How Fault Tolerant Trust—*Trust-Your-Network*—secures a *one-entity, one-vote* democracy by producing *BFT ID*.

By Chris McCoy, Rag Bhagavatha, and Craig Montuori of STORE Research

The foundation of a democracy is *one person, one vote* (1p1v). In nation-state democracies, companies don't vote, only people do. *1p1v* is secured by the voting population's trust in the identity of personhood. In America, for example, it's your state license or national ID card that gives legitimacy to identity — therefore it's the security model for liberal democracy. To preserve a liberal democracy in countries like America, if you vote on someone else's behalf, you go to prison. Trust in governance where one person only has one vote is table stakes for the efficacy and fidelity of a nation-state democracy.

In a network of computers that represent people, *1p1v* is unsolvable because the legitimacy of identity cannot be established for computers in a fault tolerant way. With computers, a voting node in a network can represent anything — a person, a company, a bot, a network of bots, etc. So far, identity with computers has proven to be unsolvable without a trusted intermediary — both in traditional computing networks and in decentralized networks. As a result, *1p1v* with computers cannot be solved in a verifiable manner. Without a mechanism for establishing certainty of *one person, one vote* in a network of computers (*nodes*), there's no way for nodes to form a governance that isn't a plutocracy (where those with the most tokens control the voting network). To work around it, Web3 systems adopt *one token, one vote* (1t1v).

Our solution, BFT ID: At STORE, we believe that ⅔+ trust in *one entity, one vote* (1e1v) can be the solution. The output is called Byzantine Fault Tolerant Identity — or *BFT ID* , which forms the security model for a *1e1v democracy* of computers. Underpinning BFT ID is novel research from STORE called *Fault Tolerant Trust* (also called *Trust-Your-Network*, or *TYN*).

What is Fault Tolerant Trust? Fault Tolerant Trust — also called *Trust-Your-Network (TYN)* — is the iterative trust-building process used by nodes in a network to reach ⅔+ trust or agreement on anything — on a fact of information, on an agreement to vote, or to take a binding vote. When used on the nature of identity, TYN can solve for ⅔+ trust on whether *one entity, one vote* is "true" or not. In other words, in a network of "voters", each voter is trusted by ⅔+ of other voters. TYN is the underlying process for miners and voters achieving Byzantine Fault Tolerance without a central party turning the trust-minimization on.

What is one entity, one vote? *1e1v* is a ⅔+ trust in digital identity. Once nodes reach ⅔+ trust that a fellow participant is indeed in power of only one computing node in the network, individual entities have sufficient trust to network and govern with it.

⅔+ trust gives digital governance Byzantine Fault Tolerance.

How does *TYN of 1e1v* secure STORE? STORE Governance uses these primitives to help STORE network operators reach ⅔+ trust that the other network operators only have a single vote in their branch of governance — without the STORE Foundation turning this trust on. *TYN of 1e1v* produces BFT ID. STORE starts trust-minimized Day 1 with this decentralized principle maintained by the network nodes as STORE grows and persists over time.

The big idea: TYN engineers ⅔+ trust in any off-chain environment — for any governance system. It can work for any app or protocol — on or off of STORE.

How TYN re-enforces the STORE infrastructure layer: Each Cloud miner on STORE gets a single vote in governance — no matter the size of their stake.

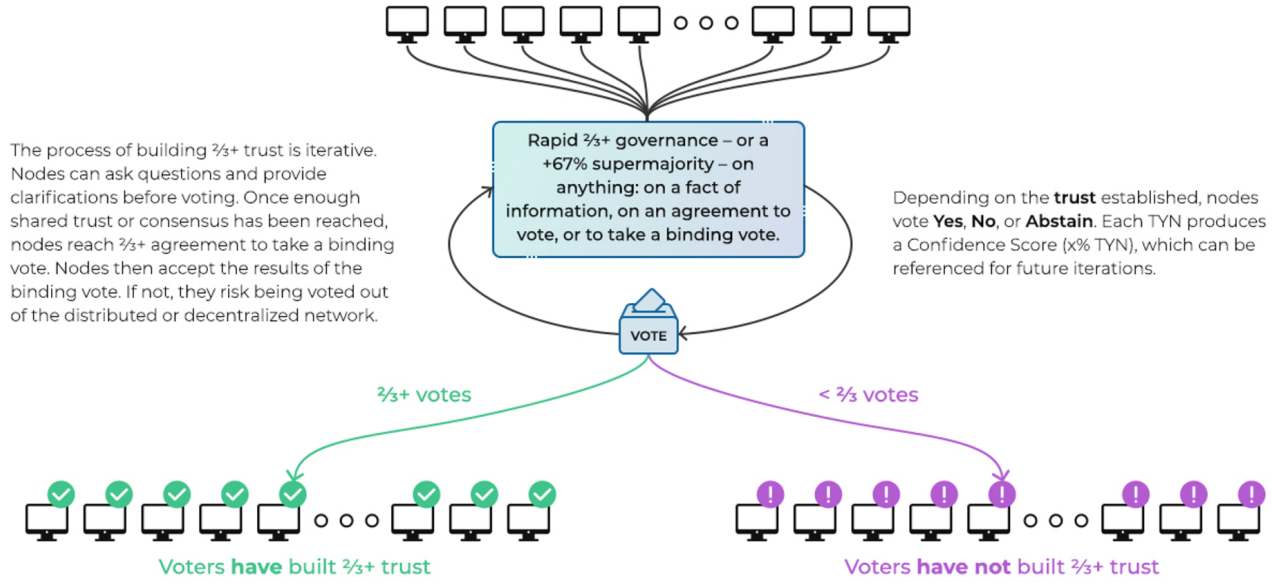
How TYN re-enforces the STORE protocol layer: Each Block miner in STORE Chain has one signature on each block. If ⅔+ of Block miners sign the block, it's finalized. *TYN of 1e1v* secures ⅔+ trust in *one entity, one signature*.

How TYN can help Web3: Infrastructure projects, and even other layer ones, can form legitimacy around identity and voting by leveraging TYN. We intend to open up the research.

RESEARCH

Achieving Fault Tolerant Trust on Identity

Fault Tolerant Trust – also called *Trust-Your-Network (TYN)* - is the iterative trust-building process used by nodes in a network to reach ⅔+ trust or agreement on anything – on a fact of information, on an agreement to vote, or to take a binding vote. When used on the nature of identity, TYN can solve for ⅔+ trust on whether one entity, one vote is "true" or not. TYN is the underlying process for achieving Byzantine fault tolerance without a central party turning the trust-minimization on.



STORE