VIRTUBLIC

CYBER-CONSTITUTION

WHITEPAPER

VIRTUBLIC

Whitepaper: *The Cyber-Constitutional Republic as a Technological Protocol*

Virtublic · 2026

Virtublican Party · Henry Irving *(5631826)*

Full theoretical basis: Virtublic Theory (Volumes I–III) — www.virtublic.one

Abstract

This document describes the Virtublic protocol — the first implementation of a cyber-constitutional governance architecture in digital space — built upon a fundamental distinction between two classes of digital institutions: DAOs (Decentralized Autonomous Organizations), which coordinate profit according to the logic of a joint-stock company, and DAIs (Decentralized Autonomous Institutions), which coordinate sovereignty according to the logic of a constitutional mandate — the same logic that distinguishes a court from an auction.

This distinction emerges as a response to a structural contradiction that state regulation, market mechanisms, and existing blockchain architectures have neither resolved nor are structurally capable of resolving: commercial logic inevitably subordinates political logic, transforming any attempt at digital institutional construction into a reproduction of plutocracy on a new substrate.

The Virtublic protocol resolves this contradiction through an architecture in which the violation of constitutional norms is not merely politically undesirable but technically impossible: the constitution is implemented as formally verified executable code — not as a text open to interpretation by those who hold the power to interpret it.

If code is law, a law over the legislator is required. The subject whose attention and will give digital space its meaning and its value has the rightful claim to power over the rules by which that space operates. This is what a digital constitution is — not a document, but

an executable protocol that makes it structurally impossible to write rules against the subject, regardless of who stands at the code.

Document Navigation

This whitepaper is written for multiple audiences simultaneously. The guidance below indicates which sections are most relevant to each reader type.

Audience	Recommended Sections
Investor / Strategic Partner	Sections 1–5, 9–10, 13
Developer / Technical Specialist	Sections 6–8, 12 (Threat Model)
Political Theorist / Human Rights Advocate	Sections 1–5, 10
Reader without blockchain background	Sections 1–5 (sufficient without loss of meaning)

1. The Problem

Every person in digital space is being worked on by a personal intelligence system — and not only the kind with a chat window. Every application, every interface, every feed, every platform is a node in a unified predictive infrastructure that does not persuade through argument but shapes desires before a person has the chance to recognize them as their own. It imposes preferences through consumer logic, captures attention through mechanisms functionally identical to addiction, and sells the precision of this control to whoever will pay — advertisers, political campaigns, states. The subject does not notice the labyrinth because the labyrinth is designed to look like freedom of choice.

Power unconstrained by a constitution does not pause — it compounds. The greater capital's control over digital space, the more effectively it suppresses even the theoretical possibility of a social counterweight: it buys regulators, marginalizes alternatives, and funds criticism that poses no threat to the underlying architecture. There is no internal saturation point. The largest single buyer of this power is the state — the very institution that is theoretically mandated to constrain it.

Societies have always moved toward equilibrium. Bitcoin removed the financial intermediary from transactions. Ethereum removed the intermediary from contracts. DAOs removed the centre from organizational governance. Each step represented genuine progress — and each reproduced the original problem at a new level: code became law, but the legislator remained whoever writes the code. Developers without a mandate. Token holders whose voice is proportional to capital, not participation. At the centre stood, as before, the protection of money rather than the protection of the subject.

> *Digital space operates according to a single operational axiom: human subjecthood is a resource, and its destruction is an acceptable cost of economic efficiency. Attention, will, and identity are not protected — they are capitalised.*

2. Why Existing Solutions Fail

2.1. State Regulation

The GDPR entered into force in 2018. By 2024, Google and Meta together controlled more than 55% of the global digital advertising market. Regulation did not change the architecture of the system — it created a compliance industry embedded within the same economic logic.

This is not a failure of particular regulators. It is a structural property: law is enacted against the existing state of technology, and by the time it comes into force the technology has already changed. The state cannot be a neutral regulator of the predictive-data market while it is also a purchaser of that market: intelligence services, electoral campaigns, and tax authorities consume the same analytics that the state is theoretically meant to constrain. This is an architectural conflict of interest, not a temporary contradiction.

2.2. Blockchain and DAOs

Blockchain provided a precise answer to the question of trust in centralised financial intermediaries. But the blockchain community made one fundamental error in transposing the success of a financial primitive to the domain of political governance.

Code executes rules. But law has always existed. Monarchies enacted laws. Dictatorships enacted laws. The question was never whether rules exist — it has always been who writes them and whether a mechanism exists to protect the individual from the lawmaker. In DAOs, contracts are written by developers and large token holders. The substrate has changed; the structure has not.

Constitutionalism emerged precisely as the answer to this pattern: not merely law, but law above law — a mechanism that constrains the very possibility of enacting unjust rules. Code can execute rules. But only a constitution protects subjective agency from the rules themselves.

DAOs implement the principle of one token, one vote. The Ethereum Governance Study of 2023 found that in the majority of large DAOs, more than 70% of effective influence is concentrated in the hands of 1% of token holders. Decentralised in form; centralised in substance.

2.3. Critical Discourse

Books on surveillance capitalism became bestsellers. After reading them, people returned to the very applications they had just read about. This is a structural property of critique without institutional alternative: it channels tension, allowing the system to demonstrate “openness to discussion” while leaving the architecture unchanged. The most precise diagnosis that fails to become an organisation works in favour of the disease.

3. The Core Distinction: DAO and DAI

Understanding why Virtublic is necessary requires understanding this distinction — it is the conceptual core of the entire protocol.

Consider a joint-stock company. Its logic is straightforward: investors contribute capital, receive shares, shares confer voting rights proportional to investment, and the goal is profit. A DAO is a joint-stock company on the internet. Tokens instead of shares; smart contracts instead of a charter. A useful form for coordinating commercial enterprises in a decentralised environment.

Now consider something different: a Constitutional Court, a central bank, an electoral commission, a jury. Their purpose is not profit but the protection of rights and the provision of fair procedures. Their legitimacy is not grounded in capital — it is grounded in a constitutional mandate from citizens. When a Constitutional Court issues a ruling with which the wealthiest people in the country disagree, the court is not dissolved. That is precisely its purpose: to say “no” to those who have the money and power to say “yes”.

Attempt to build a court on the DAO model and the result is a system in which rightness is determined by whoever holds the most tokens. That is not a court; it is an auction.

> *A DAI (Decentralized Autonomous Institution) is an institution on the internet. Not a company, not a service, but an institution with a constitutional mandate, with rules that no single person can modify unilaterally, with mechanisms protecting the minority from the majority and the citizen from the system itself.*

	DAO	DAI
Source of legitimacy	Token holders	Citizens via constitution
Voting principle	One token — one vote	One citizen — one vote (EQU⊥)
Purpose	Profit / utility	Protection of subjective agency
Rules written by	Developers and whales	Constitutionally verified code
Minority protection	No structural guarantee	Constitutionally embedded
Rule amendment	Token majority	Strict constitutional procedure

Blockchain failed to scale beyond financial applications not for technical reasons, but for institutional ones. A technology trusted with money but not with decisions is inevitably confined to a niche: decisions require legitimacy, legitimacy requires an institution, and no such institution existed. This structural absence — not network throughput, not transaction costs — was the only real barrier between blockchain and mass adoption across fifteen years of development.

Virtublic removes that barrier by establishing the first institutional layer of blockchain infrastructure. Not on top of existing protocols, but within them — built on the same foundation of zk-proofs, smart contracts, and formal verification that blockchain has already proven reliable. The difference is that this foundation now carries a constitutional superstructure for the first time: rules that no single actor can modify unilaterally, and an institution whose legitimacy derives from the mandate of citizens rather than the size of capital holdings.

The consequence is not an improvement of existing blockchain applications, but the opening of an entirely new class of applications that have remained technically possible yet institutionally blocked: digital courts, verifiable elections, constitutionally protected public spaces, systems for the collective governance of shared resources. All of these required one thing — an institution that can be trusted without understanding cryptography, in the same way that a citizen trusts a constitution without being a lawyer. Virtublic is that institution. And it is precisely this that transforms blockchain from a niche financial infrastructure into a universal technology for public governance.

4. Competitive Analysis

An honest answer to the question “how does Virtublic differ from Optimism Citizens House, Gitcoin Passport, or Worldcoin” carries more weight than any marketing claim.

Project	What it implements	Limitation
Optimism Citizens House	Bicameral system: token holders + citizens	Citizens are appointed, not verified through an independent protocol; constitutional core is amendable by the core team
Gitcoin Passport	Sybil resistance for quadratic funding	Not a governance system; solves identity verification without building institutional architecture around it
Worldcoin / World ID	Scalable uniqueness verification via biometrics	Biometric data stored centrally; iris scan is a permanent identifier with no recovery path if the database is compromised
Virtublic	DAI: identity verification as the basis of sovereignty	Verification is one layer within a broader constitutional architecture

The fundamental distinction of Virtublic lies not in verification technology but in what verification is for. Gitcoin verifies identity for funding. Worldcoin verifies identity for income distribution. Virtublic verifies identity for sovereignty. Virtublic is compatible with World ID as one input signal to the first verification layer, but does not depend on it as its sole source.

5. What Virtublic Is

Virtublic is a protocol for creating DAIs: Decentralized Autonomous Institutions with constitutional governance. In practice, this means four interconnected elements.

Constitution as executable code

Constitutional norms are not text interpreted by an arbitrator but formally verified code. A decision that violates the constitution cannot be executed — not because someone will block it, but because the protocol physically cannot carry it out. This eliminates the most common historical mechanism of constitutional erosion: the “flexible interpretation” of fundamental law by those who hold interpretive power.

Separation of political and economic sovereignty

EQU⊥ is political sovereignty: one citizen, one vote, non-transferable, non-accumulative. VIC⊥ is economic reward for verified infrastructure contribution. These two types are structurally non-convertible into one another.

Non-transferable identity

Implemented via a Soulbound NFT — a token impossible to transfer because the smart contract rejects the transfer operation by definition. Participation simultaneously remains anonymous through zk-SNARK protocols.

Verifiable institutions

Infrastructure for DAIs with capture-resistant procedures: the Civil Guard (analogous to a jury, randomly constituted via VRF protocol), the Constitutional Convention (constitutional assembly through random selection of delegates), and the Conflict-Resolution Core (dispute resolution through verification, not subjective arbitration).

6. Architectural Strategy: From L2 to Sovereign Chain

Most blockchain projects make one of two architectural choices: they either remain on an external network indefinitely (inexpensive, but dependent) or build their own blockchain from the outset (independent, but costly and risky at launch). Virtublic adopts a third approach — a three-phase trajectory with clear transition trigger points.

The core problem with permanent L2 deployment is two fundamental contradictions with Virtublic's constitutional values. The first is voting economic sovereignty: if the cost of an EQU⊥ transaction is determined by the market conditions of an external network, a citizen may face a de facto property qualification on governance participation at the moment of an important constitutional decision. A governance system cannot depend on gas prices during an NFT boom on a third-party platform. The second is censorship resistance: in principle, base-layer validators may be subject to regulatory pressure directed specifically against Virtublic.

Phase	Period	Trigger	What it provides
Phase I: L2 Bootstrap	2026	Development start	Existing ecosystem, native Groth16 in zkSync, low barrier to entry
Phase II: Appchain	2027–2028	10,000 citizens + 50+ operators	Transaction cost control, own consensus, censorship resistance
Phase III: Sovereign Chain	2029–2030	50,000 citizens + Coq Phase 3	Full architectural independence; rules defined exclusively by the Virtublic constitution

> *Each phase has measurable transition triggers, not arbitrary dates. This is more honest than a promise of immediate independence and more realistic than indefinite dependence on third-party infrastructure.*

7. Technical Architecture

7.1. Identity and Soulbound NFT

Every Virtublic citizen undergoes uniqueness verification through the Digital Census. The result is a Soulbound NFT — a non-transferable identifier stored locally on the citizen's device through the ERC-5114 standard with an extended soul_binding_proof field. No biometric data is transmitted to a centralised server.

At each vote, the citizen generates a zk-SNARK proof on their device using the Groth16 scheme: proof size is approximately 2 KB, generation time on a mobile device is approximately 3 seconds, and on-chain verification cost is approximately 500K gas on EVM-compatible networks. The proof simultaneously attests to two facts: membership in the set of verified citizens (membership proof via Merkle Tree) and the absence of a prior vote on the same proposal (nullifier hash). The protocol verifies both assertions without disclosing identity. Vote anonymity is a cryptographic guarantee, not a policy. The Digital Census is conducted every six months (re-census), keeping the identifier base current and increasing the cost of maintaining fictitious identities over time.

Full specification: github.com/virtublic/protocol (to be released after Q3 2026 audit).

7.2. Dual Sovereignty (EQU⊥ / VIC⊥)

EQU⊥ exists as an entry in a Merkle Tree of identifiers with a root verifiable on-chain. It is not held in a wallet and does not exist as a standalone token — it is an attribute of the specific citizen's Soulbound NFT. No identity means no EQU⊥. Political votes physically do not exist as an asset available for purchase.

VIC⊥ is implemented as a standard ERC-20 token with an additional constitutionalCheck modifier at the GovernanceEngine level: any attempt to use VIC⊥ as an argument to an EQU⊥ vote causes the contract to revert with the code SOVEREIGNTY_VIOLATION. This separation is implemented in code and verified at the first stage of the Coq specification. The epoch mint cap is 1 million VIC⊥, distributed proportionally to verified contribution. This parameter is governance-adjustable via EQU⊥ vote, preventing inflation as the operator base grows.

Full specification: github.com/virtublic/protocol (to be released after Q3 2026 audit).

7.3. Formal Verification: Status and Strategy

Full formal verification of a production governance system in Coq is an active research challenge — no existing blockchain project has achieved it in its entirety. Virtublic implements a staged strategy in which each phase verifies a concrete set of invariants rather than claiming abstract “verifiedness”.

Phase	Timeline	What is verified
Phase 1	Q3 2026 — Q1 2027	Impossibility of EQU⊥/VIC⊥ conversion; correctness of nullifier-protected double-vote prevention; impossibility of Soulbound NFT transfer
Phase 2	2027	Quadratic voting mechanisms, SovereigntyShield, CoalitionVerification
Phase 3	2028–2029	Full verification of constitutional core P0–P7

Phase 1 Coq files are available for audit upon request by verified partners via virtublic.one.

7.4. Madison Mode and Concentration-of-Influence Protection

The Madison Mode mechanism implements a quadratic cost function for influence: cost(n) = n², where n is the number of additional votes above the base allocation. One vote is free for every citizen. Ten votes cost 100 VIC⊥. One hundred votes cost 10,000 VIC⊥. One thousand votes cost one million VIC⊥. The mathematics makes bulk influence purchasing exponentially costly.

The Success Multiplier implements the formula effective_influence = n × √(n_supporters), where n_supporters is the number of unique citizens who have independently supported a position via separate transactions with distinct nullifier hashes. A coalition of 100 independent citizens with the same aggregate budget is 3.16 times more effective than a single actor with the same budget; a coalition of 1,000 is 5.62 times more effective. The Coalition Verification Protocol checks coalition organicity: members must not have voted identically across all of the last 10 decisions, preventing the simulation of broad support through coordinated accounts.

Full specification: github.com/virtublic/protocol (to be released after Q3 2026 audit).

7.5. Sybil-Attack Resistance: Hybrid Proof-of-Personhood

Virtublic implements a hybrid Proof-of-Personhood (Hybrid PoP) combining three layers of protection.

– Layer 1 — hardware-bound attestation: verification is bound to a physical device via TPM 2.0 or Secure Enclave (Apple SEP / Android StrongBox), requiring real hardware for each identity.

- Layer 2 — behavioral analysis: adaptive behavioural tests verifying indicators of a live subject without disclosing identity.
- Layer 3 — Civil Guard: when automatic layers fail, the case is referred to a randomly selected citizen panel.

The protocol accepts attestations from World ID, Humanity Protocol, and Human Passport as Layer 1 inputs, integrating with the emerging digital-identity ecosystem. Under the current design, the cost of creating 10,000 fictitious identities that pass all three verification layers exceeds $5 million, accounting for hardware costs, the cost of developing a system to circumvent behavioural analysis, and the probability of detection during the Dual Suspicion Protocol. Re-census every six months doubles this cost for long-term attacks.

Full specification: github.com/virtublic/protocol (to be released after Q3 2026 audit).

7.6. Proof-of-Resource and Infrastructure Economics

Node operators receive VIC⊥ for verified real-world contribution through random challenges with time windows that are mathematically impossible to simulate without genuine resources. Base rates are governance-adjustable: 1 GPU-hour corresponds to approximately 100 VIC⊥; 1 TB of storage to 20 VIC⊥ per day; 1 Gbps of bandwidth to 50 VIC⊥ per hour.

Protection against grinding attacks is provided by a Verifiable Delay Function (VDF): the VRF seed is secured such that the minimum computation time exceeds one hour, making enumeration computationally infeasible. One epoch is 30 days. Average turnout in comparable protocols (Pyth DAO, Synthetix) is 15–25%; at that level 30 days is optimal for balancing security and responsiveness. If turnout falls below 30% in two consecutive epochs, the epoch length is automatically reduced to 15 days via a governance trigger.

To support long-term infrastructure stability, multi-epoch commitments are available: an operator may lock VIC⊥ for 3–6 epochs with a reward multiplier of 1.2–1.5. CollectiveBond redistributes 20–30% of burned VIC⊥ as long-term infrastructure grants via the CivicJuryEngine.

Full specification: github.com/virtublic/protocol (to be released after Q3 2026 audit).

7.7. SovereigntyShield: State Capture Prevention

SovereigntyShield is a self-executing norm implemented as a standalone smart contract SovereigntyShield.sol with a StateAccessAttempt event that records every request from addresses included in the StateRegistry. Unratified requests return a revert with code UNAUTHORIZED_STATE_ACCESS. Ratification requires 75% EQU⊥ with explicit

specification of purpose, scope, duration, and oversight mechanism via an on-chain proposal. Mandates do not renew automatically — each renewal requires a new vote.

Full specification: github.com/virtublic/protocol (to be released after Q3 2026 audit).

8. Economic Model

Virtublic separates two economic flows whose conflation in most blockchain projects is the structural cause of plutocracy.

Infrastructure Flow (VIC⊥)	Political Flow (EQU⊥)
Convertible and accumulative asset. Demand is generated through Madison Mode, payment for protocol infrastructure services, and CollectiveBond. Epoch mint cap: 1 million VIC⊥ (governance-adjustable).	Not a financial asset. Does not trade on secondary markets. Does not exist separately from the citizen's Soulbound Identity. The political vote has no market price — an intentional design decision.

CollectiveBond protects citizens from bad-faith operators: operators lock a portion of VIC⊥ as a security deposit, automatically confiscated upon a verified breach, with 20–30% of burned funds redistributed as long-term infrastructure grants through the CivicJuryEngine.

9. Bootstrap: Party, Protocol, and Genesis

> *A protocol that claims protection against capture but does not explain who controls it at launch is not an honest document. This section is therefore mandatory.*

The Virtublican Party serves as the temporary development coordinator and initial custodian of the technical specification during the bootstrap phase. The VIC⊥ genesis distribution takes place through a publicly auditable process:

Allocation	Purpose	Control mechanism
40%	Infrastructure fund	Three-layer multisig (5-of-9)
30%	First verified node operators	Proportional to verified contribution
20%	Protocol development fund	Public governance via 12-month timelock
10%	Legal reserve	Multisig 3-of-5

The Party receives no special rights in the protocol unavailable to other participants — a constitutional obligation recorded in the genesis transaction and verified by the Coq invariant no_privileged_actor. Upon reaching 1,000 verified citizens, governance of genesis parameters passes fully and automatically to EQU⊥ voting via a smart contract with a time lock, requiring no further decision by the team.

The threshold of 1,000 citizens does not mean the system is fully protected; it marks the point at which the system becomes sufficiently self-sustaining for political self-defence. A living community of citizens undergoing genuine verification holds a structural advantage over any attacker who must conceal the origin of their identities, circumvent behavioural analysis, and pay a hardware premium for fictitious devices.

10. The Virtublican Party: From Theory to Technology

10.1. The Theory That Cannot Be Taken Away

Virtublic is, at present, a theory proven across three books:

Volume I — Digital Capital The Political Economy of Attention and the Morphology of Algorithmic Domination

Volume II — The Capital of the Digital Economy A Critique of Blockchain, Cryptocurrency, and Digital Democracy

Volume III — The Theory of the Digital Republic The Constitutional Architecture of Virtublic

Theory must become technology. That transition is impossible without organisation. But before describing that organisation, there is a question any serious participant will ask before all others: what happens if a specific implementation fails?

The answer is structural, not rhetorical. What has already been created is not a startup — it is an axiomatic theory. Theories do not die from failed implementations. Marxism did not disappear after the collapse of the states built in its name. Liberalism did not disappear after liberal regimes fell. A theory lives in discourse, in academic circulation, in the next generation of practitioners who return to it — more precisely, more deeply, having learned from what went wrong before. The three volumes that formalise cyber-constitutionalism as an axiomatic system have already claimed this ground. It cannot be taken away, cannot be purchased, cannot be refuted by the failure of any particular implementation. People will return to this theory and continue the discourse even if the startup fails a hundred times — because the problem the theory describes will compound faster than failures accumulate.

10.2. A Paradigm, Not a Product

This is the essential distinction from any commercial approach. Marketing sells a product — and dies with it. Political agitation carries an idea forward — and it lives on in those who

have taken it up, regardless of what happens to any specific organisation. A logo belongs to a company. An emblem belongs to a movement. When a company closes, the logo disappears. When a movement dissolves, the emblem remains — a symbol people return to. Virtublic is not a brand to be defended against competitors. It is a political paradigm that grows stronger with every failed implementation, because every failure is new empirical evidence for the central thesis: power without constitutional constraint reproduces concentration regardless of the substrate it operates on.

Cyber-constitutionalism as an ideology has already been claimed at the level of theory. What this means in practice is the following: anyone who builds digital institutions with constitutional architecture in the future will be working in a space that Virtublic defined first. This is how ideological priority functions — not through patents or market share, but through the fact that the language, categories, and normative principles in which the problem is framed have already been established. Whoever sets the language determines what counts as a solution.

This is precisely where the narrative opens space for action where commercial approaches hit a ceiling. A commercial project competes for market share — and loses to whoever has more capital. A political paradigm competes for minds — and here the structural advantage belongs to whoever describes most accurately what people already observe. An ideology of subjecthood protection generates the potential for emergent activism: every person who has felt that digital space works against their interests is already a potential Virtublic citizen before they have ever heard the word. The task is not to convince them — it is to give them the language for what they already know.

10.3. Six Functions of the Party

This is why the Virtublican Party is organised as a new kind of political party rather than a board of directors. A board of directors protects the interests of shareholders and ceases to exist when the project closes. A political party protects the interests of citizens and exists for precisely as long as the problem it was formed to address remains unsolved.

The Party performs six functions. It shapes discourse — explaining why the existing architecture of digital power constitutes a structural problem that cannot be corrected from within the system. It coordinates development through technical working groups and an open roadmap tied to measurable milestones rather than calendar dates. It attracts investment

from funds operating under transparent conditions and verifiable mandates. It builds legal precedent by supporting litigation in the field of digital rights. It forges coalitions with human rights organisations and the academic community. And it cultivates citizens — building the educational foundation without which any constitution remains a dead letter.

10.4. Three Principles

Three principles define the Party's operational architecture. Jurisdictional independence means the absence of registration in any jurisdiction capable of exerting pressure through corporate mechanisms.

Protocol consensus means that decisions are made through verifiable procedures, no position is held indefinitely, and financial decisions require multi-signature authorisation. Constitutional self-limitation means that the Party exists to build the Virtublic that will render the Party itself unnecessary. An organisation whose purpose is its own dissolution through success is the only form structurally protected against becoming an end in itself.

Any participant who sets out to assess the risks of this project will eventually arrive at a symmetrical question: what is the risk of not participating in the formation of the first axiomatic theory of cyber-constitutionalism — at the precise moment when the necessity of such a theory is becoming apparent to everyone except those who are structurally invested in keeping it obscure.

11. Roadmap

The Virtublic roadmap is tied to measurable metrics rather than calendar dates — a principled decision. A date without a metric is a commitment without accountability.

Period	Metric	Key milestones
Q2 2026	10,000 supporters, 500 participants	zk-Census testnet. Security audit of nullifier scheme and membership proof. Repository opened. virtublic.one launched. First 20 Party Nodes formed.
Q3–Q4 2026	1,000 citizens	Mainnet on zkSync/Arbitrum (Phase I). EQU⊥/VIC⊥ contracts + SovereigntyShield. First investment round. Automatic transfer of genesis parameters to EQU⊥ governance.
2027	10,000 citizens	Coq Phase 2. First live DAIs. Civil Guard with VRF selection. Conflict-Resolution Core. Transition to Appchain (Phase II). 15 countries.
2028–2030	100,000 citizens, 5 active DAIs	Coq Phase 3. Sovereign Chain (Phase III). International legal discourse. 30+ countries.

12. Threat Model

12.1. Attacker Classes

Class	Budget	Objective
Financially motivated	$1–50M	Control of VIC⊥ governance to redirect infrastructure grants
Politically motivated (state/corporate actor)	>$100M	Access to citizen data or blocking of SovereigntyShield
Technical attacker (researcher/group)	Variable	Vulnerabilities in smart contracts or zk-circuits
Sybil attacker	Variable	Fictitious identities for capture of EQU⊥ voting

12.2. Economic Attack Scenarios and Market Symmetry

An attack on EQU⊥ voting via influence purchase is architecturally impossible: EQU⊥ is not a market asset. Purchasing EQU⊥ votes means creating fictitious identities — which reclassifies the attack as a Sybil attack (Section 12.4).

An attack on VIC⊥ governance through Madison Mode has a fundamental property that distinguishes it from attacks on conventional DAOs: it is public and informationally symmetric. When an attacker begins accumulating VIC⊥ for governance influence, they do so on an open market where every transaction is visible on-chain. This creates two immediate defensive mechanisms. First, the accumulation itself raises the price of VIC⊥, making each subsequent step more costly than the last — an escalating rather than linear cost structure. Second, the anomalous price movement is a public signal to any interested defender, who may enter the same market. The attacker operates without informational privilege or first-mover advantage; every manoeuvre strengthens the incentive for counter-action. Meanwhile, a diffuse coalition of citizens with the same aggregate budget holds a structural advantage of 3–5 times through the Success Multiplier, meaning the cost of defence is lower than the cost of attack by protocol design.

12.3. Coordinated Collusion in the Civil Guard

With a panel size of 21, an attacker must coordinate 14 of 21 jurors to obtain a two-thirds qualified majority. The probability of an attacker controlling k fictitious citizens obtaining 14 of 21 seats in a random selection from a base of N citizens is $C(k,14)\times C(N-k,7)/C(N,21)$. At

N=10,000 and k=1,000 (10% fictitious), this probability is approximately 0.003%. At k=3,000 (30%), it rises to approximately 4.1%, which warrants additional protective mechanisms — which is precisely why the Dual Suspicion Protocol includes behavioural analysis, reducing a realistic k to below 5% of the base. Panel rotation after each Census cycle eliminates the possibility of investing in long-term corruption of permanent members.

12.4. Sybil Attack and Cost Asymmetry

The cost of creating 10,000 fictitious identities that pass all three Hybrid PoP layers exceeds $5 million: hardware costs ($1.5–2M), development of a system to circumvent behavioural analysis ($2–3M), and the probability of detection during the Dual Suspicion Protocol. Re-census every six months doubles this cost for long-term attacks.

> *The nature of the asymmetry is critical: genuine citizens do not bear these costs because they have no need to conceal the provenance of their identities. As the number of real citizens grows, system protection increases at an accelerating rate — each additional real citizen makes a Sybil attack relatively more expensive at no additional cost to the community.*

12.5. Governance Capture Simulation

Full capture of EQU⊥ governance requires control over more than 50% of verified citizens while simultaneously passing all Hybrid PoP layers. Capture of VIC⊥ governance in the presence of a diffuse coalition of 1,000 citizens each holding 1 VIC⊥ requires an effective influence of 1,000 × √1,000 = 31,623 VIC⊥ from the attacker. To exceed this value through Madison Mode requires more than $31{,}623^2 \approx 1$ billion VIC⊥ — against a mint cap of 1 million per epoch, this is technically impossible within a single epoch and requires years of accumulation during which market dynamics and community growth make the attack progressively more costly.

13. Risks

Risk	Substance	Mitigation strategy
Regulatory uncertainty	The legal status of Soulbound NFTs, EQU⊥ as a non-financial asset, and a jurisdictionally independent organisation is nowhere definitively settled. Regulatory pressure may be applied through developers and node operators.	Staged legal structuring with digital-law specialists. Beginning with technical infrastructure before advancing to politically sensitive functions.
Technical complexity of Coq verification	Ambitious timelines may not survive contact with reality.	Staged verification with explicit delineation of what is verified now and what is in development. Metrics-based rather than date-based milestones.
Low initial adoption	With few Census participants, the Civil Guard is too small for robust protection.	Minimum threshold of 500 verified citizens for full functionality activation; system operates in testnet mode below this threshold.
Dependence on external PoP protocols	World ID and Humanity Protocol may change their policies.	No external PoP is mandatory. The protocol functions with any combination of verification layers.
Bootstrap coordination risk	The transfer of governance at 1,000 citizens could become a political decision rather than a technical one.	The transfer is encoded in the genesis transaction as an automatic smart contract, requiring no team decision.

14. Open Source

The Virtublic protocol is distributed under a dual licence: AGPL-3.0 for governance components (copyleft, ensuring openness of all derivative works) and MIT for zk-circuits and Coq specifications (maximum compatibility for cryptographic primitives).

The repository will be opened following the completion of the initial security audit in Q3 2026: github.com/virtublic/protocol. Until that point, code is available for review upon request by verified technical partners via virtublic.one. Phase 1 Coq verification files are available through the same channel.

15. Conclusion

Bitcoin proved that a financial intermediary is not a necessity. Ethereum proved that programmable contracts without a trusted third party are possible. Each of these proofs exposed the next unsolved question. Virtublic answers the one that determines all the others: who protects the subject from the protocol itself.

Virtublic is not the next DAO. It is the first DAI protocol. DAOs coordinate profit. DAIs coordinate sovereignty. The difference between them is not technical — it is political. That is precisely why it matters.

Freedom is not the absence of rules.
Freedom is the rules that protect freedom.

The code serves the sovereign.
The sovereign remains a subject.

Virtublic Whitepaper · March 2026
Virtublican Party · Henry Irving · www.virtublic.one
Full theoretical basis: Virtublic Theory (Volumes I–III) — www.virtublic.one
Repository after Q3 2026 audit: github.com/virtublic/protocol
Licence: AGPL-3.0 (governance) + MIT (zk-circuits, Coq-specs) · Contact: www.virtublic.one