Fault Tolerant Trust (TYN)

Trust-Your-Network

How Storecoin's p2p, decentralized democracy is secured from Sybil attacks using Fault Tolerant Trust — also known as Trust-Your-Network (TYN). TYN can be used to help any p2p economic network reach trust on a "one entity, one vote" security model for a decentralized democracy, to vote, and more.

Chris McCoy
Storecoin.com
San Francisco CA
chris@storecoin.com

Rag Bhagavatha
Storecoin.com
San Francisco CA
rag@storecoin.com

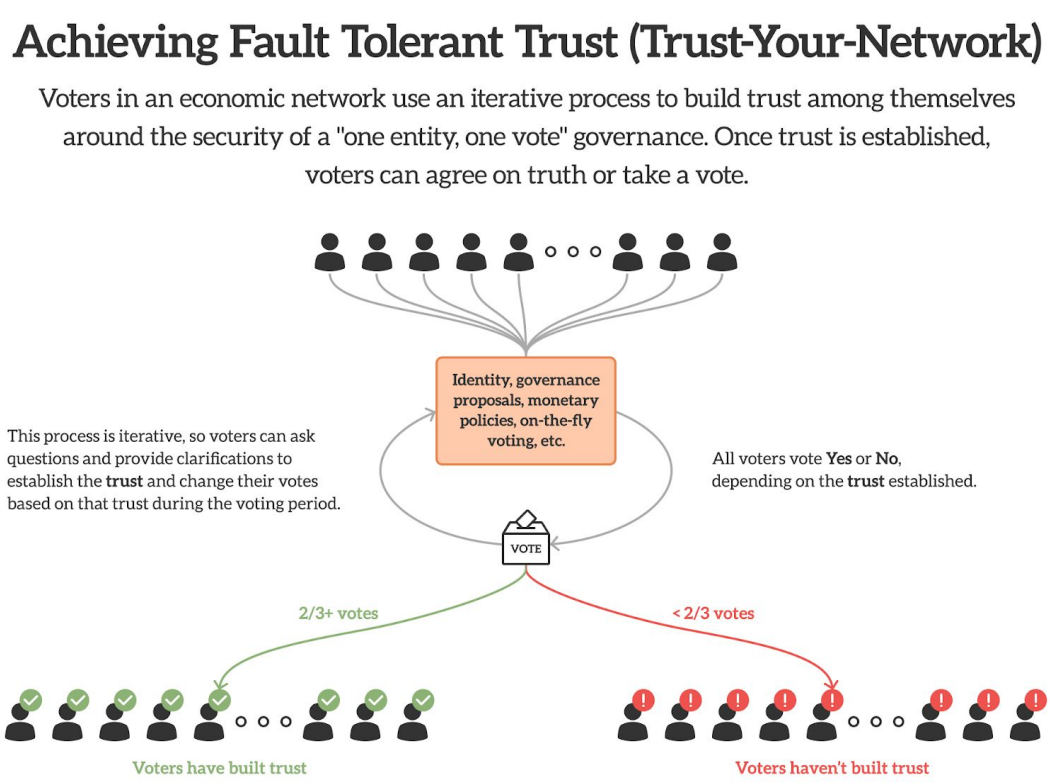
v0.1

Overview (tl;dr)

The fundamental tenet of democracy is “one person, one vote”. The security system of “one person, one vote” is some form of a centrally issued identity. But, can it work for computers voting in any system — centralized or decentralized?

No!

Sybil-resistant identity doesn’t exist in the online world because the definition of identity changes from *person* to *entity*. It is very easy for one entity to assume multiple, valid identities. This leads to an imbalance in **power**, which is harmful, especially in a decentralized democracy. A possible solution to this problem is some form of Know-Your-Customer (KYC) process, but it leads to centralized decision, forcing a decentralized democracy to start its life in a centralized manner. Instead of trying to solve this unsolvable problem, Storecoin proposes a new model called **Trust Your Network (TYN)**. This model borrows heavily from Byzantine Fault Tolerant (BFT) consensus models and achieves **fault tolerant trust** in a decentralized environment. In this proposal, we demonstrate that TYN can be used in a variety of use cases, ranging from miner onboarding, to ratifying Storecoin governance, to running on-the-fly micro-voting. TYN facilitates trust among voters around the security of a “one entity, one vote” governance. With TYN, **truth** is anything that ⅔+ voters agree on. The following diagram illustrates how TYN achieves fault tolerant trust among voters.



How Fault Tolerant Trust works

What is fault tolerant trust and why it is needed?

Voting in democratic societies is a well-established practice to arrive at consensus on any subject, such as a ballot measure or political election. The backbone of a functioning and secure democracy is “one person, one vote”. To secure democracy, a centralized government body administers identity checks with the goal of finding bad actors voting with fake identities, identities of the deceased, and more. Once a verifiable identity mechanism is in place that the electorate agrees to and trusts, voting ensures that only one vote is counted for a given identity.

Consensus, based on voting becomes tricky in a decentralized environment because one cannot trust any centralized entity to issue or verify user’s identities. This includes using decentralized identity verification services because of the **inherent trust** assumed in such setups. So, a decentralized system cannot bootstrap itself up without starting as a centralized system. This defeats the very desire to have a decentralized system in the first place.

It’s generally accepted that in order to create stable p2p decentralized democracy, the **trust system** must have the following properties:

1. **Repeat interactions** — provides an opportunity for **continued trust**.
2. **Possible win-wins** — aims for minimizing **tragedy of the commons**[1] and ensuring **incentive compatibility**[2].
3. **Low miscommunication** — with the same goal as 1 — **continued trust**.

Sybil-resistant identity doesn’t exist

In Computer Science, a Sybil attack[3] is an attack in which the attacker subverts the reputation system of a peer-to-peer network by creating a large number of pseudonymous identities and uses them to gain a disproportionately large influence. So, even if we can tolerate early centralization to achieve eventual decentralization, such

[1] https://en.wikipedia.org/wiki/Tragedy_of_the_commons
[2] https://en.wikipedia.org/wiki/Incentive_compatibility
[3] https://en.wikipedia.org/wiki/Sybil_attack

systems are not Sybil-resistant. This is because an individual can assume multiple **legal identities**, such as major ownership in a public corporation, board position in another organization, and partnerships in a few overseas shell companies. It may not always be possible to trace these corporate identities to an individual, so it is possible for an individual to control more votes than what appears on the surface in a decentralized governance process. Such an individual can easily hide their **power** across multiple entities. So, our belief is that **a Sybil-resistant identity doesn't exist**.

"Power" in identities is hard to detect

An entity, who is a 10% shareholder of a corporation may wield more **influence** in a decentralized democracy than an entity who represents themselves. So, just a verified identity is not sufficient in a "one person, one vote" based democracy because it is unable to differentiate the influences exerted by various entities.

The above two shortcomings demonstrate that traditional approaches to dealing with identities will not yield decentralized democracy. We need a different mechanism, which leads us to Fault Tolerant Trust.

Fault tolerant trust is about **building trust**, not verified identities

Instead of building identity systems that cannot be Sybil-resistant or transparent in their powers, we believe that participants in a decentralized system need to **build trust** among themselves such that ⅔+ of the participants arrive at a consensus when presented with the same set of information to all. We call such a **trust-building process as Fault Tolerant Trust, or TYN**.

The information that the participants will need to agree on can range from identities of all other participants to governance proposals to protocol changes in a decentralized governance. Since **possibility for centralization is removed** right from inception and **participants do not need to trust anyone**, a decentralized system can be bootstrapped in a decentralized way.

At Storecoin, we use TYN to create the founding miner group to launch the Storecoin network, to facilitate miners to ratify governance and establish various branches of Storecoin governance, to propose and vote on monetary and other policies. At no point in Storecoin governance, a centralized entity (such as the core development team or the foundation) can make decisions or influence the outcome.

Why TYN?

Storecoin governance uses “one entity, one vote” rather than “one token, one vote” model used by other decentralized networks. “One entity, one vote” implies that a STORE token-holder will get one vote in Storecoin governance no matter their staking size. This requires a stronger guarantees on voter identities, but as we discussed earlier, a Sybil-resistant identity doesn’t exist. So, “one entity, one vote” model can only be successful when at least majority of entities trust the identities of other entities (that they are not Sybil.) TYN achieves this goal by facilitating trust among voters around the security of a “one entity, one vote” governance.

With TYN, if the participants of a network trusts each other, they can do **micro-votes** on almost anything outside of a formal governance process.

Definitions

Identity — In the context of the “one entity, one vote” model, an identity is attached to an entity (a person) such that the entity cannot cheat the system with multiple votes derived from multiple identities that cannot be linked directly to this entity. As discussed above, Sybil-resistant identity is not possible, so identity verification is done such that all entities trust each other’s identities (that each entity can cast only one vote.)
Miner — An entity that runs a node in the Storecoin network. Storecoin network runs different types of nodes.
Validation miner — A type of miner in the Storecoin network that provides validation compute infrastructure.
Storage miner — A type of miner in the Storecoin network that provides storage and consensus infrastructure. Together with validation miners, storage miners secure transactions in the Storecoin settlement layer.

Participants or Voters — Participants who want to join Storecoin as miners. During TYN process discussed below, they are also called as voters because they vote on each others' identities.

TYN for Fault Tolerant Identity

TYN's trust-building model can be used to build a censorship-resistant identify verification system. Storecoin uses this system to onboard its miners, who need to build trust among each other before they can participate on Storecoin network.

In the identify verification model, participants who want to become Storecoin miners follow an **iterative** process to **build trust** that other participants in the system are not in power as any other entity in the system. This process works without needing any centralized verifiers, such as traditional or decentralized KYC (Know Your Customer) service providers. Participants start with little to no trust among them (because they don't know about each other) and build that trust in multiple steps. At each step, participants verify that the person is who they claim they are. We believe that Storecoin doesn't need to know the identities of the participants, but the participants themselves need to trust each other because they will be working together as miners in securing the Storecoin Network and participating in the Storecoin governance. Once participants are confident about the identities of other participants, they vote to approve or decline the identities of the participants. A supermajority vote (greater than ⅔ votes) is required to admit a participant into the Storecoin network. Storecoin is not involved in the identify verification process beyond defining what the process looks like and guidelines to verify the identities of the participants. A p2p democracy model for cryptocurrency governance requires a whole new trust model and TYN can be the facilitator for it.

Can Storecoin governance change how TYN works?

The TYN model is invented to bootstrap onboarding Storecoin miners and eventually ratify Storecoin governance. The elected miners will ratify Storecoin governance before the Storecoin mainnet launch phase. At that point, Storecoin governance can amend or replace TYN because that's precisely in the hands of the governance. So, the purpose of

TYN is to ensure that the Storecoin network doesn't start its life with centralized decision making.

Miner onboarding process with TYN

Storecoin miners are onboarded in a two-step process.

Step 1: Fault Tolerant Identity — We discussed this briefly before. A group of participants (existing/new STORE token-holders) who may not know or trust each other, validate each other's identities and vote that others are who they say they are. The participants are called voters in this step. There is a deadline to this step and at the end of this step, we have M of N voters (for example, 100 of 130) receiving supermajority (⅔ or more) votes from other voters verifying their identities.

Step 2: Auction — There are a limited number of seats (92 for the Storecoin Alpha phase) for being a Storecoin miner in a given phase. The TYN-verified voters participate in an auction to bid for the available seats. Top N (92 out of 100 here) participants will win the auction.

Step 1: Fault tolerant identity process — how it works

What do we want to prove?

1. Storecoin, any of its employees, or core developers cannot censor participants or influence who become miners.
2. It is important for participants to build trust among them, so they are confident that one entity with multiple identities is not admitted as multiple entities, thus defeating how "one entity, one vote" works.
3. Storecoin may provide tools (e.g., a website to login and go through TYN and auction processes) and recommendations (what documents to verify for various entities, how the process works, etc.) but is not involved in the decision-making process with censorship authority.
4. All participants must know that they (NOT Storecoin) are responsible for "one entity, one vote".

Process steps

1. All participants are made aware of the minimum STORE staking required, should they successfully complete TYN process. The minimum staking for a given phase may be higher than the previous phases. This means, existing miners will need to participate in both TYN and auction processes to be eligible to become miners in the future phases.
2. Participants create their accounts on TYN tool and login. The rest of the steps in this process are run on this tool.
3. The TYN process proceeds in several rounds. In each round, participants gather more information about each other and move to the next round. Participants may move at their own pace, subject to group deadlines for each round.
4. In the first round, applicants provide basic information such as name, email, address, private identities (such as a driver's license, passport, etc.), and public identities (Facebook ?). In this round, the basic information about participants' identities are verified.
5. In the second round, applicants provide their affiliation (representing oneself, a corporation, a nonprofit, etc.) and professional details (LinkedIn ?). Applicants self-report and other applicants verify the provided information. Verifying "one entity, one vote" is the goal here, so voters verify that the same person doesn’t represent multiple entities and thus gets multiple votes.
6. There may be more rounds depending on a person's profile and details required. A participant may not have submitted all the required documents for the profile they have created or other participants may have questions on the documents submitted. So, it is possible that verifying the identities of some participants may take longer than others.
7. Each round will have a deadline and as a group, the applicants may push the deadline out, if needed.
8. A voter votes for another voter if and when satisfied with all documentation provided as part of the identity verification process. Every applicant must vote either yes or no for all applicants. There is a deadline for voting. A "no" vote should contain justification(s) so the applicant knows the basis for that vote. The applicant may choose to provide missing information such that “no” voters become satisfied and change their votes to “yes” if there is time remaining in the voting period.

9. Any applicant who receives more than ⅔ of "yes" votes from other applicants is "TYN verified". It is theoretically possible that all applicants receive supermajority "yes" votes, none gets supermajority "yes" votes, or any number in between. Since TYN process proceeds in multiple rounds, a supermajority vote is required for every round, so participants can move to the next round.
10. At any point during TYN process and subjected to the deadline, some participants may receive supermajority vote later than others because of specific identity verification required for them and their response time. But, a supermajority vote is required for a given round before a participant can move to the next round.

It is important to note that there may not be any publicly available data to link different pieces of information of an entity. For example, how do you verify the LinkedIn profile of an entity to passport details or driver's license information for the same entity? Or, how do you verify the passport or driver's license information itself is genuine? If this were possible, Sybil-resistant identity verification would also have been possible. Since some information can never be verified with absolute certainty, trust building TYN process was invented. So, to answer the above questions, if supermajority of voters believe that the data submitted by an entity is genuine, then the identity of the entity is genuine.

Step 2: Auction Process

Preconditions

1. Auction takes place if and only if the number of applicants receiving supermajority "yes" votes is greater than the number of seats available in the phase for which TYN and auction are being held.
2. If fewer applicants receive a supermajority "yes" vote than the number of seats available, TYN process may be extended to allow more new applicants. All existing applicants whose identities are verified will participate in TYN process again because this is a community driven process.
3. If the number of TYN-verified voters is less than the number of seats available even after the extended TYN process, an auction is not necessary. All voters, who stake the minimum required for the upcoming phase will be able to join the Storecoin network as miners.

Process steps

1. The auction starts with the minimum stake required for the upcoming phase. This minimum bid may be higher than the stakes for existing miners. In any case, both existing miners and new STORE token holders participate in the auction. Note that the minimum stake for validation miners will be different from that for storage miners, so TYN-verified voters must also decide the function they are willing to perform.
2. The auction process is open and live with a deadline to complete it. This means, all voters know about the bids of all others and they can overbid each other. This open auction process is necessary for better transparency on how miners are selected.
3. At the end of the auction deadline, the top N voters are elected as miners for the upcoming phase, where N is the number of miners for that phase (92 in the above example).

Once voters enter the auction, they are contractually bound to accept miner positions, should they be among the top N voters. Failing to accept the position will result in forfeiting the minimum stake amount.

It is possible that existing miners are overbid by new STORE token holders. Losing miners continue to run their infrastructure and earn block rewards and bonuses until the end of the current phase.

Newly elected miners will have a bootstrap period, defaulted to one month, to build their infrastructure and join existing miners in the network. This means, TYN and auction processes for the next phase must start well in advance in the current phase.

It is important to know that miners will be running Storecoin validation and storage nodes, so they also need to have the technical skills required to run and manage these nodes.

The founding auction process — the auction process to launch the Storecoin network — is described here.

Attacks on TYN

The TYN process mimics classic Byzantine Fault Tolerant (BFT) consensus processes where ⅔+ processes must agree to arrive at the desired consensus. So, attack vectors on TYN will be similar to that of BFT's. There are two thresholds for attacks.

1. **⅓ or more entities collude** — In this scenario, ⅓ or more entities collude to make a decision that defeats governance rules. In governance voting, this collusion will mostly be undetected since it is seen simply as a vote against the proposal being voted. This collusion is easy if one entity can somehow cast multiple votes with falsified identities and this is the precise reason why participants must build trust on each other's identities in TYN process.
2. **⅔ or more nodes collude** — In this scenario, as the name suggests, ⅔ or more nodes collude to make a decision that defeats governance rules. In governance voting, this type of collusion is catastrophic, since the colluding nodes can sway the decision to their liking because of the supermajority voting. This type of collusion is much harder than the ⅓ collusion, but if one entity can somehow cast multiple votes with falsified identities, it will be relatively easier.

In the governance process, if certain proposals simply require majority votes (> 50%) a collusion between the above two scenarios would suffice. These scenarios illustrate why a good peer-verified identity system is critical to the success of any decentralized project. It is in the interest of the participating entities to have a properly vetted identity verification system, so they can work together in governance and consensus processes.

Recovering from ⅓+ attacks

As noted above, a ⅓+ attack on the governance process remains undetected, so there is no recovery possible. Since miners are assumed to be trusting each other, a ⅓+ attack shows up as ⅓+ miners rejecting the proposal tabled before them.

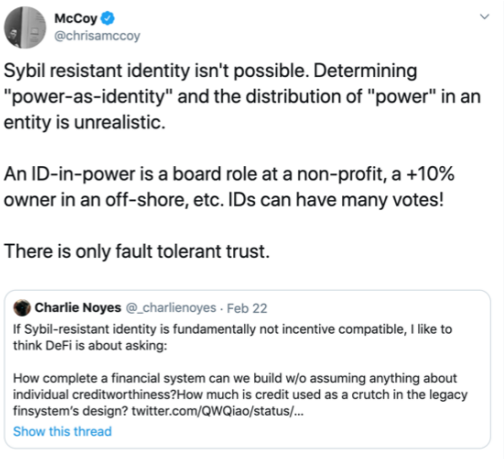
Recovering from ⅔+ attacks

A ⅔+ attack is a supermajority attack, so there is no recovery possible without a hard fork. The minority group of miners may fork away with a second network (or they continue on the existing network, if attacking miners fork away) where they can recruit more miners to secure that network. Similarly, the attacking miners do the same.

These attacks highlight why trust-building mechanism is critical to the success of decentralized democracy. With just identity-verified system, such attacks can be easily mounted, leading to catastrophic results.

TYN's similarity to Storecoin's BlockfinBFT

Storecoin's BlockfinBFT[4] consensus algorithm uses a two-tier network consisting of Validation and Storage miners. While the miners in each tier perform specific tasks, they work together to secure the Storecoin network. In other words, the Byzantine fault tolerance of the Storecoin network involves both the tiers. With TYN, similar tiering is possible for governance, economics, or any decision process. For example, Storecoin Markets, through TYN, can take a vote on a proposal at the Market level. That vote can then be a formal vote for the Market itself or the representative vote for the Market in its relationship to a larger network (i.e. the protocol). Along with the micro-voting capability discussed earlier, TYN model addresses cumbersome issues faced by typical decentralized governance models.



[4] https://research.storecoin.com/BlockfinBFT