TXN white paper

(1)

➢ Chapter One introduction and overview

(An ultra-anonymous currency dedicated to protecting privacy)

Since Mr. Nakamoto coined the concept in 2009, Bitcoin has quickly spread to mainstream and commercial USES, becoming the first digital currency to attract a large number of users

The rapid development of the Internet has made the flow of information become very efficient, thus promoting the development of human society. On the other hand, the privacy problem has become more serious because of the rapid development of the Internet. Blockchain, as the next generation of value Internet, was once regarded as a very good tool to protect privacy,

But they soon found that the current main block chain network, a denier digital wallets address that of the personal information and its owner, the owner of the wallet all account information, transaction information will be in the entire network and cannot eliminate, this can lead to more serious problem than the privacy of the Internet.

Privacy protection is a very strong demand for the blockchain industry.

TXN focuses on privacy, decentralization, and extensibility. TXN is based on Mrypto protocol. TXN has a higher degree of anonymity. The Mrypto protocol makes TXN highly anonymous, sender and untraceable

Recipient, not linked, hidden transaction amount. Anyone, anywhere in the world, can complete transactions quickly, easily and cheaply at any time.

TXN also USES a zero-knowledge proof blockchain system that provides full payment confidentiality, while still using a public blockchain to maintain a decentralized network.

➢ Chapter two team introduction

Team to distinguish

Matrix + Matrlx = (MatrixTXn), we are dividing the key members of the MatrixTXn team into the Matrix group and the matrlx group, which is being used to distinguish their contribution to the project development

The team members

Team members of TXN are from China Hongke League, former core members of hawkish League and global top blockchain geeks, and team members are from LIZARD SQUAD, ANONYMOUS, TEAMP0ISON and other well-known blockchain geeks.

Currently, the team has assembled dozens of geeks, and the organization is officially named (MatrixTXn)

➢ Chapter THREE TXN token allocation

The total circulation of TXN is only 9999999

5% early community airdrop

(Token dropped by air will be divided into several times, used for community air drop, volunteer recruitment, excellent member award, etc.)

5% team held

(TXN held by the team is frozen, and 10% will be thawed year by year on the main network)

10% community ICO

(We will conduct community ICOs year by year, and the funds will be used for emergency fund of the team)

Eighty percent is produced by mining

(TXN supporters can use GPU, professional mining machine and other higher computing power equipment for mining,

To get TXN)

Compared with TXN, which adopts another method to reduce the inflation caused by mining,

That's a 7% cut in annual supply, unlike the halving of other digital currencies.

In addition, the supply of each block is directly related to the number of miners in the whole network,

More miners means fewer rewards for digging.

(4)

➢ Chapter IV Development Plan

2019 - Q3
Matrixtxn team member founded

2019 - Q4
TXN formally completes the project setting

2020 - Q1
TXN MRypto protocol test completed

2020 - Q2
Mrypto protocol construction completed

2020 - Q3
2020/6
Early construction of community members was completed

2020/9
TXN test network run

2020 - Q4
TXN began global layout promotion

2021 - Q1

TXN TXN-1Wallet standard customization complete

TXN main network was officially launched

(5)

➢ Chapter 5 Technical introduction, Mrypto protocol

(1) Mrypto agreement

There are two types of account systems: user accounts and contract accounts. The user account is a 32byte address selected by the user, while the contract account generates a 64byte address according to the environment in which the user installs the smart contract. Both are unique and non-repeatable.

The user account can generate a 64byte private key and a 64byte public key, which is the user's payment address. When the smart contract is installed or invoked, the wallet generates a staging address based on the current situation that is not somehow associated with the user's private and public keys and will only be used once.

When the smart contract is installed, the wallet will convert the temporary address to the 64Byte smart Contract address (CADDS), depending on the current situation. When the node receives the address, it needs to make sure that the smart contract address has not appeared before

Let: Gk =NewEcc seed =New(Byte32) r =RandFr S =RandFra =RandFr M =Message

SK: ZSK =HASHzsk(seed) VSK =HASHvsk(seed) SK =(VSK, ZSK) ZVSK = ZSKVSK

PK/TK: ZPK=zskGk VPK= (ZPK,VPK) TK=(ZPK, VPK)

ZSA is an account seed that must be properly stored by the user. Is the private key, non-persistent storage, where is the tracking private key, can be provided to a trusted third party to use as an account audit. Is the public key that provides the address of the transaction destination to other users. Is a staging address, provided to an intelligent contract, that is used to temporarily receive assets.

Assets System

Input Construct

Is the value of the leaf node of the Merkle tree composed of UTXO sequence columns; Is the root of the current Merkle tree, used to locate input data; And the authentication path from to; Is a 32-bit hash string used to invalidate OUT in UTXO; Is a 32-bit hash string used to track transaction input; Is the asset commitment entered into the transaction.

License System

In the Alpha and Beta networks of Mrypto, it was necessary for the Mrypto project team to coordinate each miner node in order to ensure the initial healthy development of the network, ensure the robustness of consensus and timely update of the system. Therefore, testers with mining needs need to apply for the mining license from the Mrypto R&D team. License is not required for testing other functions other than mining. As long as the miner's identity is not revealed, the block will reveal some of the attributes in the License,

These attributes can be monitored by the Mrypto community. In the early stage of Beta network, when the network is attacked and there is a major crisis, matrixTXN team will adopt unconventional means to resist attacks through community voting, under the premise of community permission and supervision, and ensure the property security of community members. The license will be removed six months after BetaNet goes online.

The Witness System (Mrypto) protocol USES non-interactive zero knowledge Proof (NIZK). When generating transactions, it is required to provide the evidence information of asset source, and each node will verify according to the Witness information. Therefore, Mrypto will use Merkle tree to maintain a witness system to record state changes. The system provides verification function at the node and information required for authentication at the wallet side.

It's the root of the current Merkle tree, it's the first one leaf, it's the proof path to.

Proof System

Rlic =RandFr rlic =rlicGlic Slic = Rlic + SKZPK *Hash(ZPK)+skprop*prop

PROVE: R + Hash (ZPK) PKzpk + propPKprop = slic Glic

The VERIFICATION system of Mrypto includes a directed acyclic graph based computing circuit to describe the internal constraints of each TRANSACTION of Mrypto, including input and output balance of various asset types, public-private key verification, validity of commitment, validity of witness and other links.

The circuit loaded with data can generate a Proof through non-interactive zero knowledge Proof (NIZK). By submitting the Proof, the nodes can verify various parameters and constraints loaded in the circuit under the circumstance of hiding a large amount of details.

It's the public data of the transaction, it's the private data of the transaction. All variables participate in the construction and prove the process of adoption and generation. The,,, validation process is then carried through and, to verify the transaction.

Process Step

Compute, the user takes the account, asset, witness the information provided by the system, provides the input data according to the currently required computation, and then runs the computation rule under the chain to get the result.

2. Prove. The result obtained by the calculation step and random number are packaged into a transaction by the user and submitted to the node. Contains validation data, result encoding data and proof data.

3. Verify. After the node receives the transaction, it will confirm it in the witness system and the proof system. After verification, the node accepts.

Acknowledgement (Conrm) : After the asset receiver synchronizes to the verified transaction, it USES its private key to solve the secret text into clear text and input the clear text and proof into the proof system for verification.

Success means the deal is real. If a real transaction is confirmed by n blocks, the receiving party of the transaction may consider that the transaction has been confirmed.

It should be noted that the execution steps of Mrypto are open-ended, meaning that such abstract descriptions of steps and parameters can support phase one to phase three additions described in the "Implementation Scenarios" section, with minimal code restructuring during subsequent upgrades.

General Privacy Transaction

Within Mrypto, data in ordinary transactions are encrypted, and non-trading parties cannot know the source, destination, asset type, amount and other details. The system does not distinguish between the assets generated by the smart contract and its own assets in transaction processing.

Online Intelligent Contract

Mrypto's general Intelligent contract can perform public calculation and formulate statistical schemes, disposal rules and publicity rules for various assets, but input and output information must be isolated from the user's real identity through temporary address.

The Mrypto smart contract is compatible with ethereum smart Contract instructions, meaning that most of Ethereum's smart contracts can run on the Mrypto without modification. Online privacy assets

The intelligent contract calls the assets issued by the online privacy asset. The total amount of assets is public and has transaction attributes equivalent to TXN coin, which can be processed through privacy transaction.

The offline intelligent contract of Mrypto is only run on the user's machine, the calculation rules are only visible to some users, and the correctness of the operation results is verified by consensus.

Mrypto's anonymous transaction Tx has an anonymous input set of 'Z Ins', an anonymous output set of' Z outs', a common output set of 'O outs' and a staging address called' From '.

Z Outs is completely anonymous, making it impossible for third-party observers to know the source and content, Z outs is completely anonymous UTXO, and only the recipient can view and use its contents. O Outs carries content that is not hidden,

It points to the recipient in one of two ways: to an intelligent contract address, or to a temporary address. From represents the sender of the transaction and is also a temporary address. Therefore, the whole Tx has no method for people to determine who the real user is, and the asset information carried in it is also hidden to the greatest extent

(2) Master node network

Full nodes are servers running on p2p networks, allowing small nodes to use them to accept dynamic changes from the whole network. These full nodes require significant traffic and other resources that consume a lot of cost, so a steady decline in the number of these nodes on the Bitcoin network will be observed over time,

Add an additional 40 seconds to block broadcast time. To solve this problem, a number of schemes have been proposed, such as the introduction of Microsoft's new incentive scheme and the Bitnodes incentive scheme. These nodes are important to the health of the network, allowing clients to synchronize and broadcast information quickly across the network.

We propose to add a secondary network called the TXNQ node network. These nodes will be highly available and will be rewarded with master node services if they meet certain requirements for the network.

(3) Master node incentive plan -- Cost and reward

The main reason for the sharp drop in the number of full nodes on the Bitcoin network is the lack of rewards for running nodes. Over time, there will be more users with full network access, higher demand for bandwidth, and higher capital requirements for node operators, resulting in higher costs for running full nodes. Given the rising costs,

Node operators must reduce their operating costs or run light clients, which is not healthy at all.

Just like the Bitcoin network, the master node is the full node, but the difference is that the master node must provide certain services to the whole network, and a certain amount of deposit is required to join. The deposit is not lost and is secure when the master node runs. This allows investors to provide services for the whole network at the same time, earn a certain amount of investment income, reduce price volatility.

To run a master node, you need to store 10000TXN. When the master node takes effect, it serves clients across the network and is rewarded in the form of interest. This allows users to invest in the service, but at the same time get a certain return. Revenue from the master node comes from the same pool, and about 45% of the block award is included in the program.

Given the fixed percentage of the master node reward rate and the fact that the master node network nodes fluctuate, it is expected that the master node reward will vary based on the total number of master nodes currently in effect. The following calculation formula can be used to calculate the income of running the master node for a whole day

(4) Untrusted Quorum

We created a system in which no one could control the entire master node network. For example, if someone wanted to control 50% of the master node network, they would have to buy 3 million TXNS from the open market. This would greatly increase the currency's value, so getting that much TXN would be impossible.

With the master node network and guarantee conditions, we use the sub-network in a non-trust manner for highly sensitive tasks, in which no one can control the evolution of the network. N pseudo-random master nodes from the total pool are selected to perform the same task. These nodes can act as referees without the involvement of the entire network.

For example, a faithless Quorum finds InstantSend, which USES Quorum to confirm transactions and lock inputs.

Another example is that untrusted Quorum could use a master node network as a decentralized predictor of financial markets, making decentralized contracts possible. For example, if the share price of Apple exceeds $300 on December 31, 2016, convention A will be filed; otherwise, Convention B will be filed.

(5) Master node protocol

The master USES a number of extended protocols to broadcast across the network, including the master announce mechanism and the master ping mechanism. In addition to the two mechanisms used to confirm that the entire network node is in effect, PrivateSend and InstantSend are required to perform the service volume verification mechanism.

By sending 10TXN to a specific address in the wallet, the activation code naturally generates a master node that can be broadcast across the network, followed by a secondary private key generation, which is used to sign all other information and can be used to lock the wallet completely when running in stand-alone mode.

Using secondary private keys on two separate machines makes cold mode possible. The main "hot" client signs the input to 10TXN, which involves signing the information using the second private key. The "cold" client can then discover the information containing the secondary private key and activate the primary node.

This invalidates the "hot" client (the client is closed) so that an attacker accessing the activated master node cannot get the 1TXN stolen from it.

When the master node starts running, "master node broadcast" information is sent to the entire network

(6) Anonymous payment

We believe that it is important to implement a standard non-trust system in order to enhance user privacy on the client. Electrum, Android, and iPhone clients, for example, also embed the same anonymity layer directly and take advantage of protocol extensibility. This gives users the same experience when sending money anonymously using a solid system.

PrivateSend is an improved and extended version of CoinJoin, software that provides anonymous technology. In addition to having CoinJoin's core philosophy, we have made a number of improvements, such as decentralization, strong anonymity using links, same-denomination, and passive advanced coin-mixing technology.

The biggest challenge in improving privacy and the interchangeability of cryptocurrencies is the inability to encrypt the entire blockchain. Within the Bitcoin-based cryptocurrency system, you can see which output is not sent and which is sent, often referred to as UTXO, or unused transaction output.

This allows each user to act as an honest trader in the public ledger. The bitcoin protocol is designed on the premise of not relying on the participation of third parties. Without the participation of third parties, it is crucial that users' information can be read at any time through the public blockchain to realize auditing.

Our goal is to improve confidentiality and interchangeability without losing these elements, which we believe is the key to creating a successful digital currency.

With decentralized mixed-currency services within the digital currency, we can make the currency itself fully interchangeable. Interchangeability is a property of money that determines the equality of the units of money.

When you receive money in currency, the money should not keep track of previous users, or users can easily dissociate themselves from previous users, so that all currencies are equal. At the same time, any user can ensure that every transaction on the public books is honest without compromising the privacy of others.

In order to improve the interchangeability and maintain the integrity of the common blockchain, we propose to use the advanced non-trust decentralized currency mixing technology. In order to maintain the interchangeability of currency, this service is directly integrated into the currency system, making it easy and safe for every user to use

(7) Strong privacy and DOS protection

Multi-party transactions can be consolidated into a single transaction, and PrivateSend makes good use of this by combining and sending out multi-party funds so that once consolidated, they cannot be split again. Given that the PrivateSend transaction is specifically set up for user payments,

This system is highly secure against theft and the user's currency is very secure. Currently, using PrivateSend's mixed-currency technology requires at least three parties to participate.

(8) Passive capital and blockchain anonymity

PrivateSend is limited to 10000TXN per round, and multiple rounds are required to anonymously mix a significant amount of money. PrivateSend runs in passive mode to make the user experience easier and harder to attack. At the same time, set the time interval, the user's client to connect to other clients through the master node.

Once inside the master node, the face value that the user requested to be anonymous would be queued up for broadcast across the network, but no information would reveal the user's identity.

Each round of the PrivateSend process can be viewed as a separate event that enhances the anonymity of the user's funds; however, each round is limited to only three participants, so that the observer has a one-third chance to track the transaction. To improve the quality of anonymity, the link method is used to send the funds through multiple master nodes in turn.

(9) Mixed currency technology

To enhance the privacy of the system as a whole, we propose to use the same denominals of 0.1txn, 1TXN, 10TXN and 100TXN. In each round of mixing, all users should input and output funds in the same denomination. In addition to using the same denomination, the transaction fee will be removed,

And all transactions are broken down into discrete, independent, unrelated transactions

Next, in response to a possible DOS attack, we propose that all users submit the transaction to the pool as a deposit when they join, and the transaction is eventually output to the user, while paying the miners a high payment. In other words, when a user requests an increase in the pool,

A deposit is required at the beginning of the transaction. If at some point the user becomes uncooperative, for example by refusing to sign and the deposit is automatically broadcast all over the network, the cost of a sustained attack on an anonymous network is prohibitive

Darks is limited to 10000TXN per round of mixed COINS, and only multiple rounds of mixed COINS can anonymously mix a significant amount of money. Darks runs in passive mode to make the user experience easier and harder to attack. At the same time, set the time interval,

The user's client is connected to other clients through the master node. Once inside the master node, the face value that the user requested to be anonymous would be queued up for broadcast across the network, but no information would reveal the user's identity

Chapter 5 Conclusion

This white paper introduces various concepts designed to improve the Bitcoin protocol, which for ordinary users means better privacy, interchangeability, less price volatility and faster broadcast of information across the web. This is all done using the Mrypto protocol

We will release the official white paper before testing online.