Canyon: Permanent Storage Layer for Limitless Scalability

Liu-Cheng Xu

Abstract

TODO

Contents

1 Introduction

1.1 Motivation

TODO

1.2 Organization

TODO

2 Background

2.1 Filecoin

Filecoin[1] proposes a sophisticated cryptographic solution based on zero-knowledge proofs (ZKPs) to prevent the common attacks on the decentralized storage verification, which uses pure mathematical methods and is able to achieve high security guarantees. The whole mining process consumes too much computing power, making the actual storage cost prohibitively expensive. Furthermore, the extreme high hardware requirements eliminate a lot of small miners with common commodity hardwares from joining the network, the storage distribution today becomes centralized.

Due to the lack of authentic storage needs and system design of Filecoin, the miners themselves have to store tons of garbage data in the network, increasing the storage power and earning more mining rewards. Despite the off-chain governance approach like Filecoin Plus[1] being put up, it literally does not help a lot. How to promote the useful storage is still an unresolved huge challenge in Filecoin network.

2.2 Crust

To solve the problem of decentralized storage verification, Crust[2] adopts a hardware-based solution Trusted Environment Execution (TEE) to assure the client that the miners store a specific number of data copies as promised. Each of the storage nodes is required to enroll on Crust chain through TEE before it's allowed to deal with the storage orders from client. The TEE module of the nodes will periodly check and report whether the files are properly stored in the local storage space in a trusted way.

Despite Crust has a relatively low hardware demand for the mining compared with Filecoin, the miners are heavily dependent on the limited kinds of hardware that supports TEE, thus being greatly affected by the hardware manufacturers[2].

2.3 Arweave

Canyon is profoundly inspired by Arweave.

[1] `https://docs.filecoin.io/store/filecoin-plus`

[2] The three major CPU platform have different implementations: Software Guard Extensions(SGX) on the Intel platform, Secure Encrypted Virtualization (SEV) on the AMD platform, and TrustZone on the ARM platform. The SGX of Intel is the mostly widely used TEE platform.

3 System design

3.1 Consensus

3.1.1 Proof of Access

$$P(\text{win}) = P(\text{has recall block}) * P(\text{finds hash first}) \tag{1}$$

$$P(\text{win}) = P(\text{has recall block}) * P(\text{claims slot}) \tag{2}$$

Algorithm 1: Generation of POA

```
Input  :
        The random seed $S$;
        The weave size $W$;
Output:
        The proof of accesing the recall block $POA$;
Initialize the number of repeats $x$ with 1;
repeat
    Draw a random byte $B$ with $\textsc{MultiHash}(S, x) \mod W$;
    Find the $TX$ in which the random byte $B$ is included;
    $x \leftarrow x + 1$;
until The data of TX is available;
$POA \leftarrow \textsc{Construct}\text{POA}(TX)$;
return $POA$;
```

$$\hat{x} = \frac{1}{N}\sum_{i=1}^{N} x_i$$

$$R = \frac{1}{\hat{x}_{N\to+\infty}}$$

3.1.2 Proof of Stake

3.1.2.1 Staking Rewards

3.1.2.2 Stake

3.2 Economy Model

3.2.1 Perpetual Storage Cost

$$P_{GBH} = \frac{HDD_{price}}{HDD_{capacity} * HDD_{mtbf}} \tag{3}$$

- $P_{GBH} =$
- HDD_{price}

- $HDD_{capacity}$
- HDD_{mtbf}

$$P_{store} = \sum_{i=0}^{\infty}(Data_{size} * P_{GBH}[i]) \tag{4}$$

3.2.2 Transaction Fee

$$\begin{aligned} TX_{permacost} &= TX_{data\_size} * Sum &(5)\\ TX_{bandwidthcost} &= TX_{data\_size} * C_{network\_per\_byte} &(6)\\ TX_{reward} &= TX_{permacost} * C_{fee} + TX_{bandwidthcost} &(7)\\ TX_{total} &= TX_{permacost} + TX_{reward} &(8)\end{aligned}$$

- $TX_{permacost}$
- TX_{data_size}
- $TX_{bandwidthcost}$
- TX_{reward}
- TX_{total}

3.2.3 Data Oblivion

TODO

3.2.4 Multi-currency Payment

TODO

3.3 Transaction Pool

TODO

4 Roadmap

TODO

5 Conclusion

5.1 Future work

References

[1] Protocol Labs, Filecoin: A Decentralized Storage Network, https://filecoin.io/filecoin.pdf.

[2] https://crust.network/

[3] Sam Williams, Viktor Diordiiev, Lev Berman, India Raybould, Ivan Uemlianin. Arweave: A Protocol for Economically Sustainable Information Permanence.

[4] Gavid wood. Polkadot: Vision for A Heterogeneous Multi-chain Framework. https://polkadot.network/PolkaDotPaper.pdf

[5] https://github.com/paritytech/substrate

[6] Vitalik buterin. An Incomplete Guide to Rollups, https://vitalik.ca/general/2021/01/05/rollup.html

[7] A Storage-based Computation Paradigm Enabled by Arweave, https://medium.com/everfinance/a-storage-based-computation-paradigm-enabled-by-arweave-de799ae8c424

[8] https://ever.finance/

A Appendix