How the Storecoin p2p, decentralized democracy is secured from sybil attacks using Know Your Voter (KYV)

Purpose

This spec describes Know Your Voter (KYV), Storecoin's decentralized approach for the miners to arrive at *trust*.

At the core of decentralized governance is *identities of nodes* participating in the governance. We believe that it is not possible to achieve sybil-resistant identity verification, even if we use decentralized identity verification systems. 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.

Instead, we believe that participating miners need to build *trust* among themselves because they are expected to work together in analyzing and voting various proposals presented to the governance. This is especially critical for Storecoin governance because of the "one entity, one vote" model it uses. So, instead of attempting to build a sybil-resistant identity verification system, we attempt to build a *trust system* for *censorship-resistant* identity. Our solution is to introduce a novel way for miners to reach trust amongst each other without the use of a trusted third party. 1/3 and 2/3 attacks on this trust are possible but both would be difficult.

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 the KYV process discussed below, they are also called as voters because they vote on each others' identities.

About KYV

KYV is a trust building process for a censorship-resistant identify verification system.

In our proposed "Know Your Voter" (KYV) model, participants who want to become Storecoin miners verify each other's identities in a series of trust building steps 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 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 KYV 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 KYV can be the facilitator for it.

The benefits of “Know Your Voter” (KYV)

Once the democratic balance occurs, it opens up new possibilities. The first order effect of democratic governance based on “one entity, one vote” is that it allows the largest number of people to participate. In the inverse way that the plutocratic centralization crowds out space for all but those already with the most power, a “one entity, one vote” system ensures that the voices of all are heard and incorporated in governance. This will be a key differentiator and will attract validators, users, developers, enterprises and anyone else who wants to have a say in the future of the ecosystems they’re a part of.

See https://storecoin.com/governance on how separation of powers ensures checks and balances in the Storecoin governance.

Can Storecoin governance change KYV?

The KYV process is invented to bootstrap onboarding Storecoin miners. Once elected, the miners will ratify Storecoin governance before the Storecoin mainnet launch phase. At that point, Storecoin governance can amend or replace KYV because that’s precisely in the hands of the governance. So, the purpose of KYV is to ensure that the Storecoin network doesn’t start its life with centralized decision making.

Miner onboarding process

Storecoin miners are onboarded in a two step process.

Step 1: **KYV** — 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 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 (say, 92, which is expected for the Storecoin Alpha phase) for being a Storecoin miner in a given phase. The *identity-verified* voters participate in an auction to bid for the available seats. Top N (92 here) participants will win the auction.

KYV

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 KYV and auction process) 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".

How KYV works

1. All participants are made aware of the minimum STORE staking required, should they successfully complete the KYV 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 KYV and auction processes to be eligible to become miners in the future phases.**
2. Participants create their accounts on the KYV tool and login. The rest of the steps in this process are run on this tool.
3. The KYV 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 "KYV verified". It is theoretically possible that all applicants receive supermajority "yes" votes, none gets supermajority "yes" votes, or any number in between. **Since the KYV 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 the KYV 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 KYV process was invented. So, to answer the above questions, if supermajority of voters believe that the data submitted by an entity is genuine, then it must be genuine.

Auction

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 the KYV and auction are being held.
2. If fewer applicants receive a supermajority "yes" vote than the number of seats available, the KYV process may be extended to allow more new applicants. All existing applicants whose identities are verified will participate in the KYV process again because this is a community driven process.
3. If the number of *identity verified* voters is less than the number of seats available even after the extended KYV 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.

How auction process works

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 *identity-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, KYV 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.

Fault tolerant identity

The purpose of the KYV process is to facilitate for all voters to verify the identities of all other voters. This ensures that "one entity, one vote" holds good in decision making and governance. Identity-verified voters eventually become Storecoin miners and participate in its leaderless consensus protocol called BlockfinBFT, which also uses the "one entity, one vote" rule to finalize the blocks in the Storecoin blockchain. So, it is important to ensure that one entity doesn't earn multiple votes by falsifying or faking identities. Byzantine Fault Tolerance (BFT) systems have two thresholds defined on the total number of nodes (miners) in the network to model malicious behaviors.

1. ⅓ or more nodes collude — In this scenario, ⅓ or more nodes collude to make a decision that defeats governance or BlockfinBFT protocol rules. In governance voting, this collusion will mostly be undetected since it is seen simply as a vote *against* the proposal being voted. In the consensus process however, this type of collusion affects the *liveness* of the consensus. This halts or freezes the block production and the network appears to be making no progress. This collusion is easy, if one entity can somehow cast multiple votes with falsified identities.
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 or BlockfinBFT protocol rules. In governance voting, this type of collusion is catastrophic, since the colluding nodes can sway the decision to their liking, because of the super majority voting. In the consensus process also this type of collusion is catastrophic. A ⅔+ majority can accept double-spend transactions or rewrite already finalized blocks with the transactions of their choosing. 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 nodes 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. A ⅓+ attack on the consensus process can be either intentional or unintentional. An unintentional attack is possible when ⅓+ nodes go offline because of a catastrophic event, such as an earthquake or hurricane that disrupts network connectivity in the geographic areas served by those nodes. In this case, the governance can vote to work under reduced tolerance, until the underlying conditions are restored. The following example illustrates this scenario.

Assume that 40% of the nodes in the Alpha phase, which has a total of 92 nodes, went offline. So, the network now has ~55 nodes (60%) online and they learn that the remaining nodes won't be online anytime soon. So, the nodes may table a proposal to operate with 55 nodes. If voted, they will continue to produce new blocks, albeit with reduced BFT tolerance. When the nodes come back online at a later time, the network reverts to its full capacity.

It should be noted that until the miners vote to operate under reduced capacity, the network is frozen. This is the nature of any BFT protocol.

If the ⅓+ attack is intentional, the remaining honest nodes can vote to operate under reduced capacity as noted above. The attacking nodes are removed from the consensus process by honest nodes. But in this case, the malicious nodes are also penalized for their behavior and their staking may be confiscated. A KYV + Auction process is scheduled to fill up the positions vacated by the malicious nodes.

The decision as to whether the attack is intentional or unintentional can be tricky and political. This decision cannot be made with technology alone. But in both cases, the network will freeze until a recovery path (work with reduced capacity) is voted.

Recovering from ⅔+ attacks

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