WANCHAIN®

Building Super Financial Markets for the New Digital Economy

whitepaper Version 0.9.0

wanchain

Abstract

Digital currency, represented by Bitcoin and Ethereum, is blazing through traditional financial systems with the force of a prairie fire. Although blockchain technology is still in the initial stages of development, its transparent mechanisms and open concepts show tremendous vitality. Wanchain seeks to link the present to the future, through the exploration and implementation of blockchain technology.

Wanchain aims to build a distributed “bank”. Just as traditional banks are the infrastructure of the current financial framework, Wanchain seeks to build a new, distributed infrastructure of digital assets to form an improved, modern framework - an ambitious goal indeed.

Wanchain connects and exchanges value between different blockchain ledgers in a distributed manner. It uses the latest cryptographic theories to build a non-proprietary cross-chain protocol and a distributed ledger that records both cross-chain and intra-chain transactions. Any blockchain network, whether a public, private or consortium chain, can integrate with Wanchain to establish connections between different ledgers and perform low cost inter-ledger asset transfers. The Wanchain ledger supports not only smart contracts, but also token exchange privacy protection.

With Wanchain, any institution or individual can set up their own virtual teller window in the “bank” and provide services such as loan origination, asset exchanges, credit payments and transaction settlements based on digital assets. Under the guarantee of “banks” based on the blockchain infrastructure, more people can participate in financial services based on digital assets. To describe it more accurately, Wanchain is a distributed super-financial market based on blockchain.

Contents

1/ WANChain Design Concept

1.1/ Blockchain Emergence and Significance

Friedrich A. Hayek, the eminent Austrian economist, believes that if we let currencies compete in the market by survival of the fittest, like other commodities, market mechanisms can filter out the most appropriate currency for us, just like it does for those other commodities.

In January 2009, the first Bitcoin block was mined. The emergence of Bitcoin transcended Hayek' s ideal state where responsibility for controlling the total amount of money in a system is borne by specific institutions, whose self-interest keeps the total currency amount at a level acceptable to most users.

The switch from credit authorization by institutions to inviolable mathematical laws for recording the exchange of value is another great innovation. In essence, currency is a consensus. It is an agreed upon accounting representation for a more convenient exchange of value. Reviewing mankind' s financial history, from the bartering of one thing for another, to the use of cattle, sheep or shells as universal equivalents, to the use of precious metals as money, and the current use of paper currency with a strong credit base, human currency is approaching abstract mathematics and its nature as symbols or ledgers is more apparent. Blockchains make human accounting symbols align closer to mathematics.It helps the entire accounting system get away from control by a single institution and move in a more fair and transparent direction.

The concept of Financial Inclusion seeks to give disadvantaged people and small enterprises, worldwide, better access to the financial system and low-cost financial services. Two and a half billion people in the world are unable to use banks, open savings accounts or obtain credit cards and are therefore separated from the global economy. Cross-border remittances through banks incur high fees. Ordinary investors can only buy relatively low-end financial products from banks and other financial institutions and can't take part in early-stage investments of technology companies such as Google and Alibaba before they are listed. It is also difficult for a large number of small to medium enterprises to obtain loan support from banks, in spite of good credit and outstanding performance, because they are not the target customers of traditional banks under the 80/20 rule.

Georg Hegel said "Reality is a historical process," and the emergence of blockchain technology is changing the above situations. When Venezuela recently devalued its currency, Bitcoin became a popular safe-haven asset. Workers in foreign countries, such as the Philippines, remit their income to their weak hometown banking facilities through blockchain networks. Investors who participated in the ICO of well-known blockchain

projects, such as Ethereum, received returns hundreds of times the size of their initial investments. Blockchain technology is pushing Inclusive Finance to brand new heights.

As of June 2017 there are thousands of digital currencies based on blockchain technology with a total market value of over $100 billion, and the number and value of digital currencies continues to grow. Digital currency is becoming more acceptable as a form of payment in financial transactions; many organizations are exploring ways to record traditional forms of assets, such as commercial bills and loyalty points, into blockchains, usually in the form of consortium chains.

Digital asset exchanges, which are similar to traditional financial institutions, have emerged. These exchanges perform the banking function of exchanging digital assets. They are a platform for buying and trading tokens, similar to those of a stock exchange. A platform for cross-border token transfers performs functions similar to cross-border bank remittances.

However, these platforms, in various degrees, are operating in a centralized manner, which not only brings about the security risks of centralization, but also blocks the wider adoption of blockchain technology.

Based on this, we need a distributed "bank" where different digital currencies and digital assets can be transferred in, transferred out and exchanged by blockchains. A place where financial products and contracts based on digital currencies and digital assets can be created and implemented and where the transaction privacy can be effectively protected. Of course, such "banks" will be completely different from traditional banks, except for some functions such as debit and credit, remittance, settlement, and sale of financial products. With corresponding ability and capital strength, any organization or individual can set up their own business windows. They can provide various services, under the guarantee of a distributed blockchain infrastructure, to provide more financial services for more people. More accurately, this is a future financial infrastructure based on digital assets, and also a distributed financial market.

1.2/ Design Background

In the early days of traditional banks, currency exchange was their main purpose, and functions such as currency custody, payments, settlements and remittances were gradually developed. At last, modern banks with deposits and loans as their main business were born. It can be said that a bank is a ledger recording debtor-creditor relationships. Every receipt, payment and transfer of funds is, in fact, a change of corresponding assets in a bank ledger that supports more than one asset. An exchange settlement among different banks is actually an asset record change on different ledgers. It must be ensured that the assets are not double spent, regardless of whether the asset changes are in the same ledger or in different ledgers. In general, the increase or decrease in the amount of an

asset in a ledger must correspond to an equivalent opposite change in another ledger. The block chain has a good solution to the problem of double spending in the same ledger in different accounts. Solving the problem of transferring assets among different blockchain ledgers is key to the wider application of blockchain technology. Wanchain requires a distributed approach to support the access of different blockchains and the transfer of assets - that is, to support cross-chain transactions.

Effective protection of users' privacy is one of the foundations of traditional banking. Any financial transaction is needed to be protected from a third party. Wanchain needs to have the same capabilities.

Wanchain is a distributed financial market. In principle, any organization or individual can develop and provide their own financial services based on Wanchain. It requires Wanchain, a blockchain infrastructure, to support the programmable smart contract function.

In summation, Wanchain is designed under such a context.

1.3/ Design Objectives

In order to build a more widely spread blockchain technology and digital asset applications, Wanchain has set the following objectives based on the research on cross-chain technology, combined with the characteristics of decentralization and its application scenarios:

Cross-Chain Asset Transfer:

• Connect existing major digital currency networks (such as Bitcoin and Ethereum) and completing the asset exchanges without modifying the mechanism of original chains. This integrates newly generated digital currency networks with Wanchain at a very low cost.

• Integrate consortium chains with Wanchain. This fulfills the functions of transferring assets from original chains to Wanchain, transferring assets from Wanchain back to the original chains, and trading various assets on Wanchain.

• Ensure the security of cross-chain transactions and the stability of cross-chain transaction services.

Transaction Privacy Protection:

• Allow trading parties to choose to conduct transactions with privacy protection.

• Provide privacy protection for transfers and exchanges of digital assets.

• Provide anonymous protection of digital asset holders.

Functional Extensibility:

• Become a distributed platform for the exchange of various digital currencies.

• Carry out deposit and loan business for different digital currencies.

• Conduct transactions of digital assets using digital currency as a medium.

• Issue and trade brand new digital financial assets.

1.4/ Positioning

Through the establishment of links among different blockchains, the inter-ledger transfer of assets can be achieved, providing an infrastructure for financial applications based on digital currencies and digital assets. We seek to give full play to the blockchain function of carrying and transferring value, and the equal and open concept of blockchain.

From a blockchain technology development perspective, Wanchain applies secure multi-party computation, threshold secret-sharing, a ring signature scheme based on elliptic curve cryptography, a one-time account generation mechanism, and many other cutting-edge cryptographic technologies. Wanchain also solves the privacy protection problem of smart contract token transactions. To some extent, Wanchain is an advanced cryptographic application that solves the real problems of blockchains and represents the developmental direction of the blockchain technologies. Wanchain has a professional cryptography research team to apply cryptography to the blockchain field and contribute to the industry as a whole.

From a blockchain application perspective, Wanchain is more than just a blockchain project of achieving cross-chain transactions and interoperability of multiple blockchains. Wanchain is a complete blockchain development platform. Wanchain achieves the function of cross-chain transactions, but it is also a blockchain running independently; it contains native coins, supports smart contracts, and has privacy protection mechanisms for smart contract token transactions. Any developer may develop applications on Wanchain in accordance with its application development standards.

2/ Wanchain Architecture and Technology

Wanchain provides an infrastructure for cross-chain transfers between different blockchain networks.

Wanchain is a distributed ledger that:

- achieves the interconnection and interoperability between different blockchain networks.
- completes records of cross-chain transactions.
- maintains cross-chain transaction details.

Wanchain supports cross-chain transactions between mainstream public chains, between private chains, and between public and private chains.

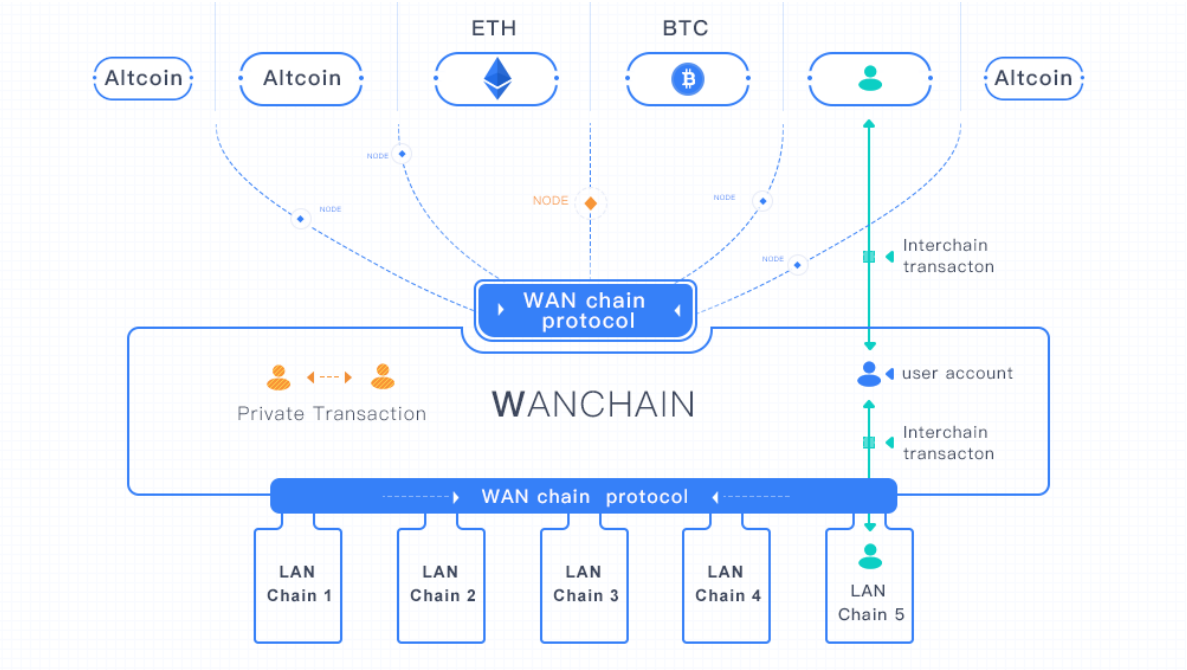

Figure 2.1: Model of WANChain

2.1/ Architecture

2.1.1 Distributed Ledger and Smart Contract Virtual Machine

Wanchain is an Ethereum-based generic ledger that runs applications independently, with account models and smart contracts that implement various original Ethereum functions. On top of those, we added cross-chain transactions and achieved smart contract token privacy protection.

2.1.2 Native Coin

Wancoin is the native coin of Wanchain. Both cross- and intra-chain transactions consume a certain amount of Wancoin. Wancoin is also used in security deposits for the cross-chain verification nodes.

2.1.3 Consensus Mechanism

Wanchain adopts a Proof of Stake (POS) consensus mechanism for ordinary transactions and implements consensus and incentive mechanisms for cross-chain transactions. These mechanisms are discussed in the following sections.

2.1.4 Intra-Chain Transactions

Common transaction methods in Wanchain are the same as in Ethereum, but we have added a privacy protection mechanism that is implemented through a ring signature scheme and a one-time account mechanism.

2.1.5 Cross-Chain Connection

Both blockchains and assets that integrate with Wanchain first need to be registered on Wanchain to make sure that they can be uniquely identified. These functions are completed via chain and asset registration protocols.

For cross-chain transactions, we use secure multi-party computing and threshold secret-sharing joint anchoring schemes to achieve minimal-cost integration through the cross-chain communication protocol without

changing the original chain's implementation. Wanchain is a complete platform that can be applied to broad financial applications with privacy protection for smart contract token transactions of public and private chains. What's more important is that other blockchains developed on Wanchain are equivalent to the homogeneous blockchains of Wanchain and have the same cross-chain mechanism and seamless integration with each other.

2.1.5 Cross-Chain Transactions

When an unregistered asset is transferred from the original chain to Wanchain, Wanchain will create a new asset using a built-in asset template to deploy a new smart contract based on the cross-chain transaction information. When a registered asset is transferred from the original chain to Wanchain, Wanchain will issue the corresponding equivalent tokens in the existing contracts to ensure that the original chain assets can still be traded on Wanchain.

In order to describe the transfer of assets between a public chain and Wanchain, we'll illustrate an example using Ethereum:

Transfer-In Process: Alice and Bob have accounts on Ethereum and Wanchain respectively, and Alice needs to transfer 10 ETH to Bob.

Alice makes a cross-chain transaction request using the Wanchain wallet and initiates a transfer on Ethereum, with the recipient being an Ethereum cross-chain Locked Account. Wanchain's validator node receives the cross-chain transaction request, verifies that the transaction has been recorded on Ethereum, and creates a new smart contract token ETH' (ether prime) on Wanchain, which corresponds to the ETH needing to be cross-transferred to to Bob on Wanchain.

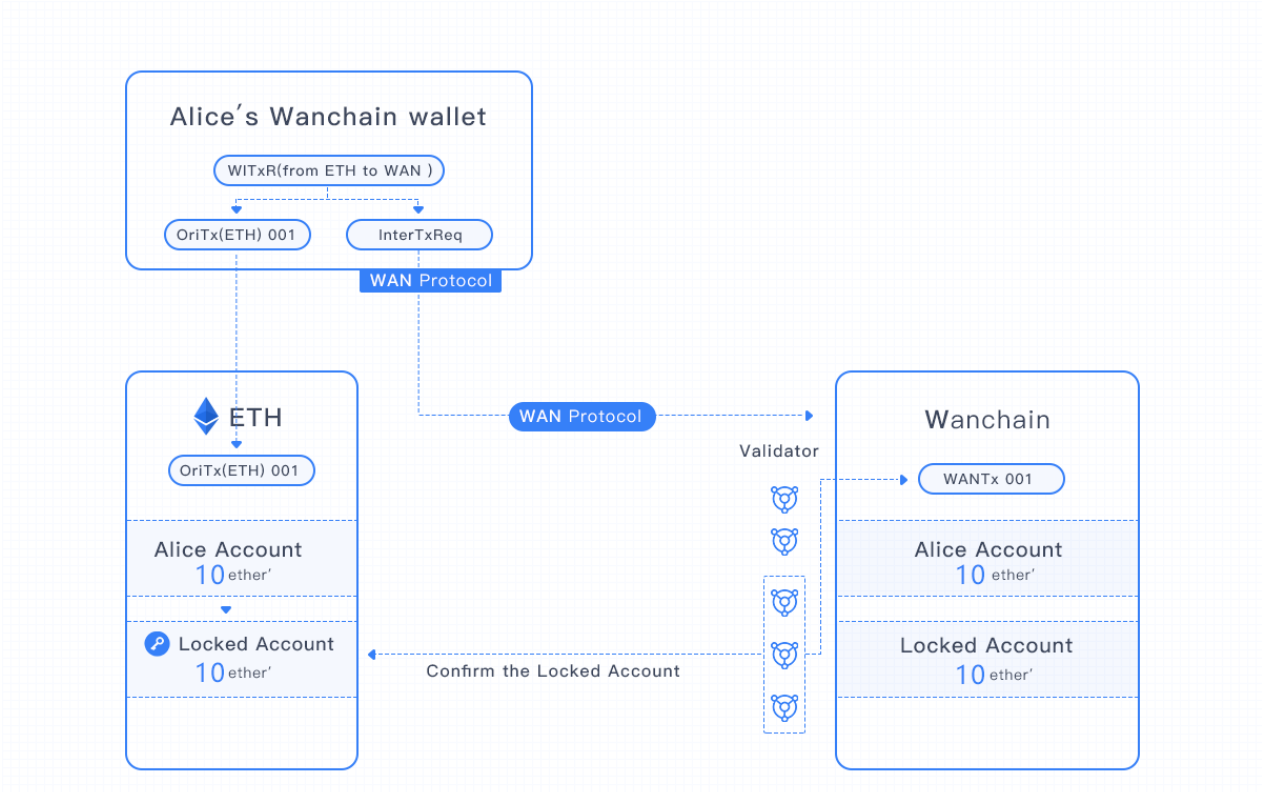

Figure 2.2: Cross-Chain Transaction From Ethereum to Wanchain

Transfer-Back Process: Bob wants to transfer the 10 ETH he received from Alice to Chris.

Bob uses his Wanchain wallet to initiate a cross-chain transaction with the ETH′ asset contract. Upon receiving the request, the validator node locks the corresponding 10 ETH′ assets. After successfully locking the assets, the validator node uses the threshold secret-sharing mechanism to create an Ethereum transaction with the transferor being the Locked Account that was previously locked by Alice' s assets and the transferee being Chris' s account on Ethereum. After the validator node verifies the confirmed transaction on Ethereum, the 10 ETH′ locked under Bob' s account will be cleared, meaning the equivalent asset is transferred back to the original chain.

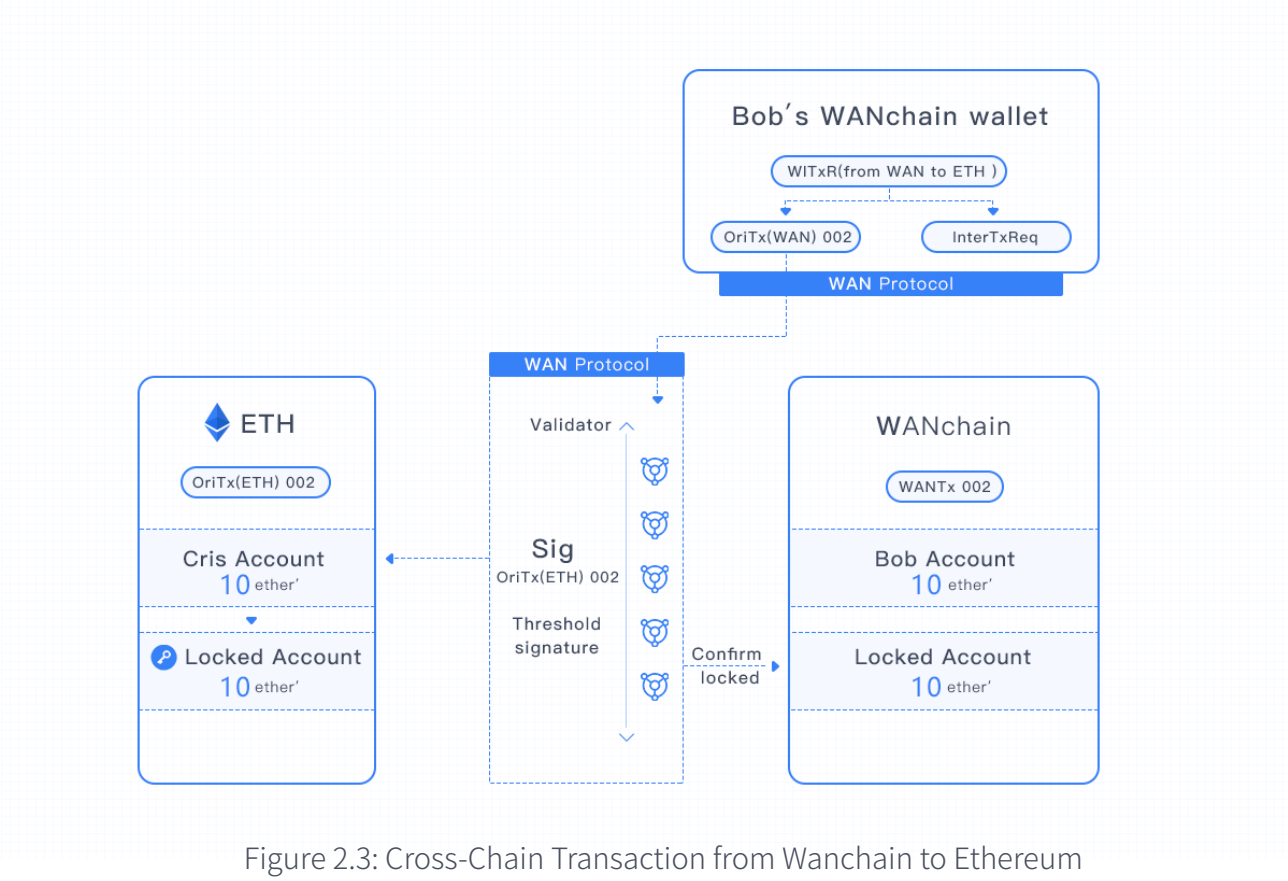

Figure 2.3: Cross-Chain Transaction from Wanchain to Ethereum

The above describes the asset transfer-in and transfer-back processes between Wanchain and the public chain, which is essentially the same as that between Wanchain and the private chain. For details of the asset transfer process and data transmission process, please refer to **Section 3.2 Cross-Chain Transaction Data Transmission Process.**

2.2/ Technology

2.2.1 Fully Decentralized and No Trusted Third-Party Participation

Currently, most cross-chain transactions are conducted through exchanges and third-party trading platforms. But the blockchain cross-chain transaction platforms need the involvement of a third-party custodian account. This leaves the secure and smooth completion of the entire transaction to the reliability of third-party participants. The locked account mechanism of Wanchain

uses fully decentralized, multi-party computing and threshold secret-sharing technology to perform the account management without the need of any third-party participation or credit endorsement of any entities.

2.2.2 Unmodified Original Chain and Low Integration Threshold

In our cross-chain transaction solution, the account locking mechanism doesn't use two-way anchoring, and doesn't need additional script extensions to identify and verify the Simple Payment Verification (SPV) proof. All transaction data is transmitted into the node network of the original chain after reconstruction and integration on the Wanchain validator node. The format of the validator node is in line with the transaction type requirements. This enables certain operations and computations of cross-chain transactions to be completed within the Wanchain network, without the need to modify the various original chain mechanisms. This allows existing public and private chains, based on other platforms, to be integrated with Wanchain with a low integration threshold, thus reducing the cost of cross-chain transactions.

2.2.3 Cryptography Based Security Guarantee

Mechanisms used by many existing cross-chain exchanges often use logical security, relying on participants to look out for their own self-interest. In other words, the participants will not break the cross-chain transactions at the expense of damaging their own interests. This can be called "The Hypothesis of Rational Participants".

In addition to the application of original elliptic curve cryptography to ensure the security of the original signature solution, Wanchain uses:

- threshold secret-sharing technology,
- the locked account management solution based on multi-party computing,
- the privacy protection mechanism for smart contract token transactions, based on ring signatures and one-time accounts.

All subsequent operations are automatically done between validator nodes of Wanchain and don't need coordination from transaction participants after initiating an cross-chain transaction. This leaves the smooth operation of the entire system to the security of cryptographic algorithms.

2.2.4 Cross-Chain Transaction Privacy Protection

In Wanchain's cross-chain transaction solution, assets on the original chain exist in the form of smart contract tokens after they are transferred into Wanchain. On one hand, we hide the initiators of smart contract token transactions in a collection of accounts, via ring signature technology, so that they are not traceable. On the other hand, we allow one-time use of accounts in smart contracts, so the corresponding relationship with the original account on Wanchain cannot be established. By using a combination of the above two methods, Wanchain achieves the confidentiality of smart contract token transactions, allows cross-chain transactions of assets under privacy protection, expands application scenarios and provides a better user experience.

3/ Cross-Chain Communication Protocol

The Wanchain cross-chain communication protocol defines the specifications for data transmission between Wanchain and other chains, allowing interconnections and data flow between chains. The following paragraphs describe the module functions and data transmission processes.

3.1/ Functional Modules

The cross-chain communication protocol consists of three functional modules:

Registration module: this module provides two functions.

The first is to register the original chain participating in cross-chain transactions. This generates a unique ID through specific algorithm rules for the original chain, maintaining the ID registry of the original chains to avoid fraud caused by false chains.

The second function is to register the asset to be transferred. This generates a unique ID through specific algorithm rules for the asset to ensure the uniqueness of the assets.

Cross-chain Transaction Data Transmission Module: this module provides three functions.

The first function is that the user on the original chain makes the cross-chain transaction request to Wanchain. This is the starting point of the Wanchain asset transfer-in transaction.

The second function is the acknowledgement of receipt of Wanchain' s validator node returning success or not.

The third function is that Wanchain' s validator node sends the legal transaction to the original chain to complete the transfer-back process.

Transaction Status Query Module: this module mainly provides the function of querying the confirmation status of the asset transfer-in transaction on the original chain to Wanchain' s locked account and the transfer-back transaction of Wanchain' s locked account to the original chain. These are the control marks of the cross-chain transaction progress.

3.2/ Data Transmission Process

Here we take the user Alice, who wants to transfer value from an original (Ori) chain to Wanchain, as an example to illustrate the asset transfer-in data transmission process:

Step1： Alice initiates a transaction OriTx with her OriAccount on the original chain to send an asset OriAssetID to Wanchain's locked account LockedAccount and broadcasts the cross-chain transaction request InterTxReq to Wanchain via the cross-chain transaction data transmission module.

The function takes the transaction data as parameters, such that:

$$\mathrm{OriT}x\mathrm{Info}=(\mathrm{OriBlockNum},\mathrm{OriT}x)$$
$$\mathrm{InterT}x\mathrm{Req}=(\mathrm{OriAccount},\mathrm{OriChainID},\mathrm{OriAssetID},\mathrm{value},\mathrm{OriT}x\mathrm{Info},\mathrm{sig})$$

Step2：：The cross-chain transaction proof node (Voucher) on Wanchain receives a cross-chain transaction request and checks whether the transaction has been confirmed on the original chain through the transaction status query module.

The function **Token Locked Flag (TLF) takes** OriTxInfo, OriChainID and OriAssetID as parameters, such that:

$$\mathrm{TLF}=\mathrm{CheckCommitment}(\mathrm{OriChainID},\mathrm{OriAssetID},\mathrm{OriT}x\mathrm{Info})$$

Step3： The cross-chain transaction proof node (Voucher) gathers consensus on the TLF results and if TLF=true, then OriTx has been confirmed. The verification node (Validator) receives the data TLF=true, and then checks the asset registry of the original chain. If it is a new asset, the asset will be registered and added into the registry. The public account WANAccount, maintained by the Validator initiates a transaction WANTx, deploys a smart contract for the new asset and distributes tokens of Value for OriAccount in the contract. If it is a registered asset, the transaction WANTx distributes tokens of Value for OriAccount directly into the existing asset contract. If WANTx is confirmed, the Validator uses the cross-chain transaction data transmission module to reply to Alice about the successful receipt of the cross-chain transaction:

$$\mathrm{response}=(\mathrm{WANAccount},\mathrm{InterT}x\mathrm{Req},\mathrm{True},\mathrm{address}_{\mathrm{SC}},\mathrm{sig}_{\mathrm{validator}})$$

If WANTx becomes invalid, the locked account management node (Storeman) initiates a transaction on the original chain to transfer Alice's locked asset back to her account OriAccount.

If the consensus result for TLF is confirmed by the Voucher as false, the cross-chain transaction is considered invalid.

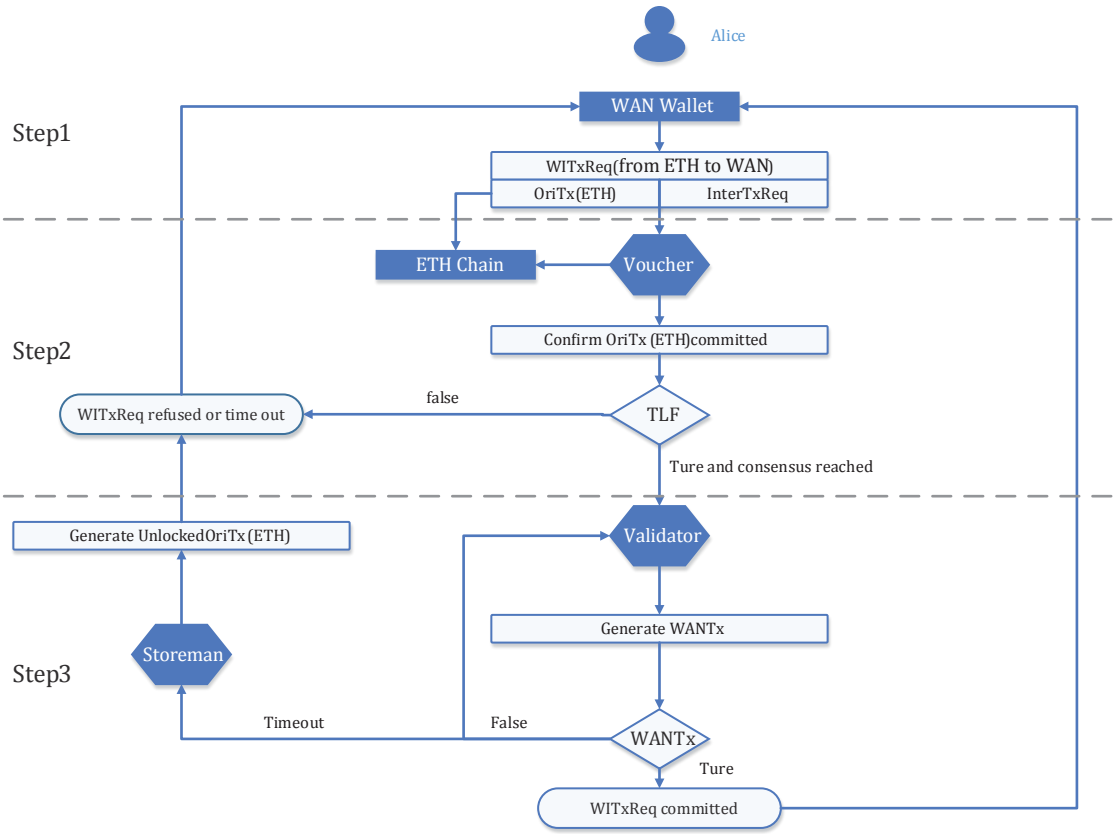

Figure 3.1: Cross-Chain Data Process from Ethereum to Wanchain

In the next example, we have user Bob transferring Value from Wanchain back to the original chain to illustrate the asset transfer-back data transmission process:

Step1: Bob uses BobAccount on Wanchain to send the transaction WANTx, which calls the asset transfer-back function of the smart contract corresponding to the asset of the original chain.

Step2: The Validator calls the smart contract after receiving the transaction. The Voucher tests the results of the contract execution and gathers consensus. If TLF=true, which means that the token value for Bob in the contract has been locked, the Storeman then broadcasts the transaction of Locked Account, which transfers Value to BobAccount on the original chain, via the cross-chain transaction data transmission module:

$$\mathrm{OriT}x=(\mathrm{LockedAccount},\mathrm{BobAccount},\mathrm{value},\mathrm{sig}_{\mathrm{storeman}})$$

The Voucher checks whether this transfer is confirmed via the transaction status query module, and gathers consensus on confirmation flag TL F.

Step3: If the Token Unlocked Flag (TUF) = true, the Validator will clear the assets locked in the smart contract; if TUF=false, it means that transaction on the original chain is not confirmed and the Storeman will re-initiate the transaction.

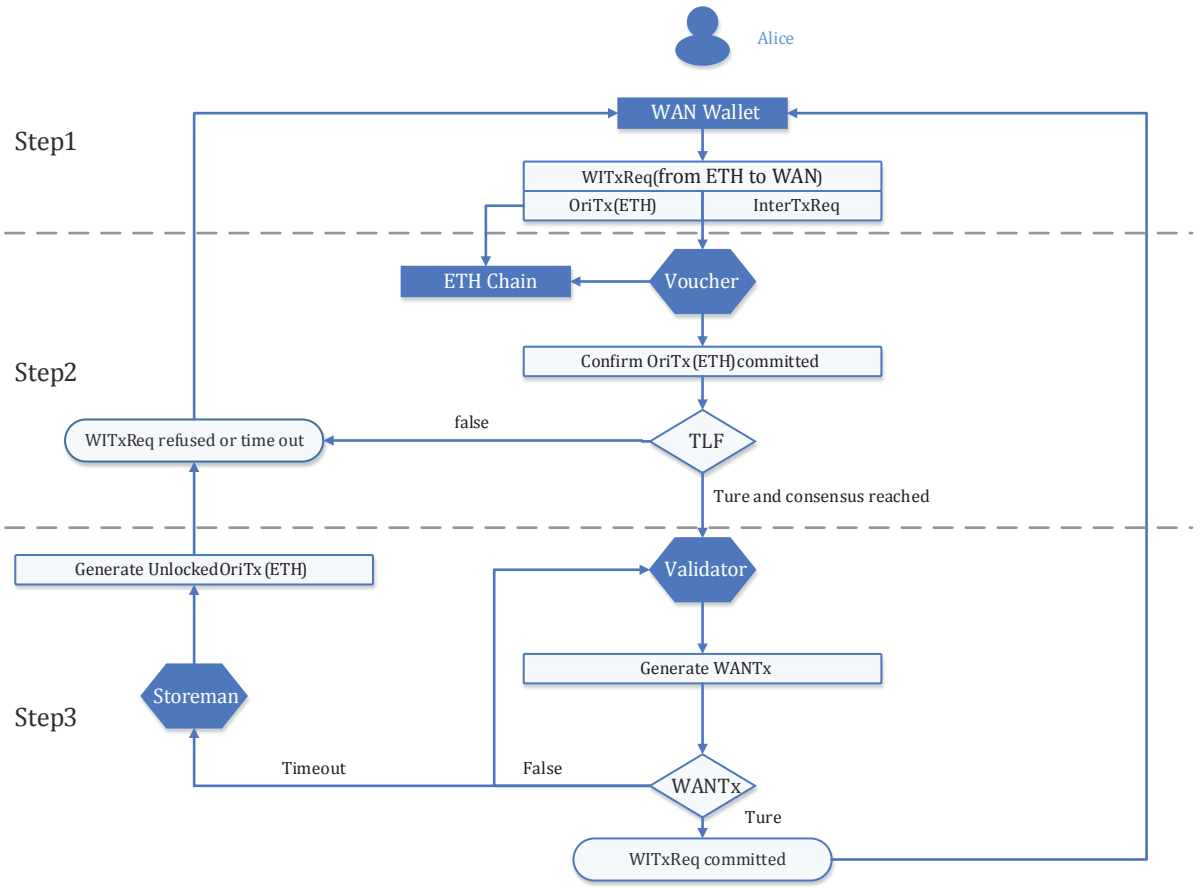

Figure 3.2: Cross-Chain Data Process from Wanchain to Ethereum

4/ Key Technologies

4.1/ Verification Node Consensus Mechanism

Wanchain adopts the Proof of Stake (POS) consensus algorithm, the description of which can be found in a series of papers from Ethereum, so it is not detailed here. Theoretically, the Proof of Work (POW) consensus algorithm is is subject to the threat of 51% power attack, while similarly, the POS consensus algorithm is theoretically subject to a threat of collusion attack of participants. As a result, Wanchain introduces the this mechanism to increase the opportunity cost of verification node collusion, allowing Wanchain to record cross-chain transactions faithfully and follow the cross-chain processes objectively.

In short, the verification nodes on Wanchain are divided into three categories:

- Cross-chain transaction proof nodes (Vouchers)
- Locked account management nodes (Storemen)
- General verification nodes (Validators)

Vouchers are used to provide proof of transactions between the original account and the locked account. A Voucher is required to pay a certain security deposit. The higher the deposit, the greater chance the proof if provides will be adopted. If the proof is found to be false, the security deposit will be deducted from the holding account and the authorization of the Voucher is revoked.

The Storeman, upon receiving a notice, is responsible for computing the signature shares according to its own part of the key and merging the signatures parts into a complete signature for the lock account. When this is done, operations related to the locked account are performed **(see the specific process in section 4.3)**.

The Validator informs the Storeman of operational actions related to the locked account and complete the record of operations on the Wanchain whenever a transaction proof reaches a consensus.

The security of the Wanchain network depends on its overall value. When the value of all cross-chain transactions is far greater than the overall value of the Wanchain network, i.e. where the gains for collusion are greater than the opportunity cost, the risk of collusion between verification nodes will increase.

On the contrary, when the overall value of the Wanchain is sufficiently high, collusion between verification nodes means giving up margin held by them that are staked to the tokens on Wanchain, greatly increasing the opportunity cost of collusion. The nodes will not collude to destroy the entire network for cross-chain asset risking their existing interests and long-term income, thus reducing the risk of collusion.

Furthermore, the more cross-chain transactions are involved in the Wanchain, the greater the value carried by Wanchain. The higher the risk for verification nodes to collude, the more secure the entire network, which will attract more and more cross-chain transactions. This is an interactive process, with the value transferring to the Wanchain network. Wanchain is bound to become increasingly robust.

4.2/ Incentive Mechanism

4.2.1 Verification Nodes

The Vouchers receive transaction fees from the corresponding shares as a security deposit. If the proof provided is found to be false, the security deposit is deducted from the holding account and the node authority status will be revoked.

A Validator completes the recording of transactions on Wanchain to gain a part of the transaction fees.

A Storeman receives a corresponding key share according to the stake it holds, and calculates the corresponding signature share to be added into the transaction. The Storeman obtains the transaction fee involved in the verification transaction according to the key share proportion. If the key share information is offline or lost, the transaction fee can not be claimed. Likewise, if the nodes sign the error transaction, the credentials of the Storeman will also be taken away.

In summary, the verification node incentive mechanism will motivate the Vouchers to provide correct transaction proof, the Validators to complete the recording of Wanchain faithfully, and the Storemen to stay online and safely keep their own key shares.

4.2.2 General Nodes

Only those holding a high enough stake in the Wanchain network can become a verification node. Nodes that fail to be verification nodes are known as general nodes. The general nodes cannot participate in the verification process of cross-chain transactions, but they can entrust the stakes they hold to the trusted verification nodes. The entrusted verification nodes distribute the transaction fees they receive to the general nodes in proportion to the entrusted stakes. If the entrusted verification node is punished, general nodes will bear a corresponding loss.

Such an incentive mechanism ensures that stakeholders in Wanchain can earn stake-related benefits while also motivating them to entrust their stakes to trusted verification nodes. This improves the security and stability of Wanchain.

4.3/ Locked Account Generation Scheme

The Locked Account Generation Scheme is based on secure multi-party computation and threshold key sharing.

4.3.1 Introduction

Secure multi-party computation is both the theoretical basis of distributed cryptography and a fundamental problem of distributed computing. The theory arises from "Yao's Millionaires' Problem" in 1982. Simply speaking, secure multi-party computation is about a group of participants, referred as $P_1 \ldots\ldots P_n$, who work together to compute the function $f(x_1,\ldots\ldots,x_n)=(y_1,\ldots\ldots,y_n)$ securely. The n inputs of function f are held, one each, by n participants. P_i holds the secret input x_i, and after computation P_i gets output y_i. In this situation, security requires that even if some participants cheat in the computing process, the correctness of the computing result must be ensured. This means that when computations are completed, every participant must get the correct output y_i and all input from participants remain privileged. P_i can get no

extra information except (x_i, y_i) through the computation.

The threshold key sharing scheme is designed to solve the secure key management problem. According to design principles of modern cryptography, the security of cryptography depends on the security of the keys. Compromised secure keys will ruin the security of cryptography. So key management is of great importance in security research and design of cryptography. In a situation when an account is managed by multiple parties with different interests, securely managing the distribution of the keys can be difficult. To solve this problem, Israeli cryptographer Adi Shamir proposed the **Shamir's Secret Sharing** threshold key sharing scheme.

In this scheme, a key is divided into n pieces and distributed to n participants. Every participant holds one piece of the key share, a minimum collection of k key shares are needed to reconstruct the key. Thus, any operation on an account will require at least k participants' participation to ensure the account is secure and trustworthy.

4.3.2 Design Description

We designed the Locked Account Generation Scheme based on secure multi-party computation and threshold key sharing. Validators of Wanchain (Storemen) are in charge of maintenance and management of the keys of the Locked Accounts to ensure they are secure and trustworthy. In addition, this mechanism lowers the risk of losing keys and has strong adaptability and stability in an ad-hoc network, which has no fixed topology.

The Locked Account Generation Scheme is as follows:

Step1： Select a secure random number.
There are n validators on Wanchain, named as P_1.....P_n. Each validator selects a secure random number di and k-degree polynomial $f_i(x)=d_i+a_{i,1}x+\cdots+a_{i,k-1}x^{k-1}$. The scheme sends $f_i(j)$ to other validators through secure channel and broadcasts $d_i G$ to every node of the network, G being the base point of the elliptic curve.

Step2： Check the correctness of the messages.
After receiving other validators' messages, P_j will check the correctness of the messages:

$$flag=Check(f_1(j),.....,f_n(j))$$

If flag=true, then P_j accepts and saves it locally.

If flag=false, then P_j rejects it and requires other validators to resend the messages.

Step3: Receive key share.
When all messages are sent and checked out, then every validator gets their key share:

$$key\_share_k=\sum_{(j=1)} f_j(k)\ ,\ k=1,.....,n$$

Step4: Compute the address of the Locked Account.

$$Locked\_Account\_Address=GenerateAddress(d_1\ G,.....,d_n\ G)$$

After all the operations above, the Locked Account is generated, its key is divided into n key shares and then distributed to n validators of Wanchain.

Any operation on the Locked Account will require at least k of n validators' participation to complete.

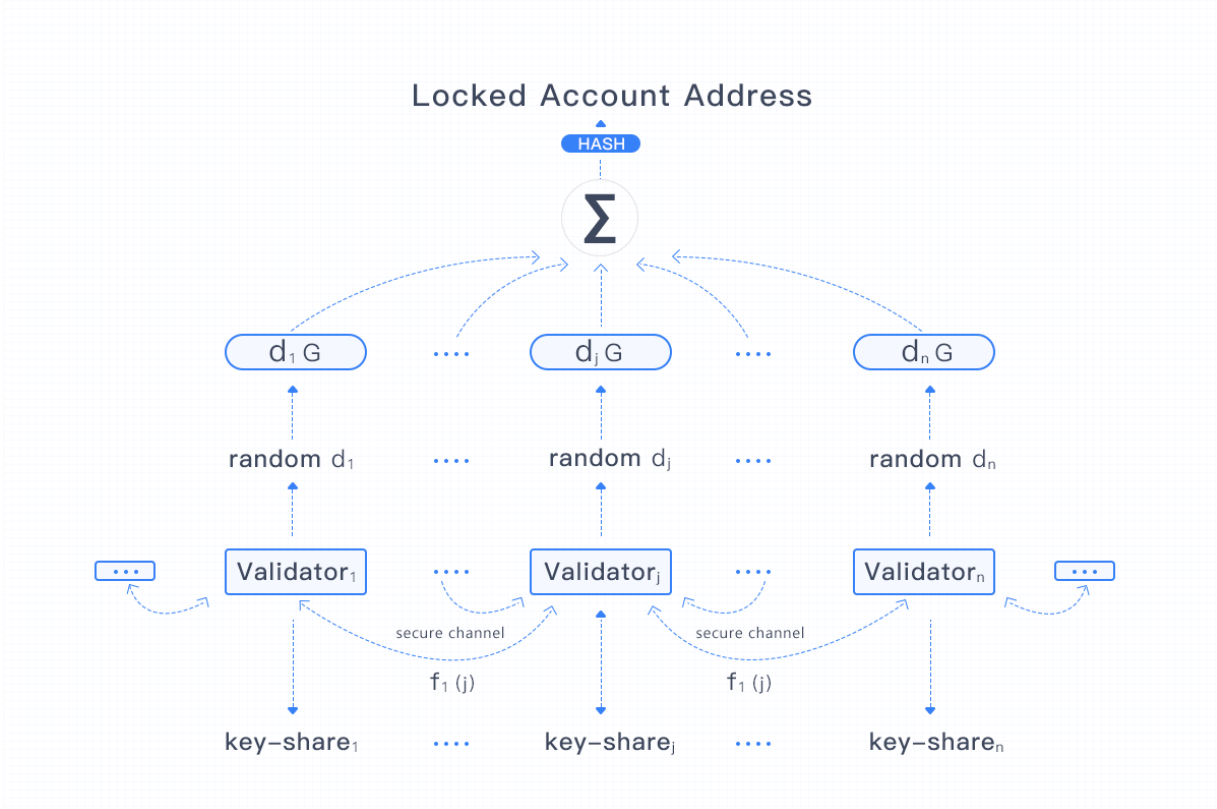

Figure 4.1: Generating Locked Account's Address

4.3.3 Scheme Generation

During the generation process of the Locked Account, the private key is never generated or reconstructed in the entire network. Generating the signature of the Locked Account needs at least k validators' participation. They compute the signature shares separately through the key shares they hold, and then reconstruct the full signature using signature shares.

The Locked Account Signature Scheme is as follows:

Step1: Compute the Signature Shares
A quantity of n Wanchain Validators compute signature shares of the message using key shares they hold:

$$signature\_share_j = Generate\_Sig(m, key\_share_j)$$

Step2: Send out the signatures shares.
Each Validator sends its signature share to other Validators.

Step3: Reconstruct and broadcast the complete signature.
When a Validator receives more than k signature shares, it will reconstruct the full signature and broadcast it to other Validators:

$$signature = Construct\_Sig(signature\_share_1, \ldots\ldots, signature\_share_k)$$

Step 4: The full signature of Locked Account is generated

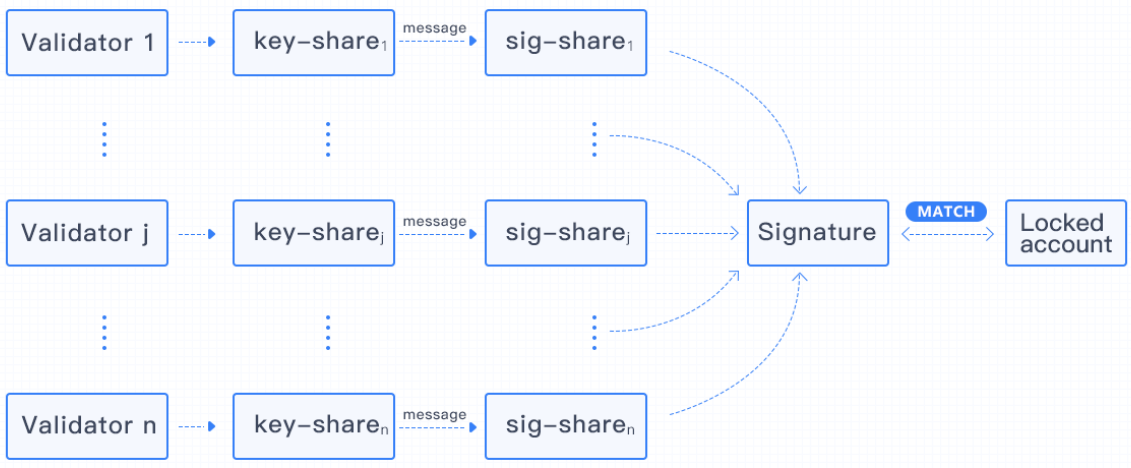

图4.2 锁定账户签名生成

4.3.4 Advantages

Almost all cross-chain transaction schemes need a mechanism to lock the assets of the original chain. Only when the triggering condition is met will the locked assets be unlocked and returned to the original account or some other account.

Existing mechanisms use the Hashed TimeLock Contract scheme, the Trusted Third-Party Escrow Account scheme and the Multi Signature Account scheme.

Compared to these mechanisms, the Locked Account scheme has several advantages:

- **Fully Decentralized without Third-Party Participation**

The Locked Account is generated through secure multi-party computation. In this process, no participation or endorsement of a trusted third-party is needed. All we need is information interaction and computation by Validators through secure channels. Compared to the trusted third-party escrow account scheme, the Locked Account generation scheme has a lower cost and more flexibility.

- **Secure and stable**

The key for the Locked Account is distributed to validators of Wanchain through Shamir' s Secret Sharing Scheme (a.k.a Shamir' s (k, n)-threshold secret sharing scheme). Each Validator holds one piece of the key share. Even when some Validators are offline or lose their key shares, the signature of the Locked Account can still be generated and the transaction can be executed with the participation of at least k validators. Therefore, the Locked Account generation scheme can ensure that the whole system operates with stability and security even in unforeseen circumstance where some part of network paralyzes or lose some key shares. At the same time, the key share of every validator is updated periodically or when a triggering condition is met, in order to eliminate the threat caused by key share exposure.

- **Easy Integration and Efficient Data Storage**

Any operation on the Locked Account is done by the original transaction of the original chain. No new transaction type or verification mechanism is added. So theoretically, any chain can be integrated with Wanchain, and the cost is negligible. At the same time, compared to the multi-signature account scheme that relies on the logic of smart contracts to achieve multiparty management, the Locked Account generation scheme achieves multiparty management through principles of cryptography. The final transaction has only one signature, not several signatures. Thus this mechanism is more efficient on data storage.

4.4/ Smart Contract Token Transaction Anonymity

On Wanchain, ring-signature and one-time accounts are implemented to achieve anonymity in smart contract token transactions. Ring-signature mixes the transaction sender in a set of fake members to make the sender untraceable. A one-time account is generated for each transaction, so it can not be linked to the true owner.

4.4.1 One-Time Account System

As a foundation for anonymity, the one-time account system is especially important. Each user has only one main account and lots of sub-accounts. So if anyone wants to keep anonymous in a smart contract token transaction, he needs to generate an associated account to create an one-time main account together with his original one.

On Wanchain, Alice has an original account (A,a). A is the public key and a is the private key. In order to create an one-time main account, she generate a new account (B,b). The main account is ((A,B),(a,b)) with main public key (A,B), main private key (a,b) and scan key (A,b). Usually a sub-account is generated by a transaction sender for the receiver. For example, Bob wants to send some tokens to Alice. He invokes the function OTA_GenerateAccount( ) with Alice`s main account as a parameter to generate Alice`s sub-account (A1,S1):

$$(A_1,S_1)=\mathrm{OTA\_GenerateAccount}((A,B))$$

Alice invokes the function OTA_ScanAccount( ) with her own scan key to scan every sub-account (A_i,S_i):

$$\mathrm{flag}=\mathrm{OTA\_ScanAccount}((A_i,S_i),(A,b))$$

When it comes to (A_1,S_1), the flag returns true. So (A_1,S_1) belongs to Alice. She invokes the function OTA_GetPrivateKey( ) with her main private key to get the private key of (A_1,S_1):

$$\mathrm{sk}=\mathrm{OTA\_GetPrivateKey}((A_1,S_1),(a,b))$$

In the One-time account system, the scankey helps Alice learn which sub-account belongs to her and the main private key guarantees that she is the only one who can get the private key. No one could change the owner of a sub-account without the associated scan key and get the private key without main private key. Therefore, anonymity and security is guaranteed.

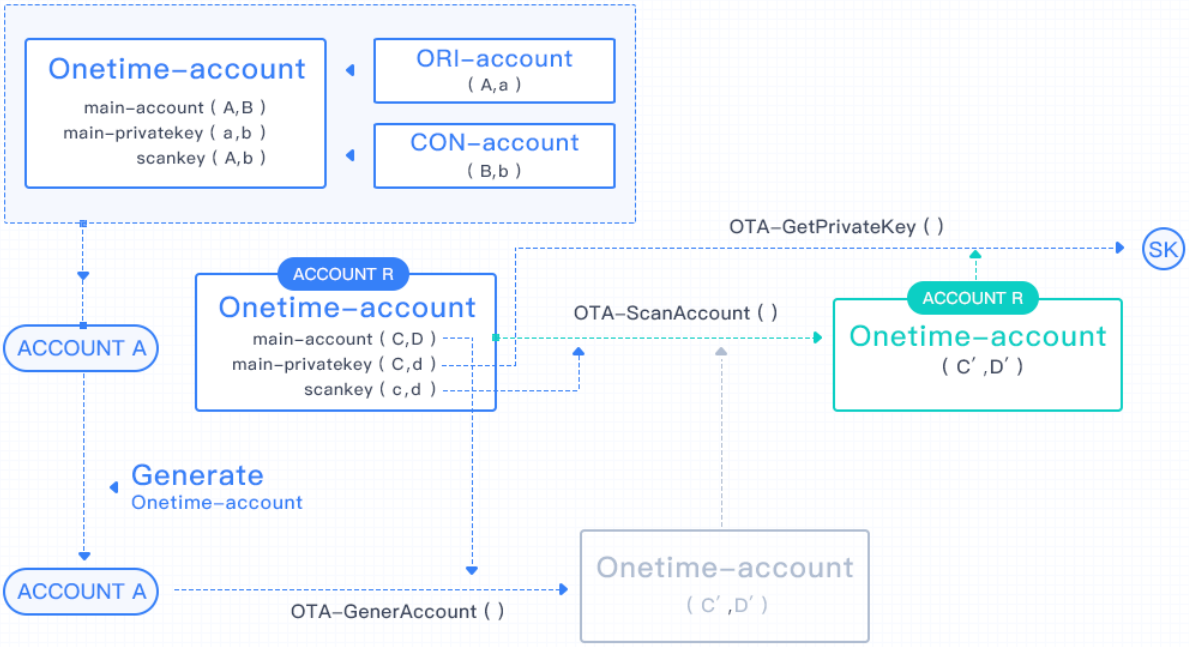

Figure 4.3: One Time Account System

4.4.2 Ring Signature Scheme

The Ring Signature scheme was first provided in 2001 by Rivest and others. It is a special kind of Group Signature scheme. A Group Signature scheme needs a trusted center and secure setup, which would mean that the signer can be traced by the trust center. The Ring Signature scheme solves this serious problem by removing the trusted center and secure setup.

Since the Ring Signature scheme was introduced, many practical schemes have been designed based on the Elliptic Curve Cryptography (ECC), such as the trapdoor technique. Generally speaking, there are four kinds of Ring Signature schemes: Trapdoor Ring Signature, Linkable Ring Signature, Anonymity Revocable Ring Signature, and Deniable Ring Signature.

In order to provide anonymity in Smart Contract Token transactions, the Ring Signature scheme based on ECC is implemented in Wanchain.

There are three parts to the Ring Signature scheme. Details are as below, taking the signer (P,x) as an example:

GEN: Get the public parameters. The signer generates a public key set including n members from the world state through the function GeneratePublicKeySet( ) with the public key as a parameter:

$$\text{publickeyset}=\text{GeneratePublicKeySet}(\text{P})$$

The signer makes a key image I by invoking GenerateKeyImage( ) with the public key and private key:

$$\text{I}=\text{GenerateKeyImage}((\text{P},x))$$

SIG: Generate the ring signature. The signer generates the ring signature of message m through GenerateRingSignature( ) with publickeyset, I and x:

$$\text{ringsig}=\text{GenerateRingSignature}(\text{m},\text{publickeyset},\text{I},x)$$

VER: Verify the ring signature. The signer verifies the ring signature of message m through VerifyRingSignature( ) which returns true or false with publickeyset, I and ringsig:

$$\text{flag}=\text{VerifyRingSignature}(\text{m},\text{publickeyset},\text{I},\text{ringsig})$$

If the flag is true, the ring signature is valid. Otherwise it`s invalid.

In the Ring Signature scheme, the key image and ring signature can not be matched with the signer who is among the publickeyset. Anyone can verify whether the signature is valid or not, but no one is able to identify the signer.

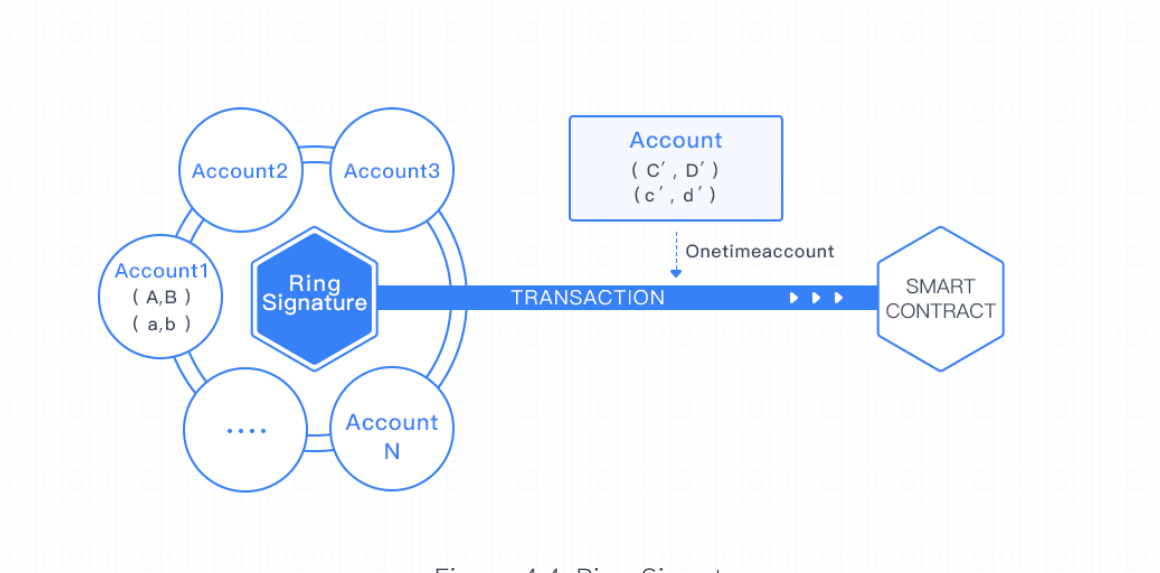

Figure 4.4: Ring Signature

4.4.3 Privacy Protection Transaction Flow

Alice wants to send some tokens to Carl in the smart contract whose address is SCAddress. Alice`s main account is (A,B) with main private key (a,b). Carl`s main account is (C,D) with the main private key (c,d). Alice has a sub-account Onetime_account1 with the private key sk1 in the smart contract. The transaction flow is as follows:

Alice sends a transaction:

Step1： Alice generates an one-time account for Carl with his main account:

$$Onetime\_account2=OTA\_GenerateAccount((C,D))$$

Step2： Alice generates the signature for the transaction data in the smart contract through GenerateSignature( ) with sk1 and makes the final data Payload:

$$sig=GenerateSignature(Onetime\_account1,Onetime\_account2,value,nonce)$$
$$Payload=(Onetime\_account1,Onetime\_account2,value,nonce,sig)$$

Step3： Alice generates the public key set:

$$publickeyset=GeneratePublicKeySet(A)$$

Step4： Alice generates the key image and makes the transaction message m:

$$I=GenerateKeyImage((A,a))$$
$$m=(publickeyset,SC\_Address,Payload)$$

Step5： Alice generates the ring signature and makes the final transaction data:

$$ringsig=GenerateRingSignature(m,publickeyset,I,a)$$
$$transaction=(publickeyset,SC_{Address},Payload,I,ringsig)$$

Step6： Alice broadcasts transaction on the Wanchain.

The Validator verifies a transaction:

Step1： The Validator receives transaction and makes the transaction data m to verify the ring signature:

$$m=(publickeyset,SC\_Address,Payload)$$
$$flag=VerifyRingSignature(m,publickeyset,I,ringsig)$$

Step2： If flag is true, the Validator goes to step 3. Otherwise the transaction is invalid and thrown out.

Step3： The Validator invokes the smart contract with Payload as a parameter. Then the smart contract verifies the signature in Payload and executes the transfer.

After step 3, the transaction is committed on Wanchain. Carl scans the sub-accounts with his scan-key and recognizes that Onetime_account2 belongs to himself. Then he gets the private key for Onetime_account2 with his main private key. Therefore he takes the tokens of Value.

5/ Wanchain Applications

5.1/ Borrowing and Lending

As digital currency becomes an important medium of value exchange and a value storage carrier, using it to create new value and generate income is an inevitable trend. For example, Bitcoin is used to invest in blockchain mining businesses and other ICO projects. With the increasing number of applications for digital currency, direct investment opportunities for digital currency have increased.

People who use digital currencies to create value need more digital currencies, and people who hold digital currencies want to increase their value, so the demand for borrowing and lending digital currencies will increase.Take Ethereum (ETH) for example. A service provider uses a smart contract to create a deposit application and set the interest rate on Wanchain. A user transfers ETH from the Ethereum blockchain to the corresponding Wanchain smart contract address through a cross-chain transaction. The deposit on Wanchain releases a corresponding voucher (tokens on Wanchain that are similar to deposit bank receipts) to the user' s account on Wanchain. The smart contract then automatically calculates the interest. When the user needs to withdraw the deposit, the voucher will be transferred back to an intermediary address, and a cross-chain transaction is executed. The ETH corresponding to the voucher is unlocked on the

original chain and transferred back to the original user' s account. The deposit reserves (the locked assets on the original chain corresponding to the intermediary address) are always transparent.

5.2/ Payment and Settlement

More and more businesses accept digital assets, like Bitcoin, as a means of payment. In the future, there will be more applications in which a variety of digital currencies are used for payments. Currently, there are many payment methods such as VISA, Paypal and Alipay, each with their own payment procedures and settlement processes. Wanchain is a distributed multi-currency platform, integrating different banking ledgers into one unified ledger. Any business or user can install the Wanchain wallet to implement multi-currency payments and settlements without having to install multiple digital currency wallets.

5.3/ Transaction and Exchange

At present, the completion of digital currency exchange depends on centralized exchanges and over-the-counter markets. All transactions are based on trust of the exchanges and intermediaries. After multiple currencies are integrated with Wanchain, the exchanges or intermediaries can achieve multi-currency auction trading and one-to-one curb transactions via smart contracts. The privacy protection transaction mechanism on Wanchain provides support for transactions that require privacy protection. Wanchain allows for importing digital currency into Wanchain, launching private transactions on Wanchain and transferring digital currency back to the original chain. To some extent, the privacy protection of the original chain is achieved by masking the fund tracking paths.

5.4/ Investment and Financing

There is a trend toward traditional institutions to use consortium chains to hold assets such as commercial bills, loyalty points, future earning rights, accounts receivable and so on. In the future, more financial assets will be recorded on distributed ledgers based on consortium chains. When these consortium chains are linked to Wanchain, they become financial asset providers, and the investors can use their digital currencies to buy these assets. As in the traditional banking business, it's akin to buying financial products in a bank. The difference is that more intermediaries can participate and that the asset holders can carry out financing directly.

An ICO has become an important means of financing in the blockchain space, and this trend is spreading into non-blockchain areas. More and more projects, especially the ones

based on Ethereum, directly use smart contracts for ICO, which makes the whole process more transparent and fair. But ICOs that only use Ether cause inconvenience to investors holding other digital currencies. On Wanchain, the ICO issuer can issue a smart contract that supports multi-currency investments. More conveniently, investors can invest by using Ethereum, Bitcoin or any other blockchain tokens integrated with Wanchain, and issuers can more easily manage their funds. Furthermore, when a new blockchain is launched, the conversion between the crowdfunded shares and the native currency can be completed via the Wanchain cross-chain transactions. With Wanchain, we are entering an era of digital right issuance fully based on blockchain.

5.5/ Other Applications

The financial applications described above are intended to give readers a better understanding of the logic and value of Wanchain. From these, we can come up with more examples such as: multi-currency credit cards based on digital currency, asset backed securities that package up a variety of assets, Peer-to-Peer lending businesses based on digital currencies, crowdfunding, and so on.

Application of blockchain technology has been regarded as an important strategy by major banks, but mostly they use of blockchain technology to transform the traditional business. In the field of digital currency, banking business, like currency exchange, has been booming. Blockchains progress in these fields on two parallel tracks, but with the rise of digital assets and their increasing integration into the real economy, these two tracks will eventually intersect. Digital assets will be included in the banks' balance sheets (banks that support the loan and deposit of digital assets) and the banks' balance sheets will be partially transferred to blockchains (fiat money is represented and accounted by blockchain tokens). Wanchain’s inter-ledger technologies will support this future integration.

Conclusion

In this paper, we put forth the concept of a future “bank”. The term “bank” is an analogy used to give readers a more intuitive understanding of the concept. Abstracting blockchain technology, from the concept of Bitcoin into a neutral technology, greatly improved the global popularization and application of blockchain, however it still faces huge obstacles. It’ s risky and expensive for traditional banks to solve existing business problems by using blockchains. Decision makers are unlikely and unwilling to take such a big risk due to investor return expectations, and for just one bank to change is not enough.

The financial framework based on digital currency, is similar to traditional banking at the business level but is different in nature and organization. Just as ecommerce did not sprout from traditional industries, but generated new commercial modalities that changed the traditional industries. As the proportion of digital currency in the economy increases, new financial industries based digital currency will flourish. Of course, given time, traditional banks will join the digital currency economy in their own ways and a financial ecosystem integrating traditional assets with digital assets will gradually be developed.

Wanchain aims to design a new decentralized financial infrastructure, that allows the exchange of value among different blockchain networks. Based on this new model, intermediaries will develop their own financial services and build a distributed super financial market via Wanchain. We believe that a flexible, decentralized, value exchange system is the future of the financial infrastructure, and will help to promote financial inclusion and standardize future financial transactions.

References

[1] NAKAMOTO.S, Bitcoin: A Peer-to-Peer electronic cash system

[2] Ethereum: https://github.com/ethereum/wiki/wiki/White-Paper

[3] Stefan.Thomas, Evan.Schwartz, A Protocol for Interledger Payments

[4] Jae.Kwon,Ethan.Buchman, A Network of Distributed Ledgers

[5] Shamir A. How to share a secret. Communications of the ACM, 1979, 24(11): 612~613

[6] Blakley G.R. Safeguarding cryptographic keys. Proceedings of the National Computer Conference, 1979, American Federation of Information Processing Societies, V.48, 1979:313~317

[7] B. Chor, S. Goldwasser, S. Micali, and B. Awerbuch. Verifiable Secret Sharing and Achieving Simultaneity inthe Presence of Faults. In Proceeding 26th Annual Symposium on the Foundations of Computer Science, IEEE,1985:383~395

[8] Desmedt Y. Society and group oriented cryptography: a new concept Advances in Cryptology-Cryp to'87, 1987:120~127

[9] Ronald L. Rivest, Adi Shamir, and Yael Tauman, How to Leak a Secret: Theory and Applications of Ring Signatures, Springer Berlin Heidelberg, 2006,22(11):164-186

[10] Man Ho Au, Sherman S.M. Chow, Willy Susilo, and Patrick P. Tsang, Short Linkable Ring Signatures Revisited, EuroPKI 2006: Public Key Infrastructure pp101-115

[11] MONERO: Nicolas.van.Saberhagen, CryptoNote v 2.0

[12] Melanie Swan, Blockchain: Blueprint for a New Economy

[13] Adam Back, Matt Corallo, Luke Dashjr,Mark Friedenbach, Gregory Maxwell, Andrew Miller, Andrew Poelstra, Jorge Timón, and Pieter Wuille:Enabling Blockchain Innovations with Pegged Sidechains

[14] Stefan Thomas & Evan Schwartz: A Protocol for Interledger Payments

[15] Paul Vigna & Michael J. Casey: Cryptocurrency: How Bitcoin and Digital Money are Challenging the Global Economic Order

Appendix: Glossary of Terms

Chain ID: The chain identifier in Wanchain' s registry. OriChainID is used to mark the original chain in transactions.

Cross-Chain Transaction: An asset transfer between two different blockchains (which means transfer-in or -out of the original chain.) When an asset on one chain is transferred to another chain, the total amount of the assets in the two ledgers stays unchanged, which will not cause any inflation or deflation.

Homogeneous Chain: Either a public or private chain developed based on Wanchain, which contains the same cross-chain protocol and asset cross-chain mapping methods, and can be integrated with Wanchain seamlessly for two-way asset transfers.

Inclusive Finance: Providing affordable financial services to disadvantaged and low-income segments of society.

ICO(Initial Coin Offering): An initial coin offering (ICO) is a means of crowdfunding the release of a new cryptocurrency. Generally, tokens for the new cryptocurrency are sold to raise money for technical development before the cryptocurrency is released. Unlike an initial public offering (IPO), acquisition of the tokens does not grant ownership in the company developing the new cryptocurrency.

Locked Account: The account to lock the assets transferred out of the chain.

Mapping Token (MT): The tokens on Wanchain corresponding to the original assets.

OriAccount: The account for the original chain that initiated the cross-chain transactions. For example, the OriAccount of Alice is written as OriAccount(Alice).

Private Chain: A blockchain network with limited openness and decentralization compared with a public chain, where authorization under specific rules is required for a new node to join the network.

Public Chain: A blockchain network fully open and decentralized, where any participants can join the network as long as they follow the protocol of the public chain.

Storeman: A Wanchain node that holds the key shares of locked accounts, uses the key shares to generate signature shares and combine them into complete signatures, and carries out other operations on locked accounts.

Token Locked Flag (TLF): During the process of asset locking, Wanchain nodes verify the transaction OriTx on the original chain and broadcasts the TLF consensus results to other nodes.

Token Unlocked Flag (TUF): During the process of asset unlocking, Wanchain nodes verify the transaction OriTx on the original chain and broadcasts the TUF consensus results to other nodes.

Validator: The blockchain node used in packaging and verifying the transactions. Wanchain' s verification nodes are divided into three categories: the general verification nodes (Validators), the cross-chain transaction proof nodes (Vouchers), and the locked account management nodes (Storemen).

Voucher: A Wanchain verification node that is responsible for verifying whether the assets on the original chain are locked or unlocked for cross-chain transactions.

WAN Account: An account maintained by Wanchain' s Validators to initiate transactions on Wanchain and deploy or call smart contracts.

Wanchain: A public blockchain referred to in this white paper, including distributed ledger, smart contract, cross-chain protocol and other contents, which can achieve the cross-chain transactions, privacy protection for token transactions and other functions.

Wanchain Cross-Chain Protocol: The communication specifications for Wanchain cross-chain transactions (WIP for short), which includes Wanchain Cross-Chain Transaction Requests (WITx-Req), Token Locked Flag (TLF), Token Unlocked Flag (TUF) and Mapping Token (MT):

Wanchain Cross-Chain Transaction Request (WITxReq): A package of information, which includes two parts - the Cross-Chain Transaction Request (InterTxReq) and the Origin Chain Transaction (OriTx). If the original chain is "BTC", then it will be written as OriTx(BTC). If the original chain is the Wanchain, then it will be written as OriTx(WAN). For the public chain, OriTx is structured as the public chain transaction data format, and the wallet uses OriTx to initiate the asset transfer to Wanchain' s locked account on the original chain. Wanchain and the homogeneous chain can construct a transaction UnlockedOriTx in accordance with the original chain transaction data format. An OriTx is used to lock the original chain assets. An UnlockedOriTx is used to unlock the original chain assets.

Contributors：Jack Lu, Boris Yang, Zane Liang , Ying Zhang, Demmon, Shi, Eric Swartz, Lizzie Lu

Reviewers：Dustin Byington, David A. Johnston, Michael Y., James Shen , Feng Han、, Albert Ching

wanchain.org

info@wanchain.org