SUPER ZERO(SERO)
TECHNICAL WHITE PAPER

The global leading privacy protecting platform
Making decentralized applications truly Secure, Private and Stable

SERO

Version 1.08
Last Update: Dec 28th, 2018

CHAPTER I
ABSTRACT

The Internet has greatly enhanced the efficiency of information dissemination, which benefits Human society; on the other hand, lack of privacy becomes more of a serious problem. Blockchain is considered a great tool to protect privacy. However, since all the transactions are recorded on the public blockchain, once the identity of the wallet holder gets uncovered, this loss of privacy is irreversible. The scenario leads to a more serious problem than the privacy disclosure of the Internet. For this reason, cryptographers and top technical experts in the blockchain industry have made relentless efforts to resolve the issue. Several teams in the industry have developed special cryptocurrencies to protect privacy, which are called "anonymous currencies". Some of the best-known anonymous currencies are Zcash (ZEC), Monero (XMR), and Dash. These cryptocurrencies with a certain degree of privacy protection, have obtained high market values based on the vast demand and have been ranked among the world's top 20 cryptocurrencies for a long time; thus, indicating a strong demand for privacy protection in the blockchain industry.

Smart contract is a computer protocol designed to distribute, verify or execute contracts in an information-based way. Turing complete smart contract system on the blockchain allows developers to write any complicated contract that lives on the blockchain and can be executed on the blockchain. Developers can use smart contract development language to produce functions such as custom token, financial derivatives, identity system, and decentralized organization, therefore, greatly expanding the application scope of the blockchain system. Smart contract is one of the foundational bases of the Internet of Value. The current shortcoming is that none of the blockchain systems support encryption and privacy protection of smart contracts. The existing use scenarios of privacy protection mechanisms are greatly reduced due to the technical limitation. Blockchain 1.0 technology originated from Bitcoin invented by Satoshi Nakamoto, has created a new paradigm. With the advent of Ethereum – blockchain 2.0, the invention of smart contracts makes the blockchain technology accessible, and the Distributed Applications (DAPPs) based on the blockchain technology more feasible, allowing blockchain technology to be applicable to more industries. Zcash and Monero which do not support smart contracts are privacy protection scheme 1.0; privacy protection scheme 2.0 that supports smart contracts is expected to be implemented in more industries and application scenarios.

There is no doubt about the high technical threshold required for developing anonymous cryptocurrencies that support smart contracts, and there are only few teams in the world who are tackling this problem. The official release of Super Zero (SERO) to the world presents the first anonymous cryptocurrency that supports smart contracts. The SERO's R&D team (SERO Team) is the only team in the world that presents a complete solution to solve the Privacy problem and has completed major R&D work. SERO team not only considers the privacy of DAPP Users' accounts and transactions but also fully considers privacy protection of DAPPs’ developers, making privacy protection of the DAPP Ecosystem truly secure and stable.

SERO team has assembled a 3 in 1 suite that can provide a complete privacy protection solution for DAPPs; including advanced innovative technology components SERO (privacy cryptocurrencies platform supporting smart contracts), ALIEN protocol (a protocol that can solve security problems within the transmission of information in decentralized networks) and CASTROL protocol (a protocol that protects decentralized networks and provides privacy protection for every node in the Internet). The white paper describes SERO's work and includes core information about the project as well as the disclosure of subsequent project plans.

CHAPTER II
INTRODUCTION

2.1 DECENTRALIZATION TECH AND PRIVACY ISSUES

At present, users have an increasing concern and demand for privacy protection; many well-known companies have leaked a large number of user privacy data, including Yahoo, Uber, PayPal, InterContinental Hotels Group, US credit agency Equifax, UK National Health Service System(NHS) etc., compromising tens of millions to hundreds of millions of user data. Facebook lost tens of billions of dollars in market value in two days due to one of the largest privacy leaks in March 2018. The issue of privacy has also attracted the attention of many governments; the European Union took the lead in promulgating the General Data Protection Regulations (GDPR) to urge companies to effectively protect users' privacy.

Majority of the privacy leaks in the Internet application scenarios are caused by the lack of adequate data security protection mechanisms in a centralized platform. Blockchain technology is thought to be able to prevent such incidents. The design of blockchain networks such as Bitcoin and Ethereum didn’t take into account the possibility of the link established between the wallet and physical identity. The extremely sensitive information such as digital assets and their transaction records in the blockchain is transparent to public and cannot be tampered with. If blockchain is used in a larger number of real scenarios, the transparency is undoubtedly unacceptable for most users.

The range of legal use cases of financial privacy is very wide. Financial privacy protection is needed for most transactions in the world. It is unreasonable to expose cryptocurrencies' assets and transactions data stored on the blockchain to the public.

Examples of real-world scenarios:

* A company wants to protect supply chain information without revealing it to the competitors.

* An individual does not want the public knowledge of paying for consultation with a bankruptcy lawyer or divorce lawyer.

*A family, fearing discrimination, wants to withhold children’s medical history from employers and colleagues.

*A wealthy individual preventing potential criminals from gaining access to his whereabouts to prevent extortion.

* Commodity buyers and sellers want to avoid the transaction being cut off by any middlemen.

* Investment banks, hedge funds and other types of entities dealing with trading financial instruments (securities, bonds, derivatives); protecting their positions or trading intentions.

In smart contracts, the entire sequence of actions is distributed through the network and recorded on the blockchain and is publicly visible. Individuals and organizations believe financial transactions (such as insurance contracts or stock transactions) are highly confidential; however, this need for the information privacy protection is not currently supported. The lack of privacy becomes the main obstacle to the widespread adoption of decentralized smart contracts. The lack of privacy protection technology is a serious bottleneck for the popularization of DAPPs. The technological development progress in related fields has attracted public attention.

2.2 BLOCKCHAIN PRIVACY RISK

Bitcoin network is a typical blockchain technology representative. Mainstream cryptocurrencies in the market are mostly based on the same technical features. The following uses Bitcoin network as an example to analyze the risk of privacy leakage.

First, from the perspective of bitcoin transaction system's structural design:

* UXTO model of transaction data contains input address and output address information, each input address points to the previous transaction, and all input transaction amount can be traced back to the source.

* Transaction data is stored in a public global ledger, and any participating user can obtain a complete global ledger. In the consensus process, the verification node needs to retrieve historical transactions, and all transaction information is not encrypted to protect data.

The addresses of participants in bitcoin transactions are created by the users and not related to the identity information. No one can directly deduce the identity information of the users in the transaction by observing the transaction records; however, there is a correlation between transactions disclosed in the global ledger, and potential attackers can deduce the transaction rules of bitcoin addresses by analyzing the transaction records in the global ledger. The transaction frequency, transaction characteristics, and correlation between addresses, etc. in the global ledger makes it possible for an attacker to associate a bitcoin address with the identity of a particular user in the real world.

One of the methods mainly obtains regular characteristics of the transaction of the address by analyzing the transaction record related to the address and estimates the identity information of the corresponding user accordingly. Since there are unique transaction characteristics in certain types of blockchain transactions, attackers can restore the actual transaction according to the transaction characteristics of the address, thereby determining possible identities of the user. Androulaki E. et al

designed a simulation experiment to match the blockchain address with the students' identities. Students used bitcoin as a payment method for daily transactions and used the one-time address method recommended by bitcoin to enhance privacy protection. Analysts were able to successfully match the student's identity and the blockchain address with 42% accuracy through behavior-based clustering technology. Moneco J. V. et al quantifies the trading behavior of bitcoin users and analyzes the trading rules of users based on twelve dimensions including trading time, interval and cash flow. After 6 months of experiments, the accuracy of using the analysis model to successfully identify users' real identities is as high as 62%, and the error rate is less than 10.1%.

Another method is to use some potential knowledge in blockchain transaction designed to cluster different addresses and get multiple addresses of the same user.

Currently, there are mainly three rules for address clustering:

* For a transaction with multiple input addresses, it is generally assumed that all input addresses come from the same user or a collection of users. When a user initiates a transaction, the digital assets may come from multiple addresses of the user, and the user needs to sign each input address separately, so most multi-input transactions come from the same user. The rule has been applied to many research projects and has achieved good clustering results.

* In the transactions organized by the mining pool, multiple output addresses in the same transaction belong to the same user group. As the difficulty of "mining" increases, individual "miners" are no longer able to win the competition, requiring hundreds of "miners" to join the "mining pool" to complete "mining" together, and the rewards will be distributed to the "miners" participating in the collective "mining".

* The change address and the input address in the transaction belongs to the same user. In one transaction, the total amount in the input address may be larger than the amount issued by the user, so the bitcoin system will automatically generate a change address for the sender to receive the change amount in the transaction. As with other addresses, the change address may be selected by the system as the input address in the new transaction, the output address will usually only be used once. Since the change address was regenerated by the system during the transaction, it is impossible for an address to be used as the input address and output address for one transaction at the same time; there must be another output address other than the change address in the output of the transaction. By using the characteristics of change addresses, we can figure out the relationship between other addresses.

Studies have found the relationship between many addresses in bitcoin system using the above clustering rules. Meikle John S. et al attained the identification of bitcoin addresses in bitcoin theft cases by using heuristic clustering methods. Dmitry E. et al also provided a method to automatically identify cluster bitcoin addresses.

2.3 DECENTRALIZED PRIVACY PROTECTION TECH

We are pleased to see teams are beginning to address privacy protection of decentralized networks; including Zcash, Monero and Dash. One widely used method is to change the transaction process without changing the transaction results, and attackers cannot directly obtain complete information about the transaction. The method is called " mixed currency". For example, in Chaum D.'s article, an anonymous communication technology is mentioned, which hides the real communication content in the communication process. The basic idea can be expressed by formula (1):

$$CM(Z1,CA(Z0,m),A)\rightarrow CA(Z0,m),A(1)$$

The left side of equation (1) is the message sent by the sender to the intermediary, and the right side is the message sent to the receiver after the information is processed by the intermediary. The sender wants to send the messages Z0 and m to the address A of the receiver. First, the message encrypts with the key CA of the receiver to obtain CA(Z0, m), then packages the authentication message Z1 of the intermediary. The encrypted message CA(Z0, m) and the address A of the receiver, then encrypts with the public key CM of the intermediary to prevent the information from being intercepted or tampered with by attackers during the sending process. After receiving the information, the intermediary decrypts it with his private key to get Z1, CA(Z0, m), A, but is unable to decrypt the content of CA(Z0, m). The intermediary sends CA(Z0, m) to address A after verifying Z1 is correct. The receiver then decrypts the message using its own private key to complete the communication.

Messages are not directly transmitted between the sender and the receiver, instead, the messages are transmitted indirectly through an intermediary, making it impossible for attackers to observe the communication behavior between the sender and receiver, thus, improving the anonymity of the communication. If the message is passed through multiple intermediaries, for the difficulty for attackers to discover the communication relationship between the sender and receiver increases.

The mixed currency mechanism in cryptocurrencies draws from the above methods (Dash and Monero) and removes the traceable relationship between the actual sender and receiver in the transaction through an intermediate hierarchy. The implementation of the currency mixing process can be implemented by a trusted third-party or other protocol. A third-party node is involved in the currency mixing process, the existing currency mixing mechanisms can be divided into two categories: the central node and the decentralized node. The two mechanisms have their own advantages and disadvantages in terms of currency mixing reliability, efficiency and cost.

More sophisticated encryption techniques have been applied to blockchain privacy protection with the development of technology - Zcash using Zero-Knowledge proof.

Brief descriptions of the three most popular cryptocurrencies with privacy protection:

Zcash

Zcash is a cryptocurrency that use encryption technology to provide users with greater privacy protection than other cryptocurrencies such as Bitcoin. Originally named ZeroCoin, the team then developed the ZeroCash system, and it was developed into Zcash cryptocurrency in 2016.

Zcash payments are published on the blockchain, users can use optional privacy function to hide the sender, receiver and amount of transactions on the blockchain. Only those who have the key can see the contents of the transaction. The user has full control and can choose to provide the key to others to prove payment for auditing purposes.

Zcash is an improvement to Bitcoin and developed on Bitcoin's infrastructure. It uses Zero-Knowledge Proof technology called zk-SNARKs to encrypt user information. Zk-SNARKs is an encryption method based on pure mathematical theory. The encryption method is self-contained, it has the advantage of not depending on external operating environment; therefore, has a wider range of application scenarios.

Since Zcash uses the same underlying architecture as Bitcoin's network, it can only support simple transactions, similar to the Bitcoin network with a pre-set privacy protection mechanism. Using Zero knowledge for the encryption of transactions is inefficient, and the application scenario is restricted further.

Monero (XMR)

Monero was founded in April 2014. Unlike Zcash, Monero did not choose to develop a blockchain system based on Bitcoin. The design is modular from the bottom and has good scalability.

Monero features the "proof of work" (POW) consensus mechanism. Unlike many previous cryptocurrencies, the Monero's algorithm CryptoNight is an AES intensive and memory-consuming operation; which significantly reduces GPU's advantage over CPU - reduces the risk of centralization of POW.

Monero uses Ring Confidential Transactions algorithm for its encryption method. The method mixes the signer's public key with another public key set and then signs the message, makes it impossible for intruders to distinguish which public key corresponds to the actual signer; therefore, protecting the user's real identity. Monero's mixed-currency participating users do not need to communicate with other participating nodes, they can participate in mixed-currency by themselves, providing effective protection measures for common distributed denial-of-service (DDOS) attacks and information disclosure in the decentralized mixed-currency mechanism.

Monero does not support smart contracts, and the high risk of being attacked is still present even though it adopts decentralized mixed currency technology. Users need to rely on the public key of other users when using Ring Confidential Transactions technology. If other users are malicious, the problem of users' privacy disclosure will arise.

Dash (DAS)

Dash is the first cryptocurrency designed to protect privacy. Dash utilizes centralized currency mixing scheme – simply transfer a sum of money to multiple addresses several times; simple to implement and easy to operate; no other technical support is needed during its currency mixing process. The centralized currency mixing scheme has high applicability in various cryptocurrency systems; however, the existing solution requires sender and receiver to mix coins online. If the sender and receiver can't reach an agreement on the amount of mixed currency, the transaction must be postponed. There is a common delay problem and the currency mixer is centrally deployed. The nodes of currency mixer can obtain all the information of the transaction and able to pilfer cryptocurrency. The most improved schemes prevent theft and information disclosure by increasing the cost of third-party violation; fundamentally, cannot eliminate the occurrence of violations. The mixed currency scheme using cryptography techniques such as blind signature increases the calculation cost. The execution of the mixed currency process by a third-party will inevitably bring additional service costs.

Dash does not support smart contracts, and the third-party mixed-currency provider mechanism relies on the credibility of the third-party and encounters unpredictable risks. In recent years, Dash has focused on the development and layout of ecological applications based on its good circulation and has strengthened cooperation with enterprises, attempting to make Dash a payment tool with strong circulation value instead of the emphasis on privacy protection.

Conclusion

From the aspect of the latest technology, solution to ensuring privacy protection by the adaptation of the latest cryptographic algorithms - the non-interactive zero-knowledge proof mechanism (NIZK), shows the most promising improvement. The use of encryption mechanism requires significant changes to the underlying protocol and consumes more computing resources, affecting the efficiency of blockchain applications. Therefore, the usage of privacy protection mechanism needs to consider the efficiency and cost of nodes in efficiency performance, and cost of computing and storage.

In the decentralized application scheme, smart contracts widely increase the application scenario of blockchain. The applications are no longer limited to the digital assets value of circulation. The current mainstream blockchain privacy protection technology does not support smart contracts, which prevents the greater establishment of practical usages. Any secure privacy protection mechanism for anonymity to support smart contracts must make major modifications to the underlying system of blockchain, the implementation will be difficult.

SERO is the solution to solve the above problems.

2.4 OVERVIEW OF SERO SOLUTIONS

SERO (Super Zero) is the world's first blockchain system that truly realizes the complete privacy protection of blockchains through non-interactive zero-knowledge proof. Compared to the existing blockchain privacy protection technologies, SERO not only can realize the privacy protection of

account and transaction information but also support Turing complete smart contracts. In addition, developers can also create their own encrypted cryptocurrencies supporting smart contracts based on SERO-Chain.

SERO re-designed the blockchain structure and various underlying protocols, making Turing complete smart contract for privacy protection come true. Making privacy protection measures available for a wider range of application scenarios, and making the attacks on user’s private data more challenging with the advanced NIZK encryption algorithm. In addition, the upcoming SERO V1.0 release, NIZK encryption algorithm is thoroughly optimized, which greatly reduces the memory resources required and improves the computational efficiency. Compared with the mainstream privacy cryptocurrencies, SERO's supports of Turing complete smart contracts, privacy protection measures and its related decentralized applications have significantly broadened its use-case scenarios.

More importantly, the SERO team considers the privacy protection measures required by the decentralized applications. The team also plans to provide solutions for the security of point-to-point network transmission and the privacy of the physical network address of the account, enables the centralized application to obtain powerful privacy protection functions when interacting with the centralized application or when interacting with the user's client.

The entire integrated solution will consist of a complete set of 3 in 1 suite, where SERO is the first publicly released project and the other two projects positioned as following:

ALIEN Protocol: A distributed DNS system that can use existing P2P network interaction information, has the functions of IP automatic switching and dynamic addressing, resists attacker blocking, and enables the entire data transmission network to achieve the ideal stable security.

CASTROL Protocol: The anonymous protection of IP addresses can be realized through decentralized network, which can be used to protect the privacy of physical nodes in both centralized and decentralized networks.

CHAPTER III
THE DESIGN OF SERO

3.1 DESIGN PRINCIPLES

The privacy protection technologies of decentralized network in the existing market do not combine with decentralized applications; particularly, the implementation of smart contracts is not protected. The sequence of actions performed in the smart contract is publicly visible throughout the network and / or recorded on the blockchain platform. In Turing complete blockchain network, SERO's design must meet several basic principles as well as meet the system's capacity requirements:

Un-traceable - every transaction in the blockchain network has an input and an output; constructing an acyclic graph of transactions, on which all of the transaction flows can be tracked, all of the transaction sequences can be concatenated and traced. SERO is designed to break the link between the two transactions, making the attack impossible.

Un-associable - each user in the blockchain network has their own collection address. Once the address is associated with the real user identity, all the transactions occurring at the address in the network can be associated with the corresponding user identity, resulting in the exposure of the associated behaviors to the address. All the transactions and balances are still publicly visible when a user creates a new pseudonym public key for anonymity. SERO uses encryption technology to make the payment address unrelated.

Anti-statistical analysis - actual user behavior has statistical characteristics. If the transaction data in the blockchain network has a correlation that reflect such statistical characteristics, it is possible to deduce the addresses belongs to a specific user through statistical analysis of the blockchain data. When ring signatures are used, the ability to resist statistical analysis will decrease if ring members or nodes are malicious. SERO must be able to completely hide the address and the relationship between addresses by technological means.

Practicality principles - SERO, while hiding the transaction data, will not take all the information into its scope, which can be uneconomical and inefficient. SERO will consider the user's existing usage habits and concerns to carry out research and development periodically.

Optional auditing solution - for the alternative audit scheme and certain complex business applications, the user may choose a trusted third-party to conduct financial audit of transactions. The user should have the ability to give the third-party to track the specific information from the transactions.

3.2 IMPLEMENTATION PLAN

In the first phase, SERO will completely protect the inputs and outputs of the trading system and the trading details through non-interactive zero-knowledge proof (NIZK). The transaction details are invisible to everyone except the two parties involved. SERO will maintain the smart contracts running on the chain and integrate the assets generated by the smart contracts with SERO's own trading system, considering that the online running smart contracts and the total number of open contracts issued assets have universal applicability. This will enable the privacy of the assets generated by the smart contract.

In the second phase, within the smart contracts running online, SERO will provide a latent structure called Hidden Data Structure(HDS) to satisfy the requirement for the total number of issued assets with protected contracts. The calculations for the HDS complete off the chain. The function will protect the total number of contractually issued assets.

In the third phase, SERO will adopt a more advanced consensus mechanism to improve the throughput of SERO networks. At the same time, SERO will decompose the operation of the contract into two steps: offline calculation and online verification. The offline calculation will fully understand the calculation rules and data, and will return the encrypted result. When the result is submitted online, the online node will only validate the result and determine whether the data conforms to the calculation rules; the node will not know the details of the data and calculation rules.

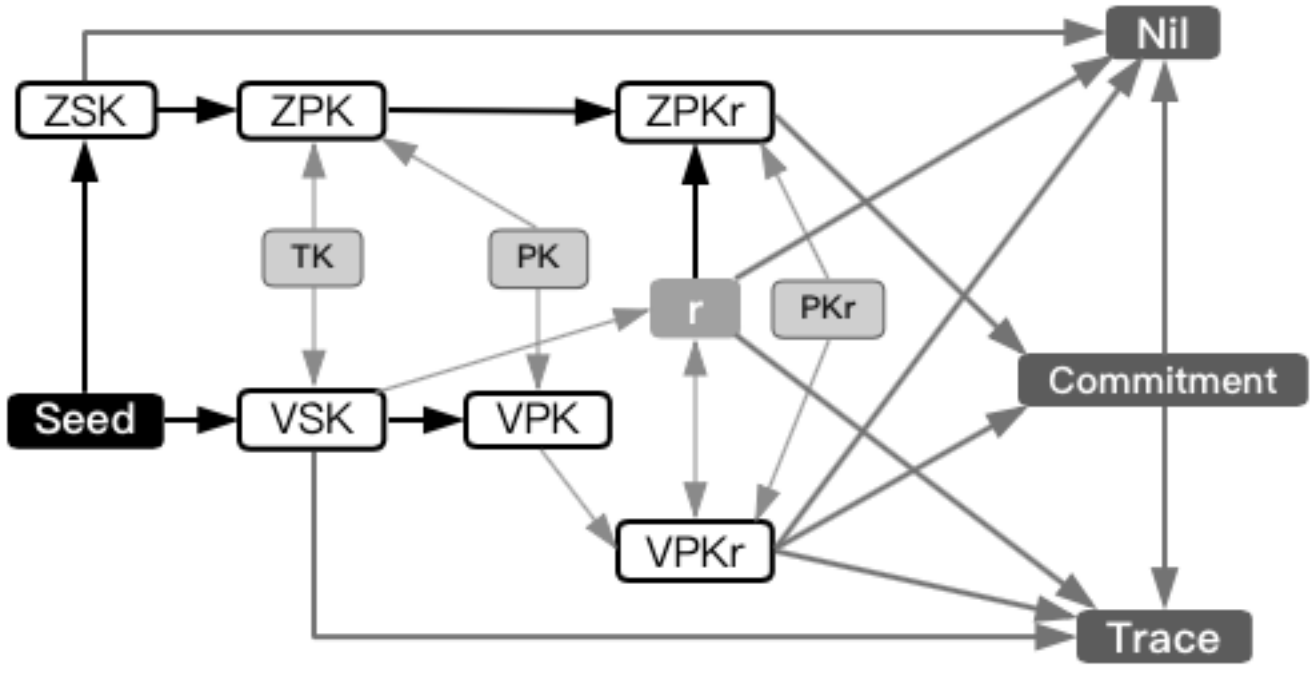
3.3 SERO PROTOCOL

Account System

Accounts are divided into two categories: user account and contract account. The user account is a 32-byte *Seed* selected by the user, the contract account generates a 64-byte address corresponding to the smart contract environment the user installed; both categories are unique and non-repeatable.

The user account can generate a 64-byte private key SK and a 64-byte public key PK, as the user's payment address. When installing or invoking the smart contract, the wallet will generate a temporary address PK_r according to the current condition. The temporary address cannot be associated with the user's private key or public key and will only be used once.

When the smart contract is installed, the wallet will change the temporary address to a 64 byte smart contract address (*CADDR*) in accordance with the current condition. As the node receives the address, it needs to ensure that the contract address has not appeared before.



$$Seed = New(Byte32)$$

$$r = Random(Byte32)$$

$$ZSK = BLAKE2B(Seed, ZSKADD)$$

$$VSK = BLAKE2B(Seed, VSKADD)$$

$$ZPK = HASH_{zpk}(ZSK)$$

$$VPK = PUBKEY(VSK)$$

$$ZPK_r = HASH_r(ZPK, r)$$

$$VPK_r = ENC_r(r, VPK)$$

$$r = DEC_r(VPKr, VSK, VPK)$$

$$TK = (VSK, ZPK)$$

$$PK = (VPK, ZPK)$$

$$PK_r = (VPK_r, ZPK_r)$$

Seed is an account seed and users must keep it securely. *SK* is a private key and cannot be stored persistently. *TK* is a tracking private key and can be provided to a trusted third-party for account

auditing. *PK* is the public key and provides the transaction destination address to other users. PK_r is a temporary address, provided to the smart contract, and temporarily used to receive the asset.

Assets System

User account or smart contract account has the attribute of managing an unlimited variety of assets with the exception of the settlement of transaction fees using SERO coins, each asset has the same transaction characteristics as SERO coins. Excluding SERO coins, the remaining assets can be generated by a smart contract. Each asset can be given a name of up to 32-byte length (token name) for mnemonic purposes and these names are also not allowed to be reused. The asset type can be specified when the account performs balance queries or transfer operations.

Witness System

SERO protocol uses non-interactive zero-knowledge proofs (NIZK) and needs to provide witness information of assets source when generating transactions. Each node will verify according to the witness information. SERO uses the Merkle Tree to maintain a witness system that records status changes. The system will provide verification function at the nodes and authentication information at the wallet side.

$$ROOT = MERKLE\_ROOT\_AUTH(POSITION, LEAF, PATH)$$

ROOT is the root of the current Merkle Tree. LEAF is the leaf at this position. PATH is the proof path from LEAF to ROOT.

Proof System

SERO's proof system includes a calculation circuit based on the directed acyclic graph to describe the internal constraints of each SERO transaction: input and output balance of various asset types, verification of public and private key, the validity of commitments, the validity of witness, etc. The circuit loaded with data can generate a *PROOF* through non-interactive zero-knowledge proofs (NIZK). From the submission of the *PROOF*, nodes can verify various parameters and constraints loaded in the circuit while hiding a large amount of detailed information.

$$S0_p = HASH_{s0}(SK, hash_e, i_p)$$

$$S1_p = HASH_{s1}(SK, S0_p, r_p, zi_{0,p}, zi_{1,p})$$

$$S0_e = HASH_{s0}(SK, hash_e, i_e)$$

$$S1_e = HASH_{s1}(SK, S0_e, r_e, zi_{0,e}, zi_{1,e})$$

$$R = RANDOM(32Bytes)$$

$$COMMITMENT_{out} = HASH_{com}(C, S1_e, VPK_{r,out}, ZPK_{r,out}, OUT)$$

$$E = ENC(C, OUT, R, VPK)$$

$$COMMITMENT_{in} = HASH_{com}(C, S1_{in}, VPK_r, ZPK_r, IN)$$

$$NIL = HASH_{nil}(ZSK, COMMITMENT_{in}, R, VPK_r)$$

$$TRACE = HASH_{nil}(VSK, COMMITMENT_{in}, R, VPK_r)$$

$$BALANCE\_CHECK = CHECK_{balance}(C, C0, C1, ZI_{p,0}, ZI_{p,1}, ZO_{e,0}, ZO_{e,1}, Value_{out}, Value_{in})$$

$$MERKLE\_CHECK = CHECK_{auth}(ROOT, COMMITMENT_{in}, PATH_{in}, Value_{in})$$

$$PRIMARY = (hash_e, ROOT, DEL, COMMITMENT_{out}, O_{e,0}, O_{e,1}, I_e, S1_e, I_p, S1_p)$$

$E, PRIMARY$ is the public data in the transaction. $hash_e$ is an external hash value used to confirm other inputs and codes attached to the transaction are correct. $ROOT$ is the root of the Merkle Tree where the input data is located. NIL is the hash of 32 Byte for destroy the used OUT, TRACE is the hash of 32Byte for transaction trace and is only valid for an OUT within the system. $COMMITMENT_{out}$ is the output commitment of the transaction. $O_{e,0}, O_{e,1}$ are public award fees such as transaction fees. I_e, I_p are the index indicating the number of descriptions inside the transaction. $S1_e, S1_p$ are the associated hash of the internal description of the transaction.

Process Step

1. Compute - the user uses the information provided by the account, assets and witness system, and provides input data according to the current required calculations. The calculation rules run under off-chain environment to obtain the results. The results will generate cipher-text (E) and a proof (P1, P2) of state change through the systems.

$$OUTPUT = COMPUTE(METHOD, INPUT, ACCOUNT, ASSETS, WITNESS)$$

$$(E, (P1, P2)) = PROVE(OUTPUT)$$

2. Commit - the user generates cipher-text (E) and proof (P1, P2), along with the randomly generated registration addresses (ZRPK, VRPK), encapsulated into a transaction (Stx), and submits it to the node.

$$FROM = (R_f, R_f PK)$$

$$STX = (E, P1, P2, FROM)$$

$$Commit(STX)$$

3. Verify - After receiving the transaction (Stx), the node confirms P1 in the witness system and sends P2 to the proof system. When certificates are verified as correct, the node will run the smart contract to receive the output, and the output will be associated with the temporary address.

$$witness\_ret = CHECK\_WITNESS(P1)$$

$$proof\_ret = CHECK\_PROOF(P2)$$

$$verify\_result = witness\_ret \,\&\, proof\_ret$$

4. Confirm - As the asset receiver synchronizes to the verified transaction (Stx), the receiver uses the private key to decipher the cipher-text (E) and generate plaintext (D). The plaintext (D) and proof (P1) are input to the proof system for verification; success indicates the transaction is validated. When the transaction is confirmed by n blocks, the transaction recipient considers the transaction has been confirmed.

$$D = DEC(E, VSK)$$

$$commitment\_ret = CHECK\_COMMITMENT(D, P1, PK)$$

$$confirm\_ret = commitment\_ret \,\&\, block\_confirm > n$$

The execution steps of SERO are open, the abstract description of the steps and parameters support the modification from phases one to three described in the " Implementation Plan" with minimal changes to the code structure during subsequent upgrades.

General Privacy Transaction

Within SERO, data in ordinary transactions are encrypted; non-trading parties will not know the details of source, destination, asset type, amount, etc. The system does not distinguish between assets generated by smart contracts and SERO's own assets in terms of consensus and transaction processing.

Online Smart Contract

SERO's General smart contract can be used for public calculations, to develop statistical plans, disposal rules and publicity rules for various assets; the input and output information must be isolated from users' real identities using temporary addresses.

SERO smart contracts are compatible with Ethereum smart contract instructions; most of Ethereum smart contracts can be run on SERO without modification.

Online Anonymous Assets

Smart contracts issue assets by calling the online anonymous asset issuance methods. The number of issued assets is visible to all users and has transaction attributes equivalent to SERO's own assets, which can be handled through private transactions.

Offline Anonymous Assets

Smart contracts issue assets by calling offline anonymous asset issuance methods. The number of issued assets is not visible to users. The assets have transaction attributes equivalent to SERO's own assets and can be processed through private transactions. Smart contracts are not visible to third-parties on the input and output of the asset. Anonymous assets have many types of usage scenarios.

Offline Smart Contract

The smart contract runs offline, the calculation rules are only visible to some users, and the number of issued assets is not visible to users. The assets have transaction attributes equivalent to SERO's own assets and can be processed through private transactions. Smart contracts are not visible to third parties on the input and output of the asset.

3.4 ORIENTED SCENARIOS

Everyone has a strong desire for privacy protection, therefore, SERO has a tremendous market prospect. SERO supports developers issuing their own anonymous digital tokens, which means SERO can be compatible with the circulation of multitude of economic ecologies. SERO's support for smart contracts widely expands the universe of privacy-focused blockchains, pushing it past anonymous cryptocurrencies, creating a complete blockchain ecosystem where everyone’s privacy can be protected without sacrificing either scalability or complexity; thus, greatly expanding the real-world use-case scenario for decentralized blockchains.

Medical and Health Industry

Digital privacy is in all aspects of the medical and health industry. From personal medical records to medical treatment records, the multi-role privacy protection and the authorization mechanisms require highly flexible and secure privacy protection capabilities, including hospitals, patients, insurance companies, pharmaceutical companies, etc. The protection of data privacy and the restriction of authorization are particularly important.

Online Auction

Online auction businesses pursue fairness, the privacy of bids is an important aspect and often difficult to obtain because of conflicting interests. In high-frequency bid auction bidders have limited or no knowledge of other competitors' bids, the privacy of bidding data represents the large return on profit. SERO can provide a completely safe, independent and fair bidding environment.

Online Forecasting Related Industry

The development of forecasting industry has always been restricted by centralized trust. Online forecasting often requires a high degree of privacy protection for competitors' strategy. The industry has large cash flow, which represents a greater need for a fair token circulation system that offers multi-person bids, payments and settlements, along with a uniform exchange rate. SERO can fully support the above criteria.

Games

Every game has its own economic ecology, the digital assets in the game are self - contained. The difficulty to manage different digital assets from different games issued by the same company arises. There is a demand to provide simplified system to manage the assets when expanding the game ecology.

Large online games often need a token system that is easy to circulate, trade and settle accounts that can issue and circulate based on smart contracts, while providing privacy protection of transactions. SERO is the only technical solution that supports a multi-token system that issues and circulates homomorphic smart contracts, with added transaction privacy for the accounts.

There are more industries that handle digital assets and sensitive digital assets: insurance industry, digital precious metal trading firms, futures trading, digital asset trading (credit reporting and intellectual property rights), credit industry, etc. SERO has significant advantages in the existing market, by supporting the demand of technology for high token liquidity, and also the establishment of an independent and well-rounded cryptocurrency ecology.

3.5 ABOUT NON-INTERACTIVE ZERO-KNOWLEDGE PROOF (NIZK) PERFORMANCE OPTIMIZATION

For the blockchain system adopting the NIZK scheme, the biggest bottleneck is the length of time to generate proof during the generation of transactions. Fortunately, the transactions are usually generated in wallets.

1. Currently, SERO uses the native zk-SNARK library to achieve NIZK, and adopt the ALT _ BN128 curve and GROTH 16 preprocessing process, which is about one-third less processing time than Zcash’s PGHR13 preprocessing scheme. At the same time, the depth of Merkle Tree can be appropriately reduced and parallel processing scheme can be added as much as possible to greatly reduce the average transaction generation time. Although zk-SNARK needs a credit installation

process, SERO's implementation will not dynamically construct the computational circuit. Therefore, zk-SNARK protocol meets SERO's requirements in all scenarios.

2. SERO's team studied Zcash's latest R&D achievement jubjub and utilized the BLS12-381 curve and Twisted Edwards curve to generate the public key and Pedersen hash to generate Merkle Tree; which increases the transaction generation speed at least by four times.

3. Bullet Proofs also has interesting features and performance advantages (performance advantages of batch verification), and naturally supports elliptic curve (EC) public keys and Pedersen commitments, is also one of our approaches.

4. zk-STARK's "Zero Knowledge Proof Mechanism" provides a simpler cryptographic hypothesis that avoids the needs for elliptic curve, pairing and knowledge of exponent assumptions, and relies only on hashing and information theory. The privacy feature is not susceptible to quantum computing attacks.

SERO uses a large number of zero knowledge proofs strategies to protect information. Although the team are still using zk-SNARK C++ implementation library libsnark in TestNet.But when the hero MainNet goes online, the SERO team will review the several NIZK protocols mentioned above and build the most efficient and secure library.

3.6 TEMPORARY ADDRESS

The on-chain calculation portion of SERO, the team uses temporary address to temporarily accept the output target of the online calculation. The non-traceability will be slightly weakened, if the output is used by this signature. SERO's solution is that when the user uses the output, the output's signature will be hidden in the proofs as other normal transactions. As a result, transactions are disconnected and cannot be traced back and once the output is used, even the temporary address is destroyed.

3.7 FUTURE PLANS

Off-Chain Computing and Homomorphic Encryption Smart Contracts

The homomorphic encryption of smart contracts has already entered development stage and is planned to be released on SERO platform of version 2.0 in March 2019. The team discovered a method to balance data security (a mechanism that completely isolate sensitive data for the computations) and performance through both on-chain and off-chain computing. The plan aims to finish the work within 6 months.

Wallets and Other Ecological Applications

SERO's decentralized wallet application is currently under development and is scheduled to be released in March 2019. SERO supports developers to issue tokens themselves, the wallet will support SERO's own tokens and the management of cryptocurrency assets corresponding to all developers-based tokens issued by SERO.

Latest Consensus Mechanism

Within one year, the team will release a new consensus mechanism SE-Random in an updated version of SERO. The design will combine the latest PBFT theory and VRF algorithm in the consensus mechanism capable of balance fairness and efficiency.

Privacy Three Swordsmen

SERO has two related protocols, the Alien Protocol and the Castro Protocol. The former provides a distributed DNS system to obtain the stable operation of the network and information transmission by means of automatic addressing. The latter implements encrypted privacy protection for the IP address of the node, forming a complete decentralized application privacy protection scheme in the 3 in 1 suite.

Secure Multiparty Computing

In many cases, data certification must combine with existing centralized data sources and can also become offline data sources. The current strategy to solve the above problems is to assume a trusted service provider or a trusted third-party exists. The risk is high in the changeable and malicious environment. A universal secure multi-party computation solution can resolve the problem.

SERO plans to introduce Secure Multi-party Computing (SMC) in the future, in order to provide extensive support of off-chain data under the premise of privacy protection.

Multi-chain system

The multi-chain system is the SERO’s scalability solution. SERO will use a mechanism similar to the Ethereum’s Plasma for performance expansion based on multi-chain system, SERO’s status updates per second can reach extremely high levels (possibly billions). This solution allows SERO to have the capability to replace today’s centralized clusters with better performance, giving SERO the prospect of handling privacy-related decentralized applications around the world.

CHAPTER IV
CHAIN FRAMEWORK

In addition to the privacy protection mechanism, the chain infrastructure also needs to have sufficient scalability, an important aspect for building a practical application platform. SERO introduces the following technologies to enhance the chain's underlying architecture:

- Consensus Optimization - SERO uses a brand-new consensus mechanism SE - Random, that combines the latest PBFT theory and VRF algorithm to form a consensus mechanism balancing fairness and efficiency.

- Plasma - a method to obtain the expanded computing of blockchain. In Plasma, many blockchains are combined into a tree structure to participate in the computing, thus obtaining the horizontal expansion of the blockchain.

- Powerful Virtual Machines – the virtual machines not only meet EVM compatibility, but are also sufficiently scalable, and have the underlying instructions to meet performance requirements.

- The following focuses on some of the specific implementation of technologies.

4.1 CONSENSUS MECHANISM

SERO proposes proprietary developed main chain consensus engine SE-Random based on the study of various consensus. The design of SE-Random Consensus Engine is influenced by the latest consensus research of Algorand and Ourboros. The verifications at the nodes have little computational overhead, and the probability of forks of the whole blockchain network is extremely limited. The engine can achieve almost unlimited scalability.

Detailed description of SE-Random consensus:

SE-Random uses Byzantine Agreement (BA*) to reach the consensus in a set of transactions. For scalability, SE-Random uses a random algorithm to select a group of users, and allows users to check privately whether they are selected or not to participate to form the consensus in the BA* protocol. With the algorithm, as the number of users increases, the BA* consensus system will not slow down.

The Use of VRF Algorithm

SE-Random consensus engine is based on the Veritable Random Function (VRF) algorithm for random verification node selection. VRF is a randomly generated function. The function is verifiable: the same private key signs the same information and only one legal signature can be verified. The function is different from the common asymmetric encryption algorithm.

The specific operation flow of VRF:

1. The prover generates a pair of keys, PUB_KEY and PRI_KEY. PRI_KEY is the private key and PUB_KEY is the paired public key.

2. The prover outputs random result: $result = VRF\_Hash(PRI\_KEY, info)$

3. The prover outputs random proof: $proof = VRF\_Proof(PRI\_KEY, info)$

4. The prover submits the random result and the random proof to the verifier. The verifier verifies whether the result and proof match, if matches, then proceeds to the next step

5. The prover submits PUB_KEY and $info$ to the verifier, and the verifier calculates whether the $VRF\_Verify(PUB\_KEY, info, proof)$ result is $TRUE$ or not. If $TRUE$, the verifier will pass the verification.

6. After verification, it can conclude whether $info$ and $result$ match; the data given by the verifier is correct. The verifier does not have the prover's private key PRI_KEY during the process.

Random Seed Generation

Seed will be used in random algorithm of some areas in SE-Random: the need of randomly selected and publicly disclosed seed in the encryption lottery of SE-Random. The seed must be known to the participating nodes but cannot be controlled by opponents. The seed generated by SE–Random in round r is determined by the seed of the previous round r-1 by VRF. The seed and the corresponding VRF certificate are included in each proposed block. Once SE-Random agrees on the block of r-1, everyone will know the pseudo-random seeder of the current round after the r round starts. The initial seed0 value is calculated together by the initial participants using multiple nodes, resulting in an absolute unpredictable random seed. The resulting seed cannot be predicted or manipulated by attackers.

Method for Selecting Verifier by Encryption of Lottery through VRF Algorithm

Se-Random uses an encrypted lottery method to select a random subset of users based on the weight of each user. The system sets a fixed number of SERO tokens as a screened candidate unit S, and specifies each node has a limited number of SERO coins W as the screening computation. The total weight of all candidate units is $W = \sum_i \frac{w_i}{s}$. If node i has a SERO token of j screening units, node

i can participate in the lottery screening as *j* different child nodes. The randomness of the cryptographic sortition algorithm comes from the random seed discussed in the previous section. SE-Random builds a VRF based on the current seed in each cycle of BA*. The private key of VRF is only known by the node itself; each node uses its own private key to run a random algorithm published by the system. The system selects the verification node based on the node holds no more than the defined proportion threshold of SERO coins.

SE-Random specifies a threshold to select the expected number of verification nodes. The expected number satisfies the probability $p = w/W$. The probability of a child verification node selection in W (total node weight) satisfies the binomial distribution:

$$B(k;W,p) = \binom{W}{K} p^k (1-p)^{w-k}, where \sum_{k=0}^{W} B(k;W;p) = 1$$

To determine the number of current verification nodes (including child verification nodes) is also determined by the cryptographic sortition algorithm. The cryptographic sortition algorithm divides the interval [0,1] into continuous intervals:

$$\mathbf{I}^j = \left[\sum_{k=0}^{j} B(k;w,p), \sum_{k=0}^{j+1} B(k;w,p) \right) for\ j \in \{0,1,...,w\}$$

If the bit length of the hash is hashlen and if $hash / 2^{hashlen}$ is between $\mathbf{I}^j$, then the node has j selected verification child nodes. The number of verification nodes selected can use π for VRF public authentication.

The characteristics of the cryptographic sortition:

1. The verification nodes randomly select N verification sub-nodes according to the weight of SERO tokens they hold.

2. Attacker that does not know the private key of node i cannot know whether i is selected, and how many sub-verification nodes are selected.

BA* consensus calculation performs in randomly selected verifier nodes

Verification nodes (including sub-verification nodes) know that they are selected in secret and can only prove their verifier qualifications by publishing credentials. For each selected node, use signed seed with its own private key and enter a hash function to obtain its own credentials. The property of the hash function dictates the certificate is a 256 length of random string, the certificates of different nodes are not the same, and the distribution of the certificate strings is uniform. Using the same method, additional candidate leader nodes are selected. The candidate leader nodes are arranged according to the certificate's lexicographic order. The smallest index order candidate is selected as the

leader node, that is, the leader node is generated through a random public selection of the candidate leader node set.

The verification node and the leader node participate in the operation of BA* protocol. In each stage and step of BA*, the node independently determines whether it is selected in the current step through private and non-interactive means. BA* has a two-stage voting mechanism. In the first stage, the verification node performs reduction consensus on the selected candidate blocks and selects the candidate block with the most consensus verification. In the second stage, binary Byzantine agreement is carried out on the candidate blocks screened in the first stage. BA* consensus needs to ensure that more than two-thirds of the honest nodes participate in consensus. If the condition is not met, multiple random selections are required, when more than two-thirds of impartial nodes participate in consensus at once, consensus is reached. The verification nodes of each step of BA* consensus is specified by cryptographic sortition in parallel to speed up the accelerate the consensus confirmation.

BA* Consensus Protocol

Every step of BA*, the temporary key of the current step is destroyed:

1. Generate Block (Step1)

1) The node checks whether it is a leader node B_i^r .

2) Generates the message of the first step $m_i^{r,1} = \left(B_i^r, ESG_i\left(H\left(B_i^r\right)\right), \sigma_i^{r,1}\right)$

3) Broadcasts B_i^r and $m^{r,1}$

$m_i^{r,s}$ is the message that node i broadcasting at the (r, s) step; B_i^r is the block generated by the node i in r round; ESG_i refers to signing information with current temporary key at (r,s); H is a hash calculation function; $\sigma_i^{r,s}$ refer to the signature $SIG_i(r,s,Q^{r-1})$ of I, which is used to prove the existence of I in the verification node set.

2. Reduction Consensus

This protocol transforms the problem of agreement on any block into an agreement on two values. The two values are the basis for the finalizing the hash of a specific block or the hash of an empty block divided into three steps. The three-step process will be described in detail in the technical yellow paper. If more than two-thirds of the messages $\left(ESG_j\left(V'\right), \sigma_j^{r,2}\right)$ match, the specific block can be broadcasted, and if not, empty block is broadcasted. The message is then used for subsequent binary Byzantine Agreement.

3. Binary Byzantine Agreement

The verification node verifies the values issued by the reduction consensus protocol. The binary Byzantine Agreement is a three-step cycle; the verification node will continuously check the historical values received to see if there are two kinds ending conditions: whether the total number of votes reaches 2/3, the number is the number of votes that the block is legal or the block is illegal. If the block is illegal, the consensus system will determine and generate an empty block. To prevent the occurrence of infinite loops, a maximum total number of loops *m* is set. If an end condition is not met after reaching *m*, the consensus system will temporarily generate a tentative consensus and form a final consensus in the subsequent process (the next few rounds) and confirms the earlier transactions.

SE-Random consensus will adapt to consensus decision in the case of weak synchronization network. Strong network synchronization will not cause block fork. If weak network synchronization occurs, a tentative consensus will be specified temporarily and the final consensus will be reached after the strong network synchronization is restored. SE-Random can prevent Sybil attacks, selfish mining attacks, Nothing-at-Stake attacks, long-range attacks, and other attacks. If the users of SERO chain spread to more than 100 million nodes, the SE-Random consensus can quickly reach a network-wide Byzantine Agreement consensus through VRF mechanism.

4.2 EXPANSION MECHANISM

Plasma is a framework for motivating and enforcing smart contracts execution. The framework can scaleto a large number of state updates per second (up to 1 billion updates per second) and supports a large number of decentralized financial applications worldwide on the blockchain. The smart contracts use network transaction fees to stimulate continuous automation and ultimately rely on the underlying blockchain to force the finalizing of the transaction status.

Plasma consists of two core parts: reorganizing all blockchains into a set of MapReduce functions, and an optional method to implement a POS token deposit mechanism based on Nakamoto consensus principle that does not encourage block withholding on existing blockchains.

The mechanism enforces state locking on the main chain by writing smart contracts on the main chain and using fraud proofs. Plasma groups the blockchains into a hierarchical tree structure, treats each blockchain as an independent branch and force the history of the entire blockchain and MapReduce calculations to be submitted to Merkle Proof. Through the main chain to force encapsulation of the account book information of a chain into a sub-blockchain. The chain will expand from the lowest trust to achieve an incredible expansion capacity.

Withholding attack on blockchain is a complicated problem surrounding the global availability of data that enforces non-global data. Plasma alleviates the problem by withdrawing the problematic chain and also creates a mechanism for encouraging and enforcing the accuracy of the execution data continuously.

By broadcasting the normal status of Merkle’s proofs to the main chain (e.g. Ethereum), this will achieve large scalability, reduces transaction costs and computational effort. Plasma supports the continuous operation of large-scale decentralized applications. The important scalability is realized by reducing the single expense financial expression to one bit in a bitmap. A transaction and a signature

represent a transaction aggregation with multiple parties. Plasma combines this feature with a MapReduce framework and use smart contracts with deposits to build a scalable computing compulsions.

The structure of the mechanism allows external participants to hold funds and calculate contracts according to their own action, similar to a miner, but Plasma runs on an existing blockchain so that users do not need to create corresponding transactions on the main chain every time the state is updated (including the addition of a new user's account ledger), only a small amount of information is written to the main chain such as the merged state change.

SERO will use a mechanism like Plasma for horizontal performance scalability base on multi-chain systems. The multi-chain parallel computation system allows SERO to have the ability to update its state at a very high level per second (possibly billions). As a result, SERO will greatly improve its performance to replace the carrying capacity of the current centralized cluster.

4.3 VIRTUAL MACHINES

At present, Ethereum has a large number of developers, and Solidity language has become the most widely used language for smart contract development. Therefore, EVM compatibility is provided in SERO systems.

EVM virtual machine was developed on the basis of Ethereum. Ethereum has a standard blockchain structure with a simplex data structure. The virtual machine is designed to resemble the ACID (Atomicity, Consistency, Isolation, Durability) feature of the database at the transaction invocation level. In Ethereum's protocol, the invocation of one smart contract may affect the status changes of multiple accounts. The state changes are rigid transactions with real-time consistency, the state changes either occur simultaneously or do not occur at all. SERO considers scalability in the future and has the underlying instructional basis to meet performance requirements. The virtual machine of SERO-Chain satisfies the concept of BASE (Basically Available, Soft State, Eventual Consistency), and the virtual machine is referred to MEVM virtual machine.

In the BASE concept, the Basic Availability means that the system is allowed to lose part of its availability in case of unexpected failure. Soft State means allowing the data in the system to have an intermediate state, but the existence of the intermediate state will not affect the overall availability of the system. Eventual Consistency refers to all copies of data will eventually be reaching consistency after synchronization. Compared to the strong consistency of ACID concept, BASE concept gains usability by sacrificing the real-time consistency and reaches a consistent state eventually. The principle of the block structure and various consensus algorithms in the blockchain are essentially the BASE concept, but they do not conform with ACID. MEVM are designed to combine with BASE semantics. Compared to the original ACID design of EVM, the design will overcome the performance bottleneck.

In addition, the Solidity language has been criticized for lack of support of standard libraries, such as the basic functions of comparing two strings. There are no standard library functions in Solidity for developers to invoke. Projects like OpenZeppelin provide some standard libraries, but they

are far from sufficient. SERO's blockchain applications require advanced mathematical and cryptographic algorithm libraries, such as Zero Knowledge Proof Protocol, RSA Public-key encryption algorithms, singular value decomposition, etc. MSolidity can refer to the implementations and add more libraries, which can be precompiled or implemented in native mode to reduce operational overhead.

In the future, SERO system may support virtual machines based on Web Assembly (WASM) to further improve performance and provide support for smart contracts written in languages other than Solidity (C, C + +, Rust, or GO). As the IELE virtual machine designed by the Cardano project team matures, Matter system will consider providing support for this virtual machine. IELE is a variant of LLVM and is expected to become a unified and low-level platform for smart contract translation and execution in high-level languages. With IELE virtual machine, SERO system can support more variety of advanced languages.

4.4 POST QUANTUM CRYPTOGRAPHY

Blockchain system commonly use asymmetric cryptographic signature algorithm, such as the RSA algorithm based on large integer factorization problem and the ECC algorithm based on the discrete logarithm computation problem on the elliptic curve, that can be easily cracked by quantum Shor algorithm which change NP problems to P problems. The SERO system will iteratively introduce encryption algorithms to safeguard against quantum computing, such as Lattice-based cryptography, code based crypto-systems, and multivariate cryptography, based on project progress and the development of quantum computer utility. The various crypto-systems such as encryption, signature, and key exchange can be designed based on the lattice password, which is an important direction of the post quantum cryptography algorithm. At the same time, the SERO team will continue to track the cutting-edge research directions of anti-quantum crypto-systems such as the Isogen problem, the conjugacy search problem, and the Braid Groups.

CHAPTER V
ECONOMIC MODEL

The traditional point-to-point communication network focuses on information transmission, a bit like the application of Internet 1.0. Things are open and shared, unlike the disruptive blockchain technology. Because all human behaviors are driven by the economic logic, human behavior in the absence of effective economic norms can only be bound by social norms (i.e. work driven by spiritual incentives of public interest), which lacks the binding needed for individuals to complete the goals together.

Bitcoin network through the POW consensus mechanism and the contribution of using computing power to obtain the bookkeeping rights to obtain the bitcoin rewards to encourage the node to participate in the consensus is undoubtedly a remarkable design. The token economic model is the core of the value of a blockchain.

However, the question is whether one type of token can solve the incentive problem of every consensus cooperative behaviors? We think the answer is NO. There are various kinds of tokens circulating in the market, and the economic models behind them are varied, but there is the lack of a unified standard that link the cost of consensus with the consensus value generated. Therefore, the secondary market circulation rules of the cryptocurrency system appear quite fragile.

Based on the same underlying consensus mechanism, Ethereum allows smart contract developers to issue their own token and use ETH as a GAS fee to pay for the consensus cost, which unifies the unit of measurement of consensus costs, and allows users to obtain different value outputs according to the token's ecosystem. The users can at least calculate the best balance between investment and return. Many in the industry criticize the issuing of ERC20 tokens on Ethereum as too simplistic and that it can result in fraud, but few critics realize the importance of Ethereum's original design.

SERO team extended the features of Ethereum when designing the SERO-Chain. First, to reduce the GAS consumption in order to reduce the hard threshold of price-performance ratio for transactions on the chain. The team have designed a new consensus mechanism, which is described in another chapter.

Assuming that the consensus cost is negligible, the value of any token depends on other costs of transactions on the chain; which are affected by the centralization of digital assets and the relationship between market supply and demand, etc. The characterization is similar to real-world currencies.

Cryptocurrencies can also be used to measure the value of goods, services or rights, and interests of goods. Therefore, the developers should have their own economic model to issue tokens. The discussion of the economic model is from the aspect of SERO token.

From SERO's ecology, the value of all goods and services has a source. The blockchain platform is essentially a fair-valued circulation market circulation. The underlying cost of all economic activities is the transaction cost, and SERO token becomes the carrier of transaction cost. From this perspective, SERO token will be used for the following incentive purposes:

- Bookkeeping rewards;
- Computational contribution rewards (more computing power consumption will be required for applications which use privacy mechanisms);
- Other roles including operational rewards for algorithm providers (by issuing smart contracts)
- In SE-Random consensus, possession of SERO's token could impact some specific scenarios (such as random selection of initial seed nodes);
- Developers of SERO ecology will get token rewards from SERO based on the actual value of the development and application. The rewards could be given in the forms of subsidize the consensus bookkeeping cost or computational power contribution.
- Users can use SERO token for various purposes in their DAPP or SERO related ecosystems.

CHAPTER VI
ROAD MAP

6.1 DRAGONS OF AUTUMN TWILIGHT (V0.X)

2018.9 Release AlphaNet Network

* Open source to GitHub

* Support anonymous transactions

* Support smart contracts

* Support issuing anonymous tokens using smart contracts

2018.11 Release BetaNet-RC Network

* Release PC Wallet

* Support issuing anonymous tickets using smart contracts

* Support decentralized mining license

2018.12 Release BetaNet-Release Network

* Support issuing encrypted package

* Support sealed bid and private OTC transactions using smart contracts

* Support paying gas on behalf in smart contracts

6.2 DRAGONS OF WINTER NIGHT (V1.X)

2019.3 Global Node Deployment, Preparing for Main Network Environment

2019.4 Release MainNet Network

* Map SERO tokens on BetaNet-Release to MainNet
* Support light wallet
* Support off-chain computing function
* Release SE-Random consensus

6.3 DRAGONS OF SPRING DAWNING (V2.X)

2019.7 Release ALIEN Protocol and CASTROL Protocol

2019.10 Add Secure Multi-Party Computation (MPC) Mechanisms

CHAPTER VII

PROJECT ECOLOGY

7.1 CORE TEAM

Leyla Q.

Leyla graduated from Wellesley College, Massachusetts, USA and majored in Computer Science. She started her career as underlying protocol developer in the telecommunication industry. She then continued on to start-ups and social media companies, she loves computer technology and invented several black technology underlying protocols. Believing blockchain represents a fundamental change in the technological space, she delves into the blockchain field. Outside of work, she likes to travel, visiting new places and spends time relaxing with her dog. She is the co-founder of GLAB Blockchain Group.

Dr. Leo Xu

Leo graduated from the doctorate program of the California Institute of Technology (CalTech) Electrical Engineering Department. He is a Tenured Computer Science Professor at Michigan Wayne State University. His research interest focuses on network, distributed system, encryption, and data security.

Robert B.

Robert is a serial entrepreneur; he participated in the early search engine database development and has years of experience in the venture capital industry. The decentralized nature of blockchain disrupts the inequalities devised by centralized entities; Robert envisions blockchain technology to level the playing field for the end users and innovative start-ups. He aspires SERO to lead the next iteration of blockchain development. In his spare time, he enjoys playing basketball, music and traveling. He gives back to the start-up community by actively involved in the Silicon Valley SOSV

Accelerator Startup as a mentor.

Jason Pope

Pope brings over 20 years of experience to SERO team, including CTO of a prominent online mapping company, technical co-founder & CTO of an automotive e-commerce corporation and VP and CTO of online finance division in a listed company. He envisions blockchain as a great experiment for a new global economic system, there are opportunities to achieve shared goals through synergy. He is particularly interested in the consensus mechanism and encryption components of blockchain. When he is not in the office, he likes to keep fit and visit different countries and places. He is a senior contributor at GLAB Blockchain Group.

Durant D.

Durant has held influential positions in many top-level online companies such as the CTO of division in a well-known online travel listed company, technical director of a well-known media streaming listed company, CTO of an online B2B company with over 10 billion in sales. ‘Blockchain represents the future’, Durant anticipates. He has the passion to develop the next iteration of blockchain with greater security, chain to chain compatibility, smart contract supports, wider DAPP applications. Watching new movies, joining social gatherings, reading are his hobbies. He is a senior contributor at GLAB Blockchain Group.

Gordon T.

Gordon held instrumental positions as Chief Architect of an online B2B organization with over 10 billion in sales. He developed FLASHGET and 3721 and was the principal developer for P2P protocol in a well-known media streaming listed company and a senior technical expert in Yahoo Inc, and CTO of R&D division in a listed Fortune 500 company. Gordon recognizes the importance of blockchain in the future technological developments and innovations, especially the consensus attribute in the financial system is an important aspect of blockchain. He takes joy in family gathering and father and son play time. He is a senior contributor at GLAB Blockchain Group.

7.2 CONSULTANT TEAM

Suyang Zhang

IDG's first honorary partner, the first batch of venture capitalists in China.
Listed as Forbes " China's best venture capitalist" and " world's best venture capitalist" for several years.

7.3 ECOLOGICAL COOPERATION

SERO received support from technology geeks including Matt Global and GLAB in is early work and thanked them. In addition, there are some institutions involved in the early investment in SERO projects, and we will officially disclose and formally thank these supporters on our website.

CHAPTER VIII
REFERENCES

[1] MONACO J V. Identifying Bitcoin users by transaction behavior[C]//The SPIE DSS, April 20-25, 2015, Baltimore, USA. Baltimore: SPIE, 2015.

[2] ZHAO C. Graph-based forensic investigation of Bitcoin transactions[D]. Iowa: Iowa State University, 2014.

[3] LIAO K, ZHAO Z, DOUPE A, et al. Behind closed doors: measurement and analysis of CryptoLocker ransoms in Bitcoin[C] //The Symposium on Electronic Crime Research, June 1-3, 2016, Toronto, Canada. Piscataway: IEEE Press, 2016: 1-13.

[4] MEIKLEJOHN S, POMAROLE M, JORDAN G, et al. A fistful of bitcoins: characterizing payments among men with no names[C]// The 13th ACM Internet Measurement Conference, October 23-25, 2013, Barcelona, Spain. New York: ACM Press, 2013: 127-140.

[5] ROND, SHAMIR A. Quantitative analysis of the full Bitcoin transaction graph[C]//The 17th International Conference on Financial Cryptography and Data Security, April 1-5, 2013, Okinawa, Japan. Heidelberg: Springer, 2013: 6-24.

[6] GENNARO R, GENTRY C, PARNO B, et al. Quadratic span programs and succinct NIZKs without PCPs [C]//The 32nd Annual International Conference on the Theory & Applications of Cryptographic Techniques, May 26-30, 2013, Athens, Greece. [S.L.:S.N.], 2013: 626-645.

[7] PARNO B, HOWELL J, GENTRY C, et al. Pinocchio: nearly practical verifiable computation[C]//The 2013 IEEE Symposium on Security & Privacy, May 19-22, 2013, San Francisco, USA. Washington, DC: IEEE Computer Society, 2013: 103-112.

[8] REID F, HARRIGAN M. An analysis of anonymity in the Bitcoin system[C]//The 2011 IEEE Third International Conference on Privacy, Security, Risk and Trust, October 9-11, 2011, Boston, USA. Piscataway: IEEE Press, 2011: 1318-1326.

[9] ANDROULAKI E, KARAME GO, ROESCHLIN M, et al. Evaluating user privacy in Bitcoin[C]//The 17th International Conference on Financial Cryptography and Data Security, April 1-5, 2013, Okinawa, Japan. Heidelberg: Springer, 2013: 34-51.

[10] CHAUM D. Untraceable electronic mail, return addresses and digital pseudonyms[J]. Communications of the ACM, 2003: 211-219.

[12] VALENTA L, ROWAN B. Blindcoin: blinded, accountable mixes for Bitcoin[J]. Financial Cryptography and Data Security, 2015: 112-126

[13] SHENTU Q C, YU J P. A blind-mixing scheme for Bitcoin based on an elliptic curve cryptography blind digital signature algorithm[J]. Computer Science, 2015.

[14] RUFFING T, MORENO-SANCHEZ P, KATE A. CoinShuffle: practical decentralized coin mixing for Bitcoin[M]// Computer Security -ESORICS 2014, Heidelberg: Springer, 2014: 345-364.

[15] BISSIAS G, OZISIK A P, LEVINE B N, et al. Sybil-Resistant mixing for Bitcoin[C]// The 2015 ACM Workshop on Privacy in the Electronic Society, November 3, 2014, Scottsdale, USA. New York: ACM Press, 2014: 149-158.

[16] DWORK C, NAOR M. Pricing via processing or combatting junk mail[C]// The 12th Annual International Cryptology Conference on Advances in Cryptology, August 16-20, 1992, Santa Barbara, USA. Piscataway: IEEE Press, 1992: 139-147.

[17] CASTRO M, LISKOV B. Practical byzantine fault tolerance and proactive recovery[J]. ACM Transactions on Computer Systems, 2002, 20(4): 398-461.

[18] BONNEAU J, NARAYANAN A, MILLER A, et al. Mixcoin: anonymity for Bitcoin with accountable mixes [C]//The 19th International Conference on Financial Cryptography and Data Security, January 26-30, 2015, San Juan, Argentina. Barbados: Financial Cryptography, 2014: 486-504.

[19] SASSON E B, CHIESA A, GARMAN C, et al. Zerocash: decentralized anonymous payments from Bitcoin[C]//The 2014 IEEE Symposium on Security and Privacy, May 18-21, 2014, San Jose, USA. Washington, DC: IEEE Computer Society, 2014: 459-474.

[20] VALENTA L, ROWAN B. Blindcoin: blinded, accountable mixes for Bitcoin[J]. Financial Cryptography and Data Security, 2015: 112-126

[21] SHENTU Q C, YU J P. A blind-mixing scheme for Bitcoin based on an elliptic curve cryptography blind digital signature algorithm[J]. Computer Science, 2015.

[22] RUFFING T, MORENO-SANCHEZ P, KATE A. CoinShuffle: practical decentralized coin mixing for Bitcoin[M]// Computer Security -ESORICS 2014, Heidelberg: Springer, 2014: 345-364.

[23] BISSIAS G, OZISIK A P, LEVINE B N, et al. Sybil-Resistant mixing for Bitcoin[C]// The 2015 ACM Workshop on Privacy in the Electronic Society, November 3, 2014, Scottsdale, USA. New York: ACM Press, 2014: 149-158.

[24] BEN-SASSON E, CHIESA A, GREEN M, et al. Secure sampling of public parameters for succinct zero knowledge proofs[C]// 2015 IEEE Symposium on Security and Privacy (SP), May 18-21, 2015, San Jose, USA. Piscataway: IEEE Press, 2015: 287-304.

[25] PEREIRAGCCF,JRMAS,NAEHRIGM, et al. A family of implementation- friendly BN elliptic curves[J]. Journal of Systems and Software, 2011, 84(8): 1319-1326.

[26] ARANHA D F, FUENTES-CASTAÑEDA L, KNAPP E, et al. Implementing pairings at the 192-bit security level[C]//The 5th International Conference on Pairing- Based Cryptography, May 16-18, 2012, Cologne, Germany. Heidelberg: Springer- Verlag, 2012: 177-195.

[27] ZIEGELDORF J H, GROSSMANN F, HENZE M, et al. Coinparty: secure multi -party mixing of Bitcoins[C]//The 5th ACM Conference on Data and Application Security and Privacy, March 2-4, 2015.

[28] JENS G. Short pairing-based non-interactive zero-knowledge arguments[C]//The 16th International Conference on the Theory and Application of Cryptology and Information Security, December 5-9, 2010, Singapore. Heidelberg: Springer, 2010: 321-340.

[29] LIPMAA H. Progression-free sets and sublinear pairing-based non-interactive zero-knowledge arguments[C]//The 9th International Conference on Theory of Cryptography, March 18-21, 2012, Sicily, Italy. Heidelberg: Springer-Verlag, 2012: 169-189.

[30] NIR B, ALESSANDRO C, YUVAL I. Succinct non-interactive arguments via linear interactive proofs[C]// The 10th Theory of Cryptography Conference on Theory of Cryptography, March 3-6, 2013, Tokyo, Japan. Heidelberg: Springer- Verlag, 2013: 315-333.

[31] BEN-SASSON E, CHIESA A, GENKIN D, et al. Verifying program executions succinctly and in zero knowledge[C]// The 33rd International Cryptology Conference(CRYPTO 2013), August 18-22, 2013, Santa Barbara, USA. Heidelberg: Springer-Verlag, 2013: 90-108.

[32] LIPMAA H. Succinct non-interative zero knowledge arguments from span programs and linear eror-correcting codes[C]//The 19th International Conference on Advances in Cryptology, December 1-5, 2013, Bangalore, India. New York: Springer-Verlag New York, Inc., 2013: 41-60.

[33] BEN-SASSON E, CHIESA A, TROMER E, et al. Succinct non-interactive zero knowledge for a von neumann architecture[C]//The 23rd USENIX Conference on Security Symposium, August 20-22, 2014, San Diego, USA. Berkeley: USENIX Association, 2014: 781-796.

[34] MENEZES A, SARKAR P, SINGH S. Challenges with assessing the impact of nfs advances on the security of pairing-based cryptography[C]// International Conference on Cryptology, December 1-2, 2016, Kuala Lumpur, Malaysia. Heidelberg: Springer- Verlag, 2016: 83-108.

[35] Shunli Ma, Yi Deng, Debiao He, Jiang Zhang, Xiang Xie. An Efficient NIZK Scheme for Privacy-Preserving Transactions over Account-Model Blockchain. Cryptology ePrint Archive, Report 2017/1239, 2017.

APPENDIX

A LEGAL STATEMENT

The sale ("Token Sale") of SERO Token is only used as an exchange medium for specific targeted crowds or participants. This is not any form of prospectus or offer document, nor is it SERO constitute any form of securities offer, unit in a commercial trust, unit in a collective investment plan or any other form of investment, or any form of investment offer in any jurisdiction. No regulatory organization has reviewed or approved any of the information listed in this white paper. This white paper has not been registered with any regulatory authority in any jurisdiction. By accessing and / or accepting any information in possession of this white paper or part thereof, as the case may be, by default you meet the following conditions:

(a) You are not in the People's Republic of China, nor are you a citizen or resident (tax or otherwise) of the People's Republic of China, or reside in the People's Republic of China;

(b) You are not in the United States of America, nor are you a citizen, resident (tax or otherwise) or green card holder of the United States of America, or reside in the United States;

(c) According to the laws, regulations or rules of your region, you are not in a jurisdiction that prohibits, restricts or unauthorized sale of tokens in any form or manner, whether in whole or in part;

(d) You agree to meet the conditions and constraints described above.

B RISK INDICATION

This information does not represent an investment proposal, or any license for sale, or to guide and attract any purchase.