic and collegial. Virtublic realizes NP: EQU⊥ is distributed with absolute equality through Soulbound Identity, not proportionally to capital. Virtublic does not realize full D within the meaning of A19: the Civic Guard is an element of human judgment, that is, an element not reducible to an automatic algorithm. However, this is a constitutionally recognized and institutionally bounded element: not a violation of a declaration but an honest constitutional acknowledgment that the verification of the physical uniqueness of subjects requires human judgment not reducible to an algorithm.

This is a normatively fundamental conclusion. Blockchain ideology declares full decentralization while in fact implementing various forms of centralization. Virtublic constitutionally acknowledges that full decentralization is an incoherent declaration with respect to the verification of the physical uniqueness of subjects — and formalizes the necessary element of human judgment as a constitutionally accountable institution with mechanisms of constraint, rotation, and verification. The gap between declaration and implementation is extirpated through the honesty of the declaration rather than through technical maneuvers that conceal this gap.

Analytical synthesis of T15

Theorem T15 in its totality establishes the following. The Sybil resistance trilemma is structural: the three requirements — decentralization, Sybil resistance, and the absence of plutocracy — are not simultaneously realizable in the space of known mechanisms. Each of the three vertices of the trilemma is empirically verified: Worldcoin (SR ∧ NP, ¬D), Ethereum PoS (SR ∧ D, ¬NP), Bitcoin PoW (partial SR, ¬D de facto, ¬NP). T15 is a theorem about the space of realizable mechanisms, not an absolute theorem about all logically conceivable mechanisms — this limitation is necessary for precision. T15 is specific to blockchain and has no direct analogue in Volume I: the Sybil problem is a product of the attempt to decentralize the verification of the uniqueness of subjects. Virtublic resolves T15 through a constitutionally recognized compromise: the Civic Guard as a temporary, rotational, randomly constituted, and accountable collegial verification body — a form that extirpates permanent centralization while preserving human judgment as a constitutionally necessary element.

Chapter Summary

The following has been proved. T15 (the theorem of decentralization versus Sybil resistance) is a structural conclusion from axioms A19, ΣA35, and ΣA36 in conjunction with T11. The trilemma D ∧ SR ∧ NP = ∅ is the result of the method of exhaustion: all three classes of known mechanisms violate one or more of the three requirements. Empirical verification through Worldcoin, Ethereum PoS, and Bitcoin PoW confirms the structural rather than incidental character of the trilemma. T15 is a theorem about the space of realizable mechanisms — not an absolute theorem about all conceivable mechanisms. Virtublic resolves T15 through a constitutionally recognized compromise: honest acknowledgment of the structural constraint and institutional formalization of the necessary element of centralization as a temporary, rotational, and constitutionally accountable body.

Transition to Chapter 18

T11–T15 in their totality have proved five structural contradictions of blockchain. Chapter 18 proceeds to T16 — the theorem of the absorption of critique, which is the most epistemologically significant of the seven theorems of Part IV. T16 proves: critical discourse without an institutional alternative is a functional element of the system it criticizes rather than a threat to it. This is the formal proof of Regularity 18, introduced in Chapter 6 — and is simultaneously an auto-referential conclusion for Volume II itself: the critique of blockchain contained in these pages is normatively coherent only to the extent that it crystallizes into the constitutional alternative of Volume III rather than remaining in the space of critical discourse without institutional embodiment.

Chapter 19. The constitutional necessity of blockchain

T17. Theorem of blockchain as a necessary but insufficient substrate

Formulation. Blockchain as technology — cryptography, zk-proof, smart contracts, formal verification — is a necessary component of the constitutional solution developed in Volume III. Blockchain as ideology — decentralization as a sufficient condition, code is law without the normative axiom, token voting as the foundation of governance — is structurally insufficient and reproduces the contradictions proved by theorems T11–T16. Consequently, a constitutional architecture that responds to the contradictions of both volumes must employ blockchain technologies without adopting blockchain ideology, and must add popular sovereignty, republican form, and the normative axiom as foundations external to the technological substrate.

Justification

T17 is the sole constructive theorem of Part IV. Theorems T11–T16 were destructive: each proved a structural contradiction of blockchain ideology. T17 is synthetic: it proves that, notwithstanding all established contradictions, blockchain as technology is a necessary component of the response to those contradictions. This distinction is determinative for understanding the analytical architecture of the trilogy as a whole. Volume I diagnosed digital capital. Volume II deconstructed blockchain ideology. T17 closes this double diagnosis into the sole possible constructive conclusion, preparing the transition to Volume III.

The structure of the proof of T17 is the method of exclusion: the demonstration that all alternative responses to the contradictions of Volumes I and II are structurally untenable, and that the sole tenable form is a constitutional architecture that employs blockchain as a technological substrate while adding constitutional foundations external to blockchain ideology.

T17 is derived from the conjunction of all preceding theorems of both volumes in their analytical sequence. Volume I (T1–T10) proved: the system of digital capital is not self-regulating, the state is not a neutral regulator, individual and collective resistance is neutralized, and constitutional architecture is a necessary condition of correction. Volume II (T11–T16) proved: blockchain ideology reproduces the contradictions of digital capital on a new substrate, resolving not one of them structurally. From the conjunction of these conclusions it follows that the response to the contradictions of both volumes cannot be

produced by market forces, state regulation, or a technological solution without a normative foundation. The sole remaining form is a constitutional architecture that employs the technological substrate of blockchain yet constructs its normative foundation from outside it.

Proof by the method of exclusion

The first step. Let us establish the set of possible responses to the contradictions of Volumes I and II. They may be structurally divided into four classes: market self-regulation, state regulation, technological solutionism, and constitutional architecture. The method of exclusion consists in the sequential demonstration of the untenability of the first three classes — grounded in theorems already proved in Volumes I and II — and in the proof that the fourth class is the sole structurally tenable form.

The second step. Market self-regulation. Hypothesis: competition in the market for digital platforms and blockchain protocols generates, over the long term, the correction of structural contradictions through the exit of users toward more just alternatives. This hypothesis is refuted by theorem T2 of Volume I (the temporal barrier): past the point of no return, competition within a homogeneous modal layer is structurally impossible without external intervention. Platforms that have accumulated predictive infrastructure have no competitors with comparable historical data depth. Blockchain protocols in which early holders have accumulated staking advantage have no mechanism for equalizing that advantage through market competition (T11). Theorem T3 of Volume I (the structural absence of correction) directly asserts: the system contains no internal mechanism for correcting concentration. Market self-regulation as the first class of responses is structurally untenable.

The third step. State regulation. Hypothesis: intensified state regulation of platforms and blockchain protocols generates the correction of structural contradictions through the external enforcement of normative standards. This hypothesis is refuted by Regularity 12 of Volume I (the state as purchaser of predictions): the state is systematically a purchaser of predictive data from the very platforms it is charged with regulating. This generates a structural conflict of interest that renders the state a structurally unreliable neutral regulator. Twenty years of regulatory attempts verify this assertion: GDPR did not alter the business models of platforms, antitrust fines did not alter the market positions of Google and Meta, and national laws governing control over technology companies have systematically lagged behind the pace of technological evolution. With respect to blockchain: states introducing regulatory restrictions on cryptocurrencies and DAOs either prohibit them entirely — thereby producing displacement into less regulated jurisdictions — or legalize them through regulatory frameworks that do not address the structural contradictions of T11–T15. State regulation as the second class of responses is structurally unreliable — not impossible in principle, but insufficient by virtue of the structural conflict of interest.

The fourth step. Technological solutionism. Hypothesis: technological innovations — a better blockchain protocol, a more efficient governance mechanism, a more reliable Sybil resistance algorithm — generate the correction of structural contradictions through technical improvements. This is the most relevant class of responses in the context of Volume II, since it is precisely the class that blockchain ideology declaratively advances. Theorems T11–T16 in their conjunction refute this hypothesis through exhaustion: each structural contradiction of blockchain is demonstrated as a consequence of architectural axioms (A19, A20, A23, A25,

ΣA31–ΣA36), not of specific implementation defects. A technically improved PoS reproduces T11 (plutocratic inevitability) while preserving A20 and A30. A technically improved DAO reproduces T12 (circular legitimation) while preserving ΣA34. Technically improved uniqueness verification reproduces T15 (the trilemma) while preserving A19. Regularity 27 (blockchain as an insufficient form) summarizes this result: blockchain resolves technical problems without resolving political ones. T16 additionally demonstrates that the critique of technological solutionism without an institutional alternative is a component of it. Technological solutionism as the third class of responses is structurally insufficient.

The fifth step. The method of exclusion is complete: three of four classes of responses have been refuted through already-proved theorems. A single class remains — constitutional architecture. This class is structurally tenable under the following necessary conditions. The first condition: the constitutional architecture must employ a technological substrate securing Byzantine fault tolerance, a verifiable transaction history, and the impossibility of identity forgery — without these properties, the constitution is not executable in a decentralized environment. The second condition: the constitutional architecture must not adopt blockchain ideology — that is, it must not construct its normative foundation on code is law without NA0, token voting without popular sovereignty, and decentralization without Sybil resistance. The third condition: the constitutional architecture must contain an external source of legitimacy — popular sovereignty — not reducible to code. From these three conditions there follows a single form: Blockchain(technology) + Constitution(P0–P18) ∧ ¬Blockchain(ideology).

The sixth step. The complete formalization of the conclusion of T17: Virtublic = Blockchain(technology) + Constitution(P0–P18) ∧ ¬Blockchain(ideology) ∧ ¬Critique(absorbed). This conclusion is not an assertion about a specific product but a proof of the necessity of a class of solutions: any architecture satisfying the three conditions of the fifth step is a structurally tenable response to the contradictions of Volumes I and II. Virtublic is the concrete instantiation of this class.

What blockchain provides to Virtublic

T17 is a constructive theorem: it not only proves the necessity of constitutional architecture but establishes precisely which technological components of blockchain are necessary for its realization. This demarcation between technology and ideology is the operational core of T17: not all properties of blockchain are inherited by Virtublic — only those that instantiate constitutional principles P0–P18 are inherited.

The first component: zk-proof (zero-knowledge proofs). Normative principle N1 of Volume I asserted that the subject possesses the right to unpredictability — to protection against the formation of an exhaustive predictive model of his behavior. The realization of N1 necessitates a mechanism enabling the subject to verify his participation in the system without disclosing personal data sufficient for the construction of such a model. zk-proof is precisely such a mechanism: it permits the proof of the truth of an assertion (I am a unique citizen with the right to vote) without disclosing the data from which that assertion follows (identity, biometrics, participation history). Without zk-proof, principle P13 (Digital Census v2) is not realizable without the creation of a central biometric database, which reproduces the privacy risk diagnosed in the analysis of Worldcoin in chapters 11 and 17. zk-proof is thus a

technologically necessary component of the constitutional architecture with respect to the protection of N1.

The second component: smart contracts. Principle P2 (Code Supremacy with NA0) asserts that the constitution of Virtublic is executable code. This means: constitutional principles P0–P18 are not declarations requiring judicial interpretation but rules executed automatically upon the occurrence of conditions. Without smart contracts, the constitution is a document subject to interpretation and potentially arbitrary application by institutional actors. Smart contracts secure the deterministic execution of constitutional rules without the possibility of arbitrary deviation. The fundamental distinction of Virtublic from traditional constitutions consists precisely in this: the constitution is not a normative text open to interpretation but executable code that has passed Formal Verification.

The third component: cryptography and the public/private key mechanism. Principle P3 (Soulbound Identity) establishes the non-transferability of citizenship: EQU⊥ may not be sold, delegated for payment, or transferred by any other means. The realization of this principle necessitates a cryptographic mechanism securing the inseparability of identity from the physical subject at the protocol level, not solely at the level of declaration. Soulbound Identity in Virtublic is cryptographically bound to the physical subject through zk-proof uniqueness verification (P13), such that the transfer of identity to a different key necessitates repeated uniqueness verification that blocks dual citizenship. Without cryptographic enforcement of non-transferability, Soulbound Identity is a declaration rather than an architectural property: any subject could transfer his credentials through the transfer of a private key. Cryptography is a technologically necessary component for the realization of T13 (accountability) through P3.

The fourth component: formal verification. Principle P2 (Code Supremacy with NA0) instantiates NA0 not through declaration but through a mathematically verifiable proof of the code's conformity with normative principles N1–N7. This is the operational instantiation of the requirement established in the analysis of T14: the smart contract as a norm, in the absence of NA0, optimizes efficiency without a normative filter. The Formal Verification Protocol in Coq is the mechanism securing that any code claiming the status of constitutionally admissible is mathematically demonstrably free of violation of the formal specification of normative principles. Without formal verification, principle P2 is declarative: a developer may assert the code's conformity with NA0, but this assertion is not verifiable. Formal verification transforms normative conformity from a declaration into a mathematically proved property.

The conjunction of the four technological components — zk-proof, smart contracts, cryptography, and formal verification — is the necessary and sufficient technological substrate for the realization of the constitutional architecture of Virtublic. Blockchain provides these components in the form of a technological substrate; Virtublic employs them as infrastructure for constitutional construction. This is the precise meaning of the formula of T17: Blockchain(technology) as a necessary component, Constitution(P0–P18) as the sufficient addition.

What Virtublic adds to blockchain

The technological components of blockchain are necessary but not sufficient for constitutional architecture. Each of the contradictions T11–T16 necessitates a constitutional addition external to blockchain technology. These additions are precisely the elements that Virtublic contributes to blockchain as a technological substrate.

The first addition: popular sovereignty (principle P0). This principle is the response to T12 (the circular legitimation of the DAO): the DAO has no external source of legitimacy — its rules are legitimized through appeal to those same rules. P0 establishes popular sovereignty as the absolute and inalienable foundation of the constitutional architecture, not derivable from code and not alterable through code. Blockchain technology does not and cannot contain popular sovereignty as an embedded property: sovereignty is a political fact, not a technical protocol. It is the external source of legitimacy that precedes the constitutional architecture and is its condition. P0 is the first and most fundamental addition of Virtublic to the technological substrate of blockchain: that which transforms executable code from a technical protocol into a constitution.

The second addition: dual sovereignty (principle P4). This principle is the response to T11 (the plutocratic inevitability of PoS): the Gini_coefficient of staking positions increases monotonically, generating increasing concentration of governance influence among early holders and large stakers. P4 severs the causal chain between economic inequality and political power through the constitutional orthogonality of EQU$\perp$ and VIC$\perp$. The symbol $\perp$ establishes precisely this: the two sovereignties exist in non-commingling spaces, and no volume of VIC$\perp$ converts into EQU$\perp$. Blockchain technology does not contain this separation: token voting by definition makes economic position the foundation of political power. P4 is a constitutional addition that has no analogue in blockchain ideology.

The third addition: Soulbound Identity (principle P3) in conjunction with zk-proof (principle P14). This addition is the response to T13 (the impossibility of accountability under anonymity): Privacy $\uparrow \rightarrow$ Accountability $\downarrow$ under A25 (subject = key). P3 alters the definition of subject: in Virtublic, subject = Soulbound Identity, verified as unique through Digital Census v2 and cryptographically non-transferable. This establishes a verifiable link between action and physical subject while preserving zk-proof as a privacy mechanism under ordinary operation. Blockchain technology provides the cryptographic instruments for the realization of Soulbound Identity — but the idea of Soulbound Identity as a constitutional principle is an addition of Virtublic, not a property of blockchain ideology, which systematically rejects any binding of identity to a physical subject.

The fourth addition: the normative axiom in code (principle P2). This addition is the response to T14 (code is law without NA0): Optimize(efficiency) $\wedge$ $\neg$Protect(subjecthood) $\rightarrow$ Exploitation. P2 embeds NA0 into executable code through the Formal Verification Protocol in Coq: any code in the constitutional architecture of Virtublic is mathematically verifiably conformant with the formal specification of normative principles N1–N7. Blockchain technology provides the instruments of formal verification — Coq is a mathematical system independent of blockchain. Yet formal verification of normative conformity is a constitutional addition: blockchain ideology does not pose the task of verifying the normative correctness of code, as distinct from its technical correctness.

The fifth addition: the Civic Guard with Dual Suspicion Protocol (principles P6, P13). This addition is the response to T15 (the Sybil resistance trilemma): Decentralization ∧ Sybil_resistance ∧ ¬Plutocracy = ∅. Virtublic acknowledges this trilemma candidly and instantiates a constitutionally responsible compromise: the Civic Guard is a temporary, rotating, randomly constituted through VRF organ of civic judgment, activated only upon passage of the Dual Suspicion Protocol. Blockchain technology provides VRF as a cryptographic instrument of random selection. The institution of the Civic Guard as a constitutionally responsible form of verification is a political addition of Virtublic — a form analogous to the jury in constitutional tradition, yet instantiated on a blockchain substrate.

The sixth addition: the constitutional form as such (P0–P18 in their conjunction). This is the response to T16 (the absorption of critique without an institutional alternative): Critique(system) ∧ ¬Alternative(institutional) → Absorption. The constitutional form is an institutional alternative in the precise sense of T16: it is an executable architecture, not a critical discourse. It cannot be monetized through the attention economy in the same manner as critique. It cannot be cited as proof of openness without compliance. It provides a point of application for political energy in the form of concrete executable principles. Blockchain technology provides the executable substrate; the constitutional form is the political addition of Virtublic that determines the content of what is executed.

Analytical synthesis of T17

Theorem T17 yields the following aggregate conclusion. Blockchain as technology is a necessary component of the constitutional response to the contradictions of Volumes I and II: without zk-proof, smart contracts, cryptography, and formal verification, constitutional principles P0–P18 are not realizable in a decentralized environment with the preservation of subject privacy. Blockchain as ideology is insufficient: it reproduces the contradictions of digital capital on a tokenomic substrate and contains no mechanisms for their structural correction. Consequently, a constitutional architecture that employs blockchain technology and adds popular sovereignty, dual sovereignty, Soulbound Identity, NA0 in code, the Civic Guard, and the constitutional form as such is the sole structurally tenable form of response to the contradictions of both volumes. This is not an assertion about the uniqueness of Virtublic as a specific project but a proof of the necessity of a class of solutions, the sole known member of which is Virtublic.

T17 concludes Part IV and the entire analytical program of Volume II. The seven theorems (T11–T17) in their conjunction constitute an exhaustive deconstruction of blockchain ideology with the simultaneous proof of a constructive conclusion: the technological substrate of blockchain is necessary and may be embedded in a constitutional architecture that neutralizes its ideological defects.

Chapter Summary

The following has been proved. T17 (the theorem of blockchain as a necessary but insufficient substrate) is the synthetic conclusion from the conjunction of T1–T16 and the entire analytical apparatus of Volumes I and II. The method of exclusion demonstrates that market self-regulation, state regulation, and technological solutionism are structurally untenable responses to the contradictions of digital capital and blockchain ideology. The sole structurally tenable response is a constitutional architecture that employs blockchain as a

technological substrate (zk-proof, smart contracts, cryptography, formal verification) and adds popular sovereignty (P0), dual sovereignty (P4), Soulbound Identity (P3), the normative axiom in code (P2), the Civic Guard (P6, P13), and the constitutional form as such. Virtublic = Blockchain(technology) + Constitution(P0–P18) ∧ ¬Blockchain(ideology) ∧ ¬Critique(absorbed) is the formalization of this conclusion.

Transition to Part V

Part IV has completed the proof of seven theorems T11–T17, exhausting the analytical program of Volume II. Part V proceeds to the construction of the matrix of correspondences between Volumes I, II, and III: the precise correspondence between contradictions (T1–T17) and constitutional solutions (P0–P18). This is not a summarization of what has been stated but an operational proof that each structural contradiction of both volumes receives a concrete constitutional resolution in Volume III — and that the conjunction of these resolutions constitutes an internally coherent architecture rather than a set of isolated responses.

Δ6 — CRISIS: THE LIMIT OF SPECULATIVE LOGIC

Part IV is exhausted. The seven theorems (T11–T17) constitute the complete formal diagnosis of blockchain as an institutional form.

T11 proved: PoS generates plutocratic concentration as a structural necessity, reproducing the temporal barrier T2 on the tokenomic substrate. T12 proved: DAO governance is plutocracy by design, generating circular legitimation in the absence of popular sovereignty. T13 proved: Privacy ↑ → Accountability ↓ under the definition of subject through key, generating the structural impossibility of political accountability. T14 proved: Optimize(efficiency) ∧ ¬Protect(subjecthood) → Exploitation, demonstrating code is law without NA0 as the reproduction of the alienation of subjecthood. T15 proved: Decentralization ∧ Sybil_resistance ∧ ¬Plutocracy = ∅, establishing the structural trilemma not resolvable within the framework of blockchain ideology. T16 proved: critique without an institutional alternative is absorbed by the system, becoming its stabilizer. T17 proved: blockchain is a necessary technological substrate and an insufficient ideological form, and that constitutional architecture is the sole structurally tenable response.

Δ6 establishes the limit of speculative logic as an analytical program as applied to blockchain. Speculative logic — the assumption that a technological substrate is a sufficient condition of political freedom — is exhausted by theorems T11–T17: each political promise of blockchain (decentralization, equal governance, anonymity as freedom) demonstrably generates a politically undesirable consequence (concentration, plutocracy, the absence of accountability). The limit of speculative logic is simultaneously the point of transition: from critique to construction, from diagnosis to architecture, from Volume II to Volume III.

PART V. THE CONNECTION TO VOLUMES I AND III

Parts I–IV of Volume II have completed the analytical program declared at its outset: the three analytical layers — ontology, anthropology, epistemology — and seven formal theorems (T11–T17) have exhausted the diagnosis of the blockchain as an institutional form. Part V performs a different task: it does not produce new analysis, but demonstrates the internal coherence of the trilogy as a unified analytical architecture. This means: every structural contradiction registered in Volumes I and II receives a specific constitutional answer in Volume III — and these answers in their conjunction constitute not a set of isolated solutions, but a mutually coherent constitutional system.

Chapter 20. The correspondence matrix

The correspondence matrix is not a summarization of what has been previously stated, but the operational demonstration of the following assertion: principles P0–P18 of Volume III constitute a constitutionally closed answer to theorems T1–T17 of Volumes I and II. Closure means: no theorem remains without a constitutional answer, and no principle is an arbitrary addition without analytical justification in the preceding volumes. The matrix demonstrates this closure through seven correspondences, each of which is triadic: the source in digital capital — its blockchain analogue — the constitutional resolution in Virtublic.

Correspondence 1. T2 → T11 → P4 + P16

The foundational contradiction is formalized in theorem T2 of Volume I (the temporal barrier): beyond the point of no return, competition within a homogeneous modal layer is structurally impossible without external intervention. A platform that first accumulated a sufficient history of predictive data acquired a predictive power unreproducible by a new competitor in the same modal space without an analogous history. This is not a temporary competitive advantage, but a structural barrier: the data accumulation curve is a self-augmenting function that produces a widening gap between early and late participants without an internal equalization mechanism.

The blockchain analogue of this contradiction, demonstrated in theorem T11 of the present volume, is structurally isomorphic upon substitution of the substrate. Early holders acquired tokens at prices inaccessible to late participants through ICO, airdrop, and early mining; the compound interest effect (Wealth(t+1) = Wealth(t) × (1 + r)) produces a widening absolute gap between large and small staking positions at any non-zero reward rate; centralization through staking pools (Regularity 22) reproduces the temporal barrier in the geographical and infrastructural dimension. The consequence is the monotonic increase of the Gini_coefficient of staking positions, producing the intensifying concentration of governance influence among early holders.

The constitutional answer of Virtublic is produced through two principles in their necessary conjunction. Principle P4 (Dual Sovereignty) severs the causal chain through which T11 reproduces T2: the symbol ⊥ registers the constitutional orthogonality of VIC⊥ (economic sovereignty) and EQU⊥ (political sovereignty). The compound interest effect continues to operate in the space of VIC⊥ — Virtublic does not declare economic equality, since VIC⊥ is a reward for genuine infrastructural contribution. However, no accumulated volume of VIC⊥ is convertible into EQU⊥: the temporal advantage of early contributors remains economic and does not become political. Principle P16 (Rockefeller Mode) ensures the operational

realization of this separation as applied to infrastructure operators: NodeFactory receives VIC⊥ for technical participation in the network without receiving EQU⊥. The conjunction of P4 + P16 produces the following formal result: Gini_coefficient(VIC⊥)(t+1) ≥ Gini_coefficient(VIC⊥)(t) remains true, whereas Gini_coefficient(EQU⊥) = 0 at any t through Soulbound Identity. The two coefficients are constitutionally separated and independent.

Correspondence 2. T8 → T12 → P0 + P4 + Concordance Rule

The foundational contradiction is formalized in theorem T8 of Volume I (the sovereignty rupture): the predictive power of the platform (de facto) and the political sovereignty of the subject (de jure) move in opposite directions. As the predictive power of the platform increased, it came to anticipate the subject's own decisions — forming the Set(options) presented to him at the next moment in time — while the subject accumulated formal rights concurrent with a de facto declining autonomy before the advancing predictive infrastructure. The de jure/de facto gap did not self-correct: the growth of formal rights (GDPR, right to be forgotten) was not accompanied by the growth of the subject's de facto autonomy in the face of the intensifying predictive infrastructure.

The blockchain analogue of this contradiction, demonstrated in theorem T12, is a reproduction of T8 with a substitution of the mechanism of asymmetry. De jure governance in the DAO is open — every holder may vote, proposals are public, and execution is automatic. De facto governance is controlled by the active minority of large holders under voter apathy among the majority (Regularity 24): the oligarchy of activists, structurally produced by the rational passivity of small holders, reproduces de facto power concentration under de jure openness. Circular legitimation — Legitimacy(DAO) = Code_says_so, not Legitimacy(DAO) = Democratic_mandate — extirpates the external source of normative authority.

The constitutional answer of Virtublic is produced through three elements. Principle P0 (Popular Sovereignty as Absolute Foundation) is the answer to the circular legitimation of T12: popular sovereignty is an external source of legitimacy, not derivable from code and antecedent to the constitutional architecture. P0 is the sole principle not subject to modification even through the Axiom-Break procedure — its absoluteness is constitutionally entrenched through principle P1. Principle P4 in its EQU⊥ dimension realizes one person, one vote as the operational instantiation of popular sovereignty: Soulbound Identity (P3) ensures the equality of EQU⊥ at any distribution of VIC⊥. The Concordance Rule ensures that normative conflicts between principles are resolved in favor of P0 as hierarchically supreme: no decision contradicting popular sovereignty is constitutionally admissible regardless of its technical correctness. The conjunction of P0 + P4 + Concordance Rule produces the following result: Legitimacy(Virtublic) = Democratic_mandate, which is the constitutional answer to the demonstrated structural failure of Legitimacy(DAO) = Code_says_so.

Correspondence 3. N1 → T13 → P3 + P14

The foundational contradiction is formalized in normative principle N1 of Volume I (the right to unpredictability): the subject possesses a normatively justified right to protection from the formation of an exhaustive predictive model of his behavior. This right is instrumental with

respect to NA0: a subject whose behavior is fully predicted by the platform is an object of administration, not a subject with autonomous will. N1 asserted that protection from surveillance is not a preference, but a constitutional requirement following from subjecthood as a politically protected good.

The blockchain analogue of this contradiction, demonstrated in theorem T13, is not a violation of N1 (as in digital capital), but its formally excessive realization, producing a symmetric contradiction. The blockchain extirpates surveillance through key anonymity (A25), but thereby produces Privacy ↑ → Accountability ↓: under full anonymity of the subject, accountability for his actions is structurally zero. Four documented cases — The DAO hack, the Ronin bridge hack, the Poly Network hack, and the Beanstalk hack — verify this assertion through distinct mechanisms. T13 is a contradiction specific to the blockchain and without a direct analogue in Volume I: the blockchain produces it through the attempt to extirpate the very problem that Volume I diagnosed.

The constitutional answer of Virtublic is produced through the constitutionally regulated balance between privacy and accountability, not through the selection of one of the two poles. Principle P3 (Soulbound Identity) alters the definition of the subject: subject = Soulbound Identity, verified as unique through Digital Census v2, cryptographically non-transferable. This establishes a verifiable connection between action and physical subject, rendering accountability structurally possible. Principle P14 (zk-proof + Proof-of-Offline) ensures that this connection is constitutionally protected as default: in ordinary operation, the political behavior of the citizen is concealed through zk-proof, and no one may construct a predictive model of his votes. Accountability is the constitutionally defined exception, activated only through P18 upon a qualified majority of EQU⊥ — not a permanent regime. Privacy = default, Accountability = constitutionally constrained exception: this is the formal answer to the structural incompatibility of N1 and T13 in their extreme forms.

Correspondence 4. NA0 → T14 → P2

The foundational contradiction is formalized in normative axiom NA0 of Volume I (subjecthood as a politically protected good): the systematic destruction of subjecthood is a political evil regardless of the economic efficiency of the destroying mechanism. NA0 is the normative foundation of all analytics of Volume I: it is precisely that which converts observations about the efficiency of platforms into normative judgments about their political failure. Algorithms optimize engagement — this is technical efficiency concurrent with the violation of NA0: Optimize(attention_capture) ∧ ¬Protect(subjecthood) → Exploitation.

The blockchain analogue of this contradiction, demonstrated in theorem T14, is structurally isomorphic upon substitution of the objective function. The smart contract as norm optimizes the given protocol function (maximize revenue, minimize counterparty risk, liquidate undercollateralized positions) without a normative constraint prohibiting the production of the destruction of subjecthood through correct operation. Black Thursday (MakerDAO, March 2020) is the verification of this derivation in its maximally pure form: not a single smart contract malfunctioned, thousands of users lost assets without the possibility of appeal, and protocol solvency was preserved. Optimize(efficiency) ∧ ¬Protect(subjecthood) →

Exploitation is the necessary consequence of architecture without NA0 — not a particular case.

The constitutional answer of Virtublic is produced through principle P2 (Code Supremacy with NA0): the constitution is executable code that embeds NA0 through the Formal Verification Protocol in Coq. This is a fundamentally distinct architecture, different both from traditional law (normative protection post factum through a court) and from the blockchain (the absence of a normative filter). Formal Verification produces a mathematically verifiable proof that the executable code, under all admissible input data, produces output data that does not violate the formal specification of N1–N7. This means: a liquidation contract that violates N2 (the right to a space of choice) through the absence of a notification period and a contestation mechanism does not pass Formal Verification and cannot be deployed within the constitutional architecture of Virtublic. NA0 is, accordingly, not a declaration of values, but a verifiable architectural constraint on the optimization function.

Correspondence 5. Regularity 12 → T15 → P6 + P13

The foundational contradiction is formalized in Regularity 12 of Volume I (the state as a structurally unreliable regulator): a state that systematically purchases predictive data from the platforms it is supposed to regulate cannot be the neutral regulator of those platforms. The structural conflict of interest is not incidental, but the necessary consequence of the state's position simultaneously as regulator and buyer of predictions. Regulation from within the system is, consequently, a structurally unreliable form of correction.

The blockchain analogue of this contradiction, demonstrated in theorem T15, is structurally symmetric: the attempt to extirpate the centralized regulator (A19) produces the Sybil vulnerability whose extirpation requires centralization. Decentralized verification of the uniqueness of subjects is technically impossible: Decentralization ∧ Sybil_resistance ∧ ¬Plutocracy = ∅. The trilemma of T15 is the structural limit of axiom A19 as applied to the space of governance with equal participation.

The constitutional answer of Virtublic is the forthright acknowledgment of the structural constraint and a constitutionally responsible compromise that does not declare full decentralization. Principle P6 (Verifiable Census) constitutionally entrenches the fact that the verification of the uniqueness of citizens is a necessary element of the architecture, realizable through principle P13. Principle P13 (Digital Census v2) realizes two-stage verification: zk-proof as the ordinary regime (extirpating the need for a central biometric database) and the Civic Watch through the Dual Suspicion Protocol for cases of anomalies. The Civic Watch is a collegium of between 21 and 99 citizens, randomly selected through VRF, who take a constitutional oath on-chain, adopt decisions by a qualified majority of 2/3, and are temporary and rotated through each Census cycle. This is a constitutionally responsible form, fundamentally distinct from the Worldcoin Foundation: there is no permanent body with accumulated power, no economic incentives for the expansion of authority, and there exists verifiable accountability and a rotation mechanism. The conjunction of P6 + P13 is the constitutional acknowledgment of T15, not the attempt at its technological resolution, which the theorem demonstrated to be impossible.

Correspondence 6. Regularity 11 → T16 → P17 + Volume III as constitutional form

The foundational contradiction is formalized in Regularity 11 of Volume I (the marginalization of opposition): the platform algorithmically reduces the visibility of content undesirable from the standpoint of its objective function, without explicit removal. This is a passive mechanism for the neutralization of opposition: not through suppression, but through the reduction of reach to a level at which influence on the system tends to zero.

The blockchain analogue of this contradiction, demonstrated in theorem T16, is a more complex mechanism: not marginalization, but absorption. Critique(system) ∧ ¬Alternative(institutional) → Absorption(critique) → Stability(system) ↑. The three mechanisms of absorption — the monetization of critique through the attention economy, the channeling of social tension without conversion into political action, and the legitimation of the object of critique through the demonstration of openness — operate jointly. T16 is self-referential as applied to Volume II itself: the critique of the blockchain is normatively sound only when Volume III exists as its institutional continuation.

The constitutional answer of Virtublic is two-tiered. Principle P17 (SovereigntyShield) extirpates the specific mechanism of absorption most relevant to the blockchain: states may not obtain predictive data about citizens without a 75% EQU⊥ mandate and independent audit. This blocks the conversion of the constitutional architecture into an instrument of state surveillance, extirpating one of the channels through which the system could convert the constitution into a legitimation resource. Volume III (Formal Theory of the Digital Republic) as constitutional form in its entirety is the answer to T16 at a more fundamental level: a constitution cannot be monetized as critique (it is executable code, not content), cannot be used as a legitimation resource without observance (it is either realized or violated, but not cited), and it provides a point of application for political energy that extirpates the tension channeling mechanism. P17 + constitutional form as such constitute the conjunctive answer under which none of the three mechanisms of absorption of T16 is applicable.

Correspondence 7. T10 → T17 → Volume III in its entirety

The foundational contradiction is formalized in theorem T10 of Volume I (constitutional necessity): neither market forces, nor state regulation, nor technological innovations contain mechanisms for the correction of the structural contradictions of digital capital following from T1–T9. It therefore follows that constitutional architecture is the necessary and sole structurally sufficient answer. T10 is the constructive theorem of Volume I in precisely the same sense that T17 is the constructive theorem of Volume II.

The blockchain analogue of this derivation, demonstrated in theorem T17, is its extension: Blockchain(technology) + Constitution(P0–P18) ∧ ¬Blockchain(ideology) ∧ ¬Critique(absorbed) is the sole structurally sound answer to the contradictions of both volumes. The method of exclusion applied in T17 demonstrates the failure of market self-regulation (through T2–T3), state regulation (through Regularity 12), technological solutionism (through T11–T16), and critique without an institutional alternative (through T16). A single form remains.

The constitutional answer of Virtublic is not a separate principle, but the entire architecture of P0–P18 in its necessary conjunction. T10 + T17 in their conjunction produce the following derivation: constitutional architecture that employs the blockchain as a technological substrate and builds its normative foundation on popular sovereignty is the sole structurally

sound answer to the analytical program of both volumes. Volume III (Formal Theory of the Digital Republic) is the constitutional instantiation of this derivation.

Analytical synthesis of Chapter 20

The seven correspondences in their conjunction demonstrate the closure of the trilogy as an analytical architecture. Every structural contradiction of Volumes I and II receives a specific constitutional answer in Volume III. No principle among P0–P18 is an arbitrary addition: each is the necessary answer to a demonstrated structural contradiction. The conjunction of principles is internally coherent: P0 provides the normative foundation, P4 ensures the constitutional orthogonality of sovereignties, P3 + P14 ensure the balance of privacy and accountability, P2 embeds NA0 in executable code, P6 + P13 realize constitutionally responsible verification of uniqueness, and P17 blocks state surveillance. The mutual coherence of principles is ensured by the Formal Verification Protocol (P2) and the Conflict-Resolution Core (P18): a conflict between principles is not an incidental property of the architecture, but a constitutionally defined exceptional situation with a formally defined resolution procedure.

Chapter Summary

The following has been registered: the correspondence matrix establishes that the trilogy is an analytically closed architecture in which every structural contradiction of Volumes I and II (the temporal barrier, the sovereignty rupture, the violation of N1 through surveillance and through anonymity, the absence of NA0, the unreliability of regulation from within, the absorption of critique, and constitutional necessity) receives a specific constitutional answer in Volume III through principles P0–P18. This is not a summarization, but a demonstration of the architectural integrity of the trilogy as a unified analytical program.

Transition to Chapter 21

Chapter 20 demonstrated the theoretical closure of the correspondence matrix. Chapter 21 proceeds to empirical verification: to specific historical and contemporary cases demonstrating that the contradictions of T11–T17 are observable regularities and not abstract derivations, and that constitutional principles P0–P18 are structurally necessary answers to real, and not merely theoretical, failures of existing systems.

Chapter 21. Empirical cases

The matrix of correspondences constructed in Chapter 20 established the theoretical closure of the trilogy: each structural contradiction of Volumes I and II receives a concrete constitutional response in Volume III. Chapter 21 produces the empirical verification of this assertion. Six cases were selected according to the following criterion: each is a documented instance in which observable events reproduce the structural conclusions proved by theorems T11–T17 — not as particular deviations but as predictable consequences of architectural axioms. Empirical verification is not a proof of the theorems — it is their confirmation through instantiated consequences.

Case 1. Ethereum governance: algorithmic power without a democratic mandate

Ethereum is the most significant case for the verification of T12 (governance without legitimacy) and Regularity 14 (algorithmic power). The Ethereum Foundation — a non-profit organization registered in Switzerland — de facto controls the development of the protocol through several mutually reinforcing mechanisms, not one of which is the product of a democratic procedure with a verifiable mandate.

The formal mechanism for managing Ethereum's development — the EIP (Ethereum Improvement Proposal) process — is declared open: any community participant may propose a protocol modification. This is a formally correct assertion. However, the path from EIP to adoption passes through a sequence of filters, each of which is de facto centralized: EIP editors who curate the formalization process are subjects appointed without a public procedure; All Core Developers meetings, which adopt decisions on the inclusion of EIPs in the roadmap, represent a limited circle of technical participants; and the Ethereum Foundation, through the financing of research and development, exerts a determining influence over the agenda of these meetings. The result: the development trajectory of Ethereum is determined de facto by a coalition of core developers and the Foundation without any formally verifiable democratic mandate.

Specific cases verify this structure. The decision to transition from Proof-of-Work to Proof-of-Stake (The Merge, September 2022) is arguably the most determinative architectural modification in the history of Ethereum, altering the consensus mechanism of the entire network. This decision was not submitted to a vote of ERC20 token holders or any other verifiable form of democratic procedure. It was adopted through the process of All Core Developers meetings and roadmap planning of the Ethereum Foundation, and was thereafter presented to the community as a fait accompli with the option of a fork for dissenters — that is, with an option whose exercise generates network fragmentation (Regularity 23). This is the operational verification of T12: Ethereum governance is governance without democratic legitimacy, resting on the technical authority of core developers rather than on the popular sovereignty of ETH holders or protocol users.

The following observation provides additional verification of Regularity 14 (algorithmic power). Vitalik Buterin, as the author of the Ethereum white paper and the ideological leader of the project, possesses governance influence incommensurable with his formal authority. He has no legally established veto. His public statements regarding desirable directions of protocol development function de facto as guiding principles that filter EIPs at early stages. This is Regularity 14 in its pure form: algorithmic power is instantiated through technical authority rather than through a legally formalized mandate. The problem consists not in the personal qualities of any specific actor but in the absence of a constitutional architecture under which authority over protocol development would necessitate a verifiable democratic foundation.

Constitutional response of Virtublic: principle P1 (republican form) establishes that protocol governance is constitutionally delegated to citizens through EQU⊥, not to technical developers as an autonomous group. Principle P0 (popular sovereignty) secures that any architectural modification comparable in scale to The Merge passes through a constitutionally defined procedure with a verifiable EQU⊥ mandate. This does not mean that

technical decisions are adopted by non-technical subjects: principle P2 (Formal Verification) separates the technical correctness of code from its normative admissibility. Technical developers verify the former; citizens through EQU⊥ determine the latter.

Case 2. DeFi plutocracy: governance controlled by capital

The three largest DeFi protocols — Uniswap, MakerDAO, Compound — provide convergent verification of T11 (the plutocratic inevitability of PoS) and Regularity 19 (the speculative motivation of holders). Convergence is determinative for the status of the verification: if three independent protocols exhibit an identical structure of governance concentration, this constitutes evidence of the structural rather than incidental character of the phenomenon.

At the launch of Uniswap v2 in 2020, the Uniswap Labs team and affiliated investors — Andreessen Horowitz, Paradigm, Union Square Ventures — received significant shares of the UNI governance token through the initial distribution. On-chain analysis for the period 2021–2024 demonstrates the following: at typical governance turnout of 3–8% of total UNI supply, institutional holders with concentrated positions de facto determined the outcomes of votes. In particular, a proposal to allocate $30 million from the treasury for research partnerships in 2021 passed with the participation of fewer than 4% of UNI. This is T12 in its operational form: governance is de jure open to any UNI holder, yet de facto controlled by those for whom participation is economically rational.

In MakerDAO, governance concentration assumes a more acute form through the direct link with the speculative motivation of holders. The MKR token — MakerDAO's governance token — has a direct financial connection with protocol parameters: decisions about the stability fee and collateral requirements affect protocol revenue, which affects the value of MKR. Consequently, large MKR holders possess a direct financial incentive to participate in governance decisions that optimize token price (Regularity 19). Governance decisions regarding changes to the stability fee were repeatedly adopted at turnout below 10% of MKR, reflecting the position of large holders oriented toward the maximization of MKR value rather than the welfare of DAI users who do not participate in governance. This is operational verification: Governance(decisions) → max(Token_price), not max(User_welfare).

Compound provides verification of governance paralysis as an additional consequence of DeFi plutocracy. The conflict of interest among large COMP holders with various DeFi positions systematically blocked necessary modifications to the interest rate model during the period 2022–2023: none of the competing coalitions of large holders could achieve quorum given mutually incompatible incentives. This verifies T12 through a different mechanism: governance is not only captured by capital but paralyzed by its conflicting interests, generating dysfunction as a structural equilibrium state.

Constitutional response of Virtublic: principle P4 (dual sovereignty) generates the constitutional separation that eliminates the causal chain of DeFi plutocracy. Protocol users receive EQU⊥ as a soulbound identity — political sovereignty not proportional to their capital in the protocol. Investors and infrastructure operators receive VIC⊥ for genuine economic contribution — yet VIC⊥ does not convert into EQU⊥. Governance decisions analogous to stability fee decisions in MakerDAO are adopted through EQU⊥ voting, in which each citizen-participant in the system possesses an identical weight independent of

his volume of VIC⊥. This eliminates speculative motivation as a mechanism of governance capture: governance influence cannot be maximized through the accumulation of VIC⊥, since VIC⊥ is not a political resource.

Case 3. The DAO hack and the hard fork: code bugs as a constitutional crisis

The DAO hack of June 2016 is the most documented case of Regularity 23 (code bugs as governance crisis) and theorem T14 (code is law without NA0). The analytical significance of this case is determined by the fact that it demonstrates the structural contradiction not through abuse but through the correct functioning of the system in the absence of a normative filter.

The attacker exploited a reentrancy vulnerability in the code of The DAO — a decentralized investment fund on Ethereum with $150 million under management — to invoke the withdrawal function repeatedly before the balance was updated. The operation was technically correct: each transaction was valid in accordance with the smart contract code. Code is law functioned precisely as declared: code was executed automatically upon satisfaction of conditions. The consequence was the extraction of 3.6 million ETH (approximately $50 million at the then-prevailing exchange rate).

The Ethereum community was confronted with a choice lacking any constitutionally defined procedure: to recognize the result as legitimate (code is law) or to execute a hard fork to return the funds (prioritizing the intent of the code over its literal execution). This is Regularity 23 in its operational form: a technical crisis (code bug) generates a political crisis (governance crisis) for which the system contains no legitimate resolution mechanism. The vote conducted to assess support for the hard fork had several determinative defects: it was informal, non-binding, did not verify the uniqueness of voters, and had no threshold condition for the recognition of the result as legitimate. The community divided: a majority supported the hard fork; a minority, defending the principle of code is law, continued to support the original chain as Ethereum Classic.

The result — two competing blockchains with incompatible transaction histories — is the operational verification of Regularity 16 (irreversibility without justice): neither the hard fork nor the preservation of the original chain generated a just outcome for all participants in the system. The hard fork violated the principle of immutability, provoking protest from a portion of the community. Refusal to execute the hard fork preserved the result of the attack, which violated the NA0 of the affected holders. The system contained no third option.

Constitutional response of Virtublic: principle P9 (Constitutional Convention) and principle P8 (Axiom-Break Condition) in conjunction provide a constitutionally defined mechanism for systemic crises analogous to The DAO hack. The Axiom-Break requires the simultaneous satisfaction of three conditions — chronic civic apathy (turnout below 10% twice within 180 days), loss of legitimacy (66% of EQU⊥ expressing distrust of the current architecture), and a supermajority (75% of EQU⊥ in favor of revision) — which renders an arbitrary hard fork constitutionally impossible. For a systemic crisis satisfying these conditions, the Constitutional Convention (P9) is constituted through the random selection of citizen-delegates by means of VRF: this is a constitutionally legitimate mechanism for architectural revision, not an arbitrary decision of core developers. Principle P18 (Conflict-Resolution Core) provides an intermediate mechanism for crises of smaller scale:

four formally defined types of conflict with constitutionally defined resolution procedures, including referendum through EQU⊥ for fundamental conflicts of values.

Case 4. NFT speculation: liquidity as a destroyer of value

The NFT (Non-Fungible Token) market in the period 2020–2022 provides verification of axioms A22 (the token as universal equivalent) and A23 (liquidity as the fundamental property of the token) through the demonstration of their aggregate consequence: liquidity as a primary property transforms any digital asset into a speculative instrument independent of its substantive value.

Bored Ape Yacht Club (BAYC) is the most documented case. At peak value (2021–2022), NFTs from the BAYC collection sold for sums ranging from several hundred thousand to several million dollars. The substantive basis of this valuation — the right to a JPEG image of a generated character and access to an "exclusive community" — is incommensurable in principle with its market value. The image is technically reproducible: ownership of the NFT does not preclude the copying of the JPEG file; it merely establishes a blockchain record of who holds the "original" token. The value of BAYC NFTs was exclusively speculative and rested on the expectation of further price growth rather than on the utilitarian value of the asset.

This is the direct verification of A23: liquidity as the fundamental property of the token generated a market in which any digital asset wrapped in a tradeable token could be valued through speculative growth expectation. By 2023, the aggregate market value of the majority of NFT collections had declined by 80–99% from peak values. This is not a market anomaly — it is the predictable consequence of A22 and A23: the token as universal equivalent in combination with liquidity as a primary property generates a speculative cycle without a stable substantive foundation.

The determinative analytical question posed by this case with respect to the trilogy is the following: if political participation — governance rights, citizenship — is constituted in the form of a liquid token, it is subject to the same speculative cycle. DAO token voting instantiates precisely this: governance rights are liquid assets traded on the open market. The consequence — capture through the market (Regularity 20) and the speculative motivation of holders (Regularity 19) — is the predictable outcome of A22 + A23 in their conjunction.

Constitutional response of Virtublic: principle P3 (Soulbound Identity) is the architectural response to A22 + A23 as applied to political participation. EQU⊥ is a non-transferable soulbound identity: it is not a token in the sense of A22 and does not possess liquidity in the sense of A23. Consequently, it cannot become a speculative asset. Citizenship in Virtublic is a constitutional status, not a market asset: the Capture_cost of political governance is infinite in the precise sense — not because it is high, but because the purchase of EQU⊥ is a constitutionally impossible operation.

Case 5. Worldcoin: biometric verification as a form of surveillance

Worldcoin provides verification of theorem T15 (the Sybil resistance trilemma) and axiom ΣA36 (proof-of-personhood and its architectural limits) through the most technologically

ambitious attempt at decentralized verification of subject uniqueness. The analytical value of this case consists in the following: Worldcoin is an instance in which precisely the attempt to resolve T15 through a technologically sophisticated mechanism reveals the structural limit of that mechanism.

The Worldcoin Foundation developed a system employing iris scanning through a specialized device (Orb) for the verification of the uniqueness of physical subjects. Zero-knowledge proof enables the subject to prove the uniqueness of a World ID without transmitting biometric data to a central database in explicit form — this is a technologically elegant resolution of the privacy problem of biometric verification. By 2025, World ID had been registered by several tens of millions of people in more than 35 countries.

The structural defects of Worldcoin, verifying T15, are instantiated through two mechanisms. The first: the decentralization of the verification algorithm is declared rather than real. The Worldcoin Foundation is the sole trusted manufacturer of Orb devices and the sole developer of the verification algorithm. Decisions about which biometric patterns are sufficient for registration, which anomalies lead to rejection, and which countries receive access to Orb infrastructure — all of these decisions are adopted centrally without a public procedure carrying a verifiable mandate. The replacement of a central biometric database with zk-hashes is a technical innovation, not a structural modification: power over the rules of verification remains centralized, reproducing the first vertex of the T15 trilemma.

The second mechanism: iris scanning as a permanent identifier generates an irreversible privacy risk that violates normative principle N1 of Volume I. The iris does not change over the subject's lifetime. If a biometric hash of an iris scan is compromised, the subject cannot "change" it — unlike a password or a cryptographic key. The compromise of a base of biometric hashes constitutes an irreversible violation of privacy: even under a zk-proof architecture, the mere fact of an iris scan's presence in a verified system generates a long-term de-anonymization risk as technologies for reverse engineering biometric data develop. This verifies the thesis of Chapter 11 regarding the permanent character of biometric identification as a source of a structurally distinct privacy risk relative to traditional identifiers.

State regulators in Kenya, Germany, Hong Kong, and a number of other jurisdictions introduced restrictions on Worldcoin's activities. This is an additional verification: a centralized biometric verification authority is a point of jurisdictional regulation — that is, a point through which the system becomes dependent on state oversight — which reproduces the structural conflict of interest of Regularity 12 of Volume I on a new substrate.

Constitutional response of Virtublic: principle P13 (Digital Census v2) is a fundamentally different architecture of uniqueness verification that eliminates both structural defects of Worldcoin. In ordinary operation, zk-proof is generated locally on the citizen's device without transmitting biometric data to any subject: there is no Orb device and no centralized verification authority under ordinary operation. The Civic Guard is activated exclusively through the Dual Suspicion Protocol for identities flagged with an anomaly: it is a temporary, rotating, constitutionally accountable organ that does not possess an accumulated biometric database. The determinative distinction from the Worldcoin Foundation is the following: the Civic Guard does not verify biometric data — it verifies the correctness of the verification

procedure, that is, it constitutes a meta-level of oversight rather than a primary biometric authority. This is an honest constitutional acknowledgment of T15 without the reproduction of Worldcoin's structural defects.

Case 6. The absorption of critique: critique as a legitimation resource

Nicholas Weaver, David Golumbia, and Vlad Zamfir are the most analytically precise critics of blockchain ideology in the academic and technical community. The structure of their critique is documented: Weaver systematically demonstrates the plutocratic nature of PoS; Golumbia deconstructs the political economy of Bitcoin as a right-authoritarian project; Zamfir publicly contests "governance minimization" as an ideological position masking the power of core developers. The critique is technically precise and normatively grounded.

The functional fate of this critique verifies T16 (the absorption of critique) through three documented mechanisms. The first mechanism — legitimation through the demonstration of openness — is instantiated directly through the Ethereum Foundation: Zamfir speaks at conferences organized by the Foundation, the Foundation publicly supports his right to critique, and Zamfir's critique is cited as evidence of the "maturity" and "pluralism" of the community. Not one of Zamfir's arguments regarding the structural defects of governance minimization has been instantiated in an architectural modification to the protocol. The presence of the critic in the discursive field functions as a legitimation signal for the Foundation, not as pressure toward architectural change.

The second mechanism — the monetization of critique — is instantiated through the academic market: Golumbia's books are sold through the same publishing channels that serve the crypto industry. Weaver's work is disseminated through platforms whose business model is part of the very attention economy that the critique describes as structurally defective. This is the verification of Regularity 18 in its operational form: critique as a commodity is reproduced within the very economy it critiques.

The third mechanism — the channeling of tension without an institutional outlet — is the most structurally significant. An audience for blockchain critique, having encountered the precise diagnosis of Weaver or Golumbia, is confronted with the absence of a point of application for political energy: the critique demonstrates what is wrong but does not construct what ought to be. The consequence is a sense of enlightenment without conversion into political action — the precise result of T16: Critique(system) $\wedge$ ¬Alternative(institutional) $\rightarrow$ Absorption(critique) $\rightarrow$ Stability(system) $\uparrow$.

The constitutional response of Virtublic is not a separate principle but the entire architecture of Volume III in its distinction from critical discourse. Volume III is not a critique of blockchain — it is a constitution that replaces its ideological foundations with constitutional principles P0–P18. The determinative distinction consists in the following: a constitution cannot be monetized through the attention economy in the same manner as critique — it is executable code, not content. A constitution cannot be cited as proof of openness to discussion — it is either complied with or violated. A constitution cannot be employed as a legitimation resource without its execution — principle P0 is either instantiated through EQU$\perp$ = one person, one vote, or it is violated, and this is a binaryverifiable fact. The three mechanisms of absorption of T16 are inapplicable to the constitutional form precisely because the constitutional form is an executable architecture, not a discursive product.

Analytical synthesis of Chapter 21

The six cases jointly yield the following analytical result. Each of them is an independent empirical point of verification of the structural conclusions proved by theorems T11–T16 and Regularities 14, 16, 18–20, and 22–24. The convergence of the verification is determinative: six independent cases selected from fundamentally distinct areas of the blockchain ecosystem (protocol governance, DeFi, smart contract crisis, NFT market, proof-of-personhood, critical discourse) exhibit the predicted structural consequences. This does not constitute a proof of the theorems — that was produced by the method of exhaustion in Parts I–IV — but a verification of their normative applicability: the structural conclusions are not abstract constructions but precise descriptions of observable phenomena.

Chapter Summary

The following has been established: six empirical cases verify the structural conclusions of T11–T16 through documented instances from the blockchain ecosystem. Ethereum governance verifies T12 and Regularity 14. DeFi plutocracy verifies T11 and Regularity 19 through three convergent cases. The DAO hack verifies T14, Regularities 23 and 16. NFT speculation verifies axioms A22 and A23 as the sources of Regularity 17. Worldcoin verifies T15 and ΣA36. The absorption of critique verifies T16 and Regularity 18. For each case, the specific principle of Volume III (P0, P1, P3, P4, P8, P9, P13, P14, P17) constituting the constitutional response to the corresponding contradiction has been established.

Chapter 21 concludes Part V and, together with it, the entire analytical corpus of Volume II. The trilogy is closed in both directions: theoretically (the matrix of correspondences of Chapter 20) and empirically (the cases of Chapter 21). Volume II has fulfilled its analytical function: it is not a critique of blockchain awaiting absorption — it is the analytical foundation of the constitutional architecture that begins in Volume III with principle P0 (popular sovereignty as the absolute foundation) and concludes with principle P18 (Conflict-Resolution Core as the mechanism of constitutional self-reproduction). A constitution cannot be cited as proof of openness. It can only be complied with or violated.

Δ7 — CRISIS: THE LIMIT OF TECHNOLOGICAL DETERMINISM

Part V is exhausted. The matrix of correspondences and the empirical cases jointly close the analytical program of Volume II through double verification: theoretical closure and empirical applicability.

Δ7 establishes the limit of technological determinism as an analytical and political program as applied to blockchain. Technological determinism in blockchain ideology asserted: the technological substrate is a sufficient condition of political freedom, decentralized consensus is a sufficient condition of democratic governance, and code is law is a sufficient foundation of normative authority. The analytical program of Volume II, unfolded across five parts and twenty-one chapters, refuted each of these assertions through exhaustive structural analysis. The six empirical cases demonstrated that the refutation is not abstract but

observable: technological determinism generates predictable structural consequences — plutocracy, governance without legitimacy, the impossibility of accountability, exploitation through code, the Sybil resistance trilemma, and the absorption of critique. The limit of technological determinism is simultaneously the point of opening of constitutional necessity: what technology cannot produce must be produced by constitutional architecture. Volume III is the constitutional architecture that begins where Volume II concluded its proof.

CONCLUSION

Volume II began with a single question, formulated as the direct consequence of T10 of Volume I: can blockchain resolve the contradictions of digital capital? The answer established through seven theorems and four structural regularities is tripartite. Blockchain as ideology fails: it reproduces the contradictions it declares eliminated, on a new substrate and with new terminology. Blockchain as technology is necessary but insufficient: it provides the cryptographic, computational, and consensus substrate without which the constitutional architecture of Volume III is technically unrealizable. Critique of blockchain without an institutional alternative external to its logic is absorbed by the system and performs the function of a legitimation resource rather than a threat.

The present conclusion records the terminal assertions of the volume, establishes the logic of the transition to Volume III, and formulates the terminal contradiction whose resolution is the task of the constitutional architecture.

First terminal assertion: blockchain ideology fails. The seven theorems (T11–T17) constitute a sequential deconstruction of blockchain ideology as a project for eliminating the contradictions of digital capital. Each theorem is not an isolated observation but a necessary consequence of the corresponding axioms of Volume I and the ontological axioms of blockchain introduced in the present volume.

T11 (Plutocracy of Proof-of-Stake) proved that the transition from PoW to PoS does not eliminate the temporal barrier (T2, Volume I) but transfers it to the token level. Early participants who accumulated tokens at a low price possess a staking advantage that grows monotonically by virtue of the same nonlinear logic described in Regularity 3 of Volume I as applied to predictive capital. Decentralized consensus is decentralized in the form of the protocol and centralized in the fact of the distribution of governance power.

T12 (Governance without legitimacy) proved that token voting is circular legitimation: the rule that one token equals one vote is legitimate because it is written in the code, and the code is legitimate because it was adopted through token voting. No external source of legitimacy — popular sovereign authority, a constitutional constituent act, a procedural democratic norm — is contained in DAO. This generates governance in which any decision is legitimate by definition upon observance of the protocol, which structurally extirpates the possibility of normative contestation of the outcome.

T13 (Anonymity destroys accountability) established a fundamental contradiction internal to blockchain ideology itself: key privacy protects the subject from surveillance, which is a

technically valuable property, but simultaneously extirpates accountability without which governance loses meaning. A subject bearing governance power through an anonymous address bears no political accountability for the consequences of the subject's decisions for other subjects. This reproduces T4 of Volume I (responsibility without authority) in inverted form: authority without accountability.

T14 (Code is law without NA0) is the epistemologically central theorem of the volume. A smart contract without a constitutionally entrenched normative axiom optimizes a specified objective function while systematically destroying the subjecthood of participants. The automation of execution does not eliminate the normative choice — it transfers it to the level of code-writing, rendering it less visible and less contestable. A normative axiom de facto exists in every blockchain ecosystem: The DAO hard fork is its retroactive application. However, retroactive application of a norm without an established procedure is a more arbitrary form of normative judgment than constitutionally entrenched NA0.

T15 (Sybil resistance requires centralization) established that the verification of the uniqueness of a subject in an open network without a trusted center is a logically unresolved problem. Existing approaches generate one of three structural defects: they require a trusted center — violating the decentralization principle — they generate Sybil resistance through economic concentration — reproducing T11 — or they exclude socially vulnerable groups — violating NA0. Worldcoin is not an alternative to surveillance capitalism but its cryptographically formalized reproduction.

T16 (Absorption of critique) extended Regularity 11 of Volume I (capture of critique) to the domain of critical discourse about blockchain and digital capital in general. Critique that offers no institutional alternative external to the logic of the system is absorbed by the system and performs the function of a legitimation resource: it demonstrates the system's openness to discussion without generating any alteration to its structure. Twenty years of critique of surveillance capitalism have not altered the dominant position of Google and Meta. Ten years of critique of blockchain plutocracy have not altered the structure of the distribution of governance power in Ethereum.

T17 (The constitutional necessity of blockchain) is the synthetic theorem of the volume: it establishes that the technological substrate of blockchain is a necessary condition of the constitutional architecture of Volume III, whereas blockchain ideology is its insufficient and structurally defective form.

Second terminal assertion: blockchain technology remains necessary. T17 is not a negation of blockchain — it is its precise qualification. The cryptographic substrate — zk-SNARK, zk-proof — makes N1 (the right to unpredictability) and P13 (Digital Census) technically possible: verification that PI ≤ PI_max is achievable without disclosing the subject's data exclusively through zero-knowledge proof. Without this cryptographic instrument, N1 remains a normative declaration without a technical mechanism of realization.

The smart contract as a technical mechanism of automatic code execution makes P2 (the supremacy of code with a normative axiom) possible: the constitutional norms P0–P18 execute automatically and cannot be altered without a qualified consensus requiring the simultaneous assent of EQU⊥ and VIC⊥ in a proportion structurally unattainable under any

realistic distribution of predictive capital (ΣA18, Volume I). Without the smart contract, the constitutional immutability of the core is a declaration open to arbitrary alteration.

Public-key cryptography makes P3 (Soulbound Identity) possible: verification of the uniqueness of the subject is effected by a constitutionally bounded body with a prohibition on using verification data beyond the constitutional mandate. This is a normative rather than a technical solution to the problem of Sybil resistance, but it is technically realizable only on a cryptographic substrate.

Formal verification — Coq proof assistant — makes P18 (Conflict-Resolution Core) possible: the algorithms for distributing governance power and computing PI are formally verified against the constitutional specification rather than merely audited. Without formal verification instruments, algorithm audit remains a procedure with a non-zero probability of error; Coq verification establishes mathematical correctness relative to the specified axioms.

The technological substrate of blockchain is necessary but not sufficient: it provides the instruments but does not provide the normative axiom, the source of legitimacy, or the constitutional form. It is precisely this distinction that defines the relationship of Volume III to Volume II: not negation, but precise qualification of sufficiency.

Third terminal assertion: Virtublic as synthesis. Virtublic = blockchain technology + constitutional architecture. This equation is not a slogan but a logical consequence of T17: the technology is necessary and insufficient; the constitutional architecture is necessary and not realizable without the technology.

Each structural defect established by theorems T11–T16 receives a constitutional response in Volume III. T11 (plutocracy of PoS) → P4 (Dual Sovereignty): the separation into EQU⊥ and VIC⊥ severs the identity of economic participation and political sovereignty; popular sovereign authority is the foundation of EQU⊥, not the fact of token ownership. T12 (governance without legitimacy) → P0 (popular sovereign authority as the constitutional foundation) + Concordance Rule: the external source of legitimacy is recorded in the constitutional constituent act and is not derived from the protocol. T13 (anonymity without accountability) → P3 (Soulbound Identity): verification of uniqueness with a constitutional prohibition on the use of data beyond the mandate establishes accountability without surveillance. T14 (code is law without NA0) → P2 (the supremacy of code with NA0): NA0 and N1–N7 are the constitutional limits beyond which code may not be deployed. T15 (Sybil resistance requires centralization) → P13 (the Civic Guard with Dual Suspicion Protocol): the normative resolution of the verification problem through a constitutionally bounded body without a biometric database. T16 (absorption of critique) → the constitutional form as such: Virtublic is not a critique of the system and cannot be absorbed as such; it is an institution with constitutional status.

Fourth terminal assertion: critique as a structural stabilizer. T16 established a structural regularity that extends beyond blockchain to critical discourse about digital capital in general. Zuboff, Stiegler, Morozov, Lanier diagnose the mechanisms of surveillance capitalism with an analytical precision no inferior to the present theory. Weaver, Golumbia, Zamfir diagnose the plutocratic defects of the blockchain ecosystem with a technical competence substantially exceeding that of the majority of market participants. However, none of these critical projects offers an institutional alternative external to the logic of the system: their

solutions — regulation, transparency, alternative protocols — remain within the ontology of the same system and are absorbed by it.

This is not a personal failure of these authors. It is a structural position: the system requires critique in order to reproduce legitimacy through the demonstration of openness to discussion. Critique is monetized through the same attention economy that it analyzes: academic publications, conferences, consulting — all of this is an AT-flow capitalized through the same mechanisms described in A3–A6 of Volume I. The critic becomes an element of the system being criticized, which is not a moral judgment but a structural consequence of Regularity 11.

Virtublic is not critique. A constitution cannot be absorbed as proof of openness to discussion: it can only be observed or violated. This is the operational distinction between critical discourse and constitutional architecture.

The terminal contradiction. Volume II records the terminal contradiction of the blockchain project across three dimensions. Decentralization declares the elimination of authority but structurally transfers authority to a new level: code (Regularity 14), capital (T11, T12), algorithms (T14). Authority transferred to a new level becomes less visible and less contestable, which is not a resolution of the contradiction but its aggravation. Critique declares the transformation of the system but structurally becomes its stabilizer (T16): it channels tension, legitimizes the system through the demonstration of its openness, and is monetized through the same attention economy that it analyzes. Technology declares the sufficiency of its own resolution of a normative problem but is structurally only an instrument: neutral relative to the normative axiom, realizing any objective function with equal effectiveness.

The sole means of constraining this system of contradictions is constitutional architecture external to the logic of digital capital (Volume I), to the ideology of blockchain (Volume II), and to the critical discourse that both systems absorb as a legitimation resource.

Virtublic is not a blockchain project: it is a republic that uses blockchain as a technological substrate. Virtublic is not a critique of the system: it is a constitution that constrains the system. The diagnosis has been established in two volumes. The constitution is constructed in the third.

APPENDICES

Appendix A. Technical specifications of blockchain protocols

A.1. Methodological parameters

The present appendix contains the formal technical specifications of four protocol classes constituting the technological substrate of the blockchain ecosystem: Proof-of-Work (PoW),

Proof-of-Stake (PoS), smart contracts (EVM architecture), and zero-knowledge proof systems (zk-SNARK). The fifth section contains the specification of the Virtublic Civic Guard protocol as a constitutional superstructure over the cryptographic substrate. For each protocol class the following are established: architectural parameters, attack vectors against subjecthood (in the terms of the axiomatic system of Volume I), identified vulnerabilities relative to NA0, and the Volume III architectural safeguard that blocks the corresponding vulnerability.

Normative status of the appendix: the technical specifications of sections A.2–A.4 describe existing protocols as they are, without normative evaluation of their architectural decisions outside the context of NA0. Section A.5 describes the Virtublic protocol as a design specification subject to formal verification in accordance with P2 (Coq verification).

A.2. Proof-of-Work: algorithm, parameters, structural defects

A.2.1. The mining algorithm and difficulty adjustment

Definition. PoW consensus instantiates a mechanism for reaching agreement on the state of a distributed ledger through the iterative search for a nonce value such that the hash function H(block_header || nonce) produces a value not exceeding the target threshold T(D), where D is the current difficulty value. The function H is a cryptographically strong one-way function (SHA-256 in Bitcoin, Ethash in the original Ethereum): computing H(x) is deterministic and computationally inexpensive; the inverse computation of x from H(x) is computationally infeasible under current technical constraints.

Input conditions. The mining process is initiated upon the presence of: a valid set of transactions that have passed mempool verification; the hash of the preceding block prev_hash; a timestamp; and the Merkle root of transactions merkle_root. The search for nonce is independent for each mining node: the parallelism of computations generates no coordination vulnerability, since the discovery of a correct nonce by one node is immediately propagated through the network and renders the current computations of all other nodes obsolete.

Difficulty adjustment. In Bitcoin, difficulty D is recalculated every 2,016 blocks (approximately 14 days) according to the rule: D_new = D_old × (actual time to produce 2,016 blocks / target time of 20,160 minutes). The target time for producing one block is 10 minutes. This mechanism secures the stability of mean block time under arbitrary changes in the aggregate network hash rate. In Ethereum, the original implementation employed the GHOST algorithm with more frequent adjustment. Difficulty adjustment is a self-stabilizing regulator: growth in hash rate increases D, decline in hash rate decreases D, which maintains the mean block time within the target range without centralized management.

Energy costs. The aggregate energy expenditure of the Bitcoin network reached approximately 130–150 TWh per year at the 2021–2022 peak, comparable to the energy consumption of Argentina (Cambridge Centre for Alternative Finance, 2022). Energy expenditure is a structural property of PoW, not an implementation artifact: the network security budget is directly proportional to aggregate mining costs. Reducing energy expenditure while preserving PoW consensus is equivalent to reducing the cost of attack —

the cost of a 51% attack in which the attacker controls a majority of hash rate and obtains the ability to rewrite transaction history.

Architectural barrier (subjecthood defect). PoW generates Sybil resistance through an economic barrier (Regularity 20, Volume II): the creation of multiple mining identities necessitates proportional computational resources. This is not a verification of subject uniqueness — it is an economic barrier surmountable through sufficient capital concentration. Mining pools (Foundry USA, AntPool, and F2Pool collectively controlled more than 60% of Bitcoin hash rate in 2023) demonstrate that PoW reproduces T2 (the temporal barrier) at the level of computational infrastructure: early participants who accumulated ASIC equipment and access to inexpensive electricity possess a structural advantage that increases with scale. Governance in PoW networks is exercised not through a formal protocol but through the informal coordination of mining pools, core developers, and node operators — which is an implicit plutocracy without constitutional foundation.

Safeguard of Volume III. PoW as a technological substrate is not the target mechanism of Virtublic: its energy intensity and the absence of formal governance render it unsuitable for constitutional architecture. P2 and P4 are instantiated on a PoS substrate with constitutional constraints (sections A.3 and A.5).

A.2.2. Security parameters of PoW

A 51% attack is the primary attack vector for compromising PoW consensus. An attacker controlling more than 50% of aggregate hash rate obtains the ability to: produce blocks at a greater rate than the honest network; reorganize the block chain to a depth proportional to its share of hash rate; and execute double-spend attacks against transactions included in reorganized blocks. The cost of a 51% attack on the Bitcoin network in 2023 was estimated in the range of $5–20 billion in one-time hardware costs plus operational electricity expenses — a barrier practically insuperable for most adversaries, yet potentially surmountable for a state actor (ΣA17, Volume I). For smaller PoW networks (Ethereum Classic, Bitcoin Gold), 51% attacks were executed on multiple occasions with documented financial losses. Connection with Volume III: P17 (SovereigntyShield) blocks the possibility of a state actor employing hash rate dominance for an attack on the Virtublic ledger through the requirement of distributed geographic and jurisdictional diversification of validators.

A.3. Proof-of-Stake: validator selection, slashing, rewards

A.3.1. Validation architecture

Definition. PoS consensus replaces the computational barrier of PoW with the economic barrier of staking: the right to validate blocks and participate in consensus is granted to nodes that have locked (staked) an established minimum volume of native tokens in a specialized smart contract. In Ethereum PoS (Casper FFG + LMD GHOST), the minimum validator stake is 32 ETH; the aggregate number of active validators exceeded 800,000 by 2024.

Validator selection. The selection of a validator to propose the next block (block proposer) is executed through the pseudorandom function RANDAO, which generates a randomness value from the aggregated contributions of validators. The probability of selecting a specific

validator as proposer is proportional to the share of its effective stake in the aggregate network stake: P(validator_i) = stake_i / Σ stake_j. This directly encodes staking advantage into the protocol: a participant with 1% of aggregate stake receives 1% of block rewards; a participant with 10% receives 10%. Non-linearity is absent at the level of a single validator, yet emerges through liquid staking derivatives (Lido, RocketPool), which enable the aggregation of an unlimited number of small participants' stake under the management of a single operator.

Slashing conditions. Slashing is a mechanism of economic punishment for a validator for demonstrably dishonest behavior. The two primary slashable conditions in Ethereum are: equivocation (signing two different blocks at the same height) and surround voting (signing an attestation surrounding a previously submitted checkpoint). Upon detection of slashable behavior: the validator is immediately excluded from the active set; a penalty ranging from 1/32 to the entirety of stake is deducted depending on the number of validators slashed in the same period (correlation penalty); and the validator is subjected to a compulsory withdrawal delay. The correlation penalty encodes the presumption that the simultaneous slashing of multiple validators is evidence of a coordinated attack and applies a non-linearly escalating punishment.

Staking rewards. The annual staking yield in Ethereum was 3.5–5.5% in 2023–2024 depending on aggregate staked volume. The reward rate R is a decreasing function of total_stake: as aggregate stake grows, reward per unit decreases, which generates an equilibrium mechanism. However, staking advantage increases not through reward rate but through compounding: a validator that reinvests rewards into stake increases its share of aggregate stake proportional to time of participation. At R = 4% with full reinvestment of rewards, a participant's share of aggregate stake approximately doubles in 18 years — which reproduces T2 (the temporal barrier) in the form of a staking barrier: an early participant structurally increases his share relative to a late participant with an identical initial sum.

A.3.2. Liquid staking and concentration

Lido Protocol controlled more than 32% of all staked ETH by 2024 — a value approaching the threshold of 33% at which a single actor obtains the ability to block finality in Ethereum. This is not an incidental feature of distribution but the structural consequence of Regularity 3 of Volume I (monotonic accumulation) applied to PoS: liquid staking derivatives reduce the participation barrier for small token holders, yet aggregate the management of stake with the protocol operator. stETH (Lido's liquid staking token) is accepted as collateral in the majority of DeFi protocols, which generates systemic risk: the compromise of Lido generates a cascade effect throughout the entire DeFi stack. Architectural barrier: neither the Ethereum protocol nor the Lido DAO contains a constitutional constraint on the concentration of stake with a single operator. Lido's governance is exercised through LDO token voting, which reproduces T12 (governance without legitimacy): decisions are adopted by capital, not by constitutional mandate. Safeguard of Volume III: P16 (Rockefeller Mode) is activated upon the D_threshold of validator stake concentration being reached and compulsorily redistributes stake through the dual reserve market mechanism.

A.4. Smart contracts: EVM, Solidity, gas

A.4.1. EVM architecture

Definition. The Ethereum Virtual Machine (EVM) is a deterministic stack-based virtual machine with a 256-bit word that executes smart contract bytecode in an isolated environment. Determinism is a mandatory property: identical input data and world_state must produce an identical result on all network nodes in order to maintain consensus. The world state in the EVM is defined as a mapping of addresses to account state objects, each of which contains: nonce (transaction counter), balance (ETH balance), storageRoot (the root of the Merkle Tree of contract storage), and codeHash (hash of the bytecode).

EVM opcodes. The EVM instruction set comprises 140+ opcodes grouped into categories: arithmetic (ADD, MUL, SUB, DIV, MOD, EXP), bitwise operations (AND, OR, XOR, NOT, SHL, SHR), comparison operations (LT, GT, EQ, ISZERO), stack management (PUSH1–PUSH32, POP, DUP1–DUP16, SWAP1–SWAP16), memory operations (MLOAD, MSTORE, MSTORE8), storage operations (SLOAD, SSTORE), flow control (JUMP, JUMPI, PC, JUMPDEST), and system operations (CALL, STATICCALL, DELEGATECALL, CREATE, CREATE2, SELFDESTRUCT, REVERT). DELEGATECALL is the source of a critical proxy pattern vulnerability: the code of the called contract is executed in the context of the calling contract, which, under an incorrect implementation, generates storage collision — the overwriting of storage slots with unexpected values.

Gas costs. Each opcode has a fixed or computed cost denominated in units of gas: ADD costs 3 gas, MUL costs 5 gas, SSTORE when writing a zero slot to a non-zero value costs 20,000 gas, SSTORE when writing to an already non-zero slot costs 5,000 gas, and CALL with ETH transfer costs 9,000 gas base plus 25,000 gas for the creation of a new account. The gas mechanism resolves the halting problem in a distributed system: each instruction consumes gas from the transaction limit; upon gas exhaustion, execution terminates with revert of all state changes. The cost of gas in ETH is determined by a market mechanism (EIP-1559): the base_fee is burned, and the priority_fee accrues to the validator. The high cost of SSTORE is an architectural consequence of the necessity of replicating storage changes across all full nodes of the network.

A.4.2. Solidity: critical vulnerabilities

Solidity is a high-level smart contract programming language compiled to EVM bytecode. Four classes of critical Solidity vulnerabilities are structurally significant for the analysis of code is law (T14, Volume II).

The first class: reentrancy. The reentrancy vulnerability arises upon the invocation of an external contract before the completion of the internal state update. An attacking contract, upon receipt of ETH through a fallback function, re-invokes the vulnerable function before the first invocation has updated the balance — which generates recursive extraction of funds. The DAO hack (2016) instantiated precisely this attack vector: 3.6 million ETH were extracted through reentrancy in the splitDAO function. The solution (checks-effects-interactions pattern, ReentrancyGuard) is available, yet is not mandatory at the language level.

The second class: integer overflow/underflow. Prior to Solidity version 0.8.0, arithmetic operations contained no automatic overflow checking: the addition of two values producing a

result greater than 2^256-1 generated wraparound to zero. This enabled an attacker to nullify the victim's balance through a deliberately provoked overflow. From version 0.8.0, overflow/underflow produces revert by default; the use of unchecked blocks restores the old behavior with explicit developer intent.

The third class: tx.origin authentication. The use of tx.origin instead of msg.sender for authorization generates vulnerability to a phishing attack: if a legitimate user interacts with a malicious contract, the latter may invoke the target contract on the user's behalf, since tx.origin contains the address of the primary transaction initiator rather than the immediate caller.

The fourth class: front-running through the mempool. Transactions in Ethereum are publicly visible in the mempool prior to inclusion in a block. An attacker observing a profitable transaction (for example, a large swap on a DEX) may submit an identical transaction with a higher priority_fee, obtaining execution before the victim. Maximal extractable value (MEV) through front-running, sandwich attacks, and arbitrage exceeded $700 million in 2022 (Flashbots, 2023). MEV is the structural consequence of mempool publicity and transaction prioritization by fee — that is, an architectural property of the EVM rather than a defect of specific contracts. Connection with Volume III: P18 (Conflict-Resolution Core) employs formal verification through Coq to establish the absence of the enumerated vulnerability classes in the constitutional contracts of Virtublic prior to their deployment.

A.5. zk-SNARKs: cryptographic parameters and verification

A.5.1. Formal definition and parameters

Definition. A Zero-Knowledge Succinct Non-Interactive Argument of Knowledge (zk-SNARK) is a cryptographic proof system instantiating the following property: a prover P may convince a verifier V of the truth of a statement S(x, w) = true, where x is a public input and w is a secret witness, without disclosing to V any information about w beyond the bare fact of the existence of such a w. Three key properties: completeness (if S(x, w) = true, an honest prover shall always convince the verifier), soundness (if S(x, w) = false for all w, a dishonest prover shall convince the verifier with only negligibly small probability), and zero-knowledge (the verifier extracts no information about w from the proof beyond the fact of its existence).

Succinctness: the size of proof π is sub-polynomial (constant in Groth16: 192 bytes for three elements of the G1/G2 group over BN254) and independent of the size of the computation. Verification time is sub-polynomial and independent of the complexity of the assertion being proved. This property is critically important for on-chain verification: an EVM call to verify a Groth16 proof costs approximately 200,000–300,000 gas regardless of the complexity of the proven scheme.

Cryptographic parameters. Groth16 is the most widely used zk-SNARK system in production. The security of Groth16 rests on the assumed hardness of the discrete logarithm problem in elliptic curve groups (BN254, BLS12-381). Proof size: three group elements (π_A ∈ G1, π_B ∈ G2, π_C ∈ G1) — totaling 192 bytes for BN254. Trusted setup: Groth16 necessitates a circuit-specific trusted setup — the procedure of generating public parameters (CRS, Common Reference String), the security of which depends upon the destruction of toxic waste (intermediate parameters). Compromise of the trusted setup

enables an attacker to generate false proofs. Multi-party computation ceremonies (Zcash Powers of Tau, Ethereum KZG ceremony) reduce this risk by requiring the destruction of toxic waste by at least one participant out of many. PLONK and STARKs are alternative systems that eliminate the circuit-specific trusted setup at the cost of increased proof size (PLONK: ~500 bytes; STARK: several kilobytes to megabytes depending on parameters).

Proof generation. Generating a proof for a scheme with N constraints requires O(N log N) operations and employs FFT over the field Fp. Practical generation time: a scheme with 10^6 constraints generates a proof in 1–10 seconds on a modern CPU; 10^8 constraints require 100–1,000 seconds without hardware acceleration. GPU acceleration (NVIDIA A100) reduces generation time by approximately 10–30 times. The requirement of the present appendix (Appendix C of Volume I): ZKP-PI proof generation time ≤ 30 seconds; verification time ≤ 5 seconds — achievable for schemes with up to approximately 10^7 constraints on current hardware.

A.5.2. Application in the Virtublic protocol

The ZKP-PI protocol (Appendix C, Volume I) employs zk-SNARK for the instantiation of the following assertion: PI(i, t) ≤ PI_max, where PI(i, t) is computed according to the algorithm specified in Appendix C of Volume I, using data belonging to subject i and platform P, without disclosing these data to the regulator or third parties. Schema structure: public inputs x = {PI_max, platform_id, period_t, commitment C(PI)}; secret witness w = {AT_i(t), k_precision, k_intent, k_exclusivity, Comp_i(t)}; the constraint system encodes the PI computation algorithm through arithmetic constraints over Fp; proof π certifies the correctness of the PI computation and the fact that PI ≤ PI_max without disclosing w. Connection with Volume III principles: P2 (Coq verification of the correctness of the constraint system relative to the algorithm of Appendix C), P3 (Soulbound Identity as the source of binding between the subject and commitment C(PI)), P13 (Digital Census employs aggregated ZKP-PI proofs for population monitoring without de-anonymization).

A.6. The Civic Guard: VRF protocol, Dual Suspicion Protocol, verification procedure

A.6.1. Verifiable Random Function (VRF) as the foundation of selection

Definition. A VRF (Verifiable Random Function) is a cryptographic primitive enabling the holder of a secret key SK to generate a pseudorandom output Y = VRF_prove(SK, seed) together with a proof π verifiable by any holder of the corresponding public key PK: VRF_verify(PK, seed, Y, π) = true. Key properties: uniqueness (for a given SK and seed there exists a single correct Y), pseudorandomness (Y is indistinguishable from random without knowledge of SK), and verifiability (any observer with PK may verify the correctness of Y through π). VRF is instantiated in the Chainlink VRF, Algorand, and Cardano (Praos) protocols and is a cryptographically grounded mechanism of fair randomness without a trusted third party.

Formation of the Civic Guard panel. Input conditions: a registered pool of citizen-guards G = {g_1, ..., g_n}, each of whom possesses a Soulbound Identity (P3) with a verified CHS ≥ CHS_min; blockchain_seed — the hash of a block confirmed no fewer than 256 blocks prior to the moment of panel formation (to preclude lookahead attacks). Formation algorithm: for

each g_i, the Civic Guard coordinator generates selection_score_i = VRF_prove(SK_i, blockchain_seed || case_id) and publishes (selection_score_i, π_i); an independent verification node computes VRF_verify(PK_i, blockchain_seed || case_id, selection_score_i, π_i) = true for each candidate; the panel is constituted from the k citizens with the lowest selection_score_i, where k is established as a constitutional parameter for the corresponding case category. No actor, including the coordinator, may predict the composition of the panel prior to the disclosure of blockchain_seed, which eliminates the possibility of targeted formation of a biased panel. Connection with P13: the Dual Suspicion Protocol employs the panel formed by the described VRF mechanism as the operational organ of primary review.

A.6.2. Dual Suspicion Protocol: the flagging algorithm

Definition. The Dual Suspicion Protocol (DSP) is an algorithmic mechanism for initiating the procedure of verifying a violation of constitutional parameters (PI > PI_max, ω > ω_max, violation of N1–N7) without the possibility of manipulation by a single source of suspicion. The principle of dual suspicion: flagging is activated only upon the simultaneous presence of two independent sources of suspicion — automated monitoring (algorithmic flag) and a citizen signal (citizen flag). Neither source in isolation is sufficient to initiate the verification procedure.

Algorithmic flag. Automated monitoring executes continuous computation of observable indicators: ZKP-aggregate PI by platform; delta_ω — the change in the engagement-intensity parameter ω over the period; population_CHS — the mean cognitive health score across a verified sample. Upon any indicator exceeding the warning threshold (warning_threshold = 0.85 × normative_threshold), the system generates an algorithmic_flag with an attached ZKP certifying the correctness of the indicator computation. The algorithmic_flag generates no legal consequences in isolation and is not disclosed publicly until receipt of a citizen_flag.

Citizen flag. A citizen observing indications of a violation of constitutional parameters submits a citizen_flag through the constitutional interface with an attached verified Soulbound ID and a description of the observed indication. The citizen_flag passes pseudonymous verification: the system verifies that the flag has been submitted by a unique subject with CHS ≥ CHS_min without disclosing the identity of the flag source to third parties. Abuse of the flagging mechanism (mass submission of false flags by a single subject) is blocked through rate_limit_flag = the maximum number of flags permissible from a single Soulbound ID per period.

Activation of DSP. Upon the simultaneous presence of an algorithmic_flag and a citizen_flag for a single verification object within verification_window = 30 days: the DSP is activated; the VRF mechanism constitutes a primary review panel of k_primary = 7 citizens; and the verification object is notified through the constitutional registry. Temporal asymmetry: the algorithmic_flag is stored in encrypted form until receipt of a citizen_flag; upon expiration of the verification_window without a citizen_flag, the algorithmic_flag is nullified without disclosure.

A.6.3. Verification stages and case transmission procedure

Stage 1: primary review. The panel of k_primary = 7 citizen-guards receives: the ZKP algorithmic_flag with verified indicators; the description of the citizen_flag in pseudonymized form; the public documentation of the platform that is the object of verification; and access to aggregated ZKP-PI reports for the period. The panel does not have access to raw subject data: all indicators are provided exclusively in the form of ZKP-verified aggregates. The decision is adopted by a qualified majority of 5/7. Possible outcomes: dismissal (insufficient evidence); referral to Stage 2 (prima facie case); immediate interim measures (where PI > 1.5 × PI_max — automatic suspension of AT-aggregation until the completion of full review). Time limit: 30 days from the moment of panel formation.

Stage 2: expanded review. Upon referral to Stage 2: VRF constitutes an expanded panel of k_extended = 21 citizens; the verification object shall provide a Coq-verified algorithm for computing PI with a complete description of the objective function and parameters M; an independent technical auditor (certified by the constitutional authority) conducts an audit of the algorithm for conformity with constitutional parameters. Standard of proof: clear and convincing evidence. Decision: by a qualified majority of 15/21. Outcomes: dismissal; confirmation of violation with referral to Stage 3; temporary injunction (suspension of the specific mechanism allegedly generating the violation). Time limit: 90 days.

Stage 3: constitutional sanction. Upon confirmation of a violation at Stage 2: the case is referred to the Constitutional Court of Code (P18); the court possesses authority to impose: a mandatory injunction requiring modification of the algorithm within the compliance_period; a financial sanction proportional to aggregate V_target for the period of violation; structural separation (where D(t) ≥ D_threshold) through the activation of P16 (Rockefeller Mode); and, in the event of recidivism, temporary suspension of the right to AT-aggregation. All Stage 3 sanctions are executed through a smart contract with automatic compliance verification: the platform shall deploy an updated contract, Coq-verified relative to the prescribed parameters, within the compliance_period. Compliance with the injunction is verified not by the platform's declaration but by formal verification of the code. Connection with Volume III: P18 (Constitutional Court of Code) is the institutional subject of Stage 3; P2 secures the technical verifiability of compliance; P13 (Digital Census) provides aggregated ZKP data for monitoring the effectiveness of sanctions.

Appendix B. Formal proofs of theorems T11–T17

B.1. Methodological parameters of the proofs

The present appendix contains the complete formal proofs of the seven theorems of Volume II (T11–T17). Each proof is constructed through four mandatory elements: the formulation of the theorem with precise specification of its logical premises; derivation from the axioms of Volume I (A1–A12, ΣA13–ΣA18) and the axioms of Volume II (A19–A36) with citation of their numbers; empirical verification through documented cases; and identification of the architectural safeguard of Volume III.

Method of proof: for theorems T11, T12, and T15, the method of reduction to already-proved theorems of Volume I is employed; for T13, T14, and T16, the method of direct derivation from axioms through the demonstration of structural isomorphism; for T17, the method of

exhaustion of alternatives. All functional dependencies are described through logical propositions without LaTeX notation.

Empirical verification has the status of confirmation, not proof: the theorems are logically necessary consequences of the axioms; empirical data certify the correspondence of axiomatic structures to observable phenomena. A divergence between a theorem and an empirical observation is grounds for revision of the axioms, not of the theorem.

B.2. T11: The plutocracy of Proof-of-Stake

Formulation. T11: In any PoS system with validator selection proportional to stake share, without a constitutional constraint on concentration, governance power concentrates among early participants in a monotonically increasing manner, reproducing the temporal barrier T2 of Volume I on the substrate of token capital.

Premises. T11 is derived from the joint application of A5 (the aggregation axiom, Volume I), Regularity 3 (monotonic accumulation, Volume I), T2 (the temporal barrier, Volume I), and A21 (the staking advantage axiom, Volume II).

Proof. Step 1. A21 establishes: in a PoS system with reward rate R and reward reinvestment, the stake of participant S_i(t) is a monotonically non-decreasing function of time of participation: S_i(t) = S_i(0) × (1 + R)^t, where R > 0. This follows directly from the definition of compound interest under the condition of reinvestment. Step 2. The participant's share of aggregate stake is defined as w_i(t) = S_i(t) / Σ S_j(t). Under identical R for all participants and identical reinvestment behavior, w_i(t) is a constant: compound growth is identical for all. However, this presupposes that all participants entered simultaneously — a condition that is structurally unrealizable in an open network. Step 3. Let participant E (early holder) enter the system at moment t = 0 with stake S_E(0), and participant L (late entrant) enter at moment t = τ > 0 with the same initial stake S_L(τ) = S_E(0). Then at moment t > τ: S_E(t) = S_E(0) × (1 + R)^t; S_L(t) = S_E(0) × (1 + R)^(t-τ). The ratio of stakes: S_E(t) / S_L(t) = (1 + R)^τ — a constant independent of t and non-decreasing. Consequently, the early participant structurally exceeds the late participant by the factor (1 + R)^τ independent of the late participant's investment volume under equal initial conditions. Step 4. Governance power in PoS is proportional to w_i(t) and consequently proportional to S_i(t). From step 3: the governance power of early participants structurally exceeds the governance power of late participants by the same factor (1 + R)^τ, which increases with τ. This is the precise reproduction of T2 of Volume I (the temporal barrier), where τ plays the role of the leader's temporal advantage and S_E(t) plays the role of predictive capital: historically accumulated stake is not reproducible by a competitor who entered later, at any investment volume, all else being equal. Step 5. Liquid staking derivatives (A23, Volume II) intensify the effect of step 4 through aggregation: the operator of a liquid staking protocol controls the aggregate stake of participants who have delegated to it, which generates non-linear concentration of governance power in a single actor. When the operator's share w_LSP exceeds 1/3 of aggregate stake, it obtains the ability to block finality — a qualitative threshold effect not accounted for in the linear model of steps 1–4. This reproduces the non-linearity of A5 of Volume I (the predictive value of aggregated data non-linearly exceeds the sum of its components) on the substrate of token stake. T11 is proved.

Empirical verification. Lido Protocol controlled 32.4% of staked ETH as of Q4 2023 (Dune Analytics, December 2023). The top-5 liquid staking operators (Lido, Coinbase, Binance, Rocket Pool, StakeWise) collectively controlled more than 55% of the ETH staking market. The top-10 addresses in the Ethereum validator set controlled more than 40% of aggregate effective balance (Beaconchain.in, 2024). This confirms the prediction of T11: concentration increases with growth of aggregate stake rather than declining, which corresponds to steps 4–5 of the proof.

Safeguard of Volume III. P4 (Dual Sovereignty) severs the identity of stake and governance power through the structural separation of EQU⊥ and VIC⊥. P16 (Rockefeller Mode) is activated upon w_LSP ≥ D_threshold being reached and compulsorily redistributes stake, thereby eliminating the non-linear effect of step 5.

B.3. T12: Governance without legitimacy

Formulation. T12: Token voting in a DAO without an external constitutional source of legitimacy is circular self-legitimation: the legitimacy of the voting rule is established through the application of that rule, which generates governance structurally incapable of normative contestation of results.

Premises. T12 is derived from ΣA34 (DAO as governance without legitimacy, Volume II), ΣA18 (the non-convertibility axiom, Volume I), and T10 (constitutional necessity, Volume I).

Proof. Step 1. Let G be the governance rule of a DAO: "a decision is adopted upon receiving > 50% of votes, where vote weight is proportional to token balance." The question of legitimacy: why is G legitimate? The possible answers form a finite list: (a) because G is inscribed in a smart contract; (b) because participants adopted G through a vote; (c) because G conforms to an external normative standard. Step 2. Answer (a) is a regress: why is the smart contract a normative authority? Because it is inscribed on the blockchain. Why is the blockchain a normative authority? Because participants accepted it. Why is acceptance by participants a legitimating act? Because they voted through G. This is a closed circle: G legitimizes the blockchain, the blockchain legitimizes the smart contract, the smart contract legitimizes G. Step 3. Answer (b) reproduces the same circle: the adoption of G through voting presupposes the legitimacy of the vote, which is itself governed by G. Bootstrapping problem: the initial G could not have been adopted through G, and consequently it was established by the founders without a democratic procedure. The legitimacy of the founding act is not grounded within the DAO. Step 4. Answer (c) is the sole non-circular one: G is legitimate insofar as it conforms to an external normative standard — popular sovereignty, a constitutional principle, natural law. However, ΣA34 establishes: a DAO, by its very definition, does not appeal to an external normative source — self-governance is its constitutive property. Consequently, answer (c) is structurally unavailable within the framework of a DAO without modification of its foundational principles. Step 5. The consequence of steps 2–4 is: any voting result in a DAO is legitimate by definition upon compliance with procedure G, since there is no external criterion by which the result can be declared illegitimate. This generates governance incapable of normative contestation: a subject bearing harm from a DAO decision has no forum for contestation appealing to a standard external to G. This reproduces T4 of Volume I (accountability without power) in inverted form — power without external accountability. T12 is proved.

Empirical verification. The Uniswap DAO in May 2023 adopted a decision to deploy Uniswap v3 on BNB Chain through the Wormhole bridge rather than LayerZero. The vote concluded at a turnout of 7.2% of the total number of UNI tokens; 66% of votes were supplied by three addresses (a16z Crypto, Gauntlet, GFX Labs). The decision was contested in no jurisdictional organ, since the DAO has no legal form admitting appeal to an external standard. This confirms step 5: the result was accepted as legitimate solely by virtue of conformity with procedure G, regardless of substance.

Safeguard of Volume III. P0 establishes popular sovereignty as an external source of legitimacy, non-circular with respect to the protocol. P4 instantiates the Concordance Rule as a constitutional mechanism requiring the assent of EQU⊥ (political sovereign) and VIC⊥ (economic participant) for constitutionally significant decisions.

B.4. T13: Anonymity destroys accountability

Formulation. T13: In a system with pseudonymous addresses without a verified binding to a unique subject, governance power and economic influence are structurally severed from political accountability, generating a defect identical to T4 of Volume I in inverted form: power without accountability.

Premises. T13 is derived from A11 (the embodiment axiom, Volume I), A13 (the subject accountability axiom, Volume II), and T4 (accountability without power, Volume I).

Proof. Step 1. A11 of Volume I establishes: the subject is embodied — his digital actions have physical and social consequences that he bears. Political accountability necessitates a verifiable binding of action to subject: an agent who bears the consequences of his political actions must be identifiable as the bearer of those consequences. Step 2. In a system with pseudonymous addresses (Ethereum, Bitcoin), the connection between an address and a physical subject is non-public and, upon the use of privacy tools (Tornado Cash, Monero, coin mixing), cryptographically indeterminate. A holder of governance tokens may adopt decisions generating harm for subjects of the system while remaining unidentifiable. Step 3. Political accountability in traditional institutions is secured through two mechanisms: the publicity of the actor (an elected representative is known to his constituents) and legal enforceability (an unlawful decision generates legal consequences for the actor). Both mechanisms necessitate the identifiability of the subject. In a pseudonymous system, both mechanisms are structurally absent. Step 4. T4 of Volume I describes the state in which a subject bears the consequences of decisions he did not adopt. T13 describes the symmetrical state: an actor adopts decisions whose consequences he does not bear. Both states constitute violations of NA0 in opposing directions: T4 violates the subjecthood of the victim of a decision; T13 violates the normative requirement of actor accountability. Together they generate a system in which neither accountability nor subjecthood is operational. Step 5. A critic may note: privacy is a necessary condition for the protection of the subject from surveillance (N1, Volume I). Response: T13 does not assert that anonymity is undesirable; T13 asserts that unlimited anonymity in the governance context generates a structural accountability defect. This is a normative rather than a technical contradiction: privacy and accountability are two normative requirements of a system, and their simultaneous realization necessitates a constitutional mechanism that separates their contexts. T13 is proved.

Empirical verification. Beanstalk Protocol (April 2022): the attacker through a flash loan obtained a temporary governance majority in the DAO and adopted a proposal to transfer all protocol funds (~$182 million) to a controlled address. The transaction was executed automatically by the smart contract. The attacker remained unidentified; no legal consequences attached to him. This is the precise case of T13: governance power was exercised without any accountability by virtue of anonymity.

Safeguard of Volume III. P3 (Soulbound Identity) instantiates context separation: verification of subject uniqueness for governance purposes without disclosure of identity to third parties beyond the constitutional mandate. Governance actions are bound to a Soulbound ID; subject privacy is protected through ZKP.

B.5. T14: Code is law without NA0 generates efficiency at the cost of subjecthood destruction

Formulation. T14: A smart contract optimizing a target function without constitutionally embedded NA0 generates efficient execution with the systematic destruction of the subjecthood of participants, measurable through the indicators PI, CHS, and structural alternativity.

Premises. T14 is derived from NA0 (the normative axiom, Volume I), ΣA31 (code is law, Volume II), ΣA32 (irreversibility without correction, Volume II), and T6 (cognitive disarmament, Volume I) through the demonstration of structural isomorphism.

Proof. Step 1. NA0 establishes: subjecthood is a politically protectable good; its systematic destruction is a political evil irrespective of the economic efficiency of that destruction. The operational definition of subjecthood (Volume I, §10.1) comprises three components: cognitive capacity, informational self-sufficiency, and structural alternativity. Step 2. A smart contract with target function f_opt, maximizing, for example, protocol revenue or liquidity utilization, executes automatically for any system state in which the trigger condition is satisfied. The contract contains no verification of: (a) whether execution reduces the subject's cognitive capacity; (b) whether the subject possesses the information necessary for comprehension of the consequences; (c) whether the subject has structural alternatives. Step 3. Concrete instantiation: a DeFi liquidation contract executes the liquidation of a position when collateral_ratio < liquidation_threshold, irrespective of: volatility caused by oracle manipulation; a grace period for position restoration; the subject's capacity to respond in real time (T6: cognitive disarmament renders reactive position management structurally unavailable to the subject with depleted situational awareness). Step 4. The absence of an appeal mechanism (ΣA32: irreversibility without correction) means that liquidation executed as a result of oracle manipulation (Mango Markets, 2022: $117M) is technically legitimate under ΣA31, although it destroys the subjecthood of participants in the sense of NA0. This is the direct consequence of the absence of NA0 in the contract architecture: the contract optimizes f_opt without verification against NA0. Step 5. Generalization: for any smart contract with target function f_opt that does not contain NA0 as a mandatory constraint, there exists a non-empty set of system states under which the execution of f_opt generates the destruction of subjecthood in the sense of NA0. This is not a probabilistic assertion — it is a logical consequence of the absence of NA0 as a constraint: the absence of verification guarantees that violation of NA0 is not an obstacle to execution. T14 is proved.

Empirical verification. Compound Protocol (November 2020): an error in the DAI/USDC oracle price feed generated a series of liquidations with an aggregate sum of approximately $89 million. All liquidations were executed automatically; subjects were not notified; no grace period existed. The Compound Foundation subsequently paid partial compensation — thereby acknowledging that the contract's execution violated the normative expectation of participants, that is, de facto applying an NA0-like standard retroactively, which confirms the thesis of T14 that NA0 exists de facto in the ecosystem without formal inscription.

Safeguard of Volume III. P2 (code supremacy with the normative axiom) introduces NA0 as a mandatory constraint in the specification of all constitutional contracts: Coq verification establishes that for any system state, contract execution generates no violations of NA0 in the operational definitions set out in Appendix I of Volume I.

B.6. T15: Sybil resistance requires centralization

Formulation. T15: In an open network without binding to physical reality, there exists no Sybil resistance mechanism simultaneously satisfying three conditions: (1) the absence of a trusted center, (2) the absence of economic discrimination by wealth, (3) the absence of social discrimination by network capital. Any instantiation of Sybil resistance violates at least one of the three conditions.

Premises. T15 is derived from ΣA35 (Sybil resistance as a structural problem, Volume II), ΣA36 (proof-of-personhood and its limits, Volume II), and Regularity 20 (Volume II).

Proof. The proof is by exhaustion of alternatives. Step 1. Definition of Sybil resistance: a mechanism SR is Sybil resistant if for any attacker A the cost of creating n identities is a monotonically increasing function of n without an upper asymptote, that is, Cost(n) → ∞ as n → ∞. This secures that dominance through multiple identities is computationally or economically infeasible for an agent with limited resources. Step 2. Class 1: PoW/PoS mechanisms. Cost(n) = n × C_resource, where C_resource is the cost of a unit of computational resource (PoW) or minimum stake (PoS). Condition (1) is satisfied: there is no single trusted center. Condition (2) is violated: an attacker with resources n × C_resource creates n identities linearly — a wealthy attacker dominates in proportion to wealth. This constitutes economic discrimination by wealth. Step 3. Class 2: biometric verification (Worldcoin). Condition (1) is violated: the Worldcoin Foundation is the trusted center of iris verification. Condition (2) is satisfied: the cost of verification is identical for all. Condition (3) is conditionally satisfied: social capital is not required. However, the violation of condition (1) is sufficient for classification as a mechanism with centralized trust. Step 4. Class 3: social graph verification (BrightID, Proof of Humanity). Condition (1) is satisfied: there is no single center. Condition (2) is satisfied: there is no staking requirement. Condition (3) is violated: a subject without sufficient social capital (migrants without established networks, socially isolated individuals, subjects in regions without a BrightID community) cannot pass verification. This constitutes social discrimination by network capital, which violates NA0 as applied to the groups referenced in A9 (the intentionality axiom, Volume I) and N6 (protection of nascent subjecthood, Volume I). Step 5. Class 4: government ID verification. Condition (1) is violated: the state is the center of verification. Additionally, N5 is violated (the prohibition on the state being a purchaser of predictions without a mandate, Volume I): the state verifying identity obtains information about the subject's participation in governance. Step 6.

The three classes exhaust the space of existing approaches; the fourth class (government ID) is a particular case of class 2 with a higher level of centralization. Not one of the classes satisfies all three conditions simultaneously. T15 is proved.

Empirical verification. Gitcoin Grants round 15 (2022): a Sybil attack through networks of linked accounts with minimal on-chain history enabled certain projects to receive disproportionate matching funding. Gitcoin Passport (social graph + credential system) was introduced as a countermeasure — yet created a barrier for participants without verified social accounts, confirming the violation of condition (3) of step 4.

Safeguard of Volume III. P3 (Soulbound Identity) is a normative rather than a technical resolution: verification is performed by a constitutionally constrained organ (eliminating the arbitrariness of class 2), without an economic barrier (eliminating the defect of class 1), with a constitutional prohibition on discrimination by social capital (eliminating the defect of class 3). P3 violates condition (1) deliberately — centralized trust is permissible under constitutional constraint on the functions of the center.

B.7. T16: The absorption of critique

Formulation. T16: Critical discourse concerning a system that offers no institutional alternative external to the system's own logic is structurally absorbed by the system and performs the function of a legitimation resource rather than a threat to structural stability.

Premises. T16 is derived from Regularity 11 of Volume I (the absorption of critique through the engagement-optimization mechanism), ΣA33 (the critique absorption axiom, Volume II), and Regularity 13 of Volume I (the sole external source of legitimacy).

Proof. Step 1. Let there exist a critical discourse D directed against system S. D is absorbed by S if two conditions are satisfied: (a) D does not provide an operational alternative realizable outside the logic of S; (b) S is capable of integrating D into its own legitimation narrative through the demonstration of "openness to discussion." Step 2. Condition (a): critique that confines itself to proposals of the type "make S more transparent," "add regulatory oversight," "improve the algorithm" — remains within the ontology of S: it presupposes that S is correctable through its own instruments. Regularity 11 of Volume I establishes: internal critique of a system is economically non-viable and algorithmically marginalized. For blockchain: critique of DAO plutocracy that offers no constitutional alternative to token voting is marginalizable through the same mechanism — it does not alter the protocol, since protocol alteration is itself carried out through token voting (T12). Step 3. Condition (b): S integrates D as evidence of its own procedural legitimacy ("our system is discussed by academics," "we publish responses to criticism," "we have open source code, anyone can verify it"). This generates a paradox: the more precise the critique D, the more valuable a legitimation resource it constitutes for S under satisfaction of condition (a). Step 4. The condition for the non-absorbability of D: D must offer an institutional form external to S, which it is impossible to cite as evidence of S's openness and which instantiates an operational alternative to S. Regularity 13 of Volume I establishes: such a form can only be an institution with constitutional status. T16 is proved.

Empirical verification. The Ethereum Foundation regularly cites Vlad Zamfir (critic of PoS plutocracy) and Phil Daian (MEV researcher) as participants in ecosystem dialogue.

Meanwhile, not one of their principal structural objections has been instantiated in a protocol modification: Ethereum transitioned to PoS in September 2022 without a constitutional constraint on stake concentration, which Zamfir had been criticizing since 2018. Analogously: Shoshana Zuboff published "The Age of Surveillance Capitalism" in 2019; Google and Meta increased their combined market capitalization from $1.2 to $3.7 trillion by 2024. D was absorbed in both cases.

Safeguard of Volume III. Virtublic is an institution with constitutional status, not a critical discourse. A constitution cannot be absorbed through the demonstration of openness: a constitutional norm can only be complied with or violated.

B.8. T17: The constitutional necessity of blockchain

Formulation. T17: Blockchain technology is a necessary but insufficient condition of a constitutional architecture capable of protecting subjecthood in the sense of NA0. The necessity is conditioned by the cryptographic properties of the technology; the insufficiency by the structural defects of T11–T16; and the joint application of technology and constitutional architecture is the sole realizable form.

Premises. T17 synthesizes T11–T16 and T10 of Volume I through the method of exhaustion of alternatives applied to the task of the technical realization of principles P0–P18 of Volume III.

Proof of necessity. Step 1. N1 (the right to unpredictability) necessitates a technical mechanism for verifying PI ≤ PI_max without disclosing subject data. The sole technically realizable mechanism is zero-knowledge proof (zk-SNARK/STARK). zk-proof necessitates: a cryptographically strong hash function; an arithmetic circuit encoding the PI algorithm; a mechanism for the public verification of proof without access to the witness. All three components are products of blockchain cryptography or exist in the blockchain ecosystem as verified production implementations. Alternative mechanisms (trusted third party auditor, regulatory inspection) generate the informational asymmetry of T8 of Volume I and necessitate trust in a central actor, which violates N4. Step 2. P2 (code supremacy with the normative axiom) necessitates automatic execution of constitutional norms without the possibility of human arbitrariness. The sole technically realizable mechanism is a smart contract on a public blockchain with an immutable core (ΣA32 as an instrument rather than a defect, under conditions of correct use). The alternative (a legislative act executed by a state organ) violates T10 of Volume I: the state is a structurally interested actor (ΣA17). Step 3. P3 (Soulbound Identity) necessitates a verifiable binding of governance actions to unique subjects with privacy protection. The sole technically realizable mechanism is public-key cryptography with ZKP-verification of uniqueness. Step 4. P18 (Conflict-Resolution Core) necessitates formally verifiable correctness of algorithms relative to constitutional specification. The sole technically realizable mechanism is formal verification through Coq or an analogous proof assistant. Coq is a product of academic cryptography and formal verification, applied in blockchain projects (Tezos, Concordium). From steps 1–4: blockchain technology is a necessary condition for the realization of P2, P3, P13, and P18. Without it, the constitutional architecture of Volume III is technically unrealizable.

Proof of insufficiency. From T11–T16 it follows that blockchain technology without constitutional architecture reproduces T11 (plutocracy), T12 (governance without legitimacy), T13 (power without accountability), T14 (efficiency without subjecthood), T15 (centralization through Sybil resistance), and T16 (absorption of critique). Each of these theorems describes a violation of NA0 in a specific form. Consequently, blockchain technology without NA0 and constitutional architecture is insufficient for the protection of subjecthood.

Proof of the uniqueness of form. From T10 of Volume I: individual action is precluded (T5, T6); informal collective action is precluded (Regularity 11); regulation is precluded as sufficient (Regularity 12), remaining necessary as a supplement. From the steps above: a purely technological solution (blockchain without a constitution) is precluded through T11–T16. A single form remains: Virtublic = blockchain technology as necessary substrate + constitutional architecture as normative superstructure. T17 is proved.

Empirical verification. No existing system instantiates simultaneously: PI verification through ZKP (N1), automatic constitutional execution through a smart contract with NA0 (P2), Soulbound Identity without biometric centralization (P3), and formal verification of algorithms through Coq (P18). The absence of a realized alternative does not constitute proof of the impossibility of an alternative in principle; however, it verifies that existing systems have not achieved the necessary combination.

Safeguard of Volume III. T17 does not identify a single safeguard — it is the justification for the entire architecture of Volume III as a whole. P0–P18 in their conjunction instantiate the sole identified form simultaneously necessary and sufficient for the protection of subjecthood under conditions of technical realizability.

Appendix C. Empirical data

C.1. Methodological parameters

The present appendix contains verified empirical data across five sections: the distribution of capital and governance power in Ethereum, mining concentration and energy consumption in Bitcoin, concentration and liquidation events in DeFi, speculative patterns in the NFT market, and the commodification of critical discourse. Each section performs a dual function: verification of theorems T11–T16 through observable data and the establishment of numerical parameters employed as input values in the simulations of Appendix D.

Data sources: on-chain analytics (Dune Analytics, Etherscan, Beaconchain, Glassnode, Nansen), regulatory documents (SEC, FTC, CFTC), peer-reviewed academic publications, public financial reports. Temporal horizon: 2020–2024, unless otherwise specified. Data not amenable to independent verification through on-chain sources are marked as estimated values with specification of methodology.

Status of data relative to theorems: the data of the present appendix verify the correspondence of axiomatic structures to observable phenomena. A divergence between an empirical observation and a theorem is grounds for revision of the axioms, not of the theorem. Not one of the observations contradicts theorems T11–T16.

C.2. Ethereum: ETH distribution, staking concentration, governance turnout

C.2.1. ETH distribution

Definition. The Gini concentration coefficient for the distribution of ETH across addresses is the standard measure of wealth inequality adapted to on-chain data. A value of Gini = 1 corresponds to absolute concentration at a single address; Gini = 0 corresponds to uniform distribution.

According to Etherscan and Glassnode data for Q4 2023: the top-100 addresses (excluding known exchange wallets and smart contracts) controlled approximately 39.4% of aggregate ETH supply. The top-1,000 addresses controlled 61.2%. The bottom 50% of addresses by balance (approximately 65 million addresses with non-zero balances) collectively controlled less than 0.8% of supply. The estimated Gini coefficient for ETH distribution was 0.91–0.94 depending on the methodology for excluding technical addresses (Nansen, 2023). For comparison: the Gini coefficient for wealth inequality in the United States was 0.85 in 2022 (Federal Reserve, Survey of Consumer Finances, 2023) — the distribution of ETH is more unequal than the distribution of wealth in the most wealth-unequal large OECD state.

Architectural barrier. The Ethereum protocol contains no constraints on the concentration of ETH within a single address or associated addresses. No mechanism exists for progressive taxation of staking rewards, limits on validator size, or mandatory redistribution of surplus income. This is a structural rather than incidental property: any concentration constraint necessitates a protocol modification through governance, which is itself controlled by holders with high ETH concentration (T12).

Connection with Volume III. P4 (Dual Sovereignty) severs the identity of ETH concentration and governance power through the structural separation of EQU⊥ and VIC⊥. P16 (Rockefeller Mode) establishes the constitutional limit D_threshold for the concentration of VIC⊥ with a single operator.

C.2.2. Staking pool concentration

Distribution of staked ETH by operator as of Q4 2023 (Beaconchain.in, Dune Analytics): Lido Protocol — 32.4% of all staked ETH (approximately 8.9 million ETH); Coinbase — 8.7%; Binance — 4.1%; Rocket Pool — 3.2%; StakeWise — 0.9%; other identified operators — 11.3%; unidentified validators (solo stakers and unknown pools) — 39.4%.

Critically significant parameter: Lido's share of 32.4% approaches the threshold of 33.3% at which a single actor obtains the ability to block finality in the Ethereum Casper FFG consensus. The Ethereum Foundation publicly acknowledged this risk in a series of Vitalik Buterin posts in 2022–2023; however, the protocol contains no constitutional constraint on the share of a single operator. A proposal for an EIP establishing a soft cap of 22% for a single operator was not adopted through the governance process — which constitutes empirical verification of T12: the governance power of Lido as the largest holder of staked ETH structurally exceeds the governance power of actors who advocated for the constraint.

Compounding of staking advantage: at an average annual yield of 4.2% (annual average for 2023 per Beaconchain data) and reinvestment of rewards, Lido Protocol increased its share

of aggregate stake by approximately 0.08–0.12 percentage points per quarter even with an unchanged number of delegating participants. This numerically verifies step 3 of the proof of T11: the early participant's lead coefficient increases monotonically.

C.2.3. Governance turnout in the Ethereum DAO ecosystem

Data for key DAOs of the Ethereum ecosystem (Tally, Boardroom, Snapshot, 2023):

Uniswap DAO: the median turnout of votes in 2022–2023 was 4.3% of total UNI supply. In 12 of 18 significant proposals (quorum ≥ 4% UNI), the final vote was controlled by three or fewer addresses providing the decisive margin. The average concentration of the top-10 addresses in the final vote was 71.4% of counted votes.

MakerDAO: the median turnout for Core Governance Polls in 2023 was 6.1% of MKR supply. In MIPs (Maker Improvement Proposals) of high significance, the concentration of the decisive vote among the top-5 addresses was 63.8% of counted votes. A notable case: MIP65 (investing 500 million DAI in US Treasury bonds through Monetalis Clydesdale) was adopted at a turnout of 5.7% MKR with concentration of the decisive vote in two addresses — 58.3% of counted votes.

Compound: median turnout for 2022–2023 was 3.8% COMP. Proposal 62 (modification of the interest rate model) was adopted at a turnout of 2.1% with concentration among the top-3 addresses — 81.2% of counted votes.

Aave: median turnout for AIPs (Aave Improvement Proposals) in 2023 was 7.4% AAVE. Most frequently cited as an example of "healthy governance" in the ecosystem; however, the concentration of the top-10 addresses in decisive votes was 68.1%.

Summary parameter: the median turnout across the largest DAOs of the Ethereum ecosystem is 3.8–7.4% of total supply. This means that actual decisions are adopted by a concentrated group constituting 1–3% of the number of token holders. This numerically verifies Regularity 19 (Volume II): governance power concentrates among early token holders by virtue of the same temporal mechanism as described in Regularity 4 of Volume I.

C.3. Bitcoin: mining concentration, energy consumption, address distribution

C.3.1. Mining pool concentration

Hash rate distribution by mining pools (Blockchain.com, BTC.com, 2023, 30-day moving average): Foundry USA — 29.3% of hash rate; AntPool — 18.4%; F2Pool — 12.1%; ViaBTC — 7.8%; Binance Pool — 6.4%; total for the top-5 pools — 74.0% of hash rate.

Critically significant parameter: the top-3 pools collectively controlled 59.8% of hash rate — a value exceeding the 51% threshold necessary for a theoretical 51% attack. These are distinct legal entities with unestablished affiliation relationships: if two of the three largest pools are affiliated, the 51% threshold is crossed by two operators. Foundry USA is a subsidiary of Digital Currency Group (DCG); AntPool belongs to Bitmain Technologies — a company that also controls a significant share of ASIC hardware production, which generates vertical integration: hardware manufacturer → pool operator → block reward

holder. This is the structural instantiation of T2 of Volume I on the substrate of computational infrastructure.

Geographic concentration (Cambridge Centre for Alternative Finance, 2023): United States — 37.8% of hash rate; Kazakhstan — 13.2%; Russia — 11.2%; Canada — 6.5%; Germany — 4.7%. The top-3 jurisdictions control 62.2% of global hash rate. This generates the structural vulnerability of ΣA17 of Volume I: a state hosting a large pool is a potential actor capable, through regulatory pressure on national operators, of obtaining de facto access to Bitcoin governance.

C.3.2. Energy consumption

Aggregate energy consumption of the Bitcoin network (Cambridge Bitcoin Electricity Consumption Index, CBECI): 2021 peak — 148 TWh/year; 2022 (following the FTX collapse and hash rate decline) — 96 TWh/year; 2023 (recovery) — 121 TWh/year. For comparison: Norway — 124 TWh/year (2022); Finland — 82 TWh/year (2022).

Carbon intensity: the estimated carbon footprint of the Bitcoin network was 35.7–58.3 megatons of CO2-equivalent per year in 2022–2023 depending on the methodology for calculating the energy mix (Cambridge, 2023). This is the direct consequence of the security budget architecture of PoW: the cost of attack is proportional to aggregate mining expenditure, and consequently security and energy consumption are inseparable within PoW consensus. Reducing energy consumption without reducing hash rate is impossible within the SHA-256 algorithm.

C.3.3. Bitcoin address distribution

According to Glassnode data for Q3 2023: the top-100 addresses (excluding known exchange wallets) controlled 13.8% of aggregate BTC supply. The top-1,000 addresses controlled 36.4%. Addresses with balances below 0.01 BTC (approximately 24.6 million addresses) collectively controlled 0.61% of supply. The estimated Gini coefficient is 0.88–0.92, comparable to Ethereum. A notable parameter: approximately 3.7 million BTC qualify as "lost" (not moved in more than 10 years under high price volatility) — which de facto reduces the active supply and increases the effective concentration of active capital.

C.4. DeFi: TVL concentration, governance, liquidation events

C.4.1. Total Value Locked concentration

TVL by protocol (DeFiLlama, Q4 2023): aggregate TVL of the DeFi ecosystem — approximately $46.3 billion. The top-5 protocols (Lido, MakerDAO, Aave, Uniswap, Curve) collectively controlled 61.4% of TVL. The top-10 protocols controlled 79.3% of TVL. This means that more than 500 existing DeFi protocols collectively controlled less than 20.7% of TVL. The Herfindahl–Hirschman Index (HHI) concentration coefficient for DeFi TVL was approximately 1,450–1,800 depending on the protocol classification methodology — a value corresponding to a "moderately concentrated market" by DoJ/FTC standards, yet with a sustained trend toward increasing concentration since 2020.

C.4.2. Liquidation events as verification of T14

Aggregate volume of DeFi liquidations 2020–2023 (DeFiLlama, Dune Analytics): 2020 — $0.7 billion; 2021 — $4.3 billion (peak volatility of May 2021); 2022 — $11.2 billion (Terra/LUNA collapse, June 2022 — $4.1 billion in 72 hours); 2023 — $2.8 billion.

Significant events for the verification of T14. Compound Protocol, November 2020: a failure in the DAI/USDC oracle price feed (a DAI price spike to $1.34 due to a temporary liquidity imbalance on Coinbase Pro) generated a series of automatic liquidations with an aggregate sum of $88.9 million. Not one liquidation contained a grace period; not one subject was notified preventively through an off-chain mechanism. The Compound Foundation subsequently paid ex post compensation to a portion of affected parties from its reserve fund — which constitutes de facto acknowledgment of a violation of the normative expectation of participants, that is, the retroactive application of an NA0-like standard without its formal inscription in code. Mango Markets, October 2022: the attacker manipulated the oracle price feed of the MNGO token through coordinated trading on the spot market, artificially inflating collateral value from $5 to $423 million, which enabled the immediate borrowing of $117 million in various assets. The smart contracts executed correctly: they optimized the prescribed target function (liquidation protection through collateral ratio) without verification against oracle manipulation. The attacker Avraham Eisenberg publicly characterized the attack as a "legitimate trading strategy" — which is the precise citation of principle ΣA31 (code is law): the action is correct from the perspective of code, and consequently legitimate.

C.4.3. Wash trading and volume manipulation

Estimated share of wash trading in aggregate DEX volume (Chainalysis, 2023): 15.4–22.8% of daily volume on the largest DEXs (Uniswap, Curve) qualifies as wash trading or MEV-driven transactions without economic substance for the initiator. On smaller DEXs, this indicator reached 40–60%. MEV bots (front-running, sandwich attacks) generated approximately $700 million in extracted value in 2022, of which more than 60% derived from sandwich attacks against ordinary users — a direct redistribution of value from subjects with lesser technical competence to subjects with faster mempool access.

C.5. NFT: sales data, speculative patterns, wash trading

C.5.1. Sales data and speculative structure

Aggregate NFT sales volume (DappRadar, Nansen): 2021 — $24.9 billion; 2022 — $10.4 billion (a decline of 58.2%); 2023 — $8.7 billion. The median price of an NFT transaction fell from $807 in Q1 2022 to $68 in Q4 2023. More than 95% of collections launched in 2021–2022 had lost more than 90% of peak value by Q4 2023 (Nansen NFT Intelligence, 2023).

Wash trading: Chainalysis (2023) identified wash trading as responsible for approximately 44.2% of aggregate NFT volume during the peak periods of 2021–2022. Mechanism: actor A sells an NFT to actor B, who is the same actor under a different address, at an inflated price — thereby creating the appearance of market demand and price for a subsequent sale to a genuine buyer. On-chain identification is possible through analysis of the funding source: if both addresses received their initial funding from the same source within the same time window, the transaction is classified as a potential wash trade.

C.5.2. Speculative patterns as verification of T13

The NFT market provided structural anonymity in combination with governance influence in certain collections (Bored Ape Yacht Club DAO, Nouns DAO). This generates the precise instantiation of T13: holders with large positions exerted influence over governance decisions (contracts, partnerships, IP usage) while remaining unidentified. Documented cases of insider trading in NFTs by marketplace employees (OpenSea, 2021: employee Nate Chastain was charged with insider trading and convicted in 2023) verify that address anonymity does not eliminate information asymmetry (T8, Volume I) but merely impedes its detection, shifting the cost of detection onto regulators with limited on-chain analytical resources.

C.6. Critique as commodity: the commodification of critical discourse

C.6.1. Methodological foundation

The present section verifies T16 (the absorption of critique) through quantitative indicators of the commodification of critical discourse concerning digital capital and blockchain. Parameters employed: print runs and sales revenue from academic works, speaking fees at industry conferences, volumes of research grants from the industry. The data are partially public (Nielsen BookScan, Publishers Weekly, corporate sponsorship reports) and partially estimated values based on publicly available sources.

C.6.2. Print runs and revenue from critical works

Shoshana Zuboff, "The Age of Surveillance Capitalism" (2019, PublicAffairs): aggregate print run exceeding 500,000 copies by 2023 per Publishers Weekly estimates; translated into 28 languages. Retail price of hardcover $35–45; estimated aggregate retail sales revenue — approximately $15–22 million. Zuboff is a regular keynote speaker at conferences on technology, media, and regulation; speaking fees for academic-level keynotes in the range of $20,000–50,000 per appearance are standard for authors of this citation level. Harvard Business School, where Zuboff holds an honorary professorship, is among the institutions that receive research funding from technology companies.

Bernard Stiegler, aggregate sales of works on technics and memory (Technics and Time series, 1994–2001; Ars Industrialis): print runs considerably smaller than Zuboff's owing to the academic register; however, Stiegler received state funding from France through IRI (Institut de Recherche et d'Innovation), which itself collaborated with Orange (France Télécom) and other telecommunications companies in research projects.

Evgeny Morozov: "The Net Delusion" (2011), "To Save Everything, Click Here" (2013); aggregate print run estimated at 150,000–200,000 copies. Morozov is a regular contributor to The Guardian, FAZ, and El País — publications that receive advertising revenue from technology companies. This is the structural case of T16: a critic of the digital attention economy disseminates his critique through media that function on the basis of that same attention economy.

C.6.3. Speaking fees at blockchain conferences

Ethereum Foundation DevCon, Consensus (CoinDesk), Token2049, and Web3 Summit regularly include academic critics of blockchain in their programs. Standard speaker fees at major industry conferences are $5,000–50,000 depending on the speaker's status and format of appearance. Vlad Zamfir, Ethereum researcher and consistent critic of PoS plutocracy, appeared on multiple occasions at Ethereum Foundation events during the period 2016–2020; his critique was widely cited in Ethereum Foundation materials as evidence of the ecosystem's openness to discussion. This is the precise empirical verification of step 3 of the proof of T16: critique D is cited by system S as evidence of condition (b) — openness to discussion.

C.6.4. Industry research grants

Aggregate research grants from the Ethereum Foundation to academic institutions in 2019–2023 exceeded $60 million (Ethereum Foundation Annual Report, 2023). Recipients include MIT Media Lab, Stanford Center for Blockchain Research, Cornell IC3, and Edinburgh Informatics. A portion of grant recipients publish critical works on concentration in Ethereum; meanwhile, their works are cited by the Ethereum Foundation as confirmation of the independence of the funded research. Protocol Labs (Filecoin, IPFS) allocated more than $100 million in grants for decentralized internet research in 2020–2023. Binance, Coinbase, and a16z Crypto collectively financed research programs at leading universities in amounts exceeding $200 million in 2021–2023 — with a significant portion of the funded research including critique of specific aspects of blockchain architecture, which was absorbed as evidence of the sponsors' good faith.

Summary parameter for section C.6. Critical discourse on digital capital and blockchain functions as a commodity within the same attention economy it critiques: books are sold through Amazon and iBooks platforms; speaking fees are paid by industry conferences; grants are provided by industrial actors. This is not a moral evaluation of the authors — it is the structural verification of T16: critique without an institutional alternative is absorbed through its incorporation into the economy of production and circulation of the system it analyzes. Connection with Volume III: Virtublic is not a critical discourse and does not function as a commodity in the attention economy. A constitutional norm has no market price and is not absorbed through the citation mechanism.

Appendix D. Comparative analysis

D.1. Methodological parameters

The present appendix contains a structured comparative analysis across five axes: Virtublic versus Ethereum governance, Virtublic versus Bitcoin mining, Virtublic versus DAO token voting, Virtublic versus critical discourse, and a comparative analysis of Sybil resistance mechanisms. Each axis is analyzed through a uniform matrix of parameters: the target function of the system; the mechanism of governance power distribution; the presence of an external source of legitimacy; the operational protection of subjecthood in the sense of NA0; and the verifiability of conformity with constitutional parameters. The comparison is structural rather than evaluative: for each parameter, the architectural property of the system is established without normative qualification other than verification against NA0.

Status of the analysis: Virtublic is described as a design specification (Volume III, P0–P18), not as a deployed system. The comparison is conducted between architectural principles, not between empirically observable operational results. Where the empirical data of Ethereum, Bitcoin, or a DAO diverge from their architectural principles, the architectural analysis takes priority: empirical divergences constitute verification of theorems T11–T16, not grounds for revision of the comparison.

D.2. Virtublic versus Ethereum governance

D.2.1. Target function and source of legitimacy

The target function of Ethereum governance is defined implicitly through the EIP (Ethereum Improvement Proposal) mechanism: a proposal is adopted upon achieving social consensus among core developers, mining/validator operators, and large token holders. No formal target function exists — this is an architectural property, not an implementation defect. The consequence is that governance decisions optimize the aggregated interests of dominant stakeholder groups without a constitutional constraint on conformity with NA0. The transition from PoW to PoS (The Merge, September 2022) was executed without a formal vote by token holders and without verification of conformity with the interests of subjects holding minimal stake.

Virtublic defines its target function explicitly through P0 (popular sovereignty) and NA0 as constitutional constraints: any governance decision is valid if and only if it does not violate NA0 in the operational definitions set out in Appendix I of Volume I. P2 establishes formal verification of this condition through Coq: a governance smart contract shall be deployed only upon the existence of a machine-verified proof of conformity with NA0.

The source of legitimacy in Ethereum is self-referential (T12): the governance rule is legitimate because it was adopted through that same governance rule. Virtublic establishes an external source of legitimacy through P0 as a constitutional founding act: popular sovereignty is the normative foundation logically antecedent to the protocol and not derivable from it.

D.2.2. Distribution of governance power

In Ethereum, governance power is distributed among three informal actor groups with unestablished weights. Core developers (the Ethereum Foundation, independent contributors) possess de facto veto power through the ability to refuse implementation of any EIP. Validator operators possess de facto veto power through the ability to refuse to update client software. Token holders possess governance power through ERC-20 token voting in ecosystem DAOs, yet have no direct participation in protocol governance. Concentration across all three groups is documented in Appendix C.

Virtublic instantiates a dual distribution through P4 (Dual Sovereignty): EQU⊥ (political sovereignty) is distributed uniformly among citizens with a verified Soulbound Identity on the principle of one person, one vote; VIC⊥ (economic participation) is distributed proportionally to verified economic contribution with a constitutional ceiling of D_threshold for a single operator. The Concordance Rule requires the assent of both spaces for constitutionally

significant decisions: neither an EQU⊥ majority without VIC⊥ qualification, nor a VIC⊥ majority without EQU⊥ assent, is sufficient.

Comparative concentration parameter: in Ethereum, the top-10 addresses control more than 40% of governance power in key DAOs at a median turnout of 3.8–7.4% (Appendix C). In Virtublic, the concentration of VIC⊥ is constitutionally constrained by D_threshold; EQU⊥ does not concentrate by definition — each verified citizen possesses one indivisible vote. Formally: Gini(EQU⊥) = 0 per constitutional specification; Gini(VIC⊥) ≤ Gini_max, as determined by D_threshold.

D.2.3. Verifiability of conformity with NA0

Ethereum contains no mechanism for verifying the conformity of governance decisions with NA0, since NA0 is not a component of the protocol. Post-factum verification through regulatory organs (SEC, EU) is reactive and jurisdictionally limited (T10, Volume I).

Virtublic instantiates proactive verification through P2 + P18: every governance smart contract is formally verified prior to deployment; the Constitutional Court of Code (P18) exercises constitutional oversight through the Dual Suspicion Protocol (Appendix A, section A.6). Verification criterion: the function V(contract, spec_NA0) = true, where spec_NA0 is the formal specification of NA0 in Coq, is a necessary condition of deployment.

D.3. Virtublic versus Bitcoin mining

D.3.1. Target function and security model

The target function of Bitcoin mining is unambiguous: maximization of block rewards and transaction fees while minimizing operational costs. The PoW security model secures the integrity of the ledger through the economic cost of attack: cost_of_attack = f(hash_rate, energy_price, ASIC_amortization). This model is correct with respect to the task of protecting the transaction ledger; it is structurally insufficient with respect to the task of protecting subjecthood (T14, Volume II).

Virtublic does not employ PoW as a consensus mechanism: the energy expenditure of PoW generates economic discrimination by capital (T15, step 2 of the proof) and creates a jurisdictional vulnerability through the geographic concentration of hash rate (Appendix C, C.3.1). Virtublic employs PoS consensus with constitutional concentration constraints (P16) as the substrate for executing constitutional contracts.

D.3.2. Governance and subject subjecthood

Bitcoin governance is the least formalized among major blockchain systems: BIP (Bitcoin Improvement Proposal) is an advisory document without binding force; consensus is achieved through the informal coordination of core developers and mining operators. Subjects with small balances have no governance representation and bear all consequences of protocol modifications without an appeal mechanism. This is the precise instantiation of T4 of Volume I (accountability without power) as applied to Bitcoin: the holder of 0.01 BTC bears the full consequences of halving events, fee market changes, and potential hard forks without any formal participatory mechanism.

Virtublic secures governance representation for all verified citizens independent of VIC⊥ balance through the uniform distribution of EQU⊥ (P0, P4). A subject with minimal economic participation possesses the same weight in EQU⊥ voting as a subject with a maximum VIC⊥ balance. This is a constitutional rupture with the Bitcoin model, in which governance representation is a monotonically increasing function of economic weight.

D.3.3. Comparative energy efficiency parameter

Bitcoin: 121 TWh/year (2023, CBECI). Ethereum PoS: approximately 0.01 TWh/year — a reduction of 99.95% relative to PoW following The Merge. Virtublic employs a PoS architecture with additional load from ZKP computations (proof generation for ZKP-PI and Digital Census) and Coq verification at contract deployment. Estimated energy load of the ZKP component: with 10 million active subjects and quarterly ZKP-PI proof generation, the aggregate GPU load is approximately 1.2–3.6 million GPU-hours per quarter at current performance parameters (NVIDIA A100 class). This is a finite and technically optimizable load, incomparably smaller than PoW consensus at any scale.

D.4. Virtublic versus DAO token voting

D.4.1. Comparison of sources of legitimacy

DAO token voting instantiates the principle of one token, one vote. The legitimacy of this principle is self-referential (T12): the rule was adopted through that same rule. No external normative standard exists: there is no constitutional act determining why token voting is a legitimate form of collective decision-making.

Virtublic separates two normatively distinct acts: political representation (EQU⊥, one person one vote) and economic participation (VIC⊥, proportional to contribution with a constitutional ceiling). The source of legitimacy of EQU⊥ is external to the protocol: P0 establishes popular sovereignty as the constitutional founding act antecedent to the protocol. This severs the self-reference of T12: the legitimacy of the voting rule is derived from P0, not from the fact of its inscription in a smart contract.

Comparative parameter: in DAO governance, the median participant does not possess real governance power (concentration of the top-10 addresses — 63.8–81.2% of counted votes; turnout — 3.8–7.4%; Appendix C). In Virtublic, governance power EQU⊥ is by definition uniformly distributed; turnout is secured through the Proof-of-Offline cognitive health bonus (P14), which reduces CL and raises PR in accordance with simulation H.4 of Volume I.

D.4.2. Mechanisms of protection against governance capture

DAO token voting contains no embedded mechanism for protection against governance capture — the seizure of control through the accumulation of a sufficient number of tokens. The flash loan governance attack (Beanstalk, 2022: $182 million) is the extreme case; systemic governance capture through long-term accumulation is a structural risk in any DAO without concentration constraints. The sole existing protection is a timelock (delay in execution of an adopted proposal), which permits exit prior to execution but does not preclude the adoption of a decision by the captor.

Virtublic instantiates three levels of protection against governance capture. The first level: EQU⊥ is an indivisible and non-transferable Soulbound token (P3) — the accumulation of EQU⊥ votes through market mechanisms is structurally impossible. The second level: the Concordance Rule requires the assent of EQU⊥ and VIC⊥ for constitutionally significant decisions — capture of a single space is insufficient. The third level: P8 (non-amendable core provisions) inscribes the constitutional core P0–P8 in an immutable smart contract, requiring for modification a qualified supermajority that is mathematically unattainable under any realistic distribution of VIC⊥ (ΣA18, Volume I). Verification criterion: the function Capture_resistance(proposal) = true if and only if the proposal does not modify P0–P8 without compliance with the constitutionally established threshold.

D.5. Virtublic versus critical discourse: why a constitution is not absorbed

D.5.1. The structural distinction between critique and constitution

T16 (Volume II) establishes the condition for the absorption of critical discourse D by system S: D is absorbed upon the simultaneous satisfaction of conditions (a) D does not provide an operational alternative outside the logic of S, and (b) S is capable of integrating D into its legitimation narrative. Analysis of conditions as applied to Virtublic:

Condition (a): Virtublic provides an operational alternative outside the logic of digital capital and blockchain ideology. The alternative is constitutionally specified (P0–P18), technically realizable (T17), and institutionally independent (P0 establishes the sovereignty of citizens, not platforms or the state). This means that condition (a) is not satisfied: Virtublic is not a critique of system S — it is an alternative system S'.

Condition (b): the citation of a constitutional norm as evidence of "openness to discussion" is a logically incorrect act. A constitutional norm is either complied with (which is established by formal verification P2) or violated (which activates constitutional sanction P18). There is no third state — "citation as proof of openness" — because a constitutional norm is a binary object of verification, not a rhetorical resource. This means that condition (b) is structurally unsatisfiable as applied to Virtublic: system S cannot integrate a constitutional norm into its legitimation narrative without thereby acknowledging the obligatory nature of its compliance.

D.5.2. The operational test of non-absorbability

Formal test: critical discourse D is non-absorbable by system S if and only if there exists a verifiable system state in which conformity with D is compulsorily enforceable independent of the will of S. For the critiques of Zuboff, Stiegler, and Morozov: no such state exists — Google and Meta bear no automatic consequences for non-conformity with "surveillance capitalism" as an analytical category. For Virtublic: such a state exists — PI > PI_max activates ZKP-PI verification, the Dual Suspicion Protocol, and constitutional sanction through P18 automatically and without discretionary intervention. Compulsory enforceability is a structural property of the smart contract, not of declarative text.

This distinction is architectural: critical discourse exists in the mode of "advice without sanction"; a constitutional norm exists in the mode of "rule with automatic sanction." System S may ignore advice; system S cannot ignore an automatically enforceable rule without incurring constitutional sanction. Connection with Volume III: P2 (automatic execution of

constitutional norms through smart contract) is the architectural foundation of non-absorbability.

D.6. Comparative analysis of Sybil resistance mechanisms

D.6.1. Comparative parameter matrix

The analysis is conducted across six parameters: the presence of a trusted verification center; the economic participation barrier; the social participation barrier; subject privacy; subject accountability; and conformity with NA0.

D.6.2. Worldcoin (biometric verification)

Definition. Worldcoin instantiates Sybil resistance through iris scanning by means of a specialized device, Orb. The verified subject receives a World ID — a cryptographically bound uniqueness identifier.

Parameter 1 (trusted center): the Worldcoin Foundation is the sole operator of Orb devices and the sole verifier of iris hashes. This is first-order centralized trust: compromise of the Worldcoin Foundation generates compromise of the entire verification registry. Architectural defect: Worldcoin's governance is exercised through WLD token voting (T12), and consequently the verification center itself is the object of governance without legitimacy.

Parameter 2 (economic barrier): absent at the verification level. However, receipt of WLD tokens, which constitute the participation incentive, requires possession of a compatible device and physical attendance at an Orb operator. In regions without Orb operators (the majority of sub-Saharan Africa, a significant portion of Asia), the economic barrier is replaced by a geographic barrier that is functionally equivalent.

Parameter 3 (social barrier): formally absent. However, iris scanning generates a permanent biometric record without a revocation mechanism. If a subject does not trust the Worldcoin Foundation with the storage of biometric data, he is structurally excluded from the system. This is a trust barrier, convertible into a social barrier in regions with high distrust of foreign corporations.

Parameter 4 (privacy): the iris is a permanent identifier. Upon database compromise, the subject cannot change his iris, unlike a password or a cryptographic key. Worldcoin declares the deletion of iris images following the generation of an iris code; verification of this declaration is structurally unavailable: the subject cannot prove or disprove the fact of deletion. This reproduces T8 of Volume I (information asymmetry) on the substrate of biometric data.

Parameter 5 (accountability): World ID secures address uniqueness but not accountability in the governance context — the World ID holder may adopt governance decisions anonymously (T13). Sybil resistance and accountability are structurally separated in the Worldcoin architecture.

Parameter 6 (NA0): violation of NA0 through permanent biometric profiling (A5, Volume I: the aggregation of biometric data non-linearly exceeds the value of its components). Worldcoin

collects iris codes from 5+ million subjects (per Worldcoin Foundation data, Q4 2023) — this constitutes a predictive profile of biometric type that is irremediable upon compromise.

D.6.3. BrightID (social graph verification)

Definition. BrightID instantiates Sybil resistance through a web of trust: subject uniqueness is verified through a sufficient number of confirmations from already-verified network participants.

Parameter 1 (trusted center): absent in the architectural sense — BrightID is a decentralized protocol without a single verifier. However, structural centralization exists through node operators controlling the verification infrastructure: the top-10 nodes processed more than 70% of verification requests in 2023 (BrightID public analytics).

Parameter 2 (economic barrier): formally absent. However, a verification meeting (connection party) necessitates physical presence or videoconference, which generates a time-cost barrier that is disproportionately high for subjects with non-standard schedules or limited mobility.

Parameter 3 (social barrier): is a structural defect. A subject without established social connections in the BrightID network cannot pass verification irrespective of his actual uniqueness. This generates digital inequality structurally correlated with pre-existing social inequality: subjects in regions without a BrightID community (the majority of developing countries as of 2023), subjects with social anxiety (A8, Volume I: cognitive limitation as a condition of exploitation), and subjects in geopolitically isolated jurisdictions are structurally excluded.

Parameter 4 (privacy): the social graph is sensitive data. Knowledge of who is connected to whom in BrightID generates a social network map potentially employable for de-anonymization through cross-analysis with other data sources.

Parameter 5 (accountability): analogously to Worldcoin — BrightID verifies uniqueness but does not secure accountability in the governance context.

Parameter 6 (NA0): the social barrier violates NA0 through the structural exclusion of socially vulnerable groups (N6, Volume I). A subject incapable of passing verification due to social isolation — rather than due to an attempted Sybil attack — bears the consequences of the system's design without an appeal mechanism.

D.6.4. Virtublic Civic Guard: VRF + Dual Suspicion Protocol + constitutional accountability

Definition. The Virtublic Civic Guard instantiates Sybil resistance through a constitutionally constrained verification organ (P3), employing VRF panel selection (Appendix A, A.6.1), the Dual Suspicion Protocol (A.6.2), and the constitutional accountability of citizen-guards.

Parameter 1 (trusted center): present explicitly — the Civic Guard is a constitutionally established organ with defined functions and prohibitions. This is a deliberate architectural decision in accordance with T15 (Sybil resistance without a trusted center is impossible): rather than eliminating the trusted center, Virtublic constitutionally constrains its functions.

The mandate of the Civic Guard is limited to the verification of subject uniqueness; the use of verification data for any other purpose constitutes a constitutional violation that automatically activates P18. This is the determinative distinction from the Worldcoin Foundation, whose mandate is not constitutionally constrained.

Parameter 2 (economic barrier): absent. Verification is a constitutional right of every subject (P0); the Civic Guard shall secure the accessibility of the verification procedure irrespective of the subject's economic position.

Parameter 3 (social barrier): absent. Verification does not necessitate a social graph: subject uniqueness is established through the Civic Guard procedure, independent of the number and quality of the subject's social connections.

Parameter 4 (privacy): verification data do not constitute a biometric database in the Worldcoin sense. The verification procedure establishes the fact of subject uniqueness and binds it to a Soulbound ID; specific biometric data are not stored in a centralized registry. ZKP-verification of uniqueness in subsequent governance actions is executed without disclosure of identity (P3 + zk-SNARK, Appendix A, A.5.2).

Parameter 5 (accountability): is a structural advantage of Virtublic over all alternatives. Soulbound ID (P3) binds a governance action to a unique subject with constitutional accountability for the consequences of the action. Privacy is simultaneously preserved through ZKP: what is publicly verified is the fact of subject uniqueness and the correctness of his action, but not his identity. This severs the contradiction of T13 (anonymity versus accountability): accountability is instantiated without identification.

Parameter 6 (NA0): the Civic Guard is the sole mechanism among the three analyzed that satisfies NA0 across all three components of subjecthood (Appendix I, Volume I): cognitive capacity (verification does not necessitate cognitive expenditure incompatible with depleted situational awareness or working memory), informational self-sufficiency (the verification procedure is transparent and constitutionally documented), and structural alternativity (the absence of an economic and social barrier eliminates de facto coercion under A11, Volume I).

D.6.5. Summary comparative table

Worldcoin: trusted center — yes (unconstrained); economic barrier — no (geographic barrier); social barrier — no (trust barrier); privacy — violated (permanent biometric); accountability — no; conformity with NA0 — no (violation through biometric profiling).

BrightID: trusted center — partial (node operators); economic barrier — no (time barrier); social barrier — yes (structural); privacy — partial (social graph exposure); accountability — no; conformity with NA0 — no (violation through social barrier).

Virtublic Civic Guard: trusted center — yes (constitutionally constrained); economic barrier — no; social barrier — no; privacy — secured (ZKP); accountability — yes (Soulbound ID); conformity with NA0 — yes.

Verification criterion for the entirety of section D.6: a Sybil resistance mechanism conforms to NA0 if and only if verification of uniqueness does not generate a permanent biometric profile, does not exclude socially vulnerable groups through a structural barrier, and secures the accountability of governance actions without de-anonymization of the subject. Of the three mechanisms analyzed, the sole mechanism satisfying this criterion is the Virtublic Civic Guard. Connection with Volume III: P3 (Soulbound Identity) is the constitutional specification for the instantiation of the described mechanism; P13 (Digital Census) employs the verified Soulbound ID registry for ZKP-aggregation of PI without de-anonymization of subjects.

Appendix E. Glossary of Volume II

E.1. Methodological parameters

The present appendix contains the complete formal registry of all theoretical elements of Volume II: axioms A19–A36, structural regularities 14–27, and theorems T11–T17. Each element includes a precise formulation, logical preconditions, normative qualification relative to NA0, and connection to the realizing principle of Volume III. Elements are presented in the logical order of dependencies within each class. In the event of discrepancy between the abbreviated formulation of the present glossary and the full proof of Appendix B, Appendix B takes precedence.

Normative status of the glossary: Appendix E is the mandatory terminological standard for the technical documentation of Volume III. The use of any term in a meaning other than that recorded here constitutes a terminological violation and is subject to correction through explicit redefinition with indication of the extension or restriction of the original meaning. P2 (Coq verification) is obligated to use the terms of the present glossary as the primary names for all corresponding formal objects.

E.2. Axioms A19–A36

A19. Axiom of technological neutrality. Blockchain technology as a set of cryptographic primitives — zk-proof, smart contract, distributed ledger — is neutral relative to normative axiom NA0: it realizes with equal effectiveness objective functions conforming to NA0 and objective functions violating NA0. Neutrality is an architectural property, not a consequence of developer intent. Preconditions: ΣA31 (code is law). Normative qualification: A19 justifies the necessity of explicitly introducing NA0 into the specification of constitutional contracts — without this, technological neutrality structurally reproduces violation of NA0 as a byproduct of the optimization of a neutral objective function. Connection to Volume III: P2 realizes non-neutral code — code with NA0 explicitly embedded as a mandatory constraint.

A20. Axiom of blockchain ideology. Blockchain ideology is the set of normative assertions that the decentralization of technology is a sufficient condition for the just distribution of authority, the elimination of intermediaries, and the protection of subjecthood. A20 records this set as an axiom of the blockchain ecosystem itself — not as a truth but as a declared foundation. Theorems T11–T16 successively refute each component of A20 through reduction to structural defects. Preconditions: none — A20 is an external observation upon the declared foundations of the ecosystem. Connection to Volume III: T17 synthesizes the

refutation of A20 with the confirmation of the technological necessity of blockchain — the technology is necessary, the ideology is insufficient.

A21. Axiom of staking advantage. In a PoS system with reward rate R > 0 and reinvestment of rewards, the stake of a participant is a monotonically non-decreasing function of participation time: S_i(t) = S_i(0) × (1 + R)^t. A participant who entered at moment t = 0 possesses a stake exceeding the stake of a participant who entered at moment t = τ with an identical initial stake by the coefficient (1 + R)^τ, independently of the subsequent investments of the late participant. Preconditions: A5 (aggregation, Volume I), Regularity 3 (monotonic accumulation, Volume I). Normative qualification: A21 establishes the mechanism for the reproduction of T2 (the temporal barrier, Volume I) on the substrate of token capital — which constitutes the foundation of T11. Connection to Volume III: P16 (Rockefeller Mode) constrains the accumulation of staking advantage through the constitutional ceiling D_threshold.

A22. Axiom of the governance token. In DAO architecture, governance power is defined as a function monotonically increasing from the governance token balance: GP_i = f(token_i), where f is a non-decreasing and, as a rule, linear function. This encodes the direct conversion of economic capital into political authority in the protocol, which violates N2 of Volume I (the prohibition on conversion of economic capital into political sovereignty). Preconditions: A21, T2 (Volume I). Normative qualification: A22 is the operational realization of the violation of N2 at the level of protocol architecture. Connection to Volume III: P4 (Dual Sovereignty) severs the function f through the separation of EQU⊥ and VIC⊥.

A23. Axiom of liquid staking derivatives. A liquid staking protocol aggregates the stake of multiple participants under the management of a single operator, issuing a derivative token — stETH, rETH — accepted as collateral in DeFi protocols. Aggregation generates a nonlinear growth of the operator's governance power relative to the total stake of those who delegated — by virtue of the same nonlinearity mechanism described in A5 of Volume I (the predictive value of aggregated data nonlinearly exceeds the sum of its constituents). When the operator's share w_LSP exceeds 1/3 of the total stake, the operator obtains the capacity to block finality — a qualitative transition absent from the linear model. Preconditions: A21, A5 (Volume I). Connection to Volume III: P16 is activated when w_LSP ≥ D_threshold.

A24. Axiom of the PoW security budget. In PoW consensus, the network's security budget — the cost of a 51% attack — is a direct function of the total costs of mining: Cost_attack = f(hash_rate, energy_price, ASIC_amortization). A reduction in energy expenditure while preserving PoW consensus is equivalent to a reduction in Cost_attack; it therefore follows that energy consumption and security are inseparable within the SHA-256 algorithm. Normative qualification: A24 establishes that the energy expenditure of PoW is not an artifact of implementation — it is a constitutive property of the consensus mechanism. Connection to Volume III: Virtublic does not use PoW as a consensus mechanism by reason of the structural conflict between A24 and the requirement of operational accessibility of P0.

A25. Axiom of address pseudonymity. In Ethereum and Bitcoin, an address is a cryptographic hash of a public key without mandatory binding to a unique physical subject. A single subject may control an arbitrary number of addresses; a single address may be transferred between subjects through transmission of the private key. This generates a

structural separation between the address as a unit of the protocol and the subject as the bearer of political accountability. Preconditions: A11 (corporeality, Volume I). Normative qualification: A25 is the ontological foundation of T13 — address pseudonymity structurally separates governance power from accountability.

A26. Axiom of MEV (Maximal Extractable Value). In a public mempool, transactions are visible prior to inclusion in a block. An actor with privileged access to the mempool — block proposer, MEV searcher — may reorder transactions to extract value at the expense of other participants. MEV is a structural consequence of mempool publicity and fee-based transaction prioritization — that is, an architectural property of the EVM, not a defect of specific contracts. Normative qualification: MEV reproduces T1 of Volume I (surplus attention) on the substrate of transactional ordering: a privileged actor extracts value from the transactions of ordinary subjects without compensation and without a mechanism of restitution. Connection to Volume III: constitutional transactions of Virtublic are executed through a protected execution environment with a constitutional prohibition on front-running for governance actions.

A27. Axiom of oracle dependency. A smart contract interacting with real-world data — prices, events, identities — requires an oracle, an external data source, trust in which is a necessary condition for the correctness of execution. An oracle is a trusted intermediary whose existence contradicts the principle of trustlessness. Compromise of the oracle produces compromise of the entire contract irrespective of the correctness of its code. Preconditions: ΣA31 (code is law). Normative qualification: A27 establishes the irremovability of human judgment in a smart contract interacting with the real world — which constitutes an operational limitation on the principle of code is law. Connection to Volume III: P2 specifies constitutional oracle requirements with constitutional accountability of oracle operators.

A28. Axiom of reentrancy vulnerability. A smart contract that calls an external contract prior to updating its own state is vulnerable to a reentrancy attack: the called contract may recursively call the vulnerable function before the state update is completed. The vulnerability is a structural consequence of the absence of a mandatory checks-effects-interactions pattern at the Solidity language level prior to version 0.8.0. Normative qualification: reentrancy is a specific realization of a bug as legitimate execution (ΣA31): the attacker does not violate the code — the attacker uses it correctly from the perspective of the EVM. Connection to Volume III: P2 mandates Coq verification of the absence of reentrancy vulnerabilities in all constitutional contracts prior to deployment.

A29. Axiom of the bootstrapping problem. The initial governance rule in a DAO cannot be adopted through that very rule: it is established by founders without a democratic procedure. This generates a constituent legitimacy deficit that is not remediable through subsequent governance procedures internal to the system. Preconditions: ΣA34 (DAO as governance without legitimacy). Normative qualification: A29 is the ontological foundation of T12 — the bootstrapping problem exposes the self-referential character of DAO legitimation. Connection to Volume III: P0 resolves the bootstrapping problem through a constitutional constituent act establishing popular sovereign authority as an external source of legitimacy logically antecedent to the protocol.

A30. Axiom of flash loan governance attack. A flash loan permits a subject to obtain temporary access to an arbitrary volume of capital within a single transaction on condition of return prior to its completion. In a DAO with instantaneous snapshot governance, a subject may obtain a temporary governance majority through a flash loan, adopt a favorable proposal, and return the loan within the same transaction. This generates a complete separation of governance power from long-term economic interest in the system. Preconditions: A22, A25. Normative qualification: A30 is the extreme case of T12 (governance without legitimacy): a decision is adopted by a subject without any long-term participation in the system, which entirely destroys the normative foundation of governance as the representation of participants' interests. Connection to Volume III: P4 structurally extirpates A30 through the impossibility of accumulating EQU⊥ through market mechanisms.

A31. Axiom of code is law. Smart contracts execute automatically without the possibility of human intervention; there are no violations — any action correct from the perspective of the code is technically legitimate within the framework of this principle, including the use of unintended execution paths — exploits — as technically correct operations. Preconditions: ΣA31 (axiom of the epistemological layer of Volume II). Normative qualification: A31 is a descriptive axiom — it records the principle adopted by the blockchain ecosystem without normative endorsement. T14 proves its normative insufficiency. Connection to Volume III: P2 realizes code is law with NA0 as a mandatory constitutional constraint.

A32. Axiom of irreversibility without correction. A smart contract deployed on the blockchain cannot be altered after deployment — with the exception of upgradeable patterns with their own contradictions. If the contract contains a vulnerability, it cannot be corrected without deploying a new contract; all funds in the old contract remain vulnerable. If the consensus in the past was unjust, its reversal requires a hard fork — a political act without an established procedure. Preconditions: ΣA32 (axiom of the epistemological layer). Normative qualification: A32 generates a conflict with the legal principle of rectification — irreversibility is a value of predictability that entails the complete abandonment of the value of correcting injustice. Connection to Volume III: P8 employs the immutability of A32 constitutionally — as an instrument for the protection of the constitutional core from alteration, not as an absolute principle.

A33. Axiom of the absorption of critique. A system absorbs any critique that offers no institutional alternative external to its logic. Critique without an operational alternative becomes a system stabilizer through the legitimation function: the demonstration of openness to discussion. Preconditions: Regularity 11 (Volume I, capture of critique). Normative qualification: A33 is the operational foundation of T16 — it describes the mechanism through which critical discourse about blockchain reproduces the legitimacy of the system it criticizes. Connection to Volume III: Virtublic is an institution with constitutional status, not a critical discourse, which structurally precludes absorption through A33.

A34. Axiom of DAO as governance without legitimacy. DAO is governed through smart contracts and token voting without appeal to an external normative source. Governance is fully automated. Authority is transferred to token holders, which structurally generates plutocracy by design. The legitimacy of the voting rule is established through the application of that same rule — circular self-legitimation. Preconditions: A22, A29, T12 (Volume II).

Connection to Volume III: P0 severs the cycle of self-legitimation through a constitutional constituent act with an external source of legitimacy.

A35. Axiom of Sybil resistance as a structural problem. Blockchain is vulnerable to Sybil attack — the creation of multiple fictitious identities for the capture of governance or rewards. Verification of the uniqueness of a subject in an open network without binding to physical reality is logically irresolvable without a trusted center while simultaneously satisfying three conditions: the absence of a trusted center, the absence of economic discrimination by wealth, and the absence of social discrimination by network capital. Preconditions: A25. Normative qualification: A35 is the ontological foundation of T15 — the three conditions are exhaustive; their simultaneous realization is impossible. Connection to Volume III: P3 violates condition (1) intentionally — a constitutionally bounded trusted center while observing conditions (2) and (3).

A36. Axiom of proof-of-personhood and its limits. Proof-of-personhood is a class of mechanisms for the verification of the uniqueness of a subject: biometric (Worldcoin), social graph (BrightID), government ID (KYC). Each mechanism violates at least one of the three conditions of A35: biometric requires a trusted center (violation of condition 1) and generates a permanent biometric profile (violation of NA0 through A5); social graph discriminates by social capital (violation of condition 3); government ID requires a state trusted center (violation of condition 1 with the ΣA17 defect). Preconditions: A35. Normative qualification: A36 establishes the exhaustion of existing technical approaches as the foundation for the normative resolution through the Civic Guard of P3.

E.3. Structural regularities 14–27

Regularity 14 (from A31 + A28 + A29). The automation of norm execution transfers the normative choice to the level of code-writing, rendering it less visible and less contestable than traditional norm-setting while preserving all of its structural significance. Automation does not eliminate normative choice — it conceals it behind the appearance of technical neutrality.

Regularity 15 (from A21 + A5, Volume I). The staking advantage of early participants in a PoS system grows monotonically with a positive second derivative after the point of no return τ^*, reproducing the mechanism of the temporal barrier T2 of Volume I on the substrate of token capital. The coefficient of advantage of the early participant relative to the late participant does not diminish over time and is not corrected by market mechanisms without external intervention.

Regularity 16 (from A22 + A29). Token voting is a self-legitimating mechanism: the voting rule is legitimated through the application of that same rule. An external normative source of legitimacy is structurally absent from standard DAO architecture, which generates the impossibility of normative contestation of voting outcomes outside the framework of the protocol.

Regularity 17 (from A23 + Regularity 15). Liquid staking derivatives generate nonlinear amplification of staking advantage through aggregation: the operator accumulates governance power proportional to the total delegated stake, which upon exceeding the

threshold w_LSP > 1/3 generates a qualitative transition to the capacity to block finality. The nonlinearity is conditioned by the same mechanism as described in A5 of Volume I.

Regularity 18 (from A25 + A31). Address pseudonymity in combination with the principle of code is law generates a structural separation of governance action from political accountability for its consequences. An actor makes decisions whose consequences are borne by other subjects while remaining unidentifiable — which constitutes an inversion of T4 of Volume I: not responsibility without authority, but authority without accountability.

Regularity 19 (from A22 + Regularity 15 + A23). In a DAO without constitutional constraint on the concentration of governance power, governance power concentrates among early token holders through the same temporal mechanism as described in Regularity 4 of Volume I as applied to predictive capital. The median DAO participant does not possess real governance power: empirically — turnout of 3.8–7.4% with concentration of the top-10 addresses accounting for 63–81% of recorded votes (Appendix C).

Regularity 20 (from A35 + A36). Every mechanism of Sybil resistance in an open network violates at least one of the three conditions of A35. The three classes of existing approaches — PoW/PoS, biometric, social graph — are exhaustive; the fourth class — government ID — is a particular case of biometric with a higher level of centralization. The normative resolution through a constitutionally bounded trusted center is the sole realizable form satisfying NA0.

Regularity 21 (from A26 + A27). MEV and oracle dependency are two forms of a single structural defect: the irremovable presence of a privileged intermediary in an architecture that declares trustlessness. MEV transfers the privilege to the level of transaction ordering; oracle transfers it to the level of the data source. Both defects reproduce the informational asymmetry of T8 of Volume I in new substrates.

Regularity 22 (from A31 + A32 + A28). The principle of code is law in combination with irreversibility without correction generates a system in which a bug constitutes technically legitimate execution. The aggregate harm from exploit attacks realizing correct execution of incorrect code exceeded three billion dollars in 2022 — not as an anomaly but as a structural consequence of A31 and A32.

Regularity 23 (from A33 + Regularity 11, Volume I). Critical discourse about blockchain functions as a system stabilizer through the same mechanism as described in Regularity 11 of Volume I for digital capital: critique is absorbed through integration into the legitimation narrative of the ecosystem — "our system is open to discussion." Thirty years of academic critique of surveillance capitalism and ten years of critique of blockchain plutocracy have not generated structural changes in the dominant architectures.

Regularity 24 (from A20 + T11 + T12 + T13 + T14 + T15). Blockchain ideology is a form of technological determinism: the assertion that the decentralization of technology is a sufficient condition for the just distribution of authority. Theorems T11–T15 refute each component of this assertion through the demonstration of the structural reproduction of the same defects — concentration, absence of legitimacy, anonymity without accountability, effectiveness without subjecthood, Sybil through centralization — in a new substrate.

Regularity 25 (from A19 + A31 + NA0, Volume I). Technologically neutral code in the absence of NA0 optimizes the specified objective function while generating violations of NA0 as a structural byproduct. The neutrality of code relative to NA0 is not an advantage but a vulnerability: in systems with engagement-optimization or profit-maximization as the objective function, NA0 violations are a determined consequence. This is an extension of T14 to the level of a general principle.

Regularity 26 (from A29 + A34 + Regularity 16). The constituent legitimacy deficit of DAO is irremediable through the internal procedures of the system: any decision adopted through token voting inherits the legitimacy deficit of the constituent act. A rupture is possible only through an external constitutional act establishing a normative foundation logically antecedent to the protocol.

Regularity 27 (from T17 + Regularity 24 + Regularity 26). The sole realizable form of protection of subjecthood in the digital domain is the combination of blockchain technology as the necessary cryptographic substrate and constitutional architecture as the necessary normative superstructure. Neither technology without a constitution nor a constitution without technology is sufficient. This is the synthetic regularity summarizing the entire analytical layer of Volume II.

E.4. Theorems T11–T17

T11. Theorem of the plutocracy of Proof-of-Stake. In any PoS system with validator selection proportional to stake share, without constitutional constraint on concentration, governance power concentrates among early participants in a monotonically increasing manner, reproducing the temporal barrier T2 of Volume I on the substrate of token capital. Preconditions: A21, A5 (Volume I), Regularity 3 (Volume I), T2 (Volume I), Regularity 15. Proof: Appendix B, section B.2. Empirical verification: Lido 32.4% ETH staking; top-10 addresses — 40%+ governance power in key DAOs (Appendix C). Connection to Volume III: P4 + P16.

T12. Theorem of governance without legitimacy. Token voting in a DAO without an external constitutional source of legitimacy is circular self-legitimation, generating governance structurally incapable of normative contestation of outcomes. Preconditions: ΣA34, A22, A29, Regularity 16. Proof: Appendix B, section B.3. Empirical verification: Uniswap governance vote (MIP BNB Chain, May 2023), turnout 7.2%, three addresses — 66% of votes. Connection to Volume III: P0 + P4 + Concordance Rule.

T13. Theorem of anonymity without accountability. In a system with pseudonymous addresses without verified binding to a unique subject, governance power and economic influence are structurally separated from political accountability, reproducing the inversion of T4 of Volume I: authority without accountability. Preconditions: A25, A11 (Volume I), Regularity 18. Proof: Appendix B, section B.4. Empirical verification: Beanstalk flash loan attack (April 2022, $182M), attacker unidentified. Connection to Volume III: P3 (Soulbound Identity + ZKP accountability).

T14. Theorem of code is law without NA0. A smart contract optimizing an objective function without constitutionally entrenched NA0 generates effective execution while systematically destroying the subjecthood of participants, measurable through the indicators

PI, CHS, and structural alternativeness. Preconditions: NA0 (Volume I), ΣA31, ΣA32, T6 (Volume I), Regularity 25. Proof: Appendix B, section B.5. Empirical verification: Compound oracle failure ($88.9M in liquidations, November 2020); Mango Markets oracle manipulation ($117M, October 2022). Connection to Volume III: P2 (NA0 as a mandatory constraint in constitutional contracts).

T15. Theorem of Sybil resistance requiring centralization. In an open network without binding to physical reality, no mechanism of Sybil resistance exists that simultaneously satisfies three conditions: the absence of a trusted center, the absence of economic discrimination by wealth, and the absence of social discrimination by network capital. Every realization violates at least one condition. Preconditions: A35, A36, Regularity 20. Proof: Appendix B, section B.6 (method of exhaustion of alternatives). Empirical verification: Gitcoin Grants round 15, Sybil attack + Passport social barrier. Connection to Volume III: P3 (constitutionally bounded trusted center as normative resolution).

T16. Theorem of the absorption of critique. Critical discourse about a system that offers no institutional alternative external to the logic of the system is structurally absorbed by the system and performs the function of a legitimation resource rather than a threat to structural stability. Preconditions: ΣA33, Regularity 11 (Volume I), Regularity 13 (Volume I), Regularity 23. Proof: Appendix B, section B.7. Empirical verification: Ethereum Foundation citation of Zamfir in the absence of structural changes to PoS; Zuboff's *Surveillance Capitalism* alongside growth in Google/Meta market capitalization from 1.2 to 3.7 trillion dollars (2019–2024). Connection to Volume III: P0–P18 as an institution with constitutional status, not a critical discourse.

T17. Theorem of the constitutional necessity of blockchain. Blockchain technology is a necessary but insufficient condition of a constitutional architecture capable of protecting subjecthood within the meaning of NA0. The necessity is conditioned by the cryptographic properties of the technology — zk-proof, smart contract, formal verification; the insufficiency — by the structural defects of T11–T16; the sole realizable form is Virtublic = blockchain technology + constitutional architecture. Preconditions: T11–T16, T10 (Volume I), Regularity 27. Proof: Appendix B, section B.8 (proof of necessity + insufficiency + uniqueness through the method of exhaustion of alternatives). Connection to Volume III: the entire volume P0–P18 as the realization of the sole identified sufficient form.

Appendix F. Bibliography of Volume II

F.1. Methodological parameters

The present appendix contains the annotated bibliography of sources upon which the analytical apparatus of Volume II rests. Each source is accompanied by: precise bibliographic data; indication of the specific axioms, theorems, or regularities of Volume II for which the source constitutes a foundation or an object of deconstruction; normative qualification relative to NA0; and connection to the realizing principle of Volume III. The bibliography is organized into six thematic sections corresponding to the analytical layers of the volume.

Status of sources: bibliographic entries perform three distinct functions in the architecture of Volume II. The first function is that of technical substrate: sources providing the cryptographic, protocol, and formal verification foundations for the specification of Virtublic — Nakamoto, Ben-Sasson et al., the Coq Reference Manual. The second function is that of object of deconstruction: sources declaring the normative foundations of blockchain that theorems T11–T16 systematically refute — Buterin, Zamfir. The third function is that of verification resource: sources that empirically confirm the structural regularities of Volume II or provide normative concepts operationalized in the architecture of Virtublic — Rawls, Habermas, Abramson, Zuboff. No source of the third function constitutes a sufficient justification without the axiomatic derivation of Volume II: bibliographic appeals do not substitute for the formal proofs of Appendix B.

F.2. Blockchain theory: primary protocol sources

F.2.1. Nakamoto, S. "Bitcoin: A Peer-to-Peer Electronic Cash System." 2008. Available: bitcoin.org/bitcoin.pdf. Function in Volume II: technical substrate of the PoW specification (Appendix A, A.2). Nakamoto introduces SHA-256 proof-of-work as a mechanism of Sybil resistance through an economic barrier — which constitutes the operational foundation of A24 (axiom of the PoW security budget) and A35 (Sybil resistance through economic concentration, class 1). The Bitcoin whitepaper declares a trustless peer-to-peer system without a trusted intermediary; T15 proves that Sybil resistance through PoW is not the elimination of a trusted center but its replacement by an economic barrier surmountable by a sufficiently capitalized attacker. Connection to Volume III: the technical architecture of SHA-256 and the structure of the UTXO ledger are precedents for the specification of the distributed ledger in P3 and P13, with constitutional elimination of the defects of A24.

F.2.2. Buterin, V. "Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform." 2013. Available: ethereum.org/whitepaper. Function in Volume II: primary source for the declaration of blockchain ideology (A20) as applied to smart contracts and DAO governance. Buterin introduces the concept of the Turing-complete smart contract as the foundation for "decentralized autonomous organizations" — which constitutes the operational basis of ΣA34 (DAO as governance without legitimacy). The whitepaper contains no external source of legitimacy for governance: the self-referential character recorded in Regularity 16 is a structural property of the original architecture, not a subsequent deviation. Buterin's subsequent works — *Proof of Stake: The Making of Ethereum and the Philosophy of Blockchains*, 2022 — partially acknowledge the concentration risks of PoS, which constitutes empirical verification of T16: critique is produced from within the ecosystem and absorbed by it without structural changes. Connection to Volume III: the EVM architecture is the technological substrate of P2, with the constitutional superstructure of NA0.

F.2.3. Buterin, V. "A Proof of Stake Design Philosophy." Medium, Ethereum Blog. 2016. Available: medium.com/@VitalikButerin. Function in Volume II: source for the declaration of the normative foundations of PoS as an improvement relative to PoW. Buterin asserts that PoS reduces concentration through the elimination of ASIC economics and the reduction of energy barriers. T11 proves that PoS transfers concentration to the level of staking advantage (A21) rather than extirpating it. This is a case of Regularity 24 (technological determinism): the change of consensus mechanism is declared to be a resolution of the normative problem without the provision of an external normative source.

F.2.4. Zamfir, V. "Against Szabo's Law, For a New Crypto Legal System." CryptoLaw Review. 2019. Function in Volume II: primary source of internal critique of blockchain ideology, which is simultaneously an object of deconstruction through T16 (absorption of critique). Zamfir correctly diagnoses the insufficiency of "code is law" as a normative principle and proposes the introduction of legal mechanisms for the correction of smart contracts. However, Zamfir's proposal remains within the logic of the blockchain ecosystem: he proposes reforming the protocol rather than establishing a constitutional architecture external to it. This is a precise case of A33: the critique has been absorbed by the Ethereum Foundation through citation of Zamfir as evidence of openness to discussion. Connection to Volume III: T16 establishes that Zamfir's position is a necessary but not sufficient step — the sole sufficient step is constitutional P0.

F.2.5. Zamfir, V. "My Concerns About Crypto Governance." Medium. 2018. Function in Volume II: source of early diagnosis of governance concentration in Ethereum PoS, antedating the transition — The Merge, 2022. Zamfir predicts that liquid staking generates concentration among large operators — which is verified by the data of Appendix C (Lido 32.4% as of Q4 2023). Regularity 19 operationalizes this mechanism through A21 and A23. Verification note: Zamfir's prediction was made four years before its realization, which confirms the structural rather than incidental character of concentration.

F.3. Critique of blockchain

F.3.1. Weaver, N. "Blockchains and Cryptocurrencies: Burn It With Fire." School of Information, UC Berkeley. 2018. Available: people.eecs.berkeley.edu/~nweaver/. Function in Volume II: technically competent critique of blockchain from a computer science perspective, verifying a number of structural defects recorded in axioms A22–A36. Weaver establishes: the majority of blockchain use cases do not require decentralization and are realized more effectively through traditional databases; cryptographic tokens generate speculative dynamics that extirpate operational subjecthood — verification of T13 and T14; the energy expenditure of PoW is an irremovable structural property, not an implementation defect — verification of A24. Weaver offers no constitutional alternative — which constitutes the basis for his classification through T16: the critique is correct; the institutional alternative is absent. Connection to Volume III: Weaver's technical arguments about PoW inefficiency verify the selection of the PoS substrate for Virtublic while preserving the constitutional constraints of A21.

F.3.2. Golumbia, D. *The Politics of Bitcoin: Software as Right-Wing Extremism.* University of Minnesota Press. 2016. Function in Volume II: politico-theoretical analysis of the ideological foundations of Bitcoin as the realization of a libertarian anti-state program. Golumbia establishes: Bitcoin ideology generates not a neutral technical platform but a political program with specific normative consequences — the elimination of state control over the monetary system as such. This verifies A20 (blockchain ideology as a normative program rather than a technical solution) and Regularity 24 (technological determinism). Normative qualification relative to NA0: the elimination of state regulation without a constitutional alternative does not protect subjecthood — it creates a space devoid of normative protection, which constitutes a violation of NA0. Connection to Volume III: Golumbia's analysis operationally justifies the necessity of P0 as a constitutional foundation external to both the state and blockchain ideology.

F.3.3. Morozov, E. "Socialize the Data Centres!" *New Left Review.* 2015; *To Save Everything, Click Here: The Folly of Technological Solutionism.* PublicAffairs. 2013. Function in Volume II: critique of technological solutionism, applicable to blockchain ideology as a particular case. Morozov establishes: technological solutions to social problems systematically redefine political problems as technical ones, extirpating the possibility of normative contestation through political institutions. This is an operational description of Regularity 14 (normative choice concealed behind the appearance of technical neutrality of code) and Regularity 24 (technological determinism). Morozov is a case of T16: the critique is precise but remains within the media and academic ecosystem that commodifies critique (Appendix C, C.6). Connection to Volume III: the conceptual apparatus of "technological solutionism" is operationalized in the justification of the necessity of P0 as a normative rather than technical foundation.

F.4. Critique of digital capital

F.4.1. Zuboff, S. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power.* PublicAffairs. 2019. Function in Volume II: primary source for the concept of "behavioral surplus" as the operational basis for A4 (crystallization of AT into predictive capital, Volume I) and T1 (surplus attention, Volume I). Zuboff's behavioral surplus is a specific case of crystallization in the terminology of the present theory: data of the subject, generated by the subject without compensation and used for predictive profiling. Zuboff is the primary precedent for academic analysis of surveillance capitalism upon which T8 and T9 of Volume I rest. Normative qualification per T16: *The Age of Surveillance Capitalism* is the most cited work of the genre; meanwhile, the aggregate market capitalization of Google and Meta grew from 1.2 trillion dollars in the year of publication to 3.7 trillion by 2024. This is a precise case of Regularity 23: critique absorbed by the system without structural change. Connection to Volume III: Zuboff's conceptual apparatus verifies the diagnosis but provides no operational alternative — which renders P0–P18 the necessary next step.

F.4.2. Stiegler, B. *Technics and Time, 1: The Fault of Epimetheus.* Stanford University Press. 1998; *For a New Critique of Political Economy.* Polity Press. 2010. Function in Volume II: philosophical foundation for the concept of cognitive disarmament (T6, Volume I) and de-subjectivation through technological systems. Stiegler establishes: technical systems generate psychic and collective individuation or de-individuation depending on the normative architecture — which constitutes the conceptual predecessor of the distinction between adaptive and maladaptive cognitive offloading in the terminology of the present theory. Stiegler's "pharmacology" — technology as simultaneously poison and remedy — is operationalized in T17: blockchain is a necessary substrate under a normative superstructure and a toxic instrument without one. Normative qualification: Stiegler's works were institutionally integrated through IRI with financing from Orange — verification of T16 (Appendix C, C.6.2). Connection to Volume III: the concept of individuation through technics is the normative foundation for the requirement of P14 (Proof-of-Offline as a constitutional guarantee of cognitive autonomy).

F.4.3. Srnicek, N. *Platform Capitalism.* Polity Press. 2017. Function in Volume II: political-economic analysis of platforms as a new type of capitalist organization, verifying Regularities 3 and 4 of Volume I. Srnicek establishes: platforms generate network effects

that render monopolistic position structurally stable through mechanisms identical to T2 (the temporal barrier) in the terminology of the present theory. The concept of "data as raw material" is the platform equivalent of A3 (Volume I): data of the subject are the raw material for the generation of predictive capital. Srnicek proposes the nationalization of platforms as a resolution — which is an internal resolution violating ΣA17 (the state as a structurally interested purchaser of data). Connection to Volume III: P5 (Non-State Public Utility) is the constitutional response to Srnicek's dilemma: neither private monopoly nor state ownership, but constitutionally governed public infrastructure.

F.5. Cryptography and formal verification

F.5.1. Ben-Sasson, E., Chiesa, A., Garman, C., Green, M., Miers, I., Tromer, E., Virza, M. "Zerocash: Decentralized Anonymous Payments from Bitcoin." *IEEE Symposium on Security and Privacy.* 2014. Function in Volume II: primary source for zk-SNARK as applied to blockchain privacy. Ben-Sasson et al. formalize the Groth16 construction — in subsequent works — as a succinct non-interactive argument of knowledge: proof π certifies knowledge of witness w without disclosing it, at a proof size independent of the complexity of the computation. This is the cryptographic foundation of the ZKP-PI protocol (Appendix C, Volume I; Appendix A, A.5 of the present volume). Parameters: completeness, soundness, and zero-knowledge as three mandatory properties, verifiable through mathematical reduction to the hardness of the discrete logarithm problem on BN254. Connection to Volume III: P2 + P13 realize verification that PI ≤ PI_max through zk-SNARK without disclosing the subject's data to the regulator.

F.5.2. Groth, J. "On the Size of Pairing-Based Non-Interactive Arguments." *EUROCRYPT 2016. Lecture Notes in Computer Science,* vol. 9666. Springer, Berlin, Heidelberg. 2016. Function in Volume II: technical specification of Groth16 — the most widely used zk-SNARK system in production. Groth establishes the minimum proof size for R1CS schemes: three elements of the G1/G2 groups of the BN254 elliptic curve (192 bytes). Verification time is subpolynomial and does not depend on the complexity of the assertion being proved. This property is critical for on-chain verification in Virtublic: an EVM call for Groth16 verification costs approximately 200,000–300,000 gas irrespective of the complexity of the scheme. The circuit-specific trusted setup is a structural vulnerability of Groth16 — which justifies the requirement of a multi-party computation ceremony for the generation of the CRS of the constitutional schemes of Virtublic. Connection to Volume III: P2 specifies Groth16 as the primary protocol for ZKP-PI verification with a mandatory MPC ceremony.

F.5.3. Ben-Sasson, E., Bentov, I., Horesh, Y., Riabzev, M. "Scalable, transparent, and post-quantum secure computational integrity." *IACR Cryptology ePrint Archive.* 2018. Function in Volume II: technical specification of zk-STARK as an alternative zk-proof protocol that eliminates the trusted setup at the cost of increased proof size. STARK is transparent — requires no CRS — and post-quantum secure — based on collision-resistant hash functions rather than on the hardness of the discrete logarithm. This constitutes the reserve cryptographic substrate for Virtublic in the event of compromise of elliptic curves: upon the attainment of quantum computing capable of solving the discrete logarithm problem, Groth16 becomes insecure, whereas STARK preserves security. Connection to Volume III: P18 (Conflict-Resolution Core) is obligated to maintain a migration path from Groth16 to STARK upon a change in the threat model.

F.5.4. The Coq Development Team. *The Coq Proof Assistant Reference Manual.* Version 8.18. INRIA. 2023. Available: coq.inria.fr/documentation. Function in Volume II: operational basis for the formal verification of the constitutional contracts of Virtublic. Coq implements the Calculus of Constructions — a dependently typed lambda calculus in which mathematical proofs and program correctness are verified mechanically through type checking. This is the technical foundation of the requirement of P2: Coq verification of a constitutional contract establishes that for every system state, execution of the contract does not violate NA0 in the operational definitions of Appendix I of Volume I. Existing precedents for the verification of blockchain code through Coq: Tezos (formal verification of consensus), Concordium (verification of the identity layer), CertiK (audit of smart contracts). Connection to Volume III: P2 mandates Coq verification of all constitutional contracts prior to deployment; P18 uses Coq as an instrument of the Conflict-Resolution Core when the correctness of algorithms is contested.

F.5.5. de Moura, L., Kong, S., Avigad, J., Van Doorn, F., von Raumer, J. "The Lean Theorem Prover." *CADE 2015. Lecture Notes in Computer Science,* vol. 9195. Springer. 2015. Function in Volume II: alternative proof assistant considered as a reserve platform for formal verification. Lean 4 implements dependent type theory with improved ergonomics relative to Coq and active ecosystem development — Mathlib. Lean is an admissible alternative to Coq for the realization of P2 while preserving the mathematical equivalence of verification guarantees. Connection to Volume III: P2 permits Lean as an alternative verification instrument on condition of a formal proof of equivalence of the specification relative to the Coq version.

F.6. Political theory

F.6.1. Lessig, L. *Code and Other Laws of Cyberspace.* Basic Books. 1999; *Code: Version 2.0.* Basic Books. 2006. Function in Volume II: primary source for the concept of "code as law" in academic political theory — the conceptual predecessor of ΣA31. Lessig establishes: the architecture of digital systems is a normative form regulating behavior on a par with law, market, and norms. This constitutes verification of Regularity 14: normative choice is embedded in the architecture of code. Lessig treats code as a regulatory problem — how to ensure that architecture conforms to public values. T14 and T17 provide the answer: NA0 as a constitutional constraint verifiable through Coq. Connection to Volume III: Lessig's concept is the normative foundation of P2 — "code with constitution" as the answer to "code as unregulated law."

F.6.2. Rawls, J. *A Theory of Justice.* Harvard University Press. 1971; *Political Liberalism.* Columbia University Press. 1993. Function in Volume II: normative foundation for the principles of just distribution operationalized in P0, P4, and N2 of Volume I. The Rawlsian "veil of ignorance" constitutes the conceptual foundation for testing the constitutionality of architectural decisions of Virtublic: does the decision satisfy the criterion that a rational subject, unaware of the subject's position in the system, would adopt? The difference principle is operationalized in the constraints of D_threshold (P16): concentration of VIC⊥ is permissible up to the point at which it generates harm for subjects with minimum participation. Normative qualification: Rawls is an external normative source for NA0 — which is the function of a source of the third category (verification resource). Connection to

Volume III: the "veil of ignorance" test is the informal verification criterion for constitutional decisions P0–P18.

F.6.3. Habermas, J. *The Theory of Communicative Action.* Volumes 1–2. Beacon Press. 1984–1987; *Between Facts and Norms: Contributions to a Discourse Theory of Law and Democracy.* MIT Press. 1996. Function in Volume II: normative foundation for the requirement of N3 (the right to undistorted communication, Volume I) and conceptual foundation for the diagnosis of persuasive loops (Regularity 11, Volume I) as a violation of the conditions of the ideal speech situation. Habermas establishes: the legitimacy of a norm is determined through a procedure of discursive justification under conditions of equal participation without compulsion. Blockchain ideology violates this requirement through T12 (governance without legitimacy): token voting is not a discursive procedure, because it does not presuppose equal participation and contains no mechanism of justification. *Between Facts and Norms* provides the conceptual apparatus for the analysis of the gap between constitutional norms (facts) and their operational realization (norms) — which is the structural question of P2. Connection to Volume III: P0 realizes the Habermasian principle of discursive legitimacy through a constitutional constituent act with constitutionally established procedures of participation.

F.6.4. Arendt, H. *The Origins of Totalitarianism.* Harcourt, Brace. 1951; *The Human Condition.* University of Chicago Press. 1958. Function in Volume II: politico-theoretical foundation for the concept of subjecthood as a politically protected good (NA0) and diagnosis of the conditions of its destruction. Arendt establishes: "the right to have rights" is the primary political right antecedent to all specific legal guarantees. This is the conceptual foundation of NA0: subjecthood is a politically protected good without which no specific rights are operational. *The Human Condition* establishes the distinction among labor, work, and action: action is the domain of genuine political subjecthood — collective action in the public space. The cognitive disarmament of T6 of Volume I is the analogue of the destruction of the public space of action in Arendt's terms. Connection to Volume III: P0 realizes the principle of "the right to have rights" through a constitutional constituent act guaranteeing subjecthood as the inalienable political foundation.

F.7. Jury theory

F.7.1. Abramson, J. *We, the Jury: The Jury System and the Ideal of Democracy.* BasicBooks. 1994; Harvard University Press paperback edition. 2000. Function in Volume II: primary source for the theoretical foundation of the institutional design of the Civic Guard (P13, Volume III) and VRF-based panel selection (Appendix A, A.6). Abramson establishes: the institution of the jury realizes the democratic principle of participation through the random selection of citizens, extirpating the systematic biases of a professional judiciary. Random selection — sortition — is an operational principle historically antecedent to electoral democracy and preserving normative advantages: the prevention of the concentration of judicial authority, the inclusion of non-specialized judgment, and the compelled participation of citizens in governance. Abramson also analyzes the pathologies of the jury system: voir dire as a mechanism of strategic exclusion of undesired jurors; the influence of jury selection consultants as a private form of governance capture. These pathologies constitute the foundation for the replacement of the voir dire procedure by the VRF mechanism in Virtublic: cryptographically verifiable randomness extirpates the possibility of strategic selection.

Connection to Volume III: the VRF protocol of Appendix A, A.6.1 realizes Abramson's principle of random sortition with cryptographic guarantee of the unpredictability of panel composition.

Appendix G. Correspondence matrix: Volume I → Volume II → Volume III

G.1. Methodological parameters

The present appendix records the systemic connections among the three analytical layers of the trilogy in the form of a direct correspondence matrix. Each row of the matrix describes a single logical vector: a diagnostic element of Volume I — axiom, theorem, or normative principle — its structural reproduction on the blockchain substrate in Volume II — theorem T11–T17 — and the constitutional safeguard of Volume III — principle P0–P18 — that blocks the corresponding defect.

The matrix performs a dual function. First, it is a navigational instrument: a reader entering the trilogy through the normative or technical layer may establish the complete logical vector of any architectural decision, from the ontological axiom of Volume I to the constitutional principle of Volume III. Second, it is a verification instrument for Volume III: each principle P0–P18 must have at least one incoming connection through the present matrix; a principle without a diagnostic foundation in Volumes I–II has no normative justification in the architecture of the trilogy.

Normative status: the matrix is a derivative document — it introduces no new theoretical elements but records connections formally established in the main text and appendices of Volumes I and II. In the event of discrepancy between the matrix and the main text, the main text takes precedence.

G.2. Correspondence matrix

Vector 1. Temporal barrier → Plutocracy of PoS → Dual Sovereignty + Rockefeller Mode.

Volume I, T2 (temporal barrier): the leading platform accumulates predictive capital C_L, growing with a positive second derivative after the point of no return TH, which renders the entry barrier D(t) = C_L — C_N structurally insurmountable by market means. Volume II, T11 (plutocracy of Proof-of-Stake): the same temporal mechanism is reproduced on the substrate of token stake — the early participant accumulates a share of the total stake by the function $S_i(t) = S_i(0) \times (1 + R)^t$, outpacing the late participant by an irremovable coefficient $(1 + R)^\tau$. Liquid staking derivatives (A23) amplify the effect nonlinearly through aggregation, reproducing the mechanism of A5 of Volume I on the new substrate. Volume III, P4 (Dual Sovereignty) + P16 (Rockefeller Mode): P4 severs the identity of economic stake and political sovereignty through the structural separation of EQU⊥ and VIC⊥, extirpating the operational foundation of T11; P16 establishes the constitutional ceiling D_threshold for the concentration of VIC⊥ at a single operator, blocking the nonlinear effect of A23.

Vector 2. Sovereignty disjuncture → Governance without legitimacy → Popular sovereign authority + Dual Sovereignty.

Volume I, T8 (sovereignty disjuncture): predictive capital generates an asymmetry of informational authority in which formal democratic procedures lose substantive legitimacy — the subject votes within an informational environment constructed by the platform. Volume II, T12 (governance without legitimacy): DAO token voting is a self-legitimating mechanism without an external normative source; the voting rule is legitimated through the application of that same rule, generating circular self-legitimation. The bootstrapping problem (A29) is the ontological foundation of the deficit: the constituent act of a DAO cannot be adopted through a DAO procedure. Volume III, P0 (popular sovereign authority as constitutional constituent act) + P4 (Concordance Rule): P0 severs the self-reference of T12 through an external source of legitimacy logically antecedent to the protocol; the Concordance Rule requires the assent of EQU⊥ for constitutionally significant decisions, extirpating the possibility of governance capture through a VIC⊥ majority.

Vector 3. Right to unpredictability → Anonymity destroys accountability → Soulbound Identity + Proof-of-Offline.

Volume I, N1 (right to unpredictability): the subject possesses the constitutional right to behavior unpredictable to the platform; PI > PI_max constitutes a constitutional violation. Volume II, T13 (anonymity destroys accountability): address pseudonymity in combination with ΣA31 generates the inversion of T4 of Volume I — authority without accountability: the holder of governance tokens makes decisions whose consequences are borne by other subjects while remaining unidentifiable (A25, Regularity 18). Volume III, P3 (Soulbound Identity) + P14 (Proof-of-Offline): P3 binds governance action to a unique subject with constitutional accountability without de-anonymization through ZKP — severing the contradiction of T13: accountability without identification; P14 ensures the cognitive autonomy of the subject as a condition of genuine consent in governance participation.

Vector 4. Normative axiom → Code is law without NA0 → Supremacy of code with normative axiom.

Volume I, NA0 (subjecthood as a politically protected good): an external Kantian axiom establishing that the systematic destruction of subjecthood is a political wrong irrespective of the economic efficiency of that destruction. Volume II, T14 (code is law without NA0): the smart contract in the absence of NA0 optimizes the objective function while systematically destroying subjecthood — DeFi liquidation without a grace period, exploit as legitimate execution, governance without normative contestation. A normative axiom de facto exists in the ecosystem — The DAO hard fork — but is applied retroactively without procedural guarantees. Volume III, P2 (supremacy of code with normative axiom): NA0 and N1–N7 are introduced as constitutional constraints into the specification of all constitutional contracts; Coq verification establishes that for every system state, execution of the contract does not violate NA0; the principle of code is law is preserved with a constitutional limit.

Vector 5. State capture → Sybil trilemma → Civic Guard + Digital Census.

Volume I, Regularity 12 (regulatory capture): predictive capital is converted into regulatory influence through lobbying mechanisms and informational asymmetry (ΣA17), generating the

structural impossibility of state neutrality in the regulation of digital platforms. Volume II, T15 (Sybil trilemma): verification of the uniqueness of a subject in an open network without a trusted center, without economic discrimination, and without social discrimination is logically irresolvable — the three existing classes of approaches — PoW/PoS, biometric, social graph — violate at least one of the three conditions (Regularity 20). State KYC violates condition 1 with the ΣA17 defect. Volume III, P6 (constitutional status of the Civic Guard) + P13 (Digital Census with Dual Suspicion Protocol): the normative resolution through a constitutionally bounded trusted center — P3 violates condition 1 intentionally while satisfying conditions 2 and 3; the mandate of the verification body is constitutionally bounded with a prohibition on the use of data beyond that mandate; VRF-based panel selection precludes the strategic formation of panel composition.

Vector 6. Marginalization of opposition → Absorption of critique → SovereigntyShield + constitutional form.

Volume I, Regularity 11 (marginalization of opposition): algorithmic engagement optimization generates a systematic reduction in the reach of content not conforming to the platform's objective function — oppositional narratives are marginalized structurally rather than through explicit prohibition. Volume II, T16 (absorption of critique): the same logic applies to critical discourse about blockchain — critique without an institutional alternative is absorbed through integration into the legitimation narrative of the ecosystem; conditions (a) and (b) of T16 are satisfied for the entire existing body of critique — Zamfir, Weaver, Golumbia. Volume III, P17 (SovereigntyShield) + constitutional form as such: P17 blocks the conversion of predictive capital into regulatory influence, extirpating the operational mechanism of marginalization; the constitutional form of Virtublic is structurally non-absorbable through T16 — a constitutional norm cannot be cited as proof of openness; it can only be observed or violated.

Vector 7. Constitutional necessity → Blockchain as necessary substrate → The entirety of Volume III.

Volume I, T10 (constitutional necessity): individual action, informal collective action, and national regulation are structurally insufficient forms of constraining predictive capital; the sole sufficient form is constitutional architecture external to the logic of digital capital. Volume II, T17 (blockchain as necessary substrate): blockchain technology is a necessary but insufficient condition of constitutional architecture — zk-proof makes N1 + P13 possible; smart contract makes P2 possible; cryptography makes P3 possible; formal verification makes P18 possible; however, blockchain without NA0 reproduces T11–T16. Volume III, P0–P18 in their totality: the entirety of Volume III is the sole identified realizable form simultaneously necessary — through T10 — and technically achievable — through T17 — for the protection of subjecthood within the meaning of NA0. No principle P0–P18 is redundant: each closes a specific structural defect recorded in Volumes I–II.

G.3. Control parameters of the matrix

Completeness of theorem coverage: all seven theorems of Volume II (T11–T17) have an incoming connection from Volume I and an outgoing connection to Volume III. An unclosed theorem would constitute evidence of either diagnostic surplus — a theorem without a

normative response — or architectural deficit — a normative response without a diagnostic foundation.

Completeness of principle coverage: P0, P2, P3, P4, P6, P13, P14, P16, P17 have direct incoming connections through the matrix. Principles P1, P5, P7–P12, P15, P18 receive justification through derivative connections from elements recorded in the matrix and are elaborated in the main text of Volume III with explicit references to the corresponding axioms and theorems.

Verification criterion: the matrix conforms to NA0 if and only if for each structural defect recorded in Volumes I–II there exists at least one principle of Volume III formally verified through P2 as blocking that defect. Verification of the completeness of the matrix is a mandatory component of the Coq specification of P18.