score-based decisions

influence · freedom · legitimacy

Ben Smyth

October 31, 2025

Executive Summary

We need to talk about DAO governance: Trillions actively managed with unfit systems. First-past-the-post decisions under representing owners. Public forums suppressing will. We need influence, freedom, legitimacy.

Say you prefer Starbucks rather than Prêt. McDonalds more than Buger King. Republicans over Democrats. Someone else fancies the opposite. Another independents. You all like coffee-burgers-America. Yet, two tea-drinking fish-and-chip eating monster-raving loony supporting Brits control the vote. Decentralised inaction?

Similar objectives create advantage for alternatives: Two votes for tea, one for each of Starbucks, Prêt, and an independent, tea-drinkers win. Two votes for fish and chips, one for each burger option, fish-and-chips win. As does monster raving loony.

Scoring is better. Instead of choosing just one option, rate each. Score Starbucks-McDonalds-Republicans five, Prêt-BK-Democrats four, independents three. Someone else switches the five and four. Another puts independents on top. Coffee-burgers-America win.

score for influence

You're the cool kid. Bravado grants freedom of expression. Elsewhere there's fear. The game is the game. You ain't the cool kid in every room; some opulent power observing, society presiding.

Freedom to express one's conscience, morals, will, without fear, a century-old innovation: Eighteen-hundreds closed with realisation — we can't vote freely in public. Decentralised inaction?

Secret ballots better. Instead of publicly declaring opinions, mark in private. Tally scores. Publicly reveal collective decisions, keep individual preferences private. Maintain confidentiality.

encrypt for freedom

Secrecy creates quandary. In public, stakeholders openly declare. Legitimacy undeniable. But in public, you aren't free. Conversely, private decisions protect freedom, give-up legitimacy — there's no evidence of fair play. Everybody lies. Decisions must demonstrably be stakeholder will. Absolute path from decision to preferences. Don't trust.

verify for legitimacy

Stakeholders deserve influence, freedom, legitimacy.

Web3, Crypto, Blockchain — decentralisation's backstory

Cryptographers know cryptographic primitives, these tiny little bits of code that encrypt information, create zero-knowledge proofs demonstrating meaning to such information (without ever revealing it, cool stuff, like proving you can afford house without revealing net worth).

Above that is CompSci, they build cryptosystems from cryptographic primitives. Then there's this abstract concept called Web3 that embraces all the things that are 'decentralised,' meaning direct ownership & control, independent of state.

Cryptocurrencies bitcoin and ethereum are the biggest successes: Tamper-proof financial transactions are recorded onto blockchain, tech better than traditional banking systems seeking fraud minimisation rather than eradication.

Decentralised Autonomous Organisation (DAO) is the idea that objectives can be written to blockchain, then run autonomously. Owners exerting control over governance, which is where decentralisation fails — cliques are embracing subversive governance tactics.

Smashing DAO for fun and profit

Governance rules are stored onchain, they're overridden by consensus, cliques are smashing DAO for personal gain. Split decisions, power dynamics, erosion of fair play. Manipulation is rational. There are plenty of assets, owners can switch between them, there's no concern for killing off DAO.

That's a shame.

Words from a16z's Chris Dixon are oddly fitting, "[they] can change the rules...at any time, for any reason. This leads to the inevitable 'attract-extract' pattern, which feels...like a bait and switch."

Shared, decentralised ownership has failed.

Without DAO, Web3 is just Crypto, world's digital currency. But there's surely more: Stock markets are redundant in Web3, exchanges take their place, each DAO offers tokens in place of shares, these tokens are purchased on exchanges, feels like foreign exchange, a currency swap.

Outlaw bait and switch.

Eradicating current shenanigans increases long-term value, we'll see exchanges demanding minimal governance standards, outlawing subversive tactics, investors opting for stability.

Good governance defacto right, not aspiration.

Market forces can save what ideology hasn't. Governance as tradeable commodity. Exchanges protecting investors. Web3's next act begins with admission — governance is flailing. Or perhaps we're watching wreckage: Bad governance driving out capital, DAO collapse.

Ecosystem deciding: Do stakeholders deserve influence, freedom, legitimacy?

Influence, freedom, legitimacy

David Chaum (in trademark Hawaiian shirt) excited many of us about crypto, way back in the eighties, nineties, and noughties, developing cryptographic fundamentals, long before their main-

stream; we were trying to establish defining principles, replicating ballot-secrecy rights for digital society, creating stronger forms of legitimacy, seeking fraud eradication rather than minimisation.

No morals, no ethics, just law.

After nine-day trial jury convicts crypto investor Avraham Eisenberg of wire fraud, for deceiving Mango Markets into believing he was taking crypto loan, when he was robbing them, and their stakeholders. Eisenberg appealed, arguing he made no false representation, autonomous platform cannot be influenced by any representation. Code is law: Court acquitted.

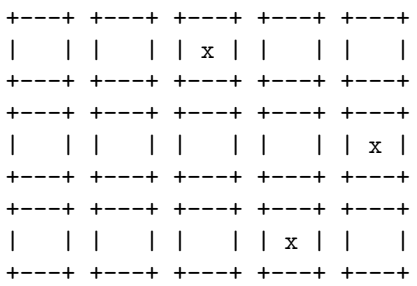
AI promising autonomous society.

We need strong governance controls. Stakeholders deserve influence, freedom, legitimacy. Let's inscribe as law. Higher-layer currencies, exchanges, DAO, with built-in investor protection. Decentralised action. Fairest system is most sustainable. Inclusivity is the broadest market. As AI and Web3 enter maturity, we need some grounding principles, guardrails.

Stakeholder control.

Autonomous operation is governed by stakeholder-prescribed rules, enforced by code. Rules aren't static; contentious regulation may be debated, overwritten by consensus on preferred proposal. Current decision making procedures lack influence, freedom, legitimacy. Here's my solution:

Score for influence. A ballot is a two dimensional boolean matrix — one-by-one for referenda, boolean array for approval and first-past-the-post, two dimensional boolean matrix for scoring and ranking — scoring (e.g., three-five-four, below) side-steps Arrow's impossibility result, avoids under-representation, collective preference (coffee-burgers-America) wins.



"Equality—impossible." Cry social choice theorists. First-past-the-post plagued by vote splitting. Borda dismissing, championing ranked voting. "Bound to lead to error," muses Condorcet. Arrow arguing incompatibility with common sense. Smith sidestepping, guided by dancing honeybees, proclaiming score voting "a larger improvement in 'democracy' than the entire invention of democracy." Bold claim, makes sense: Score for influence.

Theorem (Influence)**.** *Scoring increases stakeholder happiness — machine-checked.*

Proof sketch. There's utility in each preference winning (e.g., Starbucks gives Brit minus thirteen happiness points). Stakeholders maximise their personal happiness. Overall happiness sums utility values for collective decision. Ideally, systems should identify preference maximising collective happiness. They do not, cf. our two tea-drinking Brits. American physicist, mathematician, and theoretical scientist Warren D. Smith simulated some thirty governance systems, in one-hundred forty four configurations. Smith explains: "The amazing result is that, in all 144 scenarios, [score] voting was the best (had lowest Bayesian regret, up to statistically insignificant noise) in EVERY SINGLE ONE of those 144 with either honest [stakeholders], or with strategic votes." □

Encrypt for freedom. Iterate over a ballot matrix, encrypt one for a mark, zero otherwise:

```
matrix.forEach((row: boolean[], i: number)
  => row.forEach((mark: boolean, j: number)
    => ret[i][j] = encrypt( public_key, mark ? 1 : 0 )));

//TODO: Mention final ZKP here?
```

Mark ballots privately, encrypt for confidentiality. Sum encrypted scores homomorphically. Partial decryptions reveal only collective score.

Theorem (Freedom)**.** *Stakeholder vote is indistinguishable from any other with same collective score — individual stakeholder preferences are confidential — cryptographically-guaranteed.*

Proof sketch. Non-malleable encryption guarantees individual stakeholder preferences are private, furthermore, they remain private upon decryption of collective score; detailed proof shows formalism of "stakeholder vote is indistinguishable from any other with same collective score" follows from NM-CPA asymmetric encryption, via formalism of "observing another stakeholder's system interaction gives no advantage in casting meaningfully related preference." □

Verify for legitimacy. Everybody lies. Don't trust, verify. Checks ensure fair play: Dumpster diving start; take purported voting data, could be garbage, we don't know, check zero-knowledge proofs for legitimacy, discard everything else, only legitimate encrypted ballots remain (each with at most one mark per row).

```
Algorithm (homomorphic scoring). Recurse over encrypted score, purported
voting data, map from stakeholder identities to most-recent ballot, and
index, return encrypted score:

  1. Base case (end of data) index equals data-length,
     return encrypted score when defined, null otherwise.

  2. Recursive cases skipping ahead with incremented index
     (deserializing purported voting data fails for index,
     map doesn't include deserialized stakeholder identity
     or returns more-recent ballot).

  3. Recursive case for new most recent stakeholder-authorised ballot:
     Remove earlier ballot from encrypted score, add new ballot,
     update map, recurse with incremented index.

Homomorphic scoring over purported voting data and map: Call recursive
algorithm with undefined encrypted score and index zero.
```

Theorem (Legitimacy)**.** *Collective score sums final stakeholder scores — cryptographically-certified.*

Proof sketch. Above algo' discards garbage (unserializable to encrypted ballot), unauthorised ballots (not referencing stakeholder identity), and early votes. Stakeholder final ballots remain. Count homomorphically. Each keyholder partially decrypts, together revealing collective score. □

DAO user-interface is `index.html` inside `<dao-name>` desktop folder. Displays decision and preferences that stakeholder scores. Local encryption, then store in shared sub-folder `<decision-id>`. Verifiability's challenge (solved by `index.html` at decision-making deadline) is distillation:

Inputting potential garbage (from sub-folder), filtering non-voting data, early votes, and unauthorized ballots(, malicious parties must be thwarted when writing to shared storage), retaining final stakeholder-encrypted preferences(, anyone can perform aforementioned steps, keyholders perform the next with anyone able to verify), proving decryption onto plaintext decision. Whilst maintaining confidentiality: No cast ballot is relatable to individual preference.

Verifiability guarantees collective score sums final stakeholder scores, confidentiality asserts nothing more than revelation of plaintext decision, individual scores are private — stakeholders have freedom, decisions legitimacy. Influence follows from scoring.

What's new? Non-malleable ElGamal over boolean matrices. Autonomous zero-knowledge proof construction. Influential, free, and legitimate ownership. Tax efficiency. And, cool math.

Achieving freedom from confidentiality of encryption is the easiest bit: Pairing homomorphic encryption with zero knowledge proof achieves non-malleability, which is proven by reduction to security of underlying schemes, meaning OpenSSL is broken (unlikely), or implementation secure.

We start from ElGamal (Section 1), introduce zero-knowledge proofs (Section 2), side-step into a few details on cyclic groups and non-interactive proofs (Section 3 & 4), arrive at encryption scheme for score matrices (Section 5).

Verifiability requires thought: Consider attacker orchestrating system execution with collective score differing from sum of final stakeholder scores. In (cryptographically proven) absence of such an attacker, we infer delivery of stakeholder will. Section 6 refines algorithmically for precision.

Our above homomorphic scoring algorithm ensures verifiability partially, keyholders ensure the rest by proving decryption onto plaintext decision. Proofs of verifiability, confidentiality, and influence appear in Sections 7–9.

Locating autonomous keyholder-as-a-service in space effectively locates decision-making beyond jurisdiction of states asserting control over on-earth decisions, we touch upon such arrangements in Section 10. Prior art in terms of cryptographic encryption schemes, encryption for free decision making, and legitimacy are explored in Section 11. Finally, future possibilities are pondered.

Where's next: Does anyone care? We'll launch onstage at Black Hat, find out.

I started out certifying systems as-secure as underlying parts. Using mathematical logic for autonomous protocol verification, switching into manual cryptographic techniques for better precision, with passion (but little patience for) proven secure executables. As a prerequisite, I frequently pondered, *what is this?* For twenty-one years I've wondered what's influence-freedom-legitimacy. I have my answer; I've built voting system delivering. Bigger picture, there's opportunity to increase Web3 value with agentic DAO. Getting there requires strong governance controls.