Suterusu: a launchpad for interoperable privacy-preserving blockchains

Abstract. Suterusu implements and integrates the state-of-the-art trustless zero-knowledge non-interactive argument of knowledge (ZK-SNARK) protocol, and offers multiple technical modules based on our ZK-SNARK implementation to enable developers to build any type of privacy-preserving blockchain. Suterusu (Suter) will also provide a cross-chain blockchain protocol for anonymous assets issued in the Suterusu ecosystem to guarantee their high liquidity and exchangeability. Suterusu has chosen a community-driven approach to guide its core development path, and has allocated 76% of the tokens to the community through mining. Sutuerusu will also introduce liquid decentralized meritocracy as the on-chain governance mechanism. This will provide participants with more flexibility and autonomy compared to the existing solution.

1 Introduction

Cryptocurrency since the inception of Bitcoin has considered user anonymity as its core value [10]. 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 SNARK. 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

Archived copy · cryp2nova.com

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, 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 SuterVM based on the implementation of ZK-ConSNARK. This SuterVM will provide various technical modules, which will serve as a launchpad for developers who wish to launch their own privacy-preserving blockchains under various payment models; (3) Develop a tailored cross-chain privacy-preserving digital asset management protocol to facilitate the liquidity of anonymous digital assets issued using the blockchain technologies of the Suterusu ecosystem.

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 [7].

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

Archived copy · cryp2nova.com

We can literally "eat the cake and have it". We see two routes moving forward to design ZK-ConSNARK schemes:

- The first possible direction is by combining probabilistically verifiable proofs with the recently-proposed efficient subvector commitment [8, 5] scheme over groups of unknown order. However, the prover, in this case, might have to perform redundant computation to guarantee the soundness of ZK-SNARK. On the other hand, when the statement of ZK-SNARK is as specific as a confidential transaction with range proof, this extra computational overhead might be acceptable. On the other hand, we are also working on a tailored design of confidential transaction by drawing inspiration from similar schemes based on RSA group.
- We can base our ZK-ConSNARK scheme on the recently-proposed Spartan scheme [11]. The Spartan is a succinct variant of the sum-check protocol, which is run with a low-degree polynomial encoding a circuit satisfiability instance. Their proof size is $k \times n^{-c}$, where n is the size of the arithmetic circuit and k is a small constant. It is possible to achieve almost constant SNARK size since our confidential payment scheme has a pretty simple statement for the underlying SNARK scheme and c can be chosen to be sufficiently large.

3 A launchpad for interoperable privacy-preserving blockchains

Our ecosystem will provide a SuterVM containing several technical modules (as listed in the following subsections) to developers who are not necessarily familiar with the underlying cryptographic technologies. Developers can use these modules to instantly launch a privacy-preserving blockchain protocol under different payment models.

Archived copy · cryp2nova.com

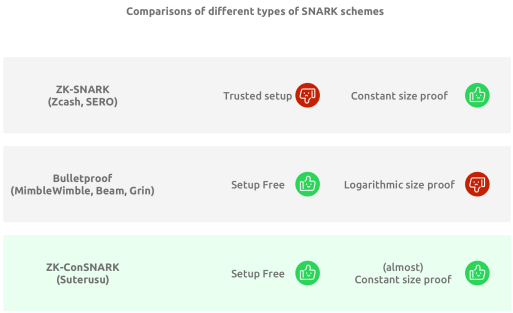


Fig. 1. Comparisons of different ZK-SNARKs

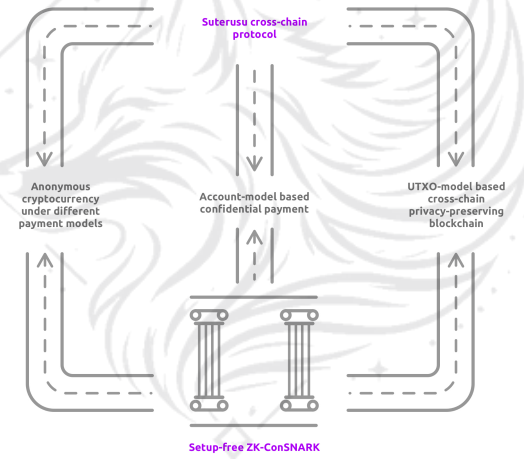


Fig. 2. Suterusu architecture

3.1 Anonymous digital cryptocurrency

Our ZK-ConSNARK allows the user to develop an anonymous cryptocurrency with either a Monero-like (UTXO model), or MimbleWimble-like (no address) transaction structure, but with a much smaller constant transaction size and

Archived copy · cryp2nova.com

more efficient verification. One could also invoke our ZK-ConSNARK modules to develop a Zcash-like anonymous cryptocurrency without the need of trusted setup.

3.2 Account-based privacy-preserving blockchains

The relatively stable privacy-preserving blockchain technique for account-based blockchains is Zether [6], which provides a confidential payment channel scheme 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 easily applied to this case.

3.3 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) [9], 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 won't 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.

Archived copy · cryp2nova.com

The existing AMHL [9] 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.

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.

Archived copy · cryp2nova.com

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.

CRYP2NOVA

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 blockchain, 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

Archived copy · cryp2nova.com

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 blockchain. Behavior pattern: vote to a node or hold Suter token.

Possible activities:

1. A Suter holder can delegate their token to a nominator node or 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. In the case of a nominator node finding misbehavior from validator nodes, the holder delegated to this nominator node will have the opportunity to share the rewards;
5. A holder will pay for a different commission rate, depending on voting, to a nominator node or a validator node;

Nominator node

Definition: a community member that will play an important role in the cold launch of the community and the introduction of community governance. Behavior pattern: delegate to other nodes or operate a node by themselves. Possible activities:

1. A nominator node does not directly process the transaction data, but will verify the transaction data based on the mechanism defined by the community;

CRYP2NOVA

Archived copy · cryp2nova.com

2. A nominator node can be voted on by delegators and share the mining rewards based on it's mining power;
3. If a nominator node finds mistakes in the record of validator node, they will be rewarded;
4. A nominator node can charge the delegator commission fee in Suter token by a rate of no less than 10%.

Validator Node

Definition: Validators secure the Suterusu blockchain 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;

CRYP2NOVA

Archived copy · cryp2nova.com

3. Financial management;
4. And other specific matters.

5.3 Featured mechanism

1. 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 doesn't 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.
2. Community Governance: Liquid Decentralized Meritocracy Suterusu will use the stake-weighted referendum before any changes made to the protocol. The basic principle is that the majority of stake commands the network. In the case of insufficient turnout, we will introduce a statement voting mechanism for liquid decentralized Meritocracy to guarantee one could always delegate its voting power to the best expert on issue they can trust. This mechanism combines the advantages of both liquid democracy [10, 18] and the meritocracy mechanism of conventional bureaucratic system of East Asia.
   Compared to the static committee voting protocols most existing blockchain ecosystems rely upon - which basically corresponds to direct/representative democracy in real life - our statement voting mechanism for liquid decentralized meritocracy is much more adaptive and flexible in the sense that it combines both the decentralized nature of liquid democracy and the "rule by experts" feature of a conventional meritocracy. As we can see from real-world cases such as the failure of Brexit voting, direct/representative democracy has many limitations and often fail to serve the best interest of the people in

CRYP2NOVA

Archived copy · cryp2nova.com

collective decision making. More specifically, it fails mainly due to a voter's lack-of-expertise on the specific issue they are voting on [16]. For instance, in the Brexit voting case, the most Googled sentence in Britain was "What Is The EU?" after the Brexit Vote.

Liquid decentralized meritocracy, on the other hand, allows the stakeholder to flexibly pick any delegate they wish whenever there is a voting issue. This, in combination with the sophisticated statement voting mechanism, ensures the stakeholder to choose the most trustworthy expert delegate on any specific topic. For instance, a stakeholder might not be a cryptographer , but they can choose a stakeholder with cryptographic expertise as their delegate when there are any governance issues regarding cryptography. On the other hand, they can designate an economist stakeholder as their delegate when a protocol change regarding economics comes up. We believe this alternative decision-making model would make better use of "the wisdom of the crowd" compared to the case where one voter can only delegate to one fixed group of committee members. It is important to note that although the meritocracy here might share certain similarity with conventional east Asian meritocracy, our design is bottom-up in nature. In other words, the voters can replace their delegate experts any time they wish. We believe this would prevent the centralization and corruption brought by the relatively static nature of ancient East Asian meritocracy.

3. Dual-layer nodes The Suterusu ecosystem will have a two-layer nodes system. The nominator nodes become community members by private sale method, and will contribute greatly to the community construction and governance introduction in the early period. Therefore, they have some advantages in sharing the mining rewards based on their mining power, which is positively related to the quantity and time of token holding. However, a nominator node is not directly responsible for the transaction validation and need not invest the hardware as a validator node does. Therefore, the system will apply a modified multiplication factor, which is greater than 1, in the calculation of mining power to a validator node after the mainnet has been launched.

CRYP2NOVA

Archived copy · cryp2nova.com

The dynamic calculation method is helpful to the introduction of community governance.

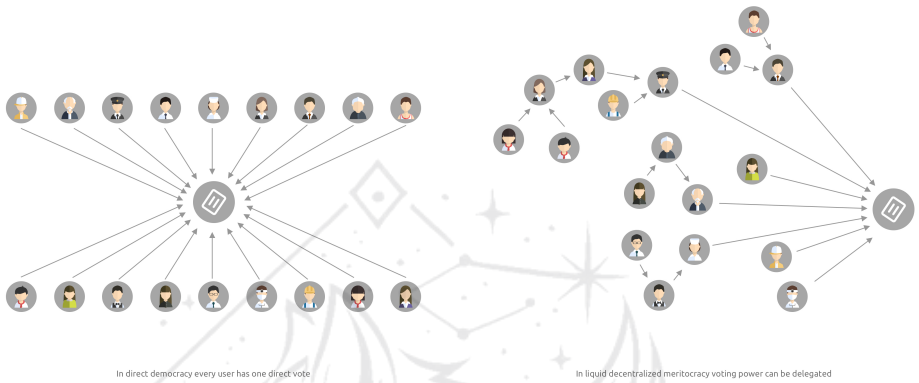


Fig. 3. Liquid decentralized meritocracy

6 Consensus

The Suterusu blockchain adopts the latest BFT protocol "que sera consensus (QSC)" as the underlying consensus mechanism. QSC employs TLC (threshold logic clock) to annotate the sequence of event processing. We develop QSC based on the deconstruction of asynchronous consensus mechanism by TLC. Under the QSC mechanism, each participant proposes a potential value to agree on (e.g., a block in a blockchain), then simply "wait" a number of TLC time steps, recording and gossiping about their observations at each step. After the preset steps have elapsed, the participants decide independently on the basis of public randomness, and the history they observed, whether the consensus round succeeded and which value was agreed on. QSC simplifies the implementation mechanism of BFT consensus and provides basic security for Suterusu blockchain.

Archived copy · cryp2nova.com

7 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, fetc. 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.

8 Potential Use Cases

Private Payments We believe our private payment scheme would be a handy tool in a privacy-aware environment where the strict data protection law, such as the General Data Protection Regulation (GDPR) is applicable.

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

CRYP2NOVA

Archived copy · cryp2nova.com

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.

CRYP2NOVA

9 Roadmap

Suterusu launched in December 2018 and it took about seven months to complete the technical design, including the proposal of the core technology ZK-conSNARK module. Starting with the selection of nominator nodes and validator nodes, the economic incentive mechanism has been introduced step-by-step, and an on-chain governance system has been gradually established from September 2019. In 2020, Suterusu will complete the development of setup-free

Archived copy · cryp2nova.com

ZK-ConSNARK. This will be followed by the implementation of SuterVM and the cross-chain protocol in the next year. We will be focusing on the implementation and testing of the Suterusu mainnet in 2022 so that it will be online by the end of that year.

10 Conclusion

Suterusu provides a handy tool for the swift development of privacy-preserving blockchains, and an interoperable ecosystem for the anonymous digital assets derived from our ecosystem based on our own design and implementation of advanced ZK-ConSNARK technology. The underlying consensus protocol is the state-of-the-art Que Sera protocol, and we have introduced liquid decentralized meritocracy as our on-chain governance mechanism.

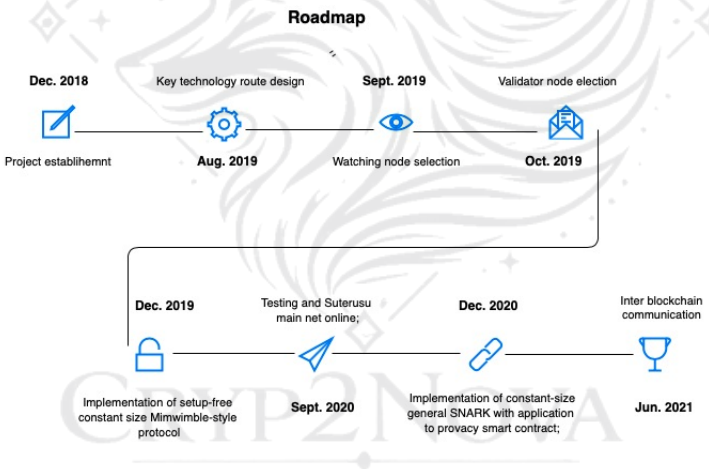


Fig. 4. Preliminary Roadmap

References

1. Beam project. https://github.com/BeamMW/beam.
2. Grin project. https://github.com/mimblewimble/grin.

Archived copy · cryp2nova.com

3. Zcash project. https://github.com/zcash/zcash.
4. Daniel Benarroch. Diving into the zk-snarks setup phase.
5. Dan Boneh, Benedikt Bünz, and Ben Fisch. Batching techniques for accumulators with applications to iops and stateless blockchains. *IACR Cryptology ePrint Archive*, 2018:1188, 2018.
6. Benedikt Bünz, Shashank Agrawal, Mahdi Zamani, and Dan Boneh. Zether: Towards privacy in a smart contract world.
7. 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.
8. Russell W.F. Lai and Giulio Malavolta. Subvector commitments with application to succinct arguments, 2019. https://eprint.iacr.org/2018/705.
9. Giulio Malavolta, Pedro Moreno-Sanchez, Clara Schneidewind, Aniket Kate, and Matteo Maffei. Anonymous multi-hop locks for blockchain scalability and interoperability.
10. Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. 2008.
11. Srinath Setty. Spartan: Efficient and general-purpose zksnarks without trusted setup. Cryptology ePrint Archive, Report 2019/550, 2019. https://eprint.iacr.org/2019/550.
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.

CRYP2NOVA

Archived copy · cryp2nova.com