Novusphere: A Censorship Resistant Liability-free Database

Abstract. A purely peer-to-peer database allows records to be stored in its dataset with state transformations preserved via decentralized consensus ensuring the records were resistant to censorship. As no individual party has the authority to remove a record from the agreed upon dataset, no party can be held completely liable for any record in the dataset. The decentralization of the administrative authority to delete records and the recording of all state transitions ensures the existence of a significant barrier to censorship. Since moderation to keep data out is significantly difficult, the only form of moderation left is voluntary opt-in.

Introduction

Censorship on the internet is a problem where large social media giants such as Facebook, Twitter, Reddit, etc. control the power to heavily influence the user base including political events such as the election of a president. Through censorship and thought policing, narratives can easily be crafted and agendas easily pushed. Existing social media platforms and content sharing mediums work sufficiently well for many people and use cases. However, they suffer from the inherent weakness that the administrators of such platforms can exploit their administrative rights to police or be forced to police content.

What is needed is a base system where information cannot be tampered with or censored. With such a system, any party can freely share content including thoughts, ideas, and media, or arbitrary files. In this paper, we propose a solution to mitigate

censorship via administrative abuse in traditional server-side database model using a peer-to-peer blockchain-based network for content-agnostic communication. The content is secure as long as censorship resistance of the underlying blockchain is secure. We propose the use of a delegated proof of stake (DPoS) model[1],[2],[3],[4],[5] secured via honest users controlling honest block producers via greater committed stake than any colluding malicious groups. In the event the system is ever fully compromised, the honest users have the option to fork the system's state to a new chain void of malicious actors' stake.

Governance

The monetary unit or token of the platform (**atmos**) must first be vested to have a stake in the system. Vested atmos referred to as **v-atmos** are a direct representation of your stake in the system. A user can have multiple vestings occuring at the same time.

When a user requests their atmos be vested, the amount becomes unspendable and will transfer over time from the atmos locked in the vested transaction to v-atmos until all atmos has become v-atmos. Likewise, a user can request their v-atmos be divested, which will initially deducted the amount from their total v-atmos. Over time the v-atmos will be released back to the user as atmos, effectively the reverse of vesting.

The system is then governed by stakeholders voting on various things such as DAO funding proposals and development decisions.

Inflation Sources

- Block Producers - *If Novusphere utilizes a self-created blockchain layer*
- Public Gateway Maintainers - *A role of block producers or its own role if there are none*
- Stakeholder Reward
- DAO

Blockchain Architecture And Requirements

- **Zero-fee model:** If users are forced to pay for every transaction they do on the application as is the case with many applications built on Ethereum, we can expect that the application will never see mainstream adoption as it requires financial loss for every transaction which will inevitably add up over time.
- **High throughput:** Applications built using Novusphere must function similar to traditional web applications thus the throughput on the underlying blockchain layer needs to sufficient to meet this demand

- **Support for inflationary token:** Inflation exists to reward stakeholders and incentivize release of funds held by the DAO to pursue development proposals as more adoption/users will bring higher demand.

While blockchains modeled after Bitcoin and Ethereum do not meet our requirements, Steem's white paper proposed "Bandwidth Instead of Micropayment Channels" as a solution to allowing zero fee transactions. A similar model is proposed in EOS[6] under "Token Model and Resource Usage" which allocates resources based on an individual's EOS holdings.

Content System

To further incentivize content being added to the database, we propose a system in which users (requesters) can create bounties rewarding atmos for specific requests which can then be fulfilled by other users (bounty hunters) to claim the reward. To mediate this system, stakeholders elect a panel of judges to help settle any disputes that may arise.
For example, two bounty hunters A and B submitted content attempting to claim the bounty. The requester has chosen B to receive the reward, however A feels cheated since they were first to submit a satisfactory request. A opens a case with the judges by offering collateral equal to the "intervention fee" which is a percentage of the total bounty reward. Should there be multiple cases opened regarding the same bounty, each person must offer their own collateral equal to that of the intervention fee upon opening the case, but once settled the intervention fee will be deducted evenly from each party with an open case meaning each person's entire collateral is not consumed.
Judges must opt-in first and accept a case and must also vote with the greatest majority to be paid subsidy from the intervention fee. As judges must vote in a blind mannerism, most people will vote what they believe to be correct or the "honest" outcome expecting the other judges to do the same. There is no financial motive to be dishonest.
Varying degrees of punishments to judges can occur if:

- A judge accepts a case and does not vote
- A judge commits to a vote, but does not reveal it
- A judge votes with the minority
- A judge votes for the majority, but the majority is a tie
- A judge is not accepting cases frequently enough

Database State

The database state is derived by the application layer from the blockchain layer. It is important to make the distinction that the application layer is agnostic to the underlying blockchain layer and only cares about data retrieval, storage and access. The blockchain layer must make reference to IPFS hashes[7] of which the application layer monitors and reconstructs into a database of state transitions. The application

layer downloads the json object referenced by the IPFS hash and then indexes it to a database model. Updates to an object can be made by providing a state transition json object which includes the changes in the object. Branches of an object can be made if someone who is not the current owner of an object creates a state transition.

When an object is retrieved from the database by, it will also return a history of state transitions that have occured by the same publisher of the object trying to be retrieved.

For example, Bob has an object which he has committed the initial state and 3 transitions to. Alice creates a branch at B2, and adds 2 transitions.
B1 ← B2 ← B3 ← B4
← A3 ← A4

When the object B1, B2, B3 or B4 is attempted to be retrieved either the most recent state “B” with all transitions applied can be retrieved or all individual transitions (B1, B2, B3, B4).

Likewise, when the object A3 or A4 is retrieved either the most recent state “A” with all transitions applied can be retrieved or all individual transitions (B1, B2, A3, A4).

This provides an immutable history of an object while still allowing a mutable object to exist.

Efficient State Storage on a 3rd Party Blockchain

Under the section *"State Storage Costs"* in the EOS whitepaper it is stated that if an application's state is never deleted then the tokens staked for the state to exist are effectively removed from circulation as they are collateral for the resources the state occupies.
Novusphere is an ever growing index of metadata which would mean if approached naively our demand for EOS also is ever growing which is not sustainable due to monetary constraints. However, instead of storing each indexed metadata as part of the state on the 3rd party blockchain, we propose only an IPFS hash which is a reference to the Novusphere index be stored on EOS.
Each time new metadata is added to the index it is then added to a block of metadata. A block refers to some known threshold of metadata, as an example 30840 entries (~1 MB). In the case of threshold+1, a new block is created which references the previous block via its IPFS hash. When metadata is added, a gateway maintainer proposes the new change to the state as an IPFS hash which can then be downloaded and validated by the other gateway maintainers. If two-thirds of gateway maintainers agree it is then accepted as the new Novusphere state.
Through this mechanism the entire state of Novusphere can be determined through a single IPFS hash which once resolved allows transversal backwards to download previous blocks. This greatly reduce the footprint of an ever growing database to that of a single IPFS hash and a contract to verify the Novusphere state via an approval

voting scheme. Gateway maintainers are incentivized to seed the state as well as all previous metadata as if other maintainers cannot validate the state two-thirds approval can never be reached which means the state cannot progress further.

Summary

The combination of a decentralized blockchain offering censorship resistance, content indexing for consumption, bounty system for creating desired content, and judge system for reviewing content start to approach a sustainable mutually beneficial system. In addition it creates opportunities and incentives for users to become part of the system be it as a block producer, voter, requester, bounty hunter, or a judge.

Figure. Graphical schematic of the mechanism for content growth of the system.

---

[1] "DPOS Consensus Algorithm - The Missing White Paper — Steemit." Accessed May 4, 2018. https://steemit.com/dpos/@dantheman/dpos-consensus-algorithm-this-missing-white-paper.

[2] "In Defense of Consortium Blockchains — Steemit." Accessed May 4, 2018. https://steemit.com/eos/@dan/in-defense-of-consortium-blockchains.

[3] "Proof of Stake versus Proof of Work - BitFury." Accessed May 4, 2018. http://bitfury.com/content/5-white-papers-research/pos-vs-pow-1.0.2.pdf.

[4] "Response to Cosmos white paper's claims on DPOS security — Steemit." Accessed May 4, 2018. https://steemit.com/steem/@dantheman/response-to-cosmos-white-paper-s-claims-on-dpos-security.

[5] "Steem White paper - Steem.io." Accessed May 4, 2018. https://steem.io/steem-whitepaper.pdf.

[6] “EOS.IO Technical White Paper v2” Accessed May 7, 2018. https://github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md

[7] “IPFS Docs” Accessed May 7, 2018. https://ipfs.io/docs/