SDC

（Sky Dynasty Coin）

White Paper (V 1.0)

Blockchain technology has entered the public view and has quickly risen to the policy level. From the Davos Forum to the International Monetary Fund, from the People's Bank digital currency seminar to the hearing of the Commodity Futures Trading Commission, from the Nasdaq, Citibank and other financial industries to IBM, Microsoft and other technology giants, blocks Chains and digital currencies are causing widespread concern and discussion in the world.

SDC is committed to building an open and comprehensive blockchain payment ecosystem

Table of Contents

Preface

In recent years, the encrypted digital currency market has become increasingly hot. The encrypted digital currency has the advantages of high circulation, high falsification costs, low production costs, decentralization, fair and transparent books, and high issuance costs. It is widely sought after by the market and its core support technology. Blockchain attracts more and more attention and is considered as the core technology for constructing next-generation value Internet. The development of blockchain has also led to the rise of Distributed Ledger Technology. In general, it is generally considered that these two concepts are interoperable and refer to the same type of technology. But in a strict sense, blockchain can be considered as an implementation method of distributed ledger technology.

The concept of decentralization of blockchain is gradually overturning the traditional currency concept, and it has had a tremendous impact in the world for a short time. Although the development of distributed ledger technology is very rapid, it is still at an early stage as a whole. The technology is far from commercial requirements. Some of the core technical bottlenecks have not been broken, which has hindered the large-scale application of the technology. Among them, the bottleneck of performance bottlenecks and cross-link communication is particularly prominent. The high independence and transaction speed of blockchain technology have greatly limited the space for the distribution and use of digital assets. Each blockchain system is not interconnected and has no agreement. They have a high degree of independence, and they are unable to communicate and collaborate with each other. As a result, the circulation and transaction of digital assets in each blockchain are also greatly limited. With the increase in the number of blockchain systems The problem of message interworking and transaction speed between different blockchain networks has become a new trend in the development of blockchain technology.

In the existing blockchain technology, the processing capability of the blockchain is mainly subject to the performance of the consensus algorithm, and the performance of the consensus algorithm is subject to the size of the system node and the processing capability of a single node. In the current state of the art, there is very limited space for performance optimization of a single blockchain, and there are performance limits, which severely restricts the application of distributed ledger technology in large-scale, high-concurrency, low-latency transactional service scenarios. For example, high transfer fees and extremely slow speeds are major drawbacks. The slow transfer rate cannot be tolerated. The high fees also make small transactions uneconomical and impossible. It can be predicted that with the rapid development of the digital economy, the frequency and scale of future transactions will far exceed the current level, and the performance bottleneck is one of the most important issues to be solved in distributed ledger technology.

In the area of payments, as the popularity of digital currencies increases and the number of currency applications increases, the demand for payment increases. Lightning and thunder and lightning networks and other technologies need to be born. However, the design of lightning and lightning networks is complex, and the technology is difficult to deploy. The development cycle is long, and the time and effect of actual application in the future are unknown.

Therefore, we proposed Sky Dynasty Coin, a layered channel payment network based on flexible multi-signature, which uses existing mature technologies and has a simple principle and simple design.

(Sky Dynasty Coin) can send and receive digital currency at a zero-speed per second for convenience and reliability.

Sky Dynasty Coin is based on the Sky Dynasty Coin created on the ground floor of ERC20. It uses a combination of 2-of-2 multi-signature, lock-in time trading, and post-transmission construction, which can be used without trust. , The zero transfer fee for the blockchain assets is transferred in seconds, which is comparable to the Lightning Network in terms of speed, security and privacy.

Tianzun's advantage lies in:

1. The underlying technology is mature: The underlying technology of Sky Dynasty Coin is based on mature multi-signature technology, time-stamp transaction technology, and transaction cold signature technology.

2, good compatibility: support for most of the major currencies, even dog-dollar such as a long-term no core maintenance and updating of the currency, as long as the digital currency, generally can support the implementation of Sky respect (Sky Dynasty Coin), and Cross-chain cross-currency payments can be implemented without any adjustments to the core wallet.

3. Flexible application: Sky Dynasty Coin technology can be integrated into the core wallet of the target currency.

4. Safe and concise: Sky Dynasty Coin compared to the Lightning Network, the underlying technology used has been applied on a large scale, it is safe enough, and the design of Sky Dynasty Coin is simple and the application is high.

Sky Dynasty Coin has provided different services to merchants and individual users, and is committed to creating the 3.0 era of blockchain payment.

1. Sky Dynasty Coin Overview

1.1 Tianzun Philosophy: Committed to Creating an Open and Comprehensive Blockchain Payment Ecosystem

Sky Dynasty Coin is committed to building an open and comprehensive blockchain payment ecosystem. Sky Dynasty Coin offers different services and products for both business users and individual users. In the face of business users, Sky Dynasty Co., Ltd. (Sky Dynasty Coin) Coin provided the Sky Dynasty Coin business platform (Dynasty), which enables one-click access to Sky Dynasty Coin payments and cross-border payment solutions. In the face of individual users, Sky Dynasty Coin offers a variety of functions that are customized for encrypted digital currency users, such as mobile DAPP wallets, communication modules based on RSA algorithm encryption, off-site secured transactions, and ultra-fast transactions.

1.2 Tianzun independently developed Sky Dynasty to realize zero-cost and high-speed transfer

Time-of-day transactions and 2-of-2 multi-signature technologies, such as mature technologies, use the payment technology (RouPay) to achieve instant payment, instant arrival, and zero handling fee, so use Sky Dynasty Coin to send (or Other encrypted digital currency) can arrive quickly and at zero fees, giving users a completely new payment experience, and unlike the centralized wallet database technology, Tianzun payment technology is decentralized, and the user's assets are completely In the user's own hands, the query channel can be accessed on the blockchain, and will not be used by the platform. It is absolutely safe.

Compared with the high transfer fees and slow transfer time of ordinary digital wallets, Sky Dynasty Coin can realize zero fees and second digits between users and users through independently developed Sky Dynasty. Asset Transfer, Bringing Blockchain Payments to the 3.0 Era!

1.3 Sky Dynasty Coin uses a universal address, a universal address to receive and send 95% of encrypted digital currency

The emergence of universal addresses can help users avoid the trouble of managing multiple currency addresses. Just as having a paypal account, it can be as convenient as sending and receiving more than 20 foreign currency coins from all over the world.
The universal address is defined by the user. It can be the currency address of a mainstream digital asset. It can also be an ID number, mailbox, or mobile phone number. Using a common address can easily receive and send and maintain its own blockchain assets.

2. The core technology of Sky Dynasty Coin

2.1RouPay: Use multi-signature technology to establish a trading channel, achieving lightning-fast transactions comparable to lightning

The core of Tianzun payment technology is to achieve speed transactions through multi-signature technology. Its security is higher than zero, and its simplicity and landing is superior to Lightning Network.

2.1.1 The Core Process of Tianzun Payment Technology Implementation

1 Collect the respective public keys of A and B to generate the multi-signature address paid by the two gods:

2. Assume that A is the holder of the 1Bit address and B is the holder of the 1Dog address. After the public key exchanges the public key location, it can generate two 2-of-2 multi-signature synthesis addresses, namely 3CSm address and 3Njd address. Public keys are publicly available information and can be made publicly available. Synthetic addresses can also be quickly generated online.

3.A constructs the transaction TX1 sent to the contract address, and sends back the transaction TX2 from the composite address lock time to B:

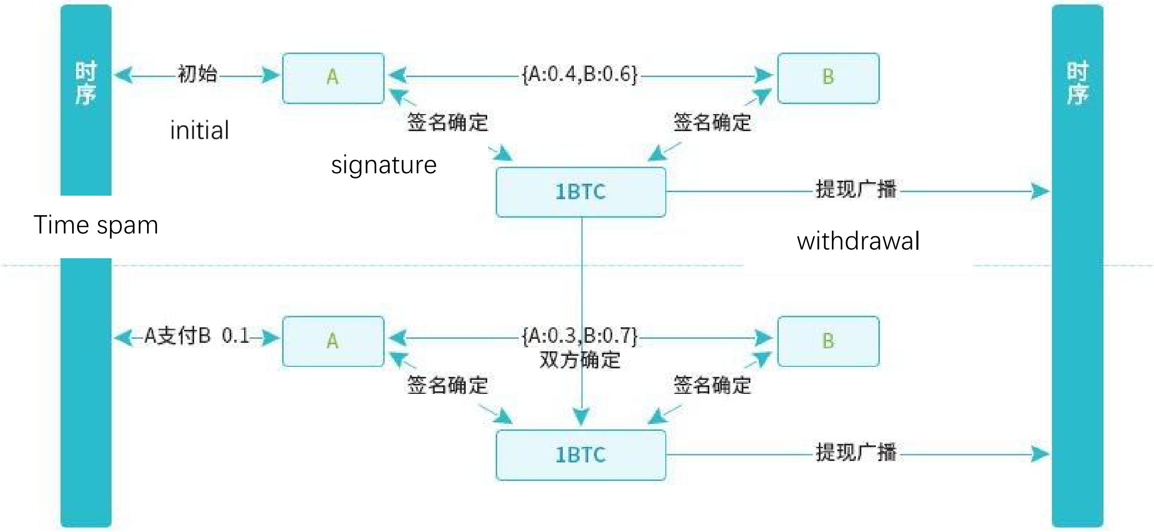
4.A Using the private key of the 1Bit address, the signature constructs a transaction sent to the 3CSm synthesis address, as long as the transaction ID and position n data is obtained after sufficient creation, it may not be broadcast first.

5. Then A or B, preferably A, is used to construct a transaction TX2 that sends back the 1Bit address from all the currencies of the 3CSm address. Note that it is a reasonable time to modify the locking time of the next nLocktime, for example, after locking for one year.

6.nLocktime, also known as LockTime or lock_time, is usually set to 0, indicating that the transaction can be sent to the network at any time. If the value of nLocktime is between 1 and 500 million, it means that the block chain can be written only when the block whose block height is greater than or equal to nLocktime is needed. If the value of nLocktime exceeds 500 million, it means that it starts from January 01, 1970, plus one time point after nLocktime seconds, that is, the Unix timestamp, for example, January 1, 2017 is 1483200000, if it is earlier than that time At this point, the transaction will not be sent to the Internet. Also note that the sequence field cannot be the INT32 maximum (0xffffffff), otherwise nLocktime is ignored.

7.A sends a transaction to B for transaction TX2. After the signature is obtained, it broadcasts TX1 to form a lightning payment channel and sends the above transaction TX2 to B. Please confirm with B that it will be returned after signing with the private key. After receiving the signature from B, A then re-signs it with its own private key to see if it is successful. If successful, the previous transaction TX1 can be exited to form a lightning-like payment channel. The TX2 transaction in the hand is kept well and may need to be retrieved by the radio after the lockout time expires.
In fact, A must be based on the trust of B, A can not manually construct the transaction TX1 not broadcast, but directly use the coin wallet software to send money to the 3CSm address. Then let B use transaction TX1 information to construct a fully signed back-to-back 1Bit address transaction with lock time, and B is signed and sent to A to keep A properly stored. The same kind of lightning payment channel can be formed, the technical requirement for A will be very low, but B needs to have sufficient credit, and the previous proposal does not require B to have any credit.

Fast and zero-rate use of transactions in lightning payment channels, and bidirectional channel implementation



After establishing a class lightning payment channel, when A needs to pay B currency, then one is sent from the 3CSm address to 1Dog.

One-to-two transactions TX3 with address and 1Bit address. Sign the signature with its private key and send it to B. When B gets a signature transaction

After TX3, it is already equivalent to confirming to get the coin. And this speed is just to generate transactions and transfer strings can be done in seconds, even under some tools can do real-time payment.

2.1.2 The specific application of Tianzun payment

If A transfers 0.1BTC to 3CSm address, A needs to pay 0.02 BTC to B, then construct a transaction TX3 to B with 1Dog address of 0.02 BTC and change to A's 1Bit address of 0.0799 BTC, and 0.0001 BTC as processing fee . A is signed with a private key and sent to B. After B receives the signature and then signs it with B's private key, it confirms that there is no problem by checking A's signature. That is, it is confirmed that the payment of 0.02 BTC has been received and there is no need to broadcast this transaction TX3. You can continue to maintain lightning-like payment channels.

Then after a few days, when A is required to pay B again this time to 0.03 BTC, plus the previous total is 0.05 BTC, then once again to construct a TX4, this time to send B to the 1Dog address of 0.05 BTC. 0.0499 BTC to the 1Bit address of A. After the signature is sent to B, it can be confirmed in seconds, and because there is no chain on the chain, there is no fee.

Note that it may be discovered that this class of lightning payment channel is one-way, but A pays for B, then what should be done when reverse B needs to be paid to A? The above steps can then be repeated to establish classes between AB. Lightning payment channel, pay attention to swap AB, and use another 2-of-2 multi-signature synthesis address 3Njd address as the main address of the class lightning payment channel, the main control of this address is B, can be B to sign The transaction is sent to A to realize B to A. In fact, this two-channel implementation of two-way will be more clear.

Essentially because the lock-time transaction TX2 exists, the coin on the 3CSm address belongs to A. The coin on the 3Njd address belongs to B. In the case of class-like lightning payments, A can sign the transaction TX3 to redistribute the currency at the 3CSm address and assign the currency to be paid to B to B. As long as the signature transaction TX3 is obtained, it is already available as soon as the lock time is announced. That is, there is no need to immediately publish and close the channel. Frequently, both parties send and receive transactions only by sending the latest signed transaction. Even if these data are obtained by a third party, it is useless and the broadcast cannot be released because there is only one. signature.

2.1.3 Two Closed Forms of Payment Channels

There is no class-like lightning payment transaction between A and B. After the lock-in time has expired, A can broadcast the transaction TX2 to get all the money back at the 3CSm address, thereby closing the channel. A loses only the lock-in time and a little processing fee. There is no big loss. The next time you turn it on, you can only open B that is likely to pay for the higher frequency, and set the lock time as long as possible. This kind of no use can be used to turn off the Lightning-like payment channel.

A has redistributed 3CSm addresses for some of the signed transactions that were sent to B by the Lightning Payment Channel transaction multiple times. Before the lockout time arrives, B signs the most favorable and generally up-to-date signature transaction, and then broadcasts itself after re-signing, so that the settlement is successfully closed on the lightning payment channel chain.

Then if there is a class-like lightning payment request, the above steps can be repeated and the 2-of-2 multi-signature synthesis address 3CSm address can be used without being replaced. Since the transaction ID in TX1 and the transaction IDs of TX2 have changed since this repetition, the previous signatures will be invalidated, so there is no need to worry about the transaction signature of the last class lightning payment channel. The new class lightning-like payment channel has an impact.

2.2 The core design of the RouPay Network:

2.2.1 Multi-Signature and Composite Address Generation

The multi-signature synthesis address is an address starting with 3, and the address at the beginning of the 3 is Mr. Cheng's acquisition of the contract script, and then the hash160 algorithm is executed on the contract script, and then it is encoded with the 0×05 version of Base58Check. . To spend the coins in these composite addresses, it is necessary to sign multiple private keys according to the requirements of the contract script created at the time of generation. Therefore, the composite address is often called a multiple signature address. In fact, specifically looking at the specific contract scripts that were created at the time of generation, some scripts can be set to require only one signature, not necessarily multiple signatures. Because it is generally composed of multiple public keys, the named composite address is better.

The multi-signature create multisig command generates a synthesis address. The generation of the "contract script" content is critical and can be generated using the createmultisig command. This command uses a wide range of applications and is very flexible, but it is very simple to use. There are only two parameters that must be entered:

One parameter is the number M, which is a positive integer and requires that M be no larger than N in the following parameters. The other parameter is an array of length N, that is, the number of public keys placed in the array is N.

The specific meaning is that any M of the private keys corresponding to the N public keys need to be provided when spending. If M=1, then the private key corresponding to any one of the public keys in the following array can be spent. If M=N, it means that all private keys must be signed to be able to spend money. The intermediate situations of these two extreme situations are often used more often.

The commonly used 2-of-3 multi-signature synthetic address generation method is that the first parameter M is set to 2, and in the second array parameter, 3 public keys are put, then the generated synthesis address is As long as any two of the private keys corresponding to the three public keys are signed, the transaction can be spent. There are also many applications in the field of e-commerce. Buyers, sellers, and platforms can each have a private key. Buyers and sellers can usually sign up for two signatures. When a dispute arises, the platform can use its signature to arbitrate to determine the allocation of currency.

2.2.2 Allocation of gold signatures to redistribute payments

This distribution is the key to achieving the payment channel. Specifically, the above-mentioned multiple signatures are used. Specifically, the 2-of-2 multi-signature is generated. In other words, the two-address can be traded only when a consensus is reached between the two addresses. The parameter M is set to 2, and the public key array is filled with two public keys. When both parties agree to sign the agreement, they can move the distribution in the 2-of-2 multi-signature synthesis address.

Lightning network and lightning network channel design ideas are both, the two sides jointly issued a certain amount of funds to form the distribution of gold, and then give the distribution of the number of each currency. Then sign the common signature to update this allocation scheme. The same is the design of some mechanisms to eliminate the historical distribution before. The difference between the latest allocation plan and the last allocation plan is the amount of money paid by the channel. Because only the signature is required, the verification is correct. It only needs to be sent to the other party and does not need to be broadcast on the main network. Therefore, the second confirmation can be realized. Although the opening and closing of the channel requires a certain fee, the transaction on the channel after the channel is established can be completely free or at a very low cost.

Tianzun payment network is also the basic principle for allocating gold channels and signing for redistribution, but it will be simpler and easier to understand and easy to implement.

2.2.3 Tianzun pays one-way channel establishment

In simple terms, the sender and the receiver, the sender sends the coin to the public key generation address of both, and then realizes the payment by increasing the distribution ratio to the recipient by multiple times. The other is that there is a timestamp transaction, and after the time has passed, all the money in the distribution can be returned to the sender.

This channel is unidirectional, only when A needs to pay B coins, and the amount allocated to B will increase. When B needs to pay to A, he needs to use 3Njd address to establish a reverse channel. Two channel interactions can be paid in both directions. And when the quota is exceeded the channel will close. Also note that you need to turn off the payment channel before nLocktime. Note that changing the nLocktime lock time to a reasonable time nLocktime, also known as LockTime or lock_time, is usually set to 0, indicating that the transaction can be sent to the network at any time. If the value of nLocktime is between 1 and 500 million, it means that the block chain can be written only when the block whose block height is greater than or equal to nLocktime is needed. If the value of nLocktime exceeds 500 million, it means that it starts from January 1, 1970, plus a time point after nLocktime seconds, that is, the Unix timestamp, for example, January 1, 2018 is 151,4736000, if earlier than that time At this point, the transaction will not be sent to the Internet. Also note that the sequence field cannot be the INT32 maximum (0xffffffff), otherwise nLocktime is ignored.

1) Collect the respective public keys of A and B to generate a multi-signature address for two days of payment

Assuming that A is the sender and B is the receiver, the public key can generate two 2-of-2 multi-signature synthesis addresses after the public key is exchanged. The public key is information that can be publicized, and can be published on its own initiative or online. Quickly generate a synthesized address.

2) A constructs a transaction TX1 to the contract address, and sends back the transaction TX2 from the composite address lock time to B

3) A sends a transaction to B for transaction TX2. After obtaining the signature, TX1 broadcasts the channel for lightning payment and sends the above transaction TX2 to B. After B confirms the error, the private key of 1Dog will be used for signature and sent back to A. After receiving the signature from B, A then signs itself

with the private key of its own 1Bit address and checks whether it is successful. If the TX2 check succeeds, the previous transaction TX1 can be sent out, thus forming a class lightning payment channel. The TX2 transaction in the hand is saved and you may need to broadcast it out after the lockout time expires.

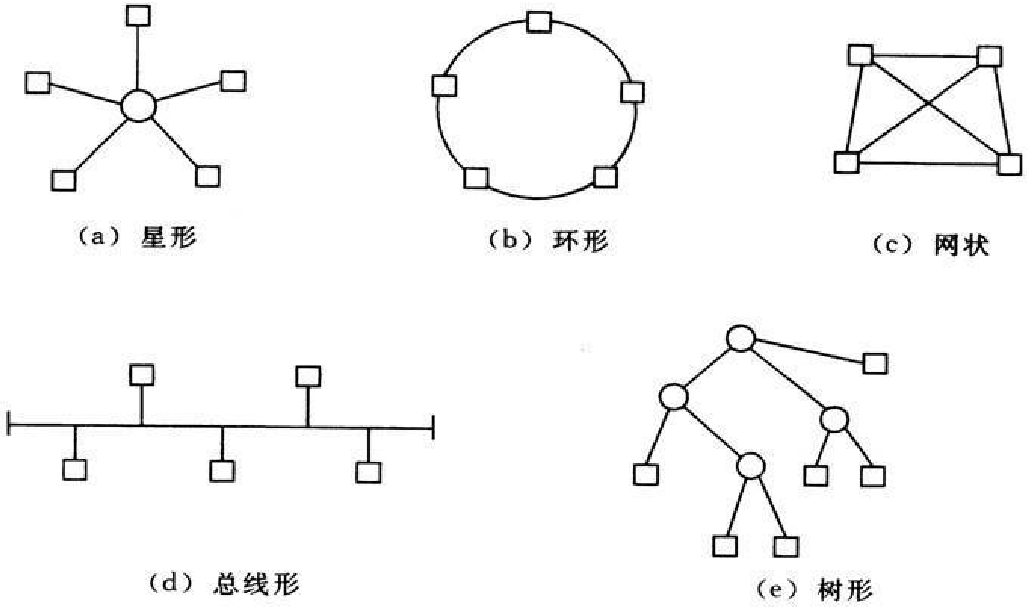
2.2.4 Days of payment channel to achieve two-way and cross-chain

This 2-of-2 multisignature equals the one-way payment of the network electrical channel. This may be the biggest difference from the lightning network. It can only increase one-wayly from one direction to the other. If you want the two sides to turn each other, you need to establish two independent channels. The Lightning Network can be increased or reduced, and can be completely redistributed, and can be increased or decreased. As long as both parties have signatures, the latest allocation scheme will prevail, and any previous allocation scheme will be invalid. The class lightning payment has no chronological order and is valid. However, as a recipient, of course, it will take the most money, and it is generally the most up-to-date distribution plan of its own. The sender of the coin cannot publish any of the allocated versions because he does not have the signature of the receiver. Wait for the time stamp, or wait for the cashier to close.

Because as long as there is support for multiple signatures, time-stamped transactions can achieve the payment channel, so you can A to B is the Bitcoin dear payment channel, and B to A is the dog-Dollar payment channel. So it is equivalent to achieving cross-chain and secure currency transactions.

2.2.5 Hierarchical tree topology of the payment network

In the network topology, the third-party payment will be (a) a star, and the peer-to-peer bitcoin will be (c) the network status. The Lightning Network estimates that the early possible bell pepper (b) ring has a six-stroke chain, and our Tianzun payment network will be barely similar to the tree


（a） 星形

（b） 环形

（c） 网状

（d） 总线形

（e） 树形

The principle of payment of Tianzun's payment is to initiate 2of2 multiple signatures, after which a time-delayed transaction for the return of all currencies is initiated. By sending the signature of the transaction, gradually increase the distribution to achieve one-way fast payment. The establishment of two channels because they only need to send the signed string, do not need to broadcast, and then can achieve a fast real-time and 0 fee transaction.

2.2.6 Tianzun payment network payment path design

The root node will be responsible for cross-branch transactions, so if only one layer is similar to a star-row network, it goes through 1 node. The two-tier network, up to the middle 3 nodes. The maximum number of Layer 3 networks is 5 in the middle. The N-layer network has a maximum of 2N-1 nodes. It is the first-to-upper layer to the root node. Go to the goal again. If it is in the same branch, it does not need to be up, similar to the domain name resolution service.

The root node can store all the latest data here, and periodically check settlements with the lower nodes.

2.2.7 Application in Special Situations

Tianzun payment node to deal with problems:

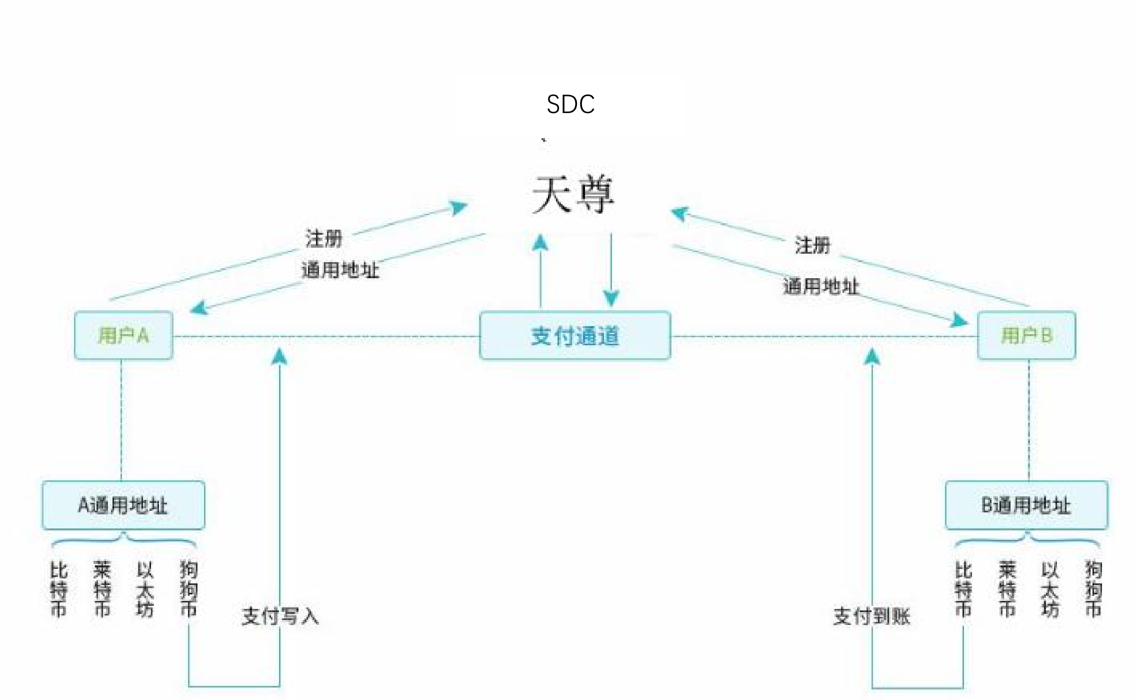
Because 2of2 requires the signature of both parties to move the currency, even if a large number of nodes have problems, there will be no financial loss.
There is no class-like lightning payment transaction between A and B. After the lock-in time has expired, A can broadcast the transaction TX2 to get all the money back at the 3CSm address, thereby closing the channel. A loses only the lock-in time and a little processing fee. There is no big loss. The next time you turn it on, you can only open B that is likely to pay for the higher frequency, and set the lock time as long as possible. This kind of no use can be used to turn off the Lightning-like payment channel.
A has redistributed 3CSm addresses for some of the signed transactions that were sent to B by the Lightning Payment Channel transaction multiple times. Before the lockout time arrives, B signs the most favorable and generally up-to-date signature transaction, and then broadcasts itself after re-signing, so that the settlement is successfully closed on the lightning payment channel chain.
Then if there is a class-like lightning payment request, the above steps can be repeated and the 2-of-2 multi-signature synthesis address 3CSm address can be used without being replaced. Since the transaction ID in TX1 and the transaction IDs of TX2 have changed since this repetition, the previous signatures will be invalidated, so you do not need to worry about the transaction signature of the last class lightning payment channel. The new class lightning-like payment channel has an impact.

2.2.8 Cross-Chain Trading Using MHT Technology (Matching hedge Technology Matching Hedging Technology)

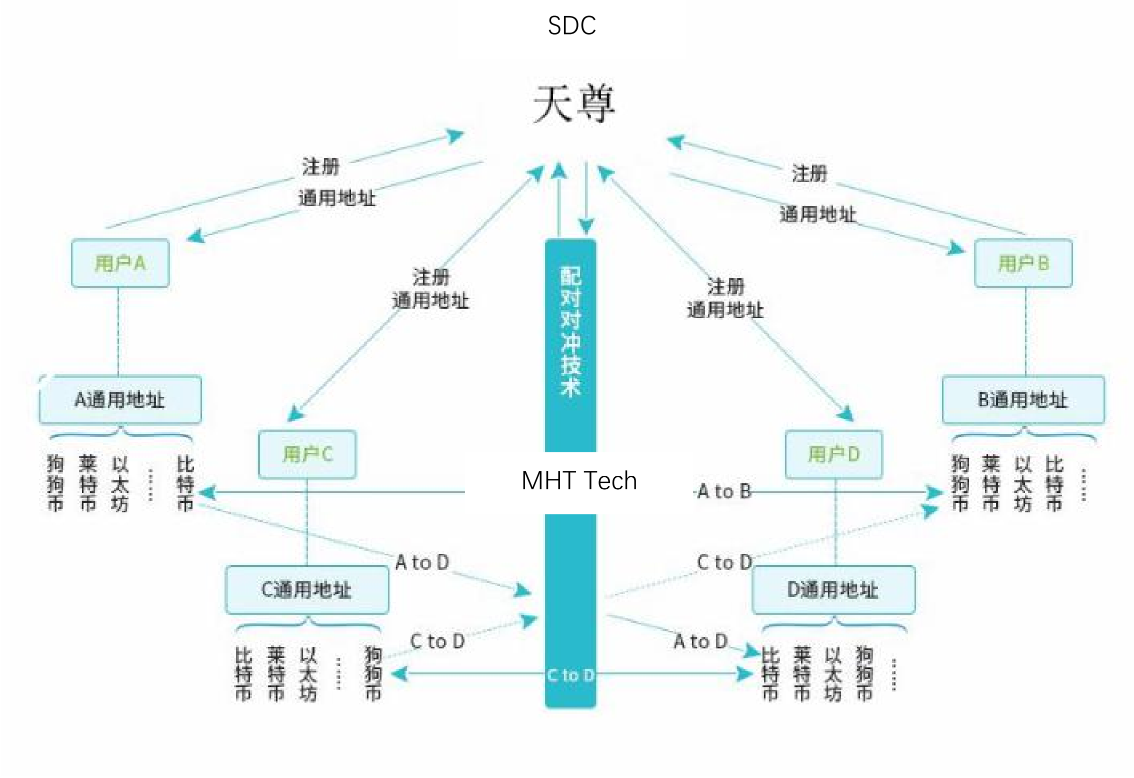
The Sky Dynasty Coin wallet client connects the user to the "RouPay Network", and the "RouPay Network" links the various users as the middle tier.
Specific case: Take the cross-chain transaction between dog currency and bitcoin as an example. The specific process is as follows:
Users obtain their own universal address in the RouPay Network through universal address technology. There is a one-to-one correspondence between dog coins and Bitcoin.

l In a single-user scenario, A pays B's btc with the dog's coin, Sky Dynasty Coin anchors the latest transaction data, and builds the Tianzun payment channel, multi-signature technology, and completes the transaction at Sky Dynasty

Coin. Broadcast transactions to the corresponding blockchain system. The flow chart is as shown below:



II In the multi-user scenario, paired hedging technology is used. A uses btc to pay B's dog's money, and at the same time someone may use dog'd to pay D's bitcoin. So you can match hedges in the past, A pays D, C pays B.

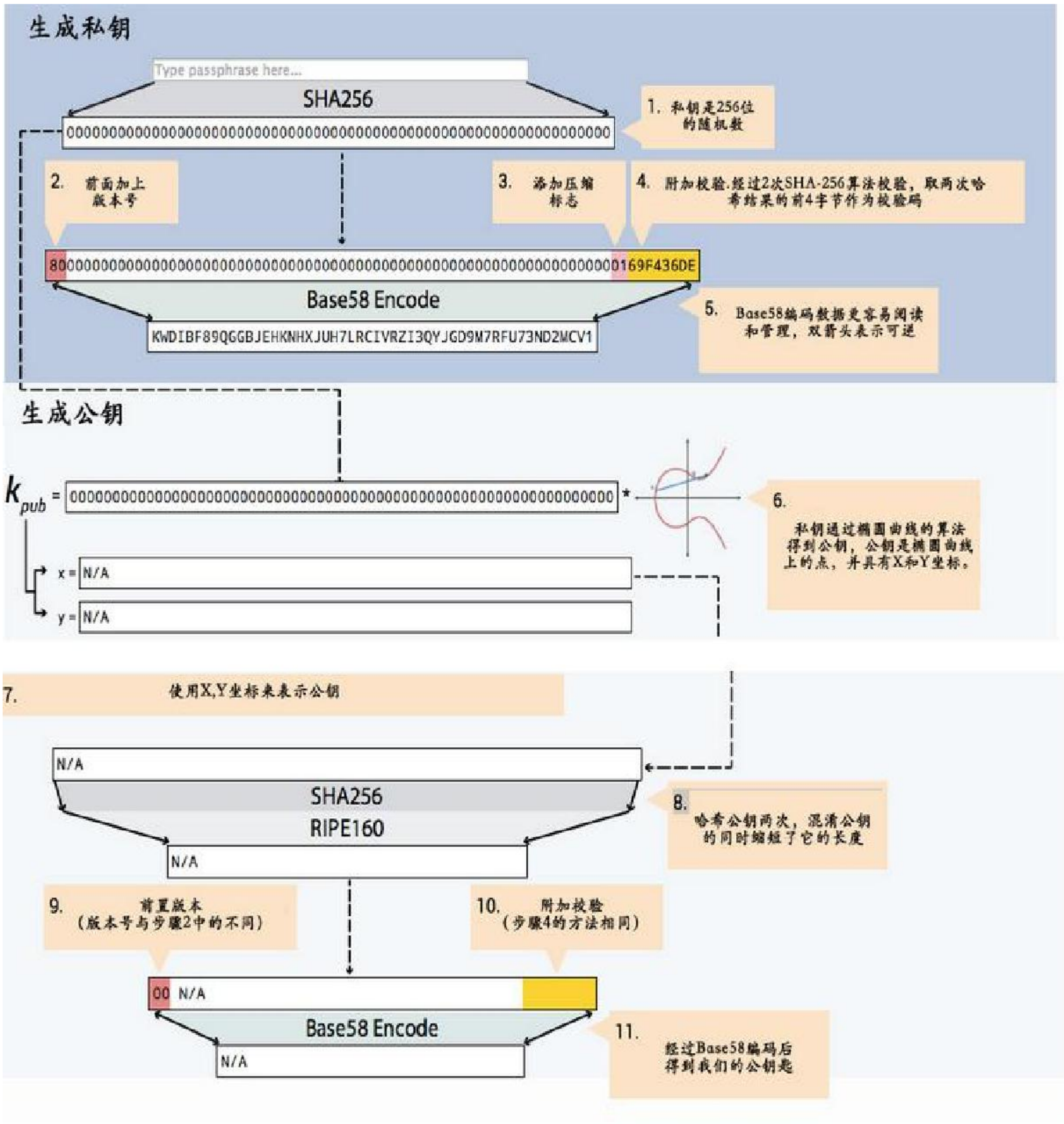


2.3 Universal Address: A Universal Address Can Receive and Send 95% of Encrypted Digital Currency

2.3.1 The principle of traditional address generation

General blockchain address generation needs to go through the following process:
Randomly select a 32-byte number as the private key, the number is between 1 ~ 0xFFFF FFFF FFFF FFFF FFFF FFFF FFFF FFFE BAAE DCE6 AF48 A03B BFD2 5E8C D036 4141
The elliptic curve encryption algorithm is used to calculate the non-compressed public key corresponding to the private key.
Calculate the SHA-256 hash of the public key, assuming A
Calculate A's RIPEMD-160 hash, assumed to be B
Add the address version number in front of B. The resulting value is assumed to be C
Calculate the SHA-256 hash of C, assuming D
Calculate the SHA-256 hash of D, Jiading E
Take the first 4 bytes of E, and load the 4 bytes behind C as a test. The result value is set to F. Use Base58 notation to transform F. The result is G, where G is the most common bitcoin address form. .

The specific flow chart is as follows:


生成私钥
Type passphrase here...
SHA256
0000000000000000000000000000000000000000000000000000000000000000
1. 私钥是256位的随机数
2. 前面加上版本号
3. 添加压缩标志
4. 附加校验.经过2次SHA-256算法校验，取两次哈希结果的前4字节作为校验码
8000000000000000000000000000000000000000000000000000000000000000000169F436DE
Base58 Encode
KWDIBF89QGGBJEHKNHXJUH7LRCIVRZI3QYJGD9M7RFU73ND2MCV1
5. Base58编码数据更容易阅读和管理，双箭头表示可逆
生成公钥
k_{pub} = 0000000000000000000000000000000000000000000000000000000000000000 *
x = N/A
y = N/A
6. 私钥通过椭圆曲线的算法得到公钥，公钥是椭圆曲线上的点，并具有X和Y坐标。
7. 使用X,Y坐标来表示公钥
N/A
SHA256
RIPE160
N/A
8. 哈希公钥两次，混淆公钥的同时缩短了它的长度
9. 前置版本（版本号与步骤2中的不同）
10. 附加校验（步骤4的方法相同）
00 N/A
Base58 Encode
N/A
11. 经过Base58编码后得到我们的公钥匙

2.3.2 specific case: mutual transformation between addresses

The public keys of Ethereum, Ethereum-based tokens, Bitcoin, and the currency addresses of mainstream currencies on the market, and the number of 40 hexadecimal digits obtained for SHA-256 and RIPEMD-160 are the same. The difference between the addresses of different currencies is different from the pre-version area shown in the figure number 9 in Figure 2.1 above. For example: Bitcoin is 0x00 in this area, dog is 0x1E, and Litecoin is 0x30.

After understanding this process, mutual conversion between currency addresses can be achieved.In the case of a dog dog coin, for example, the reverse encoding of Base58 is performed at any of the other bank addresses shown in the process 11, and the first two hexadecimal version numbers and the last 4 bytes of the checksum are removed and transferred as needed. Add the front version 0x1E of the corresponding currency and the calculation plus an additional test, and then pass the Base58 Encode to get the corresponding dog currency address.

2.3.3 Design and Application of General Address

1) The currency address Base58 decode, decoded into hexadecimal
2) Remove the first two hexadecimal version numbers and check later
3) Traverse the various version numbers and use Base58Check to perform a checksum code.
4) The checkout currency address that meets Base58Check is supported by the currency system and can be used to receive coins.

3. Expanding the application

3.1 P2P Lending

3.1.1 Point to point

Point-to-point (P2P) lending is now showing a hot trend in the payments industry. In fact, because of convenience, low interest rates, and stable return on investment, P2P lending has become the fastest growing financial technology industry. By using blockchain technology, borrowers can obtain loans directly and require the intervention of traditional banks or financial institutions.

3.1.2 Balance

Blockchain technology can make you safer and more convenient when lending money to friends through applications or social accounts such as Facebook or Twitter. Balance is a fixed quantity and can never be increased. The balance of origin is divided and transmitted to other sections. The sum of the balances of all accounts will never exceed the initial creation balance, which gives the system a quantitative limit. There is no ability to increase it.

3.1.3 Remittances

Rate: The World Bank estimates that the average global remittance cost is 7.5%, while the commercial bank is more than 10%. If this can be reduced to 5%, global consumers will save $16 billion annually.

By removing the involvement of third-party agencies, the blockchain can allow mobile users to transfer money to anyone in the world without paying high fees for services and transactions. Some companies, such as Abra and Coins.ph, have already achieved this.

3.2 Protocol Security

Multiple accounts transmitted to the same target account are asynchronous operations; network latency and sending accounts do not necessarily communicate with each other implies t. There is no universally accepted way to know which transaction is the first occurrence. Since the additions are linked, the order of the inputs is not important, so we only need a global agre. Mente. This is a key design component that converts the runtime protocol into a design-time protocol. The receiving account has the right to determine which transfer is first and is represented by the following:

The signature order of the incoming blocks.

If an account wants to make a big transfer and receives a group of many small transfers, we want to express this in a way that suits UDP packets. When the receiving account is in storage, it maintains the total number of runs for its account balance so that it has the ability to transfer any amount with a fixed-size transaction at any time. This is different from input/output transmission. Some nodes are not interested in using the full block history of resource storage accounts; they are only interested in the current balance of each block. When an account establishes a new blockchain, it encodes its cumulative balance. These nodes simply keep track of the latest blocks and can discard historical data while maintaining the correct logic.

Encryption: Even if the focus is on designing remittance agreements, due to the identification and handling of bad actors in the network, there is still a delay window when verifying transactions. Now that the agreement is reached in Tencent, we can provide users with two common types of incoming transactions, in the order of milliseconds to seconds: resolved transactions and unresolved transactions. A settlement transaction is a term used in a transaction. Received block has been generated. Transactions that have not yet been settled have not yet been credited to the receiver's accumulated balance. This is to replace other encrypted blockchains with more complex and unfamiliar confirmations.

3.3 Mobile Wallet

3.3.1 Number Trading

As we mentioned before, because of the mobile wallet, cash and checks will become artifacts, and even plastic products will become the past. Using Apple Payments, Samsung Payments, Android Payments, and retailer-provided digital wallets (such as Womatte) bring convenience and ease that are deeply appealing to mobile users.

To create an account, you need to send an open blockchain. Public transactions are always the first transaction in each account chain and can be created after the first time funds are received. The N-type account field stores the public key (address) derived from the private key used for signing. The source field contains the hash of the transaction that sent the funds. For the creation of an account, you must select a representative to code on your behalf; the account can declare itself as a block code.

However, the biggest obstacle to overcome is safety.

Blockchain technology has many functions, such as verifying shopping information through multiple signatures, and blockchain technology will make mobile wallet more secure. Blockchain technology can also increase speed and improve the user experience. Using mobile wallets can also reduce the cost of global payments.

3.3.2 Classification Calculation

The account balance is recorded in the ledger itself. Instead of recording the transaction amount, you also need to check the difference between the balance of the forest office. The balance of the block and the previous block. The receiving account can then increment the previous balance into the final balance given in the newly received block. This is done to increase the processing speed when downloading a large number of blocks. When the account history is requested, the amount has been given.

To send from the address, the address must already have an existing open block. The previous field contains the hash of the previous block in the account chain. The large segment contains the funds account to send to. Once confirmed, the sending block is immutable. Once broadcast to the Internet, the funds will not be recovered immediately.

Deducted from the balance of the sender's account and wait until the recipient signs a block to accept the funds.   Pending funds should not be considered to be confirmed because it is as good as it is from the sender's account, and the sender cannot withdraw the transaction.

```
send {previous: 1967EA355...F2F3E5BF801,
    balance: 010a8044a0...1d49289d88c,
    destination: xrb_3w...m37goeuufdp,
    work: 0000000000000000,
    type: send,
    signature: 83B0...006433265C7B204}
```

3.3.3 Awards and Loyalty Program

Consumers like to be rewarded in the process of commercial shopping.   Mobile has already proven to be a good platform for providing and managing incentives. Ask Starbucks about it. Blockchain technology can improve the way points are traded because all transactions are recorded in a public ledger and all merchants can monitor point transactions. However, this is still difficult to achieve.   For example, you can send your Starbucks or airline points to your spouse with just one click.

Account holders have the ability to choose a representative representative to vote on their behalf. This is a powerful decentralization tool that does not have strong simulation capabilities in proving work or proving interest agreements. Combined into a traditional blockchain, the account owner's node must run to select. For many users, it is not practical to run the nodes continuously; delegates are given selective power over a node. The account holder must re-allocate the block link to any account at any time. Change the subtractin change account of the transaction. There is no transfer of funds in this transaction and there is no spending power.

This occurs when the checked block declarations are the same as their previous ones.

```
change {previous: DC04354B1...AE8FA2661B2,
    representative: xrb_1anrz...posrs,
    work: 0000000000000000,
    type: change,
    signature: 83B0...006433265C7B204}
```

3.3.4 No bank account required

Whether you live in the United States or Nigeria, millions of people still do not have bank accounts. However, now only one smartphone is needed and no bank account is required. One can participate in global e-commerce via blockchain, get a loan, or make a secure transfer to a friend or family member without paying high fees.

Conflicts that result in account status must be resolved. Only the owner of the account has the ability to sign the block in their account blockchain, so the fork must be the result of the wrong program. Account owner's mining or malicious intent (double expenses).

The blockchain is entered in the classified account and broadcast to the network is the sum of the balances of the accounts represented by all the designated nodes. The node will keep accumulating the winning bid blocks (formulas) for block chains represented from other lines.

M

X_i

$$v(b_j) = \quad w_{i1^\wedge} \qquad (1)$$

$b_i=b_j$

$=1$

$$b = \arg\max v(b_j) \qquad (2)$$

b_j

3.4 Development of Wearable Devices and Internet of Things

The scope of payment is going beyond smartphones and tablets. Wearable devices such as watches, bracelets and rings have already appeared on the market. In addition, the Internet of Things is also expanding. With blockchain technology, users can store their payment information without fear of fraud.

However, what's most interesting is how easy blockchain technology will make for future payments. For example, in the future, you walk into a store to buy milk:

"Shake your hand. Your smartwatch can detect the translucent password on the milk carton, and then execute a hash function. Milk will immediately turn into yours."

For the IoT, developers can use blockchain technology to patch application program interfaces (APIs) to simplify the connection between all your devices. Imagine that after your milk is consumed, the refrigerator can automatically order and complete the payment.

4. Attack prevention

The longer the attacker holds the old private key, the higher the probability of balance because their b-level representatives will not participate. Has moved to a newer account. This means that if a node is directed to the old representation of the network, and the attacker is relative to then, delegates will be able to oscillate and vote on that node. If this new user wants to interact with anyone other than the attacking node, all their transactions are processed. NS will be rejected because they have different head blocks. The net result is that nodes can waste time on new nodes in the network by providing bad information to new nodes. To prevent this, pair the nodes to w. It is an initial database of accounts and well-known chunks; this is an alternative method for downloading the database and then returning back to the cause block. The closer to the current download, the more likely he is to defend this attack.

Finally, this attack may not be worse than providing junk data to nodes at boot time because they cannot deal with anyone who has a contemporary database.

We live in a highly regulated and monitored world and billions of individuals are deprived of basic human rights such as property ownership, privacy, freedom of association, and access to information. There are already some techniques for solving these problems. The early realization of Tencent coined exactly this way. Account holders have the ability to choose a representative representative to vote on their behalf. This is a powerful decentralization tool that does not have strong simulation capabilities in proving work or proving interest agreements. It can use OpenCL compatible GPUs. Provides a realistic benchmark comparison of various hardware. The current PoW threshold is fixed, but the adaptive threshold may be implemented. With the improvement of average computing power.

The main defense method for 51% of attacks is that voting rights are linked to system investment. The account holder is an intrinsic incentive system that maintains honest protection of the heir investment. Trying to look through the ledgers will damage the entire system, which will undermine their investment. The cost of this attack is proportional to the market capitalization of the nanometer. In power systems, technologies that give disproportionate control over monetary investment can be invented, and if the attack is successful, it can be reused after the attack is completed. For Tencent, the cost of the attack system and the system itself and if the attack is to be successful, the investment in the attack cannot be recovered.

In order to maintain the highest quorum for voters, the next line of defense is representative voting. Account holders who cannot reliably participate in the voting due to connectivity can say that they can vote with balanced power. Maximizing the number and diversity of delegates can increase the flexibility of the network.

5. Prevent congestion

The fork in the Zenith is never accidental, so the node can make decisions about how to interact with the forked block. The only situation where non-attacker accounts are vulnerable to blocked fork attacks is whether they receive bl. From the attack account. An account that wants to secure from a fork can wait longer or longer before it is received from a forked account, or choose never to receive it. Re When receiving funds from suspicious accounts, Cerivas can also generate separate accounts to isolate other accounts.

The last line of defense that has not yet been implemented is blockage. Tencent coin quickly resolved the fork problem by voting. Nodes can be configured, and after a period of time, UD prevents them from being rolled in. The network prevents the full safety of the ambiguity fork by focusing on rapid settling time.

6. Team

Liu Quanlun
Software engineers have a number of individual patents.
Proficient in Java and other development languages, for Bitcoin, Ethereum and other blockchain development in-depth research.

Shi Zhaoqing
Famous Blockchain Expert
Back-end development engineer, years of e-commerce, social mobile application design and development experience, is an important communication hub in the team

Matthew Browndorf
Founder / CEO of Plutos Sama
MD Partner of EKB Law Firm
Distiguished Member of Lawyers of Distinction

Daniel holds a bachelor's degree in language and is fluent in several languages. He has lived in the United States, Britain, Italy, Germany, United Arab Emirates and China. He has visited more than 30 countries and has extensive overseas relations. He is also an active user on the BTT Forum. He has translated many technical documents and has many fans on the BTT Forum.

CARLOS CHOONG Malaysian Chinese, who has worked for many years in the Hong Kong financial company and has lived and worked in the United States and the United Kingdom. He has extensive overseas relationships. CARLOS CHOONG has extensive experience in the traditional financial field. He is also an old Bitcoin player and has large mines in the Malaysian capital of Kuala Lumpur. field.

7. The ultimate goal of SDC

One of SDC's goals is to achieve at least $3 billion in tokens in the market within three years.

More than 10 applications were launched in three years, accumulating millions of users and thousands of businesses.

Safety traceability profit in four years. The company will be listed seven years later.

Conclusion

This paper proposes a cryptosystem with no trust, no emotion, and low delay. It adopts a new grouping grid structure and presents a certificate of entrustment for equity voting. The network requires MI NIML resources, no high-power mining hardware, and can handle high transaction throughput. All of this is achieved by setting up a separate blockchain for each account, eliminating access issues and efficiency in the global data structure. We have determined the possible attack vectors on the system and put forward arguments on how the ego can resist these forms of attacks.