Suterusu: to anonymize all the cryptocurrency in the world

Abstract. Zcash was the first to implement and apply ZK-SNARK in the decentralized cryptocurrency, but the trusted setup step of ZK-SNARK presents as a security risk. The relatively costly proof generation further reduces the likelihood of its being adopted in practice. Suterusu implements and integrates the state-of-the-art setup-free zero-knowledge proof protocol to enable trustless anonymous payment for smart contract platforms. Our proposed ZK-conSNARK scheme also attains the optimal balance between performance and security, i.e., almost constant proof size and efficient proof generation and verification. To further facilitate the adoption of zero-knowledge proof in practice, Suterusu will build a second-layer private payment protocol for smart contract platforms and UTXO payment model based on ZK-conSNARK. This in combination with Suter bridge, will anonymize any cryptocurrency including Bitcoin and Ethereum.

1 Introduction

Cryptocurrency since the inception of Bitcoin has considered user anonymity as its core value [11]. Anonymous cryptocurrencies such as Zcash [3], CryptoNote [13] and MimbleWimble [2, 1] take the protection of individual anonymity one step further by adopting more sophisticated cryptographic tools, including a one-time linkable ring signature, the confidential transaction with range proof, or even more general zero-knowledge succinct non-interactive arguments of knowledge (ZK-SNARK). At the center of these technological innovations is the adaptation and implementation of ZK-SNARK protocols in real-world applications, since loosely speaking, both linkable ring signature and range proof can be viewed

as a special kind of zero-knowledge proof. However, there is a fundamental conflict between the throughput and security that the existing anonymous cryptocurrencies fail to address due to the limitation of the SNARK schemes they have adopted. In other words, the SNARK protocols either require at least logarithmic proof size, or a trusted setup step that is indispensable, which not only implies a fundamental security flaw, but also contradicts the decentralized and transparent nature of anonymous cryptocurrency.

The core technical contribution of Suterusu is the implementation and integration of state-of-the-art, setup-free, zero-knowledge, almost constant-size, succinct non-interactive argument of knowledge (ZK-ConSNARK) schemes which can guarantee both sender and receiver anonymity, and the transaction amount confidentially. The development of this project can be divided into three phases: (1) Implementation of the ZK-ConSNARK scheme; (2) Develop a second-layer private payment protocol for both the smart contract platforms and UTXO payment model based on ZK-conSNARK. This in combination with Suter cross-chain bridge, will anonymize any cryptocurrency including Bitcoin and Ethereum.

2 Setup-free ZK-ConSNARK

The maximum throughput of a blockchain protocol is mainly determined by the maximum block size and average transaction size, which is further determined by the size of SNARK when it comes to a privacy-preserving blockchain protocol.

There are mainly two types of ZK-SNARK schemes:

- Zcash has a constant SNARK size but requires a trusted setup step, the compromise of which will allow the attacker to print infinite amounts of Zcash out of thin air without the possibility of being detected [12, 4].
- Setup-free cryptocurrency such as Monero, Grin, and Beam do not scale well due to their asymptotically larger SNARK size. Their proof size remains logarithmic even after adopting the very elegant Bulletproof technique [6].

ZK-ConSNARK schemes realize the setup-free almost constant-size SNARK for the first time. It has the advantages of both categories with none of their

downsides. We can literally "eat the cake and have it". Under the discrete logarithm assumption, our recent work [7] obtains the most compact and efficient range proof among all existing candidates (with or without trusted setup). Our proofs are 12% to 20% shorter than the state of the art Bulletproof [6] for standard choices of range size and security parameter, and are more efficient (both for the prover and the verifier) by more than an order of magnitude.

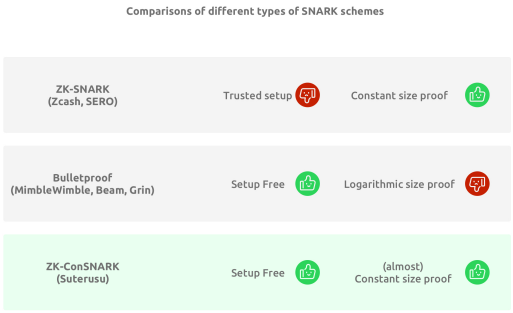

Fig. 1. Comparisons of different ZK-SNARKs

3 Interoperable privacy-preserving second-layer protocol

Our ecosystem will provide an interoperable second-layer private payment scheme that allows the confidential and anonymous payment under different payment models. More specifically, we will provide a second-layer private payment protocol for smart contract platforms and UTXO payment model based on ZK-conSNARK. In addition, we will build a cross-chain bridge that enables the interoperable private payment.

3.1 Account-based privacy-preserving second layer protocols

The relatively stable privacy-preserving blockchain technique for account-based blockchains is Zether [5], which provides a confidential payment channel scheme

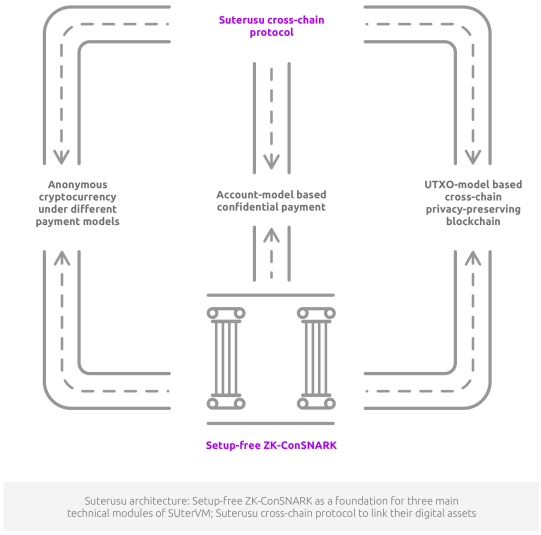

Fig. 2. Suterusu architecture

while solving the interoperability issue of smart contracts. Since the main underlying cryptographic modules are Elgamal encryption and ZK-SNARK technology, our ZK-ConSNARK technology can be easily applied to this case. The concrete design can be found in our yellowpaper [9].

Our design makes very few assumptions on the underlying platform other than assuming it is a blockchain that supports smart contracts. Consequently, the implementation of our design can be easily adapted to various existing smart contract platforms such as Ethereum, NEO, or Theta, etc.

3.2 UTXO model based privacy-preserving cross-chain technology

The developer can invoke our ZK-ConSNARK module to develop an improved version of anonymous multi-hop locks (AMHL) [10], which can be applied to implement anonymous payment channels for digital assets. The existing AMHL protocol that is resistant to wormhole attacks primarily has the following two features:

– The premise of the general construction is that the underlying algebraic structure supports the construction of a homomorphic one-way function, which both of our current ZK-ConSNARK protocols can satisfy, and hence there wont be any compatibility issue.
– However, the aforementioned general scheme only applies to blockchains with Turing-complete scripting language, such as Ethereum. We therefore need to further develop a scriptless AMHL module for the blockchain without comprehensive scripting language. In this case, the underlying algebraic structure is required to support the scriptless Schnorr signature or ECDSA signature scheme. Both aforementioned ZK-ConSNARK schemes satisfy this requirement.

The existing AMHL [10] supports limited relationship anonymity, i.e., the security model only considers the sender and receiver anonymity when the adversary is the intermediate nodes of the AMHL protocol. This security model is insufficient in the sense that it ignores the possibility that the adversary might launch the attack against the anonymity of the involved parties through analyzing the payment graph of the whole blockchain. We will solve this problem by applying our ZK-ConSNARK scheme to enhance user anonymity.

For more details regarding the cross-chain anonymous BTC transfer module, the interested readers are referred to our medium update series [8].

4 A privacy-preserving cross-chain digital asset management scheme linking anonymous digital assets of Suterusu

With the wide adoption of our launchpad for privacy-preserving blockchain technologies, we envision there will be a Cambrian explosion of anonymous assets in our ecosystem, which will enhance the decentralization and democratization of anonymous digital assets. Our ultimate mission is to provide further liquidity to those assets in our ecosystem. We will develop a privacy-preserving cross-chain

technology that can facilitate the free cross-chain movement of anonymous assets in our ecosystem. Currently, we apply our ZK-ConSNARK technique and commitment scheme to our own anonymous hash timed lock protocol to solve this issue.

If we consider the Suterusu ecosystem as an aircraft carrier, then the blockchain system built using SuterVM is the various fighters launched from this carrier. The respective digital assets are the fighter pilots that pilot the aircraft. Our privacy-preserving cross-chain protocol will guarantee these pilots can talk to each other even when they are high in the sky, and our token will serve as the medium to facilitate the exchange between these assets.

5 Governance

After research on the existing POS consensus mechanism and the behavior patterns of delegators and validators, the design of governance mechanism should address these concerns:

1. How to increase the voting turnout rate while keeping the system decentralized?
2. How to keep a balance between the number of votes and the professionalism of decision-making?
3. How to bootstrap the community and introduce the governance structure?

Based on the concerns mentioned above, we believe that the design of the governance mechanism should embody three characteristics, including "universality", "inclusiveness", and "adaptability". "Universality" means that the decision made by the governance mechanism can represent the community consensus, and be conducive to the sustainable operation of the community; "inclusiveness" means that diverse solutions can be produced under the community governance, and one can gain the best advantage of "wisdom of crowds" through decentralized decision-making process; "adaptability" means that the governance mechanism should take into account the interests of community members at different

stages, and an introduction procedure as needed. Taking these three principles into account, we present the following design for community governance framework.

5.1 How to participate

1. Become a community member by holding Suter token(s). A Suter token is not only a certificate of community participation, but also the stake of Suterusu protocol, and it will play a central role in community governance.
2. Quantifying contribution based on mining power. Mining power is the basic unit to measure contribution in the Suterusu ecosystem, and is calculated according to the quantity and holding period of Suter token. This means that the more Suter tokens and the longer the holding period, the higher the mining power will be.

5.2 Ecosystem roles and their behavior patterns

Suter holder.
Definition: a holder of the Suter token who uses some or all of the tokens to secure the Suterusu ecosystem. Behavior pattern: vote to a node or hold Suter token.

Possible activities:

1. A Suter holder can delegate their token to a validator node to obtain staking interest;
2. If a Suter holder does not vote to a node, they will pay the opportunity cost of losing staking interest;
3. In the case of misbehavior by the validator (for example, signing two different blocks at the same block height), part of the collateral deposited by both the errant validator and delegator will be slashed;
4. A holder will pay for a different commission rate, depending on voting, to a validator node;

Validator Node

Definition: Validators secure the Suterusu ecosystem by validating and relaying transactions, proposing, verifying and finalizing blocks. Behavior pattern: delegate to other nodes or operate a node by themselves. Possible activities:

1. A validator node needs to invest a certain amount of hardware equipment and pay for the maintenance costs to maintain its infrastructure to ensure reliability;
2. A validator must keep their validation key secure while connected to the P2P network to sign blocks;
3. A validator node needs to hold a certain amount of Suter tokens. The early validator nodes must hold at least 1 million tokens. There are at most 100 validator nodes in total;
4. A validator node will be slashed if any of its validated blocks is invalid;
5. A validator node can be voted on by delegators and share the mining rewards based on their mining power;
6. A validator node can stake their own Suter, or be delegated from other Suter token holders, and they can also charge the delegator commission fee in Suter token by a rate of no less than 10%.

Foundation.

Definition: a service organization and does not participate in voting Responsibilities:

1. The development progress;
2. Organize a voting process;
3. Financial management;
4. And other specific matters.

5.3 Featured mechanism

The opportunity cost of token holding: The Suter token has a constant total supply and will be released at a decreased rate. New Suter tokens are created

with every new block and distributed to validators and delegators participating in the consensus process. This provides an incentive to Suter holders to not just passively hold their tokens in wallets, but to vote for a node. Assuming a commission rate of 10%, the holder of Suter token will get 100% return in Suter by voting to a node in the first year. If a delegator doesnt vote to any nodes, they will have an annual opportunity cost around 45%. The high opportunity cost of holding token will help to achieve a high voting participation rate.

6 Token Economics

The economic model of our currency is deflation-based. At an early stage, the validators will be paid with the fee for their efforts. The fee payment process will be accompanied by a proportional Suter burning mechanism similar to Bancor.

With the development of our system, we envision our ecosystem can offer more sophisticated services other than simple payment. The potential services might include privacy-preserving proof-of-identity, confidential data source verification or secure query over private data, etc. These services can also be charged fees accompanied by a fair Suter burning process.

Token Distribution: The total amount of tokens is 10 Billion, 16% for fundraising, 4.8% for the team, 3.2% for foundation, the rest will be allocated to future mining rewards, 5% of which will be delivered to the team. All the investor tokens will be locked for 6 months, but POS mining initiates the minute the fund is transferred to the team. Both the foundation and team's token will be locked for a minimum of 3 years,and unlocked according to a predefined schedule.

7 Potential Use Cases

Private Payment for Defi

With our anonymous payment module for smart contract platforms and anonymous BTC cross-chain transfer module, one could easily build sophisticated Defi functionality such as decentralized exchange, or lending and load. To

put the cherry on top of the cake, we will guarantee all the monetary transfer in these fancy Defi functionality is privacy-preserving, meaning both the sender and receiver identity of a transaction is anonymized while the transaction amount is confidential. The plug and play nature of the technical modules provided by the Suter VM will guarantee the minimum efforts of developing the privacy-preserving Defi. Suterusu will be the top choice of Defi projects when they try to ensure maximum liquidity while still preserving their clients' financial privacy.

Proof of Identity

Zero-knowledge proof of identity is another application case of ZK-ConSNARK. When a registered user visits a website, his identity is revealed when using the conventional password-based authentication approach. On the other hand, he could run the zero-knowledge proof of identity protocol to authenticate themselves to the website without revealing exactly who they are. This serves to protect the user's browsing privacy.

Data Protection and Monetization

ZK-ConSNARK can also be deployed to protect one's digital property in a fair data monetization process. Imagine a hacker found a vital bug in a software and they try to sell their knowledge of the bug to the software vendor. But the hacker does not want to reveal this knowledge before they receive the bounty. From the software vendor's perspective, it cannot release the bounty without evidence showing that the hacker has successfully found a bug. In this case, the vendor and attacker could run a zero-knowledge test so that the attacker could indeed present a proof showing there is a bug in the software without revealing exactly what the bug is.Using the same principle, the general zero-knowledge ConSNARK could be used for proving the validity of any data in a privacy-preserving manner in any data monetization deal.

The amazing power of zero-knowledge ConSNARK can even shine in a centralized setting. For instance, companies like Uber or DiDi have long been accused of manipulating the ridesharing price. However, the price variation could just be the natural result of the algorithm they use in some cases. Nonetheless,

it might be difficult for those companies to exonerate themselves since the algorithm, especially the parameters of the algorithm, is their core trade secret. In this case, it is possible to apply the general zero-knowledge ConSNARK to efficiently prove their innocence while protecting their intellectual property. The same principle applies whenever there is a conflict between algorithmic transparency and confidentiality. Zero-knowledge ConSNARK can always be applied to realize control information leakage such that exactly the amount of balance can be achieved. For instance, the federal reserve could use our zero-knowledge ConSNARK to prove they are not reckless in terms of their currency policy, while not leaking any classified information.

8 Roadmap

Suterusu launched in December 2018 and it took about seven months to complete the literature study and research on the core technology ZK-conSNARK module. We proposed the ZK-ConSNARK and second-layer architecture design in September 2019. In March 2020, Suterusu will complete the development of setup-free ZK-ConSNARK and a test protocol capable of preserving both the sender and receiver anonymity and transaction amount confidentiality. Suter layer-2 solution that supports anonymous smart contracts will be online in the middle of 2020. The cross-chain functionality will be implemented in June of 2021. At the same time, an Android and iOS wallet that is compatible with the privacy-preserving cross-chain functionality will also be launched.

9 Core team

Suterusu's founding team consists of cryptographers from the Swiss Federal Institute of Technology (EPFL), senior engineers from ByteDance and Uber, and venture capitalists from China Renaissance.

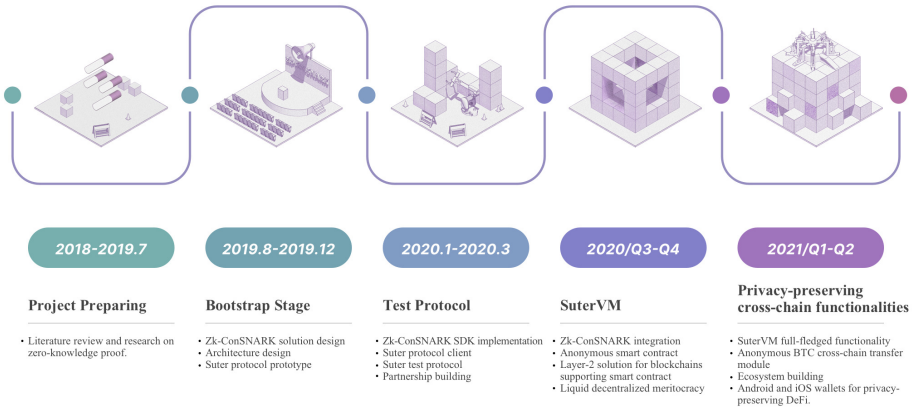

Fig. 3. Roadmap

10 Conclusion

Suterusu provides an interoperable ecosystem for the anonymous digital assets derived from our ecosystem based on our own design and implementation of advanced ZK-ConSNARK technology.

References

1. Beam project. https://github.com/BeamMW/beam.
2. Grin project. https://github.com/mimblewimble/grin.
3. Zcash project. https://github.com/zcash/zcash.
4. Daniel Benarroch. Diving into the zk-snarks setup phase.
5. Benedikt Bünz, Shashank Agrawal, Mahdi Zamani, and Dan Boneh. Zether: Towards privacy in a smart contract world.
6. Benedikt Bünz, Jonathan Bootle, Dan Boneh, Andrew Poelstra, Pieter Wuille, and Greg Maxwell. Bulletproofs: Short proofs for confidential transactions and more. In *2018 IEEE Symposium on Security and Privacy (SP)*, pages 315–334. IEEE, 2018.
7. Geoffroy Couteau, Michael Kloo?, Huang Lin, and Michael Reichle. Efficient range proofs with transparent setup from bounded integer commitments. Cryptology ePrint Archive, Report 2021/540, 2021. https://eprint.iacr.org/2021/540.

8. Dr. Lin. Suterusu yellowpaper update series: 2. anonymous btc cross-chain transfer module, 2020. https://medium.com/suterusu/suterusu-yellowpaper-update-series-2-anonymous-btc-cross-chain-transfer-module-55fe2e9fe31a.
9. Dr. Lin. Suterusu yellowpaper v 0.2, 2020. https://github.com/suterusu-team/yellowpaper.
10. Giulio Malavolta, Pedro Moreno-Sanchez, Clara Schneidewind, Aniket Kate, and Matteo Maffei. Anonymous multi-hop locks for blockchain scalability and interoperability.
11. Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. 2008.
12. Greg Slepak. How to compromise zcash and take over the world.
13. Nicolas van Saberhagen. Cryptonote v 2.0. *https://cryptonote.org/whitepaper.pdf*, 2013.