Authmen:
Secure and Economic Distributed Storage Protocol Based on Trusted Computing

Version 1.0.0

Abstract

Authmen is a new blockchain-based storage protocol which is more efficient and secure compared to existing platforms. It mainly focuses on solving the problems caused by data storage and data flow. It also provides protection against cyber security attacks, namely any kinds of tampering in terms of information security. Ideally, it ensures data integrity due to decentralization, provides other technical features such as confidentiality as well as privacy, high usability, openness and transparency.

Contents

1 Introduction

At present, the pain point of Internet storage and the rigid demand of trillion level blue ocean market is one of the urgent problems to be solved in the blockchain space. However, the distributed storage of hundreds of millions of data files on the blockchain obviously still lives in an untrustworthy environment. In the track of decentralized storage, the core problem to be solved is to make sure the data integrity with availability. There have been several solutions proposed to mitigate these issues.

1.1 IPFS

IPFS is a pioneer in the field of decentralized storage which has already stored a lot of data [1]. However, it is necessary to make IPFS a commercially available storage system rather than an arbitrary data sharing platform. Service quality assurance must be provided, which is the issue that Filecoin would like to solve, namely, the economic incentive layer of IPFS.

1.2 Filecoin

The Filecoin protocol separates storage and extraction, so that the following issues need to be solved in the implementation process [2]:

1. How to prove the authenticity of user data stored by miners?
2. How to prove that the miner kept the data as promised?
3. How to detect fake data storage? Is it possible to inject junk data to defraud additional issuance rewards?

In order to solve these three pain points, Filecoin designs the proof-of-space-time (PoST) and pledge mechanism, and introduces the authentication of real users. However, at the same time, the following issues inevitably arise:

- **Computational complexity:** it requires high computational processing power due to the complex design of the system.
- **Storage complexity:** The computation requires vast amount storage, which leads to high price of storage service.
- **Cost:** In addition to paying the necessary storage cost, miners also have to bear the high proof and pledge cost.

As a project with a long history, the technical scheme adopted in the white paper of Filecoin has been changed many times. The core consensus algorithm, post V1, changed from the earliest PoW like consensus to 2017, completely overturned the design of V1, changed to Algorand like algorithm, added the VDE implementation of Proof-of-Replication, and introduced new Verifiable Delay Function (VDF). Furthermore, the search feature on the market, micro payment, and other issues have not yet been improved. Unfortunately, Filecoin involves too many technical issues and challanges, which make the development cycle slow and tedious.

1.3 Sia & Storj

Although the technologies of Sia [4], Storj [**?**] and other protocols are different from Filecoin/ IPFS in technology, they are all contract based decentralized storage protocols, facing the same problems and transaction costs caused by the unreliability of devices.

1.4 Arweave

Arweave is a complete decentralized storage protocol that is not based on IPFS [5]. It encourages miners to save as much data as possible through the underlying architecture, and gives priority to storing scarce data with few copies, focusing on one-time payment and access to permanent file storage. Proof of Access (PoA) is a simple extension of POW. Although there is a possibility of losing blocks, considering that miners will preferentially store scarce blocks, the possibility of loss is low. Arweave has two advantages over Filecoin [2]: 1) it reduces the storage cost of users, 2) the development life cycle is relatively easy. However, Arweave still suffers from the following issues:

1. The actual application scenario is too narrow for developers to use. At present, most of the screenshots of anti-government comments from Twitter are stored in Arweave.

2. For the tamper proof function claimed, the content uploaded by users must be free from errors. It cannot be modified and must be uploaded again, resulting in a large amount of garbage storage.

3. In addition, due to the publicity of the underlying blockchain network, the content published on Arweave is open to the society and is not suitable for uploading personal content.

4. Although the team claims that Arweave is IPFS compatible, at present, developers are developing based on Arweave and cannot directly update HTML5 applications.

5. The business model is relatively simple and the technical barriers are not high, which may lead to price war of homogeneous projects.

On June 15 2020, Arweave's first large file implementation with storage function over 80Kb was available, but still with test code. Therefore, it is still far from being practical. Recent code has also been frantically trying to fix various file storage synchronization errors. Namely, if the core functions are not fixed, then it will not have much value.

To sum up, since the distributed storage proposals mainly depend on the composition of decentralized nodes, the udnerlying storage proof consensus algorithm should be adopted for spatial consensus. If the consensus algorithm is missing, other nodes would not be a able to trust each other. For example, in such a case, one cannot be sure whether the space for a node is sufficient to store the data or whether the stored files or copies have been lost cannot be recovered. At present, most of the blockchains with storage characteristics in the market only recognize the storage capacity of blockchain nodes subjectively. They cannot achieve a trusted node from a well-defined and widely accepted algorithms, and cannot achieve secure and reliable trust for the stored data. This would violate the original intention of the blockchain to be able to build trusted data and nodes.

Authmen is a middleware to solve all these kinds of confusion and problems of distributed storage protocol.

2 What is Authmen?

Authmen is a trusted blockchain storage protocol which is based on the distributed idea of blockchain. It mainly solves the problems of data storage and data flow. More concretely, it aims to provide distributed trust feature of the underlying blockchain technology, high availability, openness and transparency, tamper proof, security and privacy-preserving kinds of technical characteristics building a tamper-proof and a traceability system.

2.1 What are the characteristics of the Authmen trusted storage protocol?

1. **More Efficient and Secure Storage:** The design is exquisite and has stronger performance. It can realize the fast blockchain storage and traceability scheme corresponding to the key information system, and carry out the storage and transmission based on the blockchain in the process of data sharing.

2. **Real Tamper Proof Technology:** In a real sense, it can help users to achieve tamper proof function, instead of storage that users cannot control like Arweave. In addition, the key data of malicious tampering can be found in time, and the false data and illegally tampered malicious data can be found in the use process, and can be repaired in time.

3. **Wider Application Scenarios:** It can provide efficient and convenient blockchain services for enterprises and institutions, and directly manage data through front-end pages. It can provide users with localized deployment of blockchain system, with the help of its own anti tamper, traceability, strong disaster recovery and other features, it can save energy and improve efficiency for enterprise data management.

4. **Trusted Storage Node:** With the combination of the security technology of Trias trusted basic chain and Byzantine consensus algorithm after blockchain optimization, it innovatively increases the weight consensus proportion factor of reputation system, greatly reduces the consensus computing cost of blockchain node information, and accelerates the transmission speed of data on the blockchain [3]. By introducing the mechanism of trusted computing, the storage nodes are given credit system factors, which greatly reduces the consensus complexity of consensus nodes, and improves the execution time of existing distributed storage blockchain by more than 10 times.

Authmen adopts the three-layer computing power system based on leviatom in Trias architecture [3], and the combination of TEE (Trusted Execution Environment) trusted computing and zero knowledge proof technology to complete the right confirmation and security protection of distributed storage data.

The trusted network constructed by levitom layer of Trias maintains a unique white list for each storage node, which can prevent the loading of abnormal programs and effectively block network security attacks. At the same time, HCGgraph is a trusted computing technology based on heterogeneous TEE. With the help of Gossip protocol, a "trusted acquaintance" network is constructed between consensus nodes using different TEE technologies, and a "conspiracy default" model of global nodes is constructed to locate trusted nodes efficiently, which makes consensus more efficient and cost-effective.

At the same time, the TEE technology of Trias does not rely on a single category of hardware, so it has stronger compatibility. The use of TEE technology can verify and protect the whole life cycle of the computer running environment on the basis of the first layer of the hardware root. At the same time, under the TEE security defence model of Trias, it becomes a new incentive oriented security model, which allows the defender to actively contribute the defence nodes and computing power of TEE, and get the corresponding advantage economic stimulation according to the defence contribution provided in the Trias security network. Through the trusted computing of Trias, multi-party, remote and heterogeneous data storage, sharing and computing can be realized under the premise of maintaining data ownership and privacy. Furthermore, the data of trusted hardware and program based on Trias can ensure that the information or data will not be disclosed in the trusted program, and zkSNARKs are used to ensure the privacy of the data [**?**].

Through trusted computing, Authmen enables various TEE protocols to collect the latest status of neighbouring nodes, check and record historical information, and propagate the results among other nodes through gossip protocol, and form a reputation network. It repeatedly selects "the most difficult point to lie" as its repeated function contract presentation, forming a robust and efficient running environment, and building a trusted computing based environment which relies on the blockchain distributed storage security network.

References

[1] IPFS. IPFS powers the distributed web, 2020. https://ipfs.io/.

[2] Protocol Labs. Filecoin: A decentralized storage network, 2020. https://filecoin.io/.

[3] Trias. Trustworthy and reliable intelligent autonomous systems, 2020. https://www.trias.one/.

[4] David Vorick and Luke Champine. Sia: Simple decentralized storage, 2020. https://sia.tech/sia.pdf.

[5] Sam Williams, Viktor Diordiiev, Lev Berman, India Raybould, and Ivan Uemlianin. Arweave: A protocol for economically sustainable information permanence, 2019. https://www.arweave.org/yellow-paper.pdf.