CAN BLOCKCHAIN REALLY SOLVE VOTING?

From Crypto Narrative to Election Engineering: A BSV-Focused Research Guide

Version 1.0 — Reviewed August 15, 2026
A BitcoinSV.Guide Research Report

A practical guide to the different classes of voting, the security and governance problems they create, the capabilities blockchain may contribute, and the research required before BSV—or any blockchain—can responsibly claim to secure real-world elections.

Research Library: *BitcoinSV.Guide — Miscellaneous Reports*

PURPOSE AND SCOPE

For years, blockchain projects have pointed to voting as an obvious future use case. The logic appears simple: votes are records; blockchains create tamper-resistant public records; therefore blockchain should make elections more secure.

There is truth inside that idea. There is also an enormous amount missing from it.

“Voting” itself describes several fundamentally different problems. A token holder voting on a DAO proposal, shareholders electing a corporate board, homeowners voting on an association assessment, and citizens choosing a president may all be called votes, but they do not begin with the same definition of an eligible voter, use the same allocation of voting power, require the same level of ballot secrecy, face the same coercion risk, or carry the same consequences if the result is wrong.

This paper therefore has **two distinct stages and two audiences**.

Stage One is educational. It is intended for blockchain users, investors, policymakers, journalists, developers and interested citizens. Its purpose is to move the reader from the familiar narrative that “blockchain can solve voting” into an understanding of what election engineering actually involves. The goal is not to bury readers in cryptography, but to make the hidden problems visible.

Stage Two is a research and builder guide. Using BSV Blockchain as the principal technical focus, it identifies the areas a serious project would need to research: identity, eligibility, anonymous voting authority, endpoint security, coercion resistance, privacy, tally verification, network security, recovery, governance, accessibility and law. It also asks where existing BSV architecture may provide useful tools, where new work may be required, and where blockchain may not be the right tool at all.

This paper does **not** present a finished BSV voting system. Its purpose is more fundamental:

> **To define the terrain that must be crossed before anyone can credibly claim to have built one.**

TABLE OF CONTENTS

STAGE ONE — FROM NARRATIVE TO REALITY

STAGE TWO — A RESEARCH GUIDE FOR BUILDERS

EXECUTIVE SUMMARY

“Blockchain voting” is an appealing phrase because blockchain appears to address one obvious election problem: once a legitimate vote has been cast, nobody should be able to secretly alter or delete it.

But an election can fail without anybody altering the blockchain. An ineligible person can receive legitimate-looking voting authority. Malware can display one candidate while constructing a ballot for another. A voter can be coerced. A credential can be stolen or sold. A network can become unavailable. Encrypted ballot information preserved permanently can become readable decades later. A tally can be wrong even though every included transaction is genuine. Finally, a system can successfully prove that an election failed while possessing no independent evidence from which the correct result can be reconstructed.

Serious election engineering therefore treats voting as a **system of interdependent problems**, not a ledger problem. The U.S. Election Assistance Commission and NIST are developing a public evaluation process for cryptographic end-to-end verifiable voting protocols. Among the properties being examined are whether ballots are *cast as intended, recorded as cast and tallied as recorded*, while protecting voter privacy, ballot secrecy, usability and accessibility. The process also incorporates software independence: an undetected software error should not be able to cause an undetectable change in the election result. (eac.gov)

The blockchain industry nevertheless has a long history of presenting voting as a natural use case. Cardano describes blockchain voting in terms of voter verification, vote integrity, auditability, transparency and accessibility. Algorand Foundation has promoted research using Algorand for vote counting and validation. Ethereum provides extensive infrastructure for DAO governance and token-based participation in which holding a governance token can itself confer voting rights. (cardano.org)

These examples expose an important definitional problem. **Not all votes are the same problem.**

A DAO in which one token equals one unit of voting power begins with a blockchain that already knows who controls the voting asset. A shareholder election may derive voting weight from shares held on a record date. A homeowner association may derive voting authority from ownership of a specific lot. A governmental election must establish that a legally eligible human being belongs to a particular jurisdiction, provide the appropriate voting entitlement, prevent duplicate participation, preserve a secret ballot, resist coercion, remain accessible and recoverable, and produce a result capable of surviving legal challenge.

For that reason, this paper primarily uses the **binding governmental secret-ballot election** as its hardest test case, while retaining corporate, cooperative, property-association and token governance as comparison classes and potential pilot environments.

The paper then asks a more disciplined BSV question:

> **If the requirements of the election are defined first, which parts of the resulting system could BSV actually make better?**

One promising area may be election evidence at scale. Another may be the administration of voter eligibility itself. Instead of periodically trusting a private voter database, a future architecture might make the issuance, modification, transfer, replacement and revocation of voting authority cryptographically auditable without publishing citizen identities. This paper calls that potential architecture an **Auditable Eligibility State Machine**.

A related problem is the **Identity Firewall**: transforming a known eligible person into an unknown but provably eligible voter. The ballot side should be able to determine that an authorized voting entitlement exists and has not already been used while remaining unable to discover which citizen exercised it.

BSV's existing identity architecture may be useful on the identity side of that boundary, but it should not be confused with the anonymous proof required on the ballot side. BRC-52 certificates are associated with a subject public key and support encrypted fields, selective revelation and UTXO-based revocation. BRC-53 provides workflows for creating those certificates and revealing selected fields to a designated verifier. These are useful identity capabilities, but **selective revelation is not the same thing as anonymously proving membership in an electorate**. (bsv.brc.dev)

These are research directions, not completed protocols.

Nor is BSV—or any blockchain proposed as election infrastructure—exempt from scrutiny. Any serious BSV election project would need to examine network finality, reorganizations, censorship, infrastructure concentration, wallet compromise, privacy leakage, availability, credential recovery and the legal significance of blockchain evidence. High transaction capacity, even if fully demonstrated, would solve only a capacity problem.

This paper ultimately proposes neither “BSV voting” nor “paper forever” as predetermined conclusions. Instead it presents three architectures that should be researched independently: the strongest system obtainable from established election science, a clean-sheet BSV-native architecture, and a later hybrid derived from both.

The final objective is deliberately bounded:

> **This paper does not solve voting. It attempts to make it much harder for anyone to pretend that voting has been solved before the engineering has actually been done.**

STAGE ONE — FROM NARRATIVE TO REALITY

1. HOW “BLOCKCHAIN SOLVES VOTING” BECAME A NARRATIVE

1.1 Why the Idea Is So Attractive

Blockchain and voting appear almost made for each other when described at a sufficiently high level. Elections produce records. Records should not be secretly altered. Distributed ledgers are designed to create records whose later alteration is difficult and visible.

The resulting story practically writes itself: place votes on blockchain, remove the central database, make the records immutable and allow everyone to audit the result.

Voting therefore became a natural example of future blockchain utility alongside finance, identity, health records, property titles and supply chains. That narrative remains active today. Cardano's public materials describe voting systems as a blockchain use case and argue that cryptographic identity, immutable vote records, public auditability and scalability could support secure elections. Algorand Foundation has highlighted research testing blockchain-based vote counting and validation on Algorand TestNet. (cardano.org)

Ethereum illustrates another side of the issue. Its ecosystem contains extensive DAO governance infrastructure, including token-weighted voting, delegation and automated execution of approved proposals. Ethereum's own documentation describes DAOs as organizations whose decisions can be governed through proposals and voting and notes that simply holding a governance token may confer voting rights. (ethereum.org)

None of this is inherently unserious. Blockchains really can be useful voting infrastructure in some environments. The problem begins when the single word **voting** conceals how radically those environments differ.

1.2 Governance Voting Versus Political Elections

Consider a token-governance rule:

1 governance token = 1 unit of voting power.

If the blockchain reliably establishes control of the tokens, a major part of the electorate problem is already solved. The system does not need to prove that a wallet belongs to one unique adult human citizen residing in Georgia. It needs to determine that the required cryptographic authority controls a defined quantity of governance tokens. Ethereum documentation describes this model directly: simply holding a governance token may grant access to voting. (ethereum.org)

A national election starts somewhere completely different. Before a ballot can even be evaluated, the system must establish that a legally eligible human being possesses the right to participate in that particular jurisdiction and contest. The blockchain cannot simply look up a token balance and be done.

This difference is so important that any claim to have “solved voting” should begin with a question:

> **What kind of voting are you talking about?**

1.3 The First Reality Check: Immutability Is Not Election Security

Four examples expose the problem.

A. Immutable bad eligibility. A corrupt or mistaken official issues a valid voting credential to an ineligible person. The blockchain records everything perfectly, but the underlying electoral authority was wrong.

B. Immutable wrong intent. Malware shows the voter Candidate A while creating a properly signed ballot for Candidate B. The blockchain preserves exactly what it received; the integrity failure occurred before the ledger became relevant.

C. Immutable coercion. A parent, spouse, employer, political operative or care-home worker watches someone vote and dictates the selection. The blockchain can preserve that coerced vote flawlessly.

D. Immutable failure evidence. Cryptographic evidence proves that 20,000 ballots were improperly processed. The system has succeeded at detection, but if no independent evidence of voter intent survives, it may still be impossible to determine the legitimate winner.

This is not theoretical nitpicking. The security analysis of the Voatz mobile voting system found vulnerabilities allowing different adversaries to alter, stop or expose votes despite a system whose security claims included a permissioned blockchain, biometrics and hardware-backed key storage. (usenix.org)

The lesson is not “blockchain is useless for elections.” It is narrower and more important:

> **Blockchain integrity begins only after the system has decided what information deserves to be treated as legitimate.**

1.4 The Second Reality Check: The System Still Has to Scale

Suppose every other problem is solved. A real election architecture still has to handle the workload generated by millions of voters, credentials, proofs, challenges, administrative changes, audit events and tally evidence.

Different blockchain ecosystems respond to scale differently. There is nothing inherently wrong with Layer 2 systems, channels, batching or off-chain computation; they may be excellent engineering solutions. But in an election they do not become invisible simply because they improve performance. If ballots, eligibility proofs, nullifiers, audit information or tally evidence pass through a secondary

system, then its operators, availability, censorship possibilities, retention rules and failure modes become part of the election trust model.

This gives BSV an interesting research question. BSV has pursued a scaling model centered on much larger transaction processing at the node layer. In a 2024 controlled AWS test, six geographically distributed Teranode nodes running across more than 500 machines sustained average throughput above one million transactions per second for two weeks. Current BSV technical documentation describes Teranode as a distributed microservices architecture designed for horizontal scaling, while its public test environment remains explicitly labeled as alpha testing. These are significant capacity demonstrations, but they are not evidence that Teranode is election-grade infrastructure. (teranode.bsvblockchain.org)

The competitive question therefore should not be reduced to a TPS contest:

> **How much additional election infrastructure must be introduced because the ledger itself cannot carry the desired workload, and what new trust assumptions come with it?**

Every proposed blockchain voting architecture must answer that question, including BSV.

---

2. FIRST DEFINE THE VOTE: NOT ALL ELECTIONS ARE THE SAME

2.1 Voting Versus an Election

For this paper, a **vote** is an authorized expression of preference or choice.

An **election** is the larger system that determines who is authorized to vote, how much voting authority each participant possesses, which choices are valid, how votes are collected and counted, and what consequence the result controls.

This distinction matters because a cryptographically perfect voting mechanism can still sit inside a badly designed election system.

2.2 Binding Governmental Elections

This category includes national, state, county, municipal and similar public elections and referenda.

The electorate normally consists of legally eligible human beings rather than cryptographic assets. Voting authority depends on facts such as citizenship, age, residence and jurisdiction. Ballot secrecy is usually fundamental. Coercion matters. Accessibility matters. Results can transfer governmental authority, determine taxation, enact law and exercise state power.

Consequently, the acceptable failure threshold is extremely low.

This is the **primary security test used in this paper**.

2.3 Corporate and Shareholder Voting

Corporate voting often begins from ownership rather than citizenship.

If voting authority is based on shares, the central question may be:

Who was entitled to exercise the voting rights associated with these shares on the record date?

Voting power may legitimately be unequal. One investor may possess thousands of times the voting weight of another. Proxy mechanisms may be normal rather than suspicious. Confidentiality requirements can differ from the civic secret ballot.

Blockchain may therefore be considerably more natural for certain shareholder-voting functions than for governmental elections.

2.4 Property and Homeowner Association Voting

Homeowner associations, property-owner associations, condominium associations and similar organizations are especially interesting intermediate cases.

Eligibility can arise from ownership of a specific property or membership interest. But the real world rapidly complicates matters: a home can have multiple owners; an owner can be a trust, estate or LLC; one person can own multiple properties; proxies may be permitted; different questions may use different voting weights; quorum may be as important as majority; ownership can change between the record date and voting date.

These elections can also be highly consequential. Boards control significant budgets, assessments, common property, contracts and organizational rules. Elections may be contested and ordinary nontechnical people must participate.

For that reason, property associations may eventually be **excellent proving grounds for serious blockchain voting research**. They contain meaningful identity, eligibility, quorum, delegation, secrecy and legal-governance problems without initially carrying the systemic risk of a national election.

2.5 Cooperatives and Closed Membership Organizations

Cooperatives, unions, clubs, professional organizations and other membership bodies create another class.

Membership can be externally defined while voting rights are often closer to one-member-one-vote than shareholder voting. Some ballots may need secrecy; others may not. The membership database itself can become an eligibility problem.

This creates an attractive environment for researching credential issuance, anonymous membership voting and auditable organizational governance.

2.6 DAO and Token Governance

DAO governance may be the most blockchain-native voting category.

Where the governance rule deliberately defines voting rights through tokens or another on-chain asset, blockchain already contains much of the authoritative state required to calculate voting power.

Ethereum's documentation is explicit that DAOs can use token-based membership, delegation and proposals and that simply holding a governance token may confer voting access. (ethereum.org)

This is real voting. It simply solves a different problem.

A token election can demonstrate excellent record integrity, delegation, execution and tallying while telling us very little about whether the same architecture can prove one-human-one-vote, protect a secret civic ballot or recover a disputed governmental election.

2.7 Advisory and Nonbinding Polling

Opinion polls, community preferences and nonbinding votes have still lower requirements.

They are useful environments for experimentation precisely because failure does not transfer governmental power or large economic rights. They should not, however, be presented as evidence that an architecture is ready for high-consequence elections.

2.8 Five Questions That Define the Voting Problem

For ordinary readers, the complexity can be reduced to five questions:

1. **Who is allowed to vote?**
2. **How much voting power does each participant receive?**
3. **Must the vote be secret?**
4. **Is the result binding, and what authority does it control?**
5. **What happens if the result is wrong?**

Those five questions radically change the engineering requirements.

2.9 Primary Scope of This Paper

The main security analysis that follows uses the hardest broad case:

> **A binding governmental election involving legally eligible human voters, ordinarily requiring a secret ballot and a result capable of surviving public and legal scrutiny.**

Other voting classes return later when we ask how the architecture and deployment path should change for less demanding environments.

---

3. WHAT A TRUSTWORTHY GOVERNMENTAL ELECTION ACTUALLY HAS TO ACCOMPLISH

The easiest way to understand why voting is not simply a blockchain application is to temporarily remove blockchain from the discussion and ask what an election must actually accomplish.

3.1 Legitimate Voting Authority

The system must determine whether a real person possesses the legal right to vote in the election in question. That can involve citizenship, age, residence, jurisdiction and legal status. People move. People die. Administrative records contain mistakes. Records can be duplicated. Exceptional and provisional procedures may exist.

The question is therefore not merely **“Can this private key sign?”** It is **“Why should whoever controls this credential possess political voting authority in this election?”**

3.2 Correct and Unique Voting Entitlement

Once eligibility is established, the correct election entitlement must be issued. For ordinary one-person-one-vote contests, one human should not obtain multiple usable entitlements, nor should the credential be trivially transferable, copied or sold.

This is where simplistic blockchain voting tokens encounter a problem: **one token that cannot be double-spent is not automatically one human who cannot vote twice.** Digital uniqueness and human uniqueness are different things.

3.3 Ballot Secrecy and Voter Freedom

The election must normally prevent other people from discovering how a specific voter voted, but secrecy is only half of the problem. The voter must also be able to exercise the choice freely.

A perfectly anonymous ballot submitted while someone is standing behind the voter with a threat is still not a free vote. Secret-ballot design, coercion resistance and vote-buying resistance therefore overlap but are not identical.

3.4 Capturing the Voter's Actual Intent

The election must ensure that the ballot represents what the voter meant to select.

Current EAC work on cryptographic end-to-end voting makes this distinction explicit through the property **cast as intended**, alongside recorded-as-cast and tallied-as-recorded. This is especially difficult with remote electronic voting because a compromised device occupies the space between human intention and cryptographic record. (eac.gov)

3.5 Preserving the Ballot

Once a legitimate ballot exists, the system must ensure it is not silently changed, deleted or replaced.

This is where blockchain begins to look much more naturally useful. Durable public evidence can potentially make later manipulation easier to detect and harder to hide, but preservation is only one stage.

3.6 Producing and Verifying the Correct Result

A collection of valid ballots does not automatically prove that the reported tally is correct. The public needs a way to establish that the announced result follows from the legitimate ballot set.

This can involve cryptographic tally proofs, public audit evidence, independent tabulation or physical recount mechanisms.

> **An inclusion proof is not a tally proof.**

3.7 Availability and Resilience

A voting system must function while under attack. The ballot may be immutable once submitted, but that provides little comfort if voters cannot submit ballots because the system is unavailable, election transactions are censored, credential services fail or networks are overwhelmed.

Election security therefore includes **availability**, not merely integrity.

3.8 Detection, Recovery and Legal Accountability

A secure system should detect serious failure. A complete election system must additionally answer what happens afterward.

If 50,000 ballots are proven unreliable, can the correct result be reconstructed? Does independent evidence exist? Is a partial rerun possible? Must the whole election be repeated? Who decides?

At some point technology hands the problem to law. The National Academies has emphasized human-readable paper ballots, independent auditing and risk-limiting audits in part because election systems need evidence that remains meaningful when software is distrusted. (nationalacademies.org)

3.9 Human Usability and Accessibility

A mathematically perfect election that ordinary citizens cannot use correctly is not a successful election.

The EAC's current cryptographic E2E evaluation framework explicitly treats usability and accessibility as requirements alongside security and privacy. Voters should not need to understand zero-knowledge mathematics or Merkle trees; the complexity belongs behind an interface that still allows meaningful, independent verification. (eac.gov)

4. BEFORE THE LEDGER AND AFTER THE LEDGER

4.1 What a Blockchain Can Potentially Protect

Blockchain is naturally strongest after legitimate evidence has been created.

Depending on the architecture, useful election evidence could include commitments to:

- electorate state;
- credential issuance and revocation events;
- election rules and configuration;
- anonymous voting-entitlement consumption;
- ballot-set state;
- trustee activity;
- tally evidence;
- audit and certification events.

If independently observable public evidence replaces a private database that can silently be rewritten, blockchain may genuinely improve accountability.

4.2 What a Blockchain Cannot Make True

A blockchain cannot independently determine whether a birth certificate is legitimate, whether a person actually resides in a county, whether an election official should have issued a credential, whether the voter was threatened, or whether a compromised display showed the voter the same ballot it encrypted.

It can record assertions and evidence about those things. It cannot transform a false assertion into truth.

This is the **before-the-ledger problem**.

4.3 The Deeper Objective: Reducing Invisible Trust

The goal should therefore be larger than ballot immutability:

> **Reduce the number of places throughout the election where a hidden actor can change something important without leaving independently verifiable evidence.**

That concept reaches from voter eligibility through ballot casting, tallying and certification. It also opens a much more interesting role for BSV than simply “store the vote.”

5. WHAT ELECTION SECURITY RESEARCH HAS ALREADY LEARNED

A clean-sheet project should challenge assumptions. It should not ignorantly repeat old failures.

5.1 Software Independence

Software independence asks whether an undetected software change can produce an undetectable change in the result.

The EAC's current VVSG 2.0 process states that software-independent voting systems must either produce voter-verifiable paper records or implement an approved cryptographic end-to-end verifiable protocol. Paper has historically been powerful because it creates evidence outside the software system. That does not prove paper is the only imaginable way to achieve the underlying property, but it establishes a demanding benchmark that any alternative must meet. (eac.gov)

5.2 Cast as Intended, Recorded as Cast, Tallied as Recorded

These three concepts organize the election pipeline:

Cast as intended: Did the machine correctly represent what the voter chose?

Recorded as cast: Was that ballot actually incorporated into election evidence?

Tallied as recorded: Does the announced result correctly follow from the recorded ballots?

The distinction is crucial because blockchain primarily helps with evidence after the ballot exists. It does not automatically solve the first stage. The EAC's emerging cryptographic protocol process explicitly evaluates these properties. (eac.gov)

5.3 End-to-End Verifiability

End-to-end verifiable systems attempt to provide evidence allowing voters and observers to check meaningful properties of the election rather than simply trusting election software.

The philosophical change is from **“Authority announces result”** to **“Authority publishes evidence from which result can be independently checked.”**

That shift is highly compatible with blockchain thinking, but blockchain is only one possible public evidence mechanism.

5.4 Mixnets, Homomorphic Tallying and Threshold Cryptography

Existing election research has developed tools for preserving privacy while proving results.

A **mixnet** repeatedly shuffles encrypted ballots through independent participants in an attempt to break the link between input and output.

Homomorphic tallying permits useful operations on encrypted votes, potentially allowing totals without revealing individual selections.

Threshold cryptography divides sensitive power across multiple independent trustees so no single party alone controls decryption or another critical operation.

A BSV project should ask whether these techniques should be incorporated, not whether everything must be recreated using Bitcoin transaction scripts.

5.5 Cast-or-Audit, Return Codes and Independent Verification

The malicious-device problem has generated techniques allowing ballot construction to be challenged or checked through evidence the primary voting device cannot completely control.

Return-code systems give the voter verification information produced through a channel or secret that the primary voting device does not control. For example, a voter may possess independently issued codes corresponding to ballot choices and compare the code returned after casting with the expected code. The security value comes from independence: compromising the voting device alone should not give the attacker everything needed to fabricate a convincing confirmation.

The deeper lesson is more valuable than any single method:

> **Instead of attempting to make the primary voting computer perfectly trustworthy, design the system so that its dishonesty can be independently detected.**

That is an important first-principles target for any future BSV architecture.

5.6 Risk-Limiting Audits and Independent Evidence

Risk-limiting audits use statistical examination of durable election evidence to obtain strong assurance that a reported result is correct, escalating when the evidence is insufficient. The National Academies specifically recommended risk-limiting audits before certification and tied their current use to independently inspectable paper evidence. (nationalacademies.org)

Their relevance here is broader than procedure: independent evidence gives an election a way to survive distrust of the primary electronic process.

5.7 Internet Voting and the Malicious Endpoint Problem

Serious warnings about Internet voting should not be dismissed as hostility toward innovation.

The National Academies concluded in 2018 that marked ballots should not be returned through Internet-connected systems until robust guarantees of secrecy, security and verifiability exist, while also recommending expert and public review of proposed new election technologies before pilots. (nationalacademies.org)

The Voatz security analysis provides a concrete example of why. Researchers found vulnerabilities that could permit adversaries to alter, stop or expose votes at parts of the architecture that blockchain did not protect. (usenix.org)

A credible BSV proposal must answer those attacks specifically. “BSV scales” is not an answer to compromised ballot-construction software.

5.8 Existing Research as a Library, Not a Boundary

Existing election science should be treated as a collection of expensive lessons. Some current practices may reflect fundamental constraints; others may reflect technologies and assumptions available when the systems were designed.

The proper position is neither **“Experts already decided everything”** nor **“Legacy experts don't understand blockchain.”**

It is:

> **Understand why every important mechanism exists, preserve the problems it solves, and then ask whether newer technology permits a better solution.**

STAGE TWO — A RESEARCH GUIDE FOR BUILDERS

6. WHAT BSV POTENTIALLY CHANGES

At this point the question can become specifically BSV-facing.

Not **“How do we put voting on BSV?”**

But:

> **Which election functions could become materially better if BSV were a native component?**

6.1 Scale as an Architectural Property

Scale matters because architecture changes when scarce transaction capacity forces evidence to be aggregated, periodically anchored, moved to secondary systems or handled through centralized services.

A high-capacity public transaction architecture could potentially support more granular evidence.

BSV Association testing provides a relevant capacity data point: a controlled six-node Teranode deployment distributed across multiple geographic regions sustained average throughput above one million transactions per second for two weeks. Teranode's documented architecture divides node processing into specialized microservices intended to scale horizontally. The public Teranode testing environment remains labeled as alpha testing, so these results should be treated as demonstrated **test capacity**, not as proof of production election-grade security, availability, decentralization or finality. (teranode.bsvblockchain.org)

That is not automatically superior. Granular public evidence can also create privacy, metadata and storage problems.

The builder's task is therefore to determine:

What election evidence would we want publicly and independently observable if capacity were not the first constraint?

Only after answering that should throughput become relevant.

6.2 Public Evidence Rather Than Private Databases

One promising BSV concept is replacing certain private administrative records with publicly verifiable **commitments to state**.

The sensitive underlying data does not necessarily have to be public. The public may instead be able to verify that:

- an authorized election state existed;
- changes occurred through defined rules;
- extraordinary changes were visible;
- administrators could not silently rewrite history.

That distinction between **public evidence** and **public personal data** must remain central.

6.3 SPV and Independent Verification

Bitcoin's architecture emphasizes verification of relevant transaction evidence without requiring every user to operate the complete transaction-processing infrastructure.

BRC-67 gives this idea a more precise BSV formulation. Its specified SPV checks include script evaluation, verifying that input satoshis exceed output satoshis, associating transaction inputs with

Merkle paths to blocks, and checking relevant `nLocktime` and `nSequence` values. It is therefore more than a simple statement that “a transaction appeared in a block.” (bsv.brc.dev)

For an election, this raises an interesting possibility: voters, observers, journalists, campaigns and watchdog organizations could potentially run independent verification software against public BSV transaction evidence.

But an important boundary remains:

> **BRC-67 can help establish Bitcoin-transaction validity and chain evidence. It does not establish election-semantic validity.**

A transaction can satisfy Bitcoin's scripts and chain-verification requirements while still representing an ineligible voter, a duplicated electoral entitlement, a ballot created by a compromised device, or an event that violates election rules.

Blockchain validity and election validity are different layers of the problem.

6.4 Identity, Credentials and State

BSV already has an ecosystem of identity, certificate, key-derivation and verification standards. Those should be studied as potential building blocks rather than assumed to be election protocols.

BRC-52 defines identity certificates associated with a subject public key. Certificate fields are encrypted, selected fields can be revealed to particular verifiers, and certificates can use a UTXO outpoint for revocation. BRC-53 defines wallet/application procedures for creating these certificates and proving them by re-encrypting selected field-revelation keys for a designated verifier. (bsv.brc.dev)

These capabilities may be useful on the **identity and eligibility side** of an election. But they require careful wording:

> **Selective revelation is not anonymous proof of eligibility.**

A BRC-52 verifier receives an identity certificate whose subject is a public key and is given the means to examine selected certified fields. That is different from proving, for example, “I am one valid member of this electorate” while preventing the verifier from determining which member.

Key derivation creates another important distinction. BRC-42 derives child keys between parties using ECDH-based shared secrets and master keypairs and is designed to improve privacy from outsiders who do not possess the shared secret. BRC-69, however, deliberately defines mechanisms for revealing relationships within that key architecture: one method reveals a counterparty shared secret capable of linking interactions between two entities, while another reveals the association between a root identity key and a particular derived child key. (bsv.brc.dev)

Therefore:

> **Derived keys are not the same thing as anonymous keys.**

This does not make BRC-42 or BRC-69 undesirable. Auditable linkage can be useful in many applications. It means only that an election architecture cannot assume ordinary BSV key separation automatically provides the anonymity required for a secret ballot.

The immediate builder questions are therefore:

- Which existing BRCs can represent civic or organizational credentials?
- How are certificates issued and revoked?
- What identity linkage is created?
- Can election-specific credentials be separated from permanent identity?
- Can a verifier prove eligibility without learning identity?
- Does key recovery reintroduce an identity link?
- Can multiple authorities jointly establish a credential?

The preliminary map later in this paper is intentionally a research index rather than a claim of solved functionality.

6.5 What Should Not Automatically Be Put on BSV

Capacity does not justify publication.

Strong candidates for **not** being permanently public include:

- raw civic identity information;
- credentials directly linkable to ballots;
- unnecessary network metadata;
- private recovery material;
- individual ballot ciphertext if future decryption would violate secrecy.

The first principle should be:

> **Put election evidence on a permanent public ledger because permanence adds security —not because permanence is available.**

6.6 A Current BSV Implementation: Votari

The BSV voting question is no longer entirely theoretical. **Votari**, a BSV-based private and verifiable voting application, is currently available for iOS and Android. Its published architecture uses biometric-passport verification performed on the voter's device, including NFC-based passport checks, while recording ballot evidence on BSV. Votari states that raw identity information does not leave the device and that election results can be independently verified from published evidence. The platform supports small organizational elections and trials, with a free tier advertised for elections of up to ten ballots.

Votari is particularly useful in the context of this paper because it provides something more valuable than another theoretical claim: **a working implementation against which the questions in this paper can begin to be tested.** Its existence does not establish that governmental-election problems such as coercion resistance, anonymous electoral eligibility, endpoint compromise, long-term privacy, recovery or legal certification have been solved. Rather, it gives BSV researchers a live system from which to measure what has already been built, identify what remains unresolved, and avoid unnecessarily starting from zero.

---

7. THE AUDITABLE ELIGIBILITY STATE MACHINE

7.1 The Voter Roll as a Hidden Trust Assumption

Much of the public conversation about election integrity begins when ballots are cast, but an enormous decision has already occurred:

Who is allowed to create a legitimate ballot?

Traditional systems largely answer that through administrative records. Even if the ballot system is perfectly auditable, the electorate itself may remain a trusted input.

This is an area where blockchain may offer something more interesting than ballot storage.

7.2 From Static Database to Auditable Lifecycle

Instead of imagining a voter roll as a spreadsheet of names, imagine electoral authority as a sequence of state transitions:

recognized person → qualifying status → jurisdiction → active voting authority → election entitlement → expiration or transition

Over a citizen's life, additional transitions may include:

- relocation;

- name or status changes;
- credential replacement;
- duplicate resolution;
- legal suspension or reinstatement;
- death;
- changes of jurisdiction.

The public need not see the person's name or address. But it may be possible to create cryptographic evidence that legitimate rules governed each transition.

The fundamental question changes from **“Do we trust this voter list?”** to:

> **“Can independent observers verify how voting authority was administered?”**

7.3 Issuance, Movement, Replacement and Revocation

Issuance deserves particular scrutiny because cryptography cannot fix fraudulent issuance after the fact.

A future system might therefore explore:

- multiple-source eligibility evidence;
- threshold approval for sensitive actions;
- replacement credentials that invalidate prior authority;
- synchronized jurisdiction changes;
- transparent aggregate statistics;
- expiration rules;
- public evidence of revocation without public identity disclosure.

The goal is not to eliminate human administration. It is to make consequential administration difficult to perform invisibly.

7.4 Exceptional Actions and Administrative Abuse

Exceptional cases are where otherwise strict systems often become flexible. Provisional credentials, emergency corrections, reinstatements and administrative overrides may be necessary, but they are also natural attack surfaces.

A future election state machine might require unusual actions to generate additional evidence: multiple signatures, reason classifications, time-stamped challenges or observer notification.

> **The more extraordinary the administrative power, the more visible its use should become.**

7.5 Distributed Attestation

No blockchain knows by itself whether a human is a citizen or lives at an address. Someone must attest to those facts, but that does not necessarily mean one institution must control every fact.

A future architecture might combine independent attestations covering different eligibility conditions. The exact authorities will vary by jurisdiction and law.

This does not create a “trustless” election. It could potentially create a **less invisibly trusted election**.

---

8. THE IDENTITY FIREWALL

8.1 Known Citizen to Unknown Valid Voter

The registration side of an election may need significant identity information. The ballot side should ideally need almost none.

Conceptually:

IDENTITY SIDE
Known person; eligibility established; jurisdiction known.

↓ CRYPTOGRAPHIC PRIVACY FIREWALL ↓

BALLOT SIDE
Authorized election participant; valid unused entitlement; identity unknown.

That transformation may be one of the hardest and most important problems in any digital governmental election.

8.2 Anonymous Single-Use Electoral Entitlement

The desired voting authority should prove something like:

1. I belong to the electorate authorized for Election X.
2. I possess one valid entitlement for this contest.
3. That entitlement has not already been exercised.
4. You do not need to know which eligible person I am.

Existing cryptography contains relevant concepts: anonymous credentials, membership proofs, blind issuance and zero-knowledge systems.

BSV's current BRC identity stack should not be described as already providing this property. BRC-52/53 selective revelation allows specified certificate fields to be disclosed to a verifier while other fields remain concealed, but the certificate itself remains associated with a subject public key. An

anonymous electoral membership proof would therefore require additional cryptographic design beyond ordinary BRC-52 selective revelation. (bsv.brc.dev)

The research task is to integrate appropriate mechanisms into an election architecture without creating a hidden path back to civic identity.

8.3 Nullifiers and Election-Specific Uniqueness

A nullifier is one possible mechanism for preventing repeated exercise of anonymous authority.

Conceptually, a legitimate voter secret can produce an election-specific value. The voter proves that the value originates from legitimate authority without revealing the identity behind it. The same entitlement used again in the same election produces a detectable duplicate condition.

A properly designed system would also need to prevent correlation across different elections.

This is not novel cryptography by itself. Its value would lie in its integration with an auditable BSV-based eligibility architecture.

8.4 Why a Voting Token Is Not Enough

Suppose every voter receives one digital asset. The blockchain can ensure that the asset is not spent twice.

But several questions remain: Who received it? Could the private key be sold or stolen? Could one person obtain multiple assets? Can the issuance transaction be linked to the eventual ballot? Can an authority revoke it selectively?

Therefore:

> **One UTXO equals one spend. It does not automatically equal one legitimate human voter.**

8.5 Identity Spillover as a Design Failure

One of the greatest dangers of sophisticated digital identity infrastructure is that convenient identity reuse gradually destroys the secret ballot.

A credential that is excellent for proving age, citizenship or membership may be disastrously inappropriate if the same persistent key follows the voter into ballot submission.

The current BSV key architecture makes this boundary especially important. BRC-42 can create derived keys that improve privacy from unrelated outsiders, but BRC-69 also permits certain key relationships to be revealed for audit purposes. A design cannot therefore assume that “different key” necessarily means “cryptographically unlinkable identity.” (bsv.brc.dev)

This limitation is also recognized within the BRC literature itself. BRC-93 identifies independent-verifiability problems in both BRC-69 linkage-revelation methods. BRC-94 subsequently provides a Schnorr-based zero-knowledge proof for counterparty-level revelation, while BRC-97 defines an

extensible proof format for specific-key linkage claims into which future proof schemes can be incorporated. These mechanisms address verification of key-linkage claims; they do **not** provide anonymous electorate membership. (bsv.brc.dev)

The identity firewall should therefore be considered a **hard architectural boundary**, not a privacy setting.

---

9. THE BALLOT AND THE HUMAN ENVIRONMENT

9.1 The Malicious Device Problem

Imagine the voter selects Candidate A, the device displays Candidate A, but the device cryptographically constructs Candidate B. Every later stage can operate correctly relative to the fraudulent digital ballot.

This attack occurs before ledger security helps.

9.2 Independent Verification of Voter Intent

Rather than asking only how to make the phone trustworthy, a stronger question is:

> **How can the voter verify the ballot through evidence the potentially compromised phone cannot fabricate?**

Research areas include separate devices, return-code systems, **cast-or-audit mechanisms such as Benaloh-style challenges**, hardened devices, pre-issued secrets and physical verification channels. Other approaches include second-device protocols such as CAISED, which uses interactive zero-knowledge proofs to verify ballot construction while attempting to preserve cryptographic deniability rather than creating a transferable voting receipt.

The important property is **independence of failure**. If the same compromised software both creates and “verifies” the ballot, verification is largely theatrical.

9.3 Receipt-Freeness and the Verification Paradox

The voter wants evidence that the ballot counted. A coercer or vote buyer wants evidence that the voter selected the demanded candidate.

A simplistic receipt can satisfy both.

Good election architecture must therefore distinguish participation verification from transferable proof of ballot contents. The EAC's current E2E process explicitly requires that a receipt not display ballot selections or otherwise enable the voter to prove those selections to others. (eac.gov)

9.4 Coercion and the Kitchen-Table Attack

Remote voting introduces an attacker that no cryptographic ledger sees: **the person standing beside the voter.**

This can be a spouse, employer, political organizer, caregiver or government agent. The secret ballot was historically protected partly by physical space.

Recent research such as Votegral/TRIP demonstrates a practical direction for coercion resistance using deniable real and fake credentials, while also relying on an initial private in-person credential ceremony. That illustrates an important constraint: advanced cryptography may still depend on protected physical election infrastructure.

Any remote system must either replace that protection technologically or openly acknowledge a weaker coercion model.

9.5 Remote and Supervised Voting May Require Different Designs

It may be a mistake to demand one identical architecture for every voter.

A supervised polling environment can provide physical privacy and independent equipment. An overseas voter may face different risks and practical alternatives. A property association conducting remote voting faces a different consequence model again.

Architecture should follow the actual threat environment rather than ideological preference for either “everything online” or “nothing online.”

---

10. PRIVACY, PERMANENCE AND PUBLIC EVIDENCE

10.1 The Blockchain Privacy Paradox

Blockchains are valuable because they remember. Secret ballots may require some things to remain unknowable forever.

If individually encrypted ballots are permanently published and the encryption becomes breakable in thirty years, the blockchain has helpfully preserved the evidence needed to reconstruct historical votes.

That would be a serious privacy failure.

10.2 An Election Data Lifecycle

Every proposed data object should be classified.

Data Class	Illustrative Examples	Desired Lifecycle
Permanent public evidence	Election configuration commitment, tally proof	Indefinite
Public but privacy-preserving state	Anonymous entitlement/nullifier state	Depends on linkage analysis
Sensitive temporary evidence	Certain ballot cryptographic material	Limited by protocol/law
Private administrative data	Identity documents, recovery material	Never public
Potentially dangerous permanent data	Individually linkable encrypted ballots	Strong presumption against publication

This is a better design discipline than “put everything on-chain.”

For evidence that must remain public indefinitely, designers should distinguish computational secrecy from information-theoretic hiding. Where appropriate, perfectly hiding commitments—such as Pedersen-style commitments—may reduce the risk created by permanently publishing decryptable ballot ciphertext. Their hiding property does not depend on future computational limits, although their binding properties and any accompanying proofs must still be evaluated separately for long-term and post-quantum security.

Long-term privacy systems such as Koinonia have explored secret-sharing and commitment-based voting architectures specifically intended to preserve ballot secrecy against future computational advances, showing that permanent public evidence need not take the form of permanently decryptable ballot ciphertext.

10.3 Metadata, Timing, Funding and Network Linkage

Encryption protects content, not necessarily context.

A voter can potentially be identified through:

- transaction funding history;
- submission timing;
- network address;
- wallet behavior;
- transaction structure;
- authentication timing;
- issuer information.

Election privacy must therefore be analyzed as a **system property**, not merely an encryption algorithm.

---

11. TALLYING, VERIFICATION AND RESULTS

11.1 Inclusion Is Not Tally Correctness

A blockchain can prove that evidence exists. It cannot by itself prove that the announced election result was computed correctly from all legitimate ballots.

That requires additional rules and evidence.

11.2 Distributed Trust

Critical tallying authority should not necessarily belong to one actor.

Threshold cryptography and independent trustees can distribute sensitive powers among parties whose interests may differ, potentially including political interests, independent observers, courts or other institutions depending on the election.

BSV could record evidence of their actions without needing to become the tallying authority itself.

11.3 Public Tally Evidence

The desired end state is not **“Trust the election server's database.”**

It is closer to:

> **“Here is the evidence from which independent software can verify that the announced result follows from the legitimate ballot set.”**

Different cryptographic systems may achieve this through homomorphic tallying, mixnets or proof systems. The blockchain's role may be publication and synchronization rather than computation.

11.4 Provisional Results Versus Legal Certification

Digital systems may produce results very quickly, but that does not mean legal certification should become instantaneous.

Audits, challenges, contested ballots and evidence review may remain necessary. The goal should be rapid **verifiable provisional evidence**, followed by an explicitly defined certification process.

---

12. BSV MUST ALSO BE PART OF THE THREAT MODEL

Using BSV—or any other proposed blockchain solution—does not permit the underlying blockchain to disappear from the adversarial analysis.

12.1 Finality and Reorganization

A binding election needs defined answers to questions such as:

- When is election evidence considered sufficiently final?
- What happens after competing chain histories?
- Which evidence survives a reorganization?
- At what point does legal finality override later technical events?

These rules cannot be invented during a post-election lawsuit.

12.2 Mining, Censorship and Availability

Election activity can become a political attack target.

Research must evaluate whether infrastructure providers can identify, delay or censor relevant transactions and what alternate publication routes exist. Transaction capacity and censorship resistance are different properties; both matter.

Teranode's controlled testing demonstrates the potential for very high transaction throughput, but it does not by itself answer questions about election-specific censorship resistance, network concentration, adversarial availability or legal finality. (teranode.bsvblockchain.org)

Threat models must also account for close-of-polls surges, mempool pressure, differing transaction-processor fee policies, transaction eviction and deliberate submission delays. The election protocol must define what constitutes timely casting—including whether independently verifiable submission before the deadline remains valid if blockchain inclusion occurs afterward—and should provide redundant submission paths and appropriate fee handling.

12.3 Wallets, Relays and Other Infrastructure

The blockchain is only one part of the path. Wallet software, identity services, transaction processors, relays, networking and verification clients can all become failure points.

BRC-100 is relevant because it defines a broad wallet-to-application interface encompassing transactions, key derivation, signatures, encryption, certificates and permissioned access to wallet functions. That breadth makes it potentially useful for a dedicated election application, but also

reinforces the need for strong application isolation and permissions around identity- and key-related operations. (hub.bsvblockchain.org)

A project that claims “decentralized election” while every voter depends on one wallet provider or submission gateway has simply moved centralization somewhere less visible.

12.4 Evidence Diversity

This paper proposes a broader resilience principle:

> **Election-critical facts should, where practical, be represented through independent evidence systems that do not share the same failure mode.**

Examples might include BSV evidence, threshold digital signatures, independent observer archives, public mirrors, other cryptographic logs, and human-readable physical evidence where appropriate.

This should not be understood as “BSV needs a backup because BSV is bad.” It is the same engineering logic behind redundant safety systems: a system important enough to determine political power should not fail because one technical domain failed.

---

13. FAILURE AND RECOVERY

13.1 Detection Is Not Recovery

Suppose the system proves that a tally is wrong. That is progress—but now determine the winner.

If the intended ballots no longer exist independently, detection may merely tell society that it has no trustworthy election result.

A recovery architecture is therefore part of security, not an afterthought.

13.2 Why Paper Remains Powerful

The National Academies recommended human-readable paper ballots because they provide evidence independently auditable from voting software and warned against Internet return of marked ballots under then-existing technology. (nationalacademies.org)

Paper is not powerful because it is old. It is powerful because its failure modes differ from those of software.

13.3 Can Software Independence Be Achieved Another Way?

A first-principles project should nevertheless be allowed to challenge the implementation rather than the requirement.

The research question should be:

> **Which properties make voter-verifiable paper evidence independent, and can another system reproduce or exceed those properties?**

Possible candidates might involve independent hardware, separate execution environments, independently generated cryptographic artifacts or combinations of digital and physical evidence.

The answer may ultimately be no, but that conclusion should be earned rather than inherited.

13.4 Governance of a Failed Election

Technology must eventually hand evidence to a governance process.

A complete protocol should define responses to:

- corrupted eligibility state;
- missing ballots;
- tally-proof failure;
- unavailable trustees;
- network disruption;
- conflicting evidence;
- chain reorganization;
- discovered endpoint compromise.

Possible outcomes could range from accepting a verified result to recount, partial rerun or complete election rerun.

A serious recovery design should therefore specify, before the election, what evidence must survive for a result to be reconstructed; which independent parties retain that evidence; what technical or evidentiary threshold constitutes a declared failure; what conditions trigger recount, partial rerun or complete rerun; and how those technical findings pass into the legally authorized certification or judicial process.

> **The technology can help determine what happened. The law must determine what happens next.**

---

14. MATCHING THE ARCHITECTURE TO THE TYPE OF VOTE

We can now return to the taxonomy introduced near the beginning.

Different vote types do not require identical systems.

14.1 Requirements Comparison

Requirement	Government Election	HOA / POA	Corporate	Cooperative / Member	DAO / Token
Establish real-world eligibility	**Critical**	**Important**	Important	**Important**	Often minimal
One human = one vote	Often **critical**	Rules vary	Usually no	Often yes	Usually no
Ownership determines voting weight	Usually no	Sometimes	Frequently	Sometimes	Frequently
Secret ballot	Usually **critical**	Often desirable	Varies	Varies	Often optional
Strong coercion resistance	**Critical**	Moderate	Moderate	Moderate	Often lower
Proxy/delegation	Legally constrained	Often relevant	Common	Varies	Common
Quorum rules	Important	**Very important**	Important	Important	Protocol-specific
Public auditability	**Very high**	High	High	High	Often native
Recovery after error	**Extreme importance**	High	High	High	Protocol-specific
Legal consequence	State power	Property/ governance	Corporate control	Organizational	Protocol/ economic
Blockchain-native electorate	No	Usually no	Sometimes	Usually no	Often yes

The table reveals why statements such as “our blockchain already supports voting” need qualification. It may support **exactly the voting class for which it was designed**, but that tells us little about other classes until their requirements are separately tested.

14.2 Where Blockchain-Native Voting Is Already Natural

Token governance is a particularly natural use case because the chain itself can define voting power.

Corporate voting becomes more blockchain-friendly if ownership records are already digitally authoritative. Closed membership voting becomes easier when membership credentials are well defined.

The farther the system moves toward **legal human political rights**, the more external identity, privacy, coercion and recovery enter the problem.

14.3 Property Associations as a Research Environment

HOAs, POAs and condominium associations deserve particular attention as potential BSV research environments because they combine:

- real-world eligibility;
- ownership transitions;
- ordinary voters;
- multiple ownership structures;
- proxies;
- quorum requirements;
- potentially secret board elections;
- legally meaningful outcomes;
- contested governance;
- meaningful financial consequences.

They are complicated enough to expose serious design flaws while remaining much more bounded than a national governmental election.

An effective HOA voting system would not prove that governmental elections were solved. It could, however, test meaningful portions of eligibility-state management, credential issuance, privacy, quorum, delegation and public auditability.

14.4 From Low-Risk Pilot to Government Election

The deployment path should therefore move through increasing consequence rather than jumping directly from demo to democracy.

That ladder is developed in Section 18.

---

15. THREE ARCHITECTURAL RESEARCH PATHS

The research should deliberately avoid choosing its conclusion too early.

15.1 Established Best-of-Breed

Construct the strongest system supported by current election-security research.

No BSV requirement.

Include whatever combination of independent evidence, E2E verification, physical controls, trustees and cryptography survives serious review.

This becomes the **control architecture**.

15.2 BSV-Native Clean Sheet

Now independently design from first principles assuming BSV is available as a native infrastructure component.

Do not assume:

- voter rolls must remain private administrative databases;
- public bulletin boards must look like existing systems;
- evidence must be periodically aggregated because of blockchain capacity;
- paper is the only theoretically possible independent evidence;
- registration and election execution must be technically isolated systems.

But retain every underlying security requirement.

The goal is to challenge implementations without forgetting why those implementations evolved.

15.3 Hybrid Architecture

Only after the first two paths exist should a hybrid be designed.

It may ultimately combine:

- established ballot cryptography;
- physical privacy where appropriate;
- BSV eligibility-state evidence;
- anonymous entitlements;
- public blockchain commitments;
- independent trustees;
- physical or other independent recovery evidence.

Hybrid may prove strongest. But it should **win**, not be selected before the experiment because it resembles current professional consensus.

---

16. A BSV VOTING RESEARCH PROGRAM

This section is the practical handoff.

A serious project should not begin with a development ticket reading **“Build blockchain voting.”** It should begin with separate research workstreams.

16.1 Threat Model

Question: Who can attack the election and what powers do they possess?

Include malicious voters, election officials, credential issuers, software vendors, wallet providers, miners, infrastructure operators, political organizations, coercers and network attackers.

Required output: A formal adversary model against which every later component is tested.

16.2 Eligibility

Question: How does legitimate voting authority arise?

Study identity sources, jurisdiction, duplicate prevention, movement, death, exceptional issuance and administrative correction.

Required output: Eligibility-state specification and audit model.

16.3 Identity Firewall

Question: How does known civic identity become anonymous election authority?

Study anonymous credentials, zero-knowledge membership, blind issuance, election-specific nullifiers and unlinkability.

Existing BRC-52/53 selective-revelation capabilities should be evaluated as identity-side tools, not treated as an existing anonymous electoral proof. (bsv.brc.dev)

Required output: Privacy model demonstrating exactly what each party can learn.

16.4 Credential Recovery and Uniqueness

Question: What happens when a legitimate voter loses a credential or an attacker steals it?

Recovery cannot permanently disenfranchise the voter, but easy recovery cannot create duplicate voting authority.

Required output: Revocation, recovery, replacement and duplicate-prevention protocol.

16.5 Endpoint Security

Question: How does the voter detect a device that lies about the ballot?

Study independent channels, cast-or-audit systems, return-code designs, reproducible software, hardware isolation and alternate verification devices.

Required output: Cast-as-intended threat model and verification method.

16.6 Coercion Resistance

Question: What can a voter safely do while being observed?

Study receipt-freeness, revoting, decoy credentials, supervised privacy and different remote-voting threat models.

Required output: Explicit coercion model rather than a claim that encryption provides privacy.

16.7 Privacy

Question: What information could reveal voter identity now or decades later?

Include transaction history, wallet fingerprinting, timing, network metadata, issuer knowledge and future cryptanalysis.

Required output: Formal data lifecycle and linkage analysis.

16.8 Tally

Question: How can anyone prove the announced result follows from legitimate ballots?

Evaluate homomorphic systems, mixnets, threshold decryption and publicly verifiable proof systems.

Required output: Public verification protocol and independent reference verifier.

16.9 BSV Network Security

Question: What happens when BSV itself becomes an election attack target?

Research finality, reorganization, censorship, propagation, infrastructure concentration, failure domains and availability during adversarial load.

Teranode's high-throughput controlled testing establishes a capacity research baseline; it does not establish the answers to these election-security questions. (teranode.bsvblockchain.org)

Required output: Quantitative election-grade operating assumptions and failure thresholds.

16.10 Evidence and Recovery

Question: If verification detects failure, how is legitimate state reconstructed?

Study physical evidence, redundant public records, cross-anchoring, independent archives and explicit rerun rules.

Required output: Recovery decision tree.

16.11 Human Factors

Question: Can ordinary people use and understand the system?

Study credential management, verification rates, confusing failures, accessibility and confidence.

Required output: Tested voter workflows rather than screenshots from developers.

16.12 Law and Governance

Question: How does cryptographic evidence acquire legal meaning?

Study certification, retention, recount, privacy, accessibility, dispute procedures and authority to halt or rerun an election.

Required output: Jurisdiction-specific legal deployment map.

---

17. PRELIMINARY BSV/BRC RESEARCH MAP

The BSV ecosystem already contains technical standards and proposals relevant to pieces of a possible election architecture. Their existence should not be mistaken for election readiness. The BRC repository includes work covering key derivation, identity certificates, SPV, overlay networks, tokens, wallets, permissions and related infrastructure. (hub.bsvblockchain.org)

Each candidate should be evaluated for its actual guarantees, maturity, privacy properties and relevance to a particular election requirement.

Component	Potential Election Relevance	Critical Limitation / Research Question
BRC-42 — BSV Key Derivation Scheme (BKDS)	Election- or counterparty-specific derived keys; separation of key use across applications	Child keys derive from master-key relationships and ECDH shared secrets. Privacy from outsiders is not the same as anonymous electoral authority.
BRC-52/53 — Identity Certificates	Civic or organizational eligibility credentials; encrypted certified fields; selective disclosure; certificate revocation	Selective revelation is not anonymous zero-knowledge electorate membership. The certificate subject is a public key, and the proof workflow reveals chosen certificate fields to a designated verifier.
BRC-59/60 — Overlay and State Concepts	Possible research basis for persistent electoral-state/event architectures	They are architectural building blocks, not election protocols; suitability for electoral state and implementation assumptions require separate analysis.

Component	Potential Election Relevance	Critical Limitation / Research Question
BRC-67 — Simplified Payment Verification	Independent validation of Bitcoin transaction rules and associated chain evidence	BRC-67 checks more than inclusion, including scripts, value balance, Merkle-path association and timing constraints, but does not prove election-semantic facts such as voter eligibility, intent or tally correctness.
BRC-69 — Revealing Key Linkages	Potential accountability or authorized audit mechanism	Explicitly permits revelation of BRC-42 relationships. Method 1 can expose a counterparty shared secret enabling linkage across interactions; Method 2 reveals a specific child-key association. This is a major Identity Firewall consideration.
BRC-93/94/97 — Key-Linkage Verification	Documents limitations in BRC-69 linkage revelation and subsequent work toward independently verifiable proofs	BRC-93 identifies trust-dependent verification problems; BRC-94 supplies a Schnorr-based proof for Method 1, while BRC-97 defines an extensible proof format for Method 2 but does not itself supply a complete proof scheme.
BRC-77 — Message Signature Creation and Verification	Trustee, election-authority and administrative attestations	A valid signature authenticates a cryptographic signer; it does not prove that the underlying administrative or eligibility assertion is true.
BRC-100 — Wallet-to-Application Interface	Dedicated election application interaction with wallet functions including transactions, cryptographic operations, certificates and permissions	Its broad access to identity-, key- and certificate-related capabilities makes strict election-specific application permissions and separation particularly important. BRC-100 is infrastructure, not a voter-identity or anonymous voting protocol.
BRC-108 — Identity-Linked Token Protocol	Research precedent for identity-conditioned digital rights, compliance restrictions and identity-based recovery	The proposal intentionally links token use to BRC-52/53 identity conditions. That may be useful for eligibility research but potentially inappropriate for secret-ballot authority without an additional privacy firewall.
BRC-116 — Wallet Permissions and Counterparty Trust	Candidate research area for controlling what election applications may request from a user's wallet	Permission boundaries can reduce application access risk, but they do not solve electorate eligibility, anonymity, coercion or ballot correctness.
Teranode	Potential high-volume public evidence infrastructure	Controlled geographically distributed testing sustained average throughput above 1M TPS, and the architecture is designed for horizontal microservice scaling. Those results do not establish

Component	Potential Election Relevance	Critical Limitation / Research Question
		election-grade production security, decentralization, availability, censorship resistance or finality.

For every candidate BRC, builders should answer four questions:

1. **What does the standard actually guarantee?**
2. **Which election requirement could use that guarantee?**
3. **What does the standard not guarantee?**
4. **Does using it create identity, privacy, centralization or recovery problems elsewhere?**

A voting architecture should drive future BRC development.

> **The desire to create a "Voting BRC" should not drive the architecture.**

Possible future standards—if research justifies them—could formalize interfaces such as an **Anonymous Electoral Entitlement Envelope**, an **Election-Specific Nullifier Standard**, eligibility-state commitments, threshold election attestations or evidence-diversity formats. **These are working research concepts, not proposed or assigned BRC numbers.**

At this stage they are research topics, not specifications.

---

18. A PRACTICAL PILOT AND DEPLOYMENT LADDER

A serious election project should progress through increasing complexity and consequence.

Level 1 — Experimental and Advisory Voting

Community polls, test elections and nonbinding decisions.

Useful for testing interfaces, public evidence and throughput.

Failure cost is intentionally low.

Level 2 — Blockchain-Native DAO and Token Governance

The electorate and voting weight are already defined cryptographically.

Useful for testing delegation, public tallying, audit evidence and user tools.

This is real governance but does not test the hardest identity problems.

Level 3 — Clubs, Professional Associations and Closed Membership Bodies

Membership is externally defined.

Useful for testing credential issuance, membership state, secret ballots and eligibility transitions.

Level 4 — HOA, POA and Condominium Association Elections

A particularly promising intermediate environment.

Adds real property, changing ownership, trusts and corporate owners, proxies, quorum, ordinary users and legally meaningful governance.

This begins to test serious real-world eligibility.

A live BSV starting point already exists. Votari is currently available for iOS and Android and is designed for communities, organizations and membership groups. Its current platform supports small trial elections, making it useful not as proof that the higher levels of this deployment ladder have been solved, but as a practical environment in which BSV developers, researchers and organizations can begin testing portions of the architecture today. Readers interested in the BSV voting problem therefore do not need to treat every concept in this paper as hypothetical; some of the underlying ideas can already be experienced and tested in working software.

Level 5 — Corporate and Shareholder Voting

Adds sophisticated ownership records, record dates, proxies, weighted voting and potentially significant economic control.

Level 6 — Narrow Governmental Pilot

Only after extensive independent review.

A constrained election context should be selected because the architecture demonstrably improves the existing alternative, not because government deployment provides publicity.

Level 7 — Binding General Public Election

This is the highest burden.

It should require mature cryptography, public specifications, reference implementations, hostile review, operational testing, accessibility work, legal authorization and demonstrated recovery.

The National Academies specifically recommended expert and public comment on new election technology before pilots and concluded that substantial scientific advances would be required before secure Internet voting could become viable. (nationalacademies.org)

---

19. BEFORE ANYONE SAYS “BLOCKCHAIN SOLVES VOTING”

The first question should be:

What kind of voting do you mean?

After that, a serious public-election claim should be able to answer at least the following:

1. Who is entitled to vote?
2. How is that eligibility established?
3. Who has authority to issue a voting credential?
4. How can fraudulent issuance be detected?
5. How are duplicate people or duplicate credentials handled?
6. How are moves, deaths, corrections and revocations handled?
7. How is one legitimate human prevented from receiving multiple valid entitlements?
8. Can a credential be sold, copied or stolen?
9. How does an identifiable person become an anonymous voter?
10. Can the credential issuer later link that person to a ballot?
11. Can blockchain funding or transaction history reveal identity?
12. Can timing or network metadata reveal identity?
13. How does the voter know the device encoded the intended candidate?
14. What happens if the voting device is compromised?
15. Can the voter verify participation without proving the ballot choice to a vote buyer?
16. How is coercion handled?
17. Is remote voting permitted, and under what threat model?
18. How are valid ballots protected from deletion, substitution or insertion?
19. How does the public verify that the recorded ballot set is complete?
20. How does anyone independently verify the tally?
21. Which sensitive information becomes permanently public?
22. What happens if current encryption becomes breakable decades later?
23. What happens if the blockchain is unavailable?
24. What happens if relevant infrastructure censors election activity?

25. What happens after a chain reorganization?
26. Which additional services—wallets, relays, sequencers, committees, Layer 2 systems or servers—must be trusted?
27. Does the architecture actually scale under adversarial conditions?
28. What independent evidence survives failure of the primary electronic system?
29. If corruption is proven, can the correct result be reconstructed?
30. Who decides when technical failure invalidates an election?
31. Can ordinary voters use the system correctly?
32. Can disabled voters use it independently?
33. Has the **entire system**, rather than merely its blockchain component, undergone independent adversarial review?

If the proposal cannot answer those questions, that does not necessarily make it worthless.

It means the proposal is still research.

And that distinction should be made clear before “blockchain voting” becomes a marketing claim.

---

20. CONCLUSION — FROM NARRATIVE TO ENGINEERING

Can blockchain really solve voting?

The answer depends first on what the word **voting** means.

For a DAO in which the blockchain itself defines membership and voting weight, blockchain may already solve a large portion of the problem. Token ownership, proposals, voting, tallying and execution can all exist inside one digital environment.

For corporate, cooperative and property-association elections, the problem expands because voting authority originates partly outside the blockchain.

For binding governmental elections, it expands dramatically. Now the system must deal with legally eligible human beings, jurisdiction, unique electoral authority, secret ballots, coercion, malicious devices, accessibility, privacy, public proof, hostile infrastructure, recovery and legal legitimacy.

That changes the central question.

The wrong question is:

> **“How do we put voting on BSV?”**

The more useful question is:

> **“Starting with everything a legitimate election must accomplish and survive, which of those problems can BSV materially improve?”**

Several areas deserve serious investigation.

BSV's scaling architecture may permit more granular public election evidence than systems where base-layer capacity forces significant activity into secondary execution environments. Its BRC ecosystem already includes work on key derivation, digital identity certificates, selective revelation, revocation, signatures, SPV and wallet-to-application permissions. But these are **building blocks with specific guarantees**, not election-security primitives that can simply be assembled by name.

BRC-52/53 may help establish certified identity information, but their selective-revelation model is not anonymous electoral membership. BRC-42 provides useful derived-key privacy properties, but BRC-69 demonstrates that certain key relationships can deliberately be revealed. BRC-67 provides meaningful Bitcoin-transaction verification beyond simple inclusion, but cannot determine whether a transaction represents a legitimate voter or a correctly constructed ballot. BRC-100 offers a broad application/wallet interface, but election security would require strict control over which capabilities an election application could access.

Those limitations do not weaken the case for research. They help define it.

Most interestingly, blockchain may allow us to reconsider the voter roll itself—not merely as a trusted administrative input, but as the visible output of an auditable process governing the creation and modification of electoral authority. The **Auditable Eligibility State Machine** and **Identity Firewall** therefore emerge from this paper as particularly promising research directions.

But they remain research directions.

BSV cannot determine citizenship by examining a transaction, prevent somebody from threatening a voter at the kitchen table, know that a compromised phone displayed the same candidate it encrypted, or turn an incorrect credential into a legitimate one merely by making it immutable. Nor should claims about scaling, decentralization or privacy—whether made for BSV or any competing blockchain—be exempt from the same adversarial scrutiny.

Teranode has demonstrated sustained transaction throughput above one million TPS in controlled distributed testing, and its architecture is designed to scale horizontally through distributed microservices. That potentially removes an important capacity constraint from the design exercise. It does **not** remove the need to establish election-grade security, availability, censorship resistance, privacy, recovery and legal finality.

The strongest contribution BSV could make to voting may ultimately be large. It may also be narrower than advocates hope. Either result is useful if it emerges from serious engineering.

This paper may itself contain assumptions that later research, adversarial review or implementation experience proves incomplete or wrong; those discoveries should be treated as progress rather than as failures of the research process.

That is why the proper evolution of the blockchain-voting discussion is:

From narrative to implementation. From slogans to threat models. From “could” to “prove it.”

This paper is not the solution to blockchain-based governmental voting. Other classes of voting—particularly blockchain-native governance and some organizational elections, including HOA/POA, cooperative and corporate elections—already have many of the necessary building blocks in place and can be implemented or meaningfully tested today.

For binding governmental elections, this paper is intended to be the point at which a serious attempt to build one begins.

APPENDIX A — DEFINITIONS AND KEY CONCEPTS

Anonymous Credential: A credential allowing its holder to prove an authorized property or membership while revealing less information than a normal identity credential.

Ballot Commitment: A cryptographic commitment to ballot-related data that can later support verification without necessarily exposing the underlying vote.

Ballot Secrecy: The inability to associate an individual voter with the voter's selections.

Binding Election: An election whose result formally controls governmental, organizational, property or economic authority rather than merely expressing preference.

Cast as Intended: The property that the ballot produced by the system accurately represents the voter's intended choices. The EAC includes this among the core properties of cryptographically verifiable election protocols.

Coercion Resistance: Protection against an attacker forcing or purchasing a particular vote and verifying compliance.

Commitment: A cryptographic mechanism that binds a party to information while potentially keeping that information hidden until later or indefinitely.

Credential Revocation: The process through which previously valid authority is rendered invalid.

DAO: A decentralized autonomous organization whose rules and governance can be implemented through blockchain-based software.

Election-Specific Nullifier: In this paper, an anonymous value designed to make repeat use of a particular election entitlement detectable without revealing the voter's identity.

Electoral State Machine: The proposed treatment of voting eligibility as a sequence of auditable state changes rather than merely a periodically exported voter database.

End-to-End Verifiability (E2E-V): An election property allowing meaningful verification across the ballot process, commonly including cast-as-intended, recorded-as-cast and tallied-as-recorded properties.

Evidence Diversity: A resilience principle under which critical facts are supported by evidence systems with different failure modes.

Homomorphic Tallying: Cryptographic processing allowing aggregate operations over encrypted ballot data without necessarily exposing individual votes.

Identity Firewall: The architectural separation proposed in this paper between known civic identity and anonymous ballot authority.

Mixnet: A system that cryptographically shuffles messages or ballots through one or more operations to make input-output correlation difficult.

Nullifier: A value used in some privacy systems to show that anonymous authority has already been exercised without directly revealing the identity behind it.

Public Bulletin Board: A consistently observable repository for election evidence. A blockchain can potentially act as one, but public bulletin boards need not be blockchains.

Recorded as Cast: Evidence that the ballot actually cast by the voter is represented in the election record.

Risk-Limiting Audit: A statistical audit designed to obtain strong evidence that the reported election outcome is correct and to escalate examination when evidence is insufficient.

Selective Revelation: Disclosure of selected certified information while other certificate fields remain concealed. In BRC-52/53, this involves encrypted certificate fields and verifier-specific revelation of selected field keys; it should not be confused with anonymous zero-knowledge proof of membership.

Software Independence: A property under which an undetected software fault or change cannot cause an undetectable change in the election result.

SPV — Simplified Payment Verification: A Bitcoin verification approach allowing parties to verify relevant transaction and blockchain evidence without relying solely on a central database. BRC-67 specifies checks including script evaluation, transaction value balance, Merkle-path association and applicable locktime/sequence conditions.

Tallied as Recorded: Evidence that the announced result correctly follows from the recorded ballots.

Threshold Cryptography: Cryptographic control divided among multiple parties such that a defined subset must cooperate for a sensitive operation.

UTXO: An unspent transaction output controlled according to Bitcoin transaction rules. Its single-spend property does not by itself establish unique human identity.

Zero-Knowledge Proof: A cryptographic method for proving a statement without necessarily exposing the underlying secret information used to prove it.

APPENDIX B — VOTING-TYPE REQUIREMENTS MATRIX

Dimension	Government	HOA / Property	Corporate	Cooperative	DAO / Token
Electorate basis	Legal person eligibility	Ownership/ membership	Share ownership	Membership	Token/key control
Human uniqueness	Usually essential	Often	Usually not central	Often	Usually irrelevant
Voting weight	Usually equal per voter	Governing rules	Shares/ classes	Often equal	Token/protocol rule
Identity privacy	Important	Moderate/high	Varies	Varies	Often pseudonymous
Ballot secrecy	Usually essential	Often desirable	Varies	Varies	Frequently public
Coercion concern	Extreme	Moderate	Moderate	Moderate	Context-dependent
Delegation/ proxy	Restricted	Common in some systems	Common	Varies	Often native
Quorum	Election-law dependent	Often crucial	Often crucial	Common	Protocol-defined
Audit burden	Extreme	High	High	High	Often digitally native
Recovery burden	Extreme	High	High	High	Protocol-defined
Consequence of failure	Political legitimacy/state power	Property/ governance	Corporate control	Member rights	Treasury/protocol
Suitable early BSV pilot?	Late stage	**Strong candidate**	Candidate	**Strong candidate**	**Immediate candidate**

APPENDIX C — THREAT AND ADVERSARY MATRIX

A serious builder should model at least the following adversaries:

Adversary	Example Capability	Primary Risk
Fraudulent voter	Attempts duplicate/unauthorized participation	Eligibility
Credential thief	Obtains voter secret	Impersonation
Coercer	Watches or threatens voter	Ballot freedom
Vote buyer	Demands proof of selection	Receipt-freeness
Corrupt registrar	Issues/withdraws authority improperly	Eligibility state

Adversary	Example Capability	Primary Risk
Election administrator	Manipulates configuration or evidence	Governance
Voting-device malware	Alters ballot before submission	Voter intent
Wallet/provider	Links identity, blocks transactions	Privacy/availability
Network attacker	Observes or disrupts traffic	Privacy/availability
Miner/processor	Delays, censors or reorganizes evidence	Ledger reliability
Trustee	Abuses tally/decryption authority	Privacy/tally
Software vendor	Introduces hidden behavior	System integrity
Future cryptanalyst	Breaks historical encryption	Long-term secrecy
Political/legal actor	Misuses emergency/dispute process	Certification/recovery

---

APPENDIX D — BUILDER'S RESEARCH CHECKLIST

Before implementation, define:

Election Class: governmental, corporate, property, cooperative, DAO or advisory.

Electorate: who qualifies and why.

Voting Weight: human, property, shares, tokens or another rule.

Identity: what must be known, by whom, and for how long.

Eligibility Lifecycle: issuance, modification, transfer, replacement and revocation.

Privacy Firewall: where identity ends and anonymous voting authority begins.

Uniqueness: what prevents duplicate entitlement.

Credential Recovery: what happens after loss, theft or compromise.

Ballot Construction: how voter intent is verified.

Coercion: what the system assumes about the voter's physical environment.

Receipt-Freeness: whether voters can prove ballot contents to others.

Public Evidence: precisely what becomes observable.

Permanent Data: what survives indefinitely and why.

Sensitive Data: what must never be public.

Tally: how correctness is independently established.

BSV Role: exactly which properties depend on BSV.

Additional Infrastructure: wallets, relays, gateways, Layer 2 systems, trustees or off-chain computation.

Finality: when election state becomes authoritative.

Availability: what happens during congestion, censorship or outage.

Recovery: how the correct result is reconstructed after failure.

Evidence Diversity: which independent evidence systems exist.

Governance: who can change rules, halt the election or resolve failure.

Legal Integration: how technical evidence becomes legally actionable.

Accessibility: whether all eligible voters can participate independently.

Adversarial Review: whether outsiders have been encouraged to break the entire architecture.

APPENDIX E — IMPORTANT SYSTEMS, RESEARCH AND HISTORICAL WARNINGS

EAC/NIST Cryptographic E2E Protocol Evaluation

In December 2025, the EAC announced a public process, with NIST technical support, for evaluating cryptographic end-to-end verifiable voting protocols under VVSG 2.0. The process calls for detailed specifications, security analysis, reference implementations and public technical review. This provides a useful benchmark for how seriously an election cryptographic protocol should be evaluated.

National Academies — *Securing the Vote*

The National Academies' 2018 report recommends human-readable paper ballots, risk-limiting audits and strong caution toward Internet return of marked ballots without robust secrecy, security and verifiability. Importantly for this paper, the report also encourages research and expert/public review of new election technologies.

Voatz

The 2020 USENIX security analysis of Voatz found vulnerabilities capable of altering, stopping or exposing votes despite an architecture whose security claims included blockchain-related mechanisms. It remains a useful reminder that securing the ledger does not secure the entire voting path.

Votegral / TRIP

Votegral and the related TRIP credential system provide an important contemporary research benchmark for coercion-resistant voting. Their approach uses real and fake credentials so that a voter under coercion can present apparently valid voting authority without necessarily revealing which credential will produce a counted ballot. The architecture demonstrates meaningful progress on

deniable credentials while also relying on an initial private in-person credential ceremony, showing that advanced cryptography does not automatically eliminate the role of protected physical processes.

CAISED

CAISED explores cast-as-intended verification using a separate audit device and interactive zero-knowledge proofs. Its relevance is not that it represents the only solution to a malicious voting device, but that it demonstrates independent verification in which the device constructing the ballot does not alone control the evidence used to check it. Its use of cryptographic deniability also illustrates the tension between meaningful voter verification and transferable voting receipts.

Koinonia

Koinonia explores long-term election privacy through secret sharing and cryptographic commitments rather than relying solely on the permanent confidentiality of encrypted ballots. It is relevant to the blockchain privacy problem because public election evidence may survive indefinitely while the computational assumptions protecting ordinary ciphertext may not.

Cardano Voting Narrative

Cardano presents “Voting Systems” as a blockchain use case and describes blockchain as potentially providing voter verification, vote integrity, auditability, transparency, accessibility and scalability. This illustrates why blockchain-native governance experience should not be confused with full public-election engineering.

Ethereum DAO Governance

Ethereum provides a mature example of blockchain-native organizational governance. Its documentation describes token-based membership, delegation, proposals and governance actions. These are legitimate voting systems, but their blockchain-defined electorates demonstrate why DAO voting should not be treated as equivalent proof of governmental-election readiness.

Algorand Election Research

Algorand Foundation has publicized research involving blockchain-based vote counting and validation using Algorand TestNet. It represents another example of continuing blockchain interest in electoral applications.

BSV Identity and Key Architecture

BRC-52/53 provide identity certificates, encrypted certified fields, selective field revelation and certificate-management workflows. BRC-42 defines ECDH-based key derivation, while BRC-69 permits certain key relationships to be revealed. BRC-93/94/97 further document and address verification limits surrounding those revelations. Together they illustrate both the usefulness of BSV identity infrastructure and why a secret-ballot Identity Firewall cannot be assumed merely from key derivation or selective disclosure.

BRC-67 and SPV

BRC-67 defines transaction-verification steps including script evaluation, value-balance checking, Merkle-path association and timing constraints. It may therefore support independent verification of Bitcoin transaction evidence, but its guarantees should not be confused with election-semantic validity.

Votari

Votari is a currently available BSV-based voting application for iOS and Android. Its published architecture uses biometric-passport and NFC-based identity verification performed on the voter's device and records election evidence using BSV. Votari is relevant to this paper as a live implementation that can be examined and trialed against many of the research questions identified here; its existence should not be interpreted as evidence that the broader governmental-election problem has been solved.

Teranode

A controlled 2024 BSV Association test ran six geographically distributed Teranode nodes using more than 500 machines and sustained average transaction throughput above one million TPS for two weeks. Current BSV documentation describes Teranode as a horizontally scalable distributed microservices architecture. These results demonstrate potential transaction-processing capacity; they do not establish election-grade production security or reliability.

WORKING REFERENCES

A. Election Standards and Government / Institutional Sources

1. **U.S. Election Assistance Commission.** *End to End (E2E) Protocol Evaluation Process.* December 23, 2025.
2. **National Academies of Sciences, Engineering, and Medicine.** *Securing the Vote: Protecting American Democracy.* Washington, DC: The National Academies Press, 2018. DOI 10.17226/25120.

B. Election-Security Research

3. **Specter, Michael A.; Koppel, James; Weitzner, Daniel.** *The Ballot is Busted Before the Blockchain: A Security Analysis of Voatz, the First Internet Voting Application Used in U.S. Federal Elections.* 29th USENIX Security Symposium, 2020, pp. 1535–1553.
4. **Benaloh, Josh.** *Ballot Casting Assurance via Voter-Initiated Poll Station Auditing.* 2007.
5. **EPFL.** Votegral / TRIP coercion-resistant voting research, 2025.

6. **Koinonia.** Long-term-private electronic voting using secret sharing and cryptographic commitments. ACSAC, 2019.
7. **CAISED.** Cast-as-intended verification using a second audit device, interactive zero-knowledge proofs and cryptographic deniability. E-Vote-ID, 2023.
8. **Pedersen, Torben P.** *Non-Interactive and Information-Theoretic Secure Verifiable Secret Sharing.* CRYPTO '91, pp. 129–140. DOI 10.1007/3-540-46766-1_9.

C. Primary BSV Technical Specifications and Documentation

9. **BRC-42.** *BSV Key Derivation Scheme (BKDS).*
10. **BRC-52.** *Identity Certificates.*
11. **BRC-53.** *Certificate Creation and Revelation.*
12. **BRC-67.** *Simplified Payment Verification.*
13. **BRC-69.** *Revealing Key Linkages.*
14. **BRC-77.** *Message Signature Creation and Verification.*
15. **BRC-93.** *Limitations of BRC-69 Key Linkage Revelation.*
16. **BRC-94.** *Verifiable Revelation of Shared Secrets Using Schnorr Protocol.*
17. **BRC-97.** Extensible proof format for specific-key linkage revelation.
18. **BRC-100.** *Unified, Vendor-Neutral, Unchanging, and Open BSV Blockchain Standard Wallet-to-Application Interface.*
19. **BRC-108.** *Identity-Linked Token Protocol.*
20. **BSV BRC Repository / Index.** Current technical proposal index, including BRC-116, *Wallet Permissions and Counterparty Trust.*
21. **BSV Association.** *Teranode Testing Success — Six Nodes, 1M+ TPS for Two Weeks.*
22. **BSV Skills Center.** *Teranode* — distributed microservices architecture and Teratestnet documentation.
23. **Votari.** *Votari — Private, Verifiable Voting on BSV.* Current official application and technical information, 2026.

D. Blockchain Voting and Governance Narrative Sources

24. **Cardano.** *Voting Systems.* Current official use-case documentation.
25. **Ethereum.org.** *What Is a DAO?* Current official DAO and governance documentation.
26. **Algorand Foundation.** *Improving Election Integrity: Blockchain and Byzantine Generals Problem Theory in Vote Systems.* May 9, 2024.

A BitcoinSV.Guide Research Report — https://BitcoinSV.Guide/for-ai/#miscellaneous-reports

- ➔ **Direct Link :** https://bitcoinsv.guide/wp-content/uploads/2026/09/BSV-Voting_Can-Blockchain-Really-Solve-Voting.pdf