Suterusu: a privacy-protection infrastructure for Web 3.0

Dr. Lin

Abstract. Web 3.0 enables individual internet users to become the owner of their content, data, and assest. However, without a privacy-protection infrastructure that can protect the users' content, data, or digital assets from unwanted attention, it would be impossible for the users to have full control of their digital life. Suterusu will play a central role in protecting the users' privacy in the world of Web 3.0. Our current product Suter Shield, as a private payment infrastructure for smart contract platforms, has achieved tremendous success in terms of both user accounts and processed transaction volume. This white paper will show how we will build on Suterusu's existing work to establish a fully-fledged privacy-protection infrastructure that is accessible to every single Web 3.0 user.

1 Introduction

We live in a swiftly changing world. The emerging thesis of the internet economy that could potentially change every aspect of human life is Web 3.0, in which each internet user will have full ownership of their content, data, and assets. Suterusu, previously a leading private payment infrastructure for smart contract platforms, will become a privacy-protection infrastructure for Web 3.0 in this new age.

Our leading product Suter Shield has attracted over 15 thousand users and processed over 200 million USD worth of transactions as of today, which will continue to protect the users' transaction privacy. We will continue improving the performance of ZK-ConSNARK technology, and adopt aggregated proof to reduce the transaction cost.

Based on our existing zero-knowledge proof technology, we will design and implement an on-chain auction scheme that guarantees the fairness of on-chain auction and thus bring Web 3.0 experience to every internet user.

Non-fungible token (NFT) has detonated the explosion of gamefi summer of this year. It has been recognized by the Messari report as a foundation for Web 3.0, and could potentially become a universal building block for metaverse, decentralized identity, and decentralized social networks. We will extend Suter Shield to protect the payment privacy of non-fungible tokens. This not only means Suterusu will provide privacy protection service for the essential building block of Web 3.0, but is also a testament to Suterusu's resolve to become the dominant player in the Web 3.0 world.

2 Cost-efficient Suter Shield

Suter Shield has achieved great success, with over 15 thousand users and 200 million USD worth of transactions processed. It has also demonstrated its flexibility and composability since its launch. We have developed various derivative products based on Suter Shield such as the Suter privacy mining program, xSuter auction, Suter NFT, etc. Despite our novel ZK-ConSNARK technology, there remains room for us to further improve the performance of Suter Shield. Our next step will be adopting an aggregate zero-knowledge proof to reduce the proof size and thus related gas cost. The gas saving rate could range from 5x to 100x depending on the level of aggregation. Suter Shield will be a product that is affordable to every single Web 3.0 user.

3 Fair on-chain auction

The story of blockchain is that it requires no trusted third party and hence guarantees the transparency and fairness of online transactions. But hold your horses, due to the transparent nature of the blockchain-based solutions, the price manipulation, and front-running by a technically sophisticated bidder [1]

is indeed a lot easier than in the traditional setting. As a matter of fact, it has been indicated in a well-known report from Paradigm [1], the ability to prevent front-running attacks and guarantee the fairness of the auction is considered one of the most important feature of a fair NFT auction.

Suterusu project will build a fair auction scheme based on Suter Shield and public-key encryption. The bidding price will be protected by encryption and the bidders' committed tokens will be locked during the entire auction period. The contract will automatically enable the exchange of auctioned goods such as NFT and the unlocked committed token of the auction winner. It will guarantee the following properties:

1). No competitive conditions: Since all the bidding prices will be encrypted and kept secret from the other bidders, the competitive conditions mentioned in [1] will be eliminated. It would be meaningless now for the buyers to race to get their bidding offer to be mined before their competitors since they dont even know their competitors bidding price. This would significantly improve the fairness of the auction, and hence provide a better price discovery mechanism for the auctioned goods.

2). Not restricted by time zone: Since before the end of the auction, all the bidding price is encrypted and no bidders have any advantage over their competitors regardless of their bidding orders, one could join the auction at any time before the auction ends as they wish. We could set the length of the auction to be more than 24 hours so that any interested bidders from all time zones can join the auction at their most convenient time.

3). Resistance to Sybil attacks: As the bidders are required to commit a certain amount of Suter tokens before joining the auction, this alone will protect the auction against the Sybil attacks due to the economic and computational cost of registering and depositing operation.

4) No trust: our underlying encryption scheme be decentralized and the zero-knowledge proof scheme is trustless.

4 Anonymous vault for non-fungible token (NFT)

The existing Suter Shield scheme aims to sever the connection between the layer-1 addresses that deposit tokens to the Suter network and those that withdraw from the Suter network. The Suter transfer functionality further guarantees a network of Suter accounts obfuscates the flow of tokens in the Suter pool. We also apply a homomorphic encryption scheme to hide the transactional amount.

Since by definition, each non-fungible token is unique. Therefore, it is impossible to sever the link of incoming and outgoing layer-1 addresses holding the NFT. However, once an NFT is deposited into the Suter contract, we can apply the Suter transfer contract to anonymize the holders of non-fungible tokens. This essentially will create an anonymous vault for NFT. Our anonymous vault scheme will guarantee the holder anonymity of the NFT before it is withdrawn from our network, and thus create a dark period of NFT's lifetime.

5 Conclusion

This white paper summarizes how Suterusu intends to become essential privacy-protection infrastructure for Web 3.0. We explain the three main products that we intend to deliver in the next few months: 1. cost-efficient Suter Shield, 2. fair on-chain auction, and 3. anonymous vault for non-fungible tokens.

References

1. Anish Agnihotri Hasu. Nft efficient startup mechanism design guide, 2021. https://www.paradigm.xyz/2021/10/a-guide-to-designing-effective-nft-launches/.