Void chain white paper

Points

1. This is a blockchain operating system

2. Provide accounts, authentication, databases, asynchronous communications, and program scheduling on hundreds of CPUs or clusters

Problems with current blockchain platforms

1, can support millions of users visits

2, whether free service, find value-added service fees

3, smooth upgrade to avoid bugs

4, low latency user experience

5, serial capabilities

6, parallel capabilities

DPOS consensus algorithm

Insert a BTS DPOS

DPOS was invented by Dan Larimer.
First of all, to clarify two concepts: the owner of the equity is the shareholder, the authorized representative (that is, the appointed witness) is the member of the board of directors, and the creation of the block is a matter of appointing a witness, and has nothing to do with the shareholder.

1, the election mechanism
In the BTS network, there is a 24-hour general meeting of shareholders. Each shareholder elects an authorized representative to exercise the right to the production block on his behalf (shareholders can see the status of the authorized representative on the status indicator in their wallet). The authorized representative needs to perform due diligence, otherwise the shareholder can cancel the authorization and then authorize other representatives. 2. Production block
The top 100 most votes represent the right to produce blocks. The sorting of production blocks is performed in accordance with a previously determined table. Each representative is assigned a period of time to start production. The representative did not have the right to modify the details of the transaction, such as the originator, recipient, or balance. If, for a certain period of time, the representative is unable to produce a block or put transaction information into a block for various reasons, then the block created by the next representative will become twice as large. The block, including the previous one represents the missing transaction information, and the confirmation time will be extended to 20 seconds instead of 10 second. An erroneous representative will be cast a vote of no confidence and will be removed from the state of production. The number of 100 delegates can

be changed so that the network overhead can be adjusted.

3, to avoid the fork

As representative in order to avoid loss of mining fees, will certainly strive for 100% online, if the occurrence of the above mentioned representatives missed

In the case of its own time period, the transaction confirmation time will be longer. If it is found that the trader finds that 5 of the 10 blocks have missed the production time period, they can basically confirm that they are in the fork blockchain and should stop trading. Waiting for fork back

Return.

There is also a mechanism to avoid bifurcation, that is, there is a direct connection between the production representatives of adjacent blocks. This connection is related to the compensation of the generated block. 4, decentralized skepticism

Someone wonders if the excavation right is concentrated in 100 people, is it still decentralized? (V God 2017.7.28 speech in Shenzhen mentioned that VOIDCHAIN is not decentralized) Actually these 100 people are equal in rights and cannot concentrate their rights in the hands. For fewer nodes. More than one representative can work together to cope with evil, but the possibility of 51 representatives working together to cope with evil is still very small (This is much better than the concentration of bitcoin mining rights).

Taking a step back even if they can work together, but the impact is not great, because other representatives will soon identify blockchains that correct the fork and ignore the evil attackers.

DPOS in VOIDCHAIN

Basically the same thing is that the owner of the token is an election agent. The difference is that each round is the first 21 delegates who are selected as the miners, the top 20 are automatically sorted by the system, and the 21st is selected according to the probability of the number of votes obtained. The selected producer will mix based on the pseudo-random numbers derived from the block time. In order to ensure the connection between the blockers as far as possible.

At the same time, there is only one producer. The frequency is one block every 3

seconds, which is 63 seconds.

If a representative misses a block time and does not produce a block within 24 hours, the system considers that this representative has been lost and will cancel the rights of mining delegates.

1, transaction confirmation

Under normal circumstances, 15 confirmations are required to complete the transaction confirmation, and the maximum is 45 seconds. If a node observes a continuous loss of 2 blocks in the network, it considers 95% of its possibilities to be on the bifurcation branch of the blockchain. If there are three consecutive lost packets, there is a 99% chance that it will be on a forked blockchain. In order to avoid bifurcations, a predictive model can be generated to form a strategy that will lose information on the node, the latest participation rate, and other factors to quickly warn the user.

Dealing with forked 15/21 confirmation is a relatively simple and effective method. 2. Proof of transaction (TaPoS)

Based on transaction-based proof of interest, each transaction is required to include a hash of the most recent header. This can prevent a large number of transactions on the forked chain, and the system can sense the user on the forked chain.

Account

The account should be the owner of the DAPP, 2-32 characters can be used as an option, the account should be reserved for the token payment management fee, and the account name also supports the namespace, so the owner of the account @domain is the only one that can create an account

User of @user.domain.

1, message processing

Each account can send structured messages to other accounts and can define acceptance of processing scripts and can also forward messages. Each account has its own database and can only be accessed by its own program. 2. Role-based rights management

Rights management is to check the signature of a thing.

VOIDCHAIN software provides a declarative rights management system that allows accounts to fine-grained and high-level control over who can do what and when.

In particular, identity authentication and rights management are separate from the application logic of the account. This facilitates development. The account also supports multi-level management, which is to implement additional private key of other accounts. Hierarchical permission structure that meets organizational conditions in the real world. It also supports the separation of privilege of the same account, for example, without providing a private key, allowing the account to perform other functions such as social networking.

Named permission levels

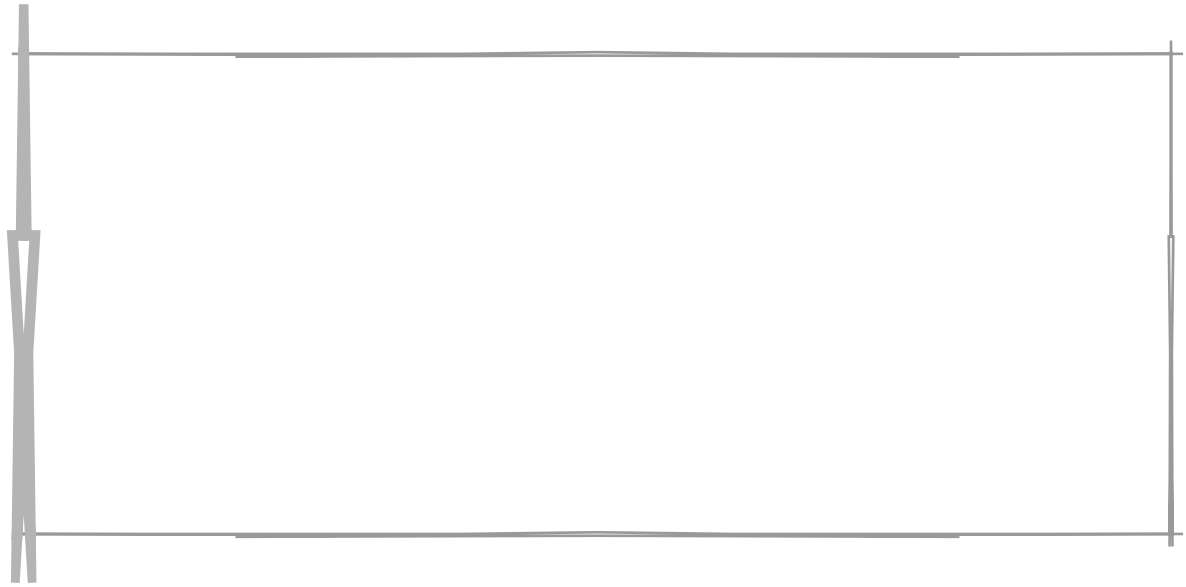
Use an account for naming permission levels to perform decentralized management. Each named privilege level defines a power, which can be the threshold of a multi-signature check composed of other accounts' key and/or naming privilege levels.

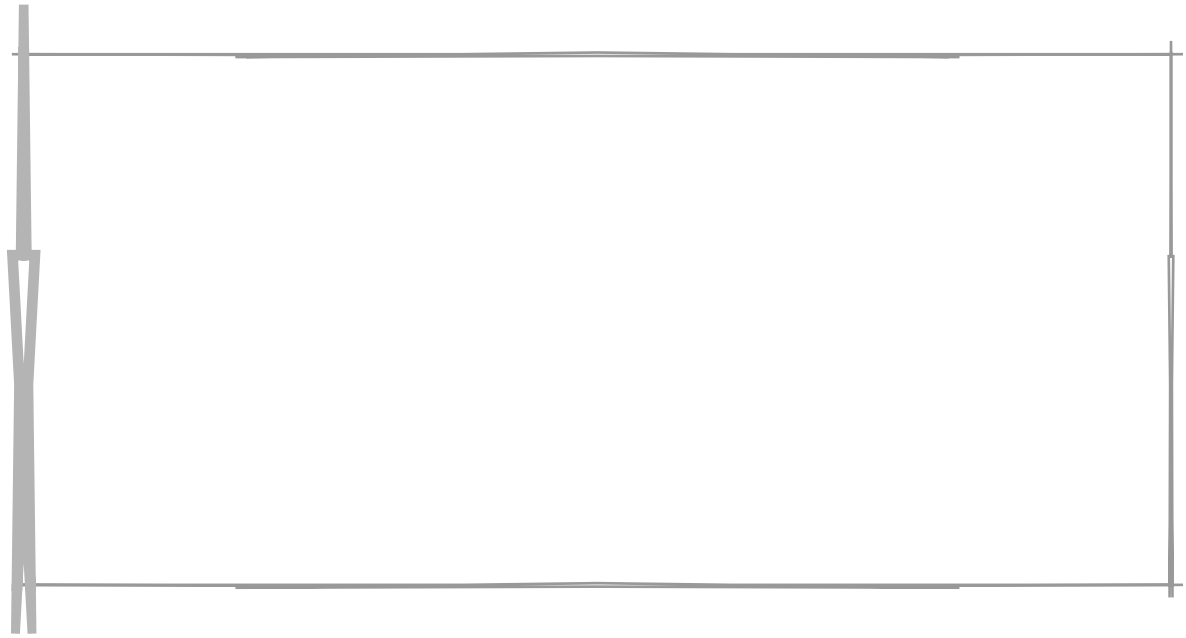
Named permission levels

All accounts have an "owner" permission group that can do everything, and an "active" permission group that can perform all actions except changing the owner group. All other permission groups are derived from the "active" permission group.

Named message handler groups: Each account organizes its own message handlers by naming their names. These named message handler groups can be referenced

by other accounts by configuring their privilege levels.





Limit the mapping between levels.

Permissions read-only attribute evaluation: rights are read-only during the evaluation process, which means that permission evaluation can be parallel, it means that you can quickly verify permissions without having to consider the expensive application logic to start rolling back. Finally, this means

that when the pending transaction continues to execute, the evaluation of the transaction privilege can continue without having to be re-executed from the beginning.
Forced delay in the system: Things must wait for a relatively small period of time before the application. In the meantime, these messages can be cancelled. This is the mandatory delay. The length of the mandatory delay depends on the degree of importance of the operation, the more important the longer the time.

VOIDCHAIN software provides users with a way to restore their account control when the key is stolen.

The account owner can use any of his approved account activity partners that have been active in the last 30 days to recover the partner's key and reset the owner's key on their account after their account recovery partner's permission. Without the account owner's cooperation, account recovery partners cannot reset their account control.
For hackers attacking an account, there is no gain in attempting to perform the recovery process because it has "controlled" the account. In addition, if they do the process of recovery, recovery partners may require authentication and multifactor authentication (such as phone and email). This may reveal the identity of the hackers, or the hackers

Application deterministic parallel execution

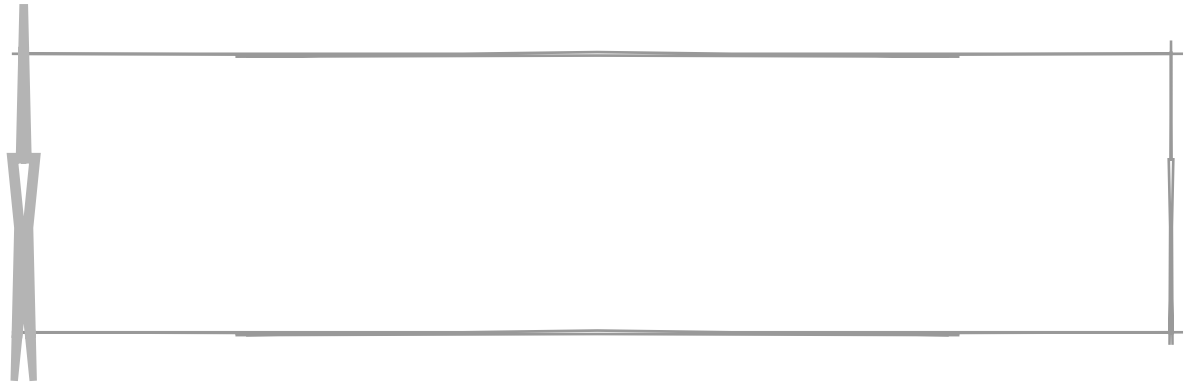
1, communication delay optimization

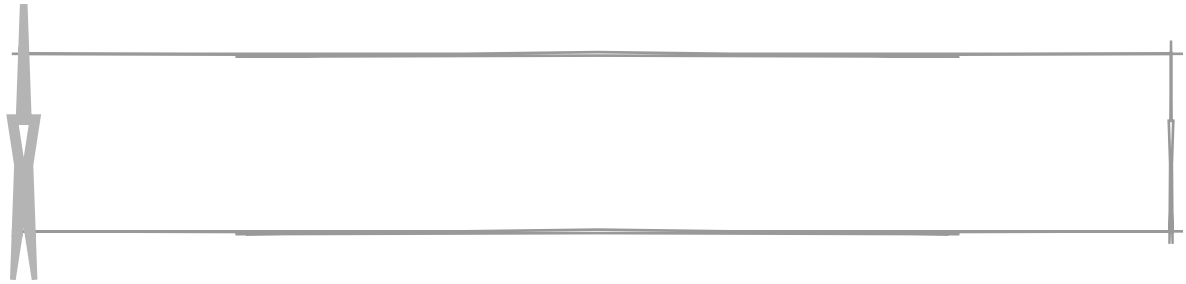
The delay is the time it takes for an account to send a message to another account and receive a response. The goal of VOIDCHAIN software is to enable two accounts to exchange messages back and forth within a single block without having to wait 3 seconds between each message. To achieve this, VOIDCHAIN software divides each block into cycles (cycle). Each cycle is divided into threads, each thread containing a list of transactions. Each transaction contains a set of messages to be delivered. The structure can be visualized as a tree where layers are processed sequentially or in parallel depending on their characteristics.
The transactions generated in one cycle can be transmitted in any subsequent cycle or block. The block generator will continue to add cycles to the block until the longest block time interval is reached, or no new deliverable transaction is generated.

2. The blockchain technology components are modular, that is, each application only calls the modules it uses.

3. Autonomous optimal task scheduling: The producers of each block have their own subjective judgments on the complexity of the transaction. Specific to the network layer, each block producer uses its own algorithms and metrics to measure the network resources occupied by the transaction. Some people think

that the transaction consumes a lot of resources and can choose to reject the transaction in its own block, and some people do not recognize this. In this perspective, the transaction will be included in its own block. So as long as the transaction covered by any block is eventually





Token (token) model and resource usage

Resource limits:

The resources to keep the system running reliably include the following three aspects

1. Bandwidth and log storage (disk);
2. Calculate and calculate the backlog (CPU);
3. Status memory (RAM).

Logs exist in all nodes and are mainly used to reconstruct the state of all

applications.

The computational debt refers to the calculated consumption through the regeneration of the message log. If the technical debt growth is too great, it is necessary to photograph the current status of the blockchain and discard the historical status of the blockchain. If the calculated debt growth is too fast, the blockchain will use six months to replay one year of transactions. Therefore, the careful management of the accrued debt is crucial.

The storage state is data accessed from the application logic, such as transaction information.

Authorization ability

The system supports the owner of the VOIDCHAIN account to transfer or sublet other people their idle or incomplete bandwidth. Blockchain producers can recognize this behavior and execute their decision to allocate bandwidth.

One of the main advantages of the VOIDCHAIN system is that the bandwidth available to the application is completely independent of any token price.

The fluctuation of token prices has nothing to do with the available bandwidth, but higher token prices will affect the amount of bandwidth, storage, and computation that a block producer can purchase, and in turn can use the rising token value to improve network performance.

State storage cost

The developer of the application must always hold tokens until the bandwidth and computing resources are committed. Each account requires a certain amount of storage space, so it must also hold a certain amount of tokens.

Block reward

Every time a block is generated, the system rewards a certain number of new tokens. The new tokens are the issuance mechanism. The number of tokens obtained by a blocker is determined by the median expected return of all block generators. The system can be set to limit the upper limit of tokens obtained.

The median (also known as Median), a proper noun in statistics, represents a value in a sample, population, or probability distribution that divides a set of values into equal upper and lower parts. For a finite set of numbers, you can find the median of the median by sorting all observations. If there is an even number of observations, the average of the two most intermediate values is usually taken as the median. (Baidu Encyclopedia)

Community welfare applications

In addition to becoming a miner, you can also choose to become a vote supporter for 3 smart contracts (applications). The system sets a percentage of the revenue for these smart contracts (need to subtract mining incentives). In other words, these smart contracts receive tokens based on the number of votes they receive from shareholders. If you do not gain trust, you will be replaced by the newly elected smart contract.

Governance

The right to govern is attributed to the owner of the currency, which is the shareholder. All changes to the blockchain must be approved by the shareholders. The diggers have enforcement and supervisory authority, such as freezing accounts, updating programs, and making changes to the underlying agreement. If the diggers refuse to implement the voting results, then the non-mining nodes (non-production full-node verifiers (exchangers, etc.)) will negate the resolution of the diggers.

freeze the account

In order to prevent abnormal behavior or unpredictable behavior of smart contracts, a block producer has the right to choose which transactions to include in the generated block, so that they have the ability to freeze accounts. The system authorizes this ability by voting on a 17/21 active block producer in an account. If generators abuse their power, they can be eliminated and the account will be thawed.

Change account code

When the application is abnormal and unstoppable, the vote-authorized miner (17/21 vote of the selected block producer) has the right to directly modify the application's code.

constitution

The constitution is the stipulation of VOIDCHAIN. It mainly defines the obligations between users when the code cannot be implemented, establishes some accepted guidelines, and establishes the boundaries between law and judicial power. Each transaction broadcast on the network must include the constitutional hash in its signature information to explicitly constrain the contract signer. The Constitution also defines the meaning of humanity beyond the code

In the figure, when an error occurs in the system, this intention can be

clearly identified as a bug or a system feature, and it is judged whether the community's repair measures are correct.

Upgrade agreement and constitution

To make changes to the constitution or agreement, you need to complete the following steps:

1. The block producer (original miner/delegate/witness, therefore not translated as a miner) submitted a constitutional change motion and obtained a positive vote of more than 17/21;
2. The block producer maintains over 17/21 votes for 30 consecutive days;
3. Ask all users to use the hash value of the new constitution to confirm the transaction;
4. The block producer uses the modified source code to reflect the constitutional changes and uses the hash value submitted by git to submit the changes to the blockchain.
5. Block producers continue to maintain their 17/21 or more positive votes for 30 consecutive days;
6. The changed code takes effect after 7 days. After the source code is modified, it will have 1 week to upgrade all the nodes. 7. All nodes that have not been upgraded to new code will be automatically closed. According to the default configuration of the VOIDCHAIN operating

In special circumstances, block producers can speed up the constitutional change process when harmful loopholes or security breaches that harm user interests occur.

Scripts & Virtual Machines

VOIDCHAIN supports scripts and virtual machines developed in any language that can be integrated via api.

Mode defined message

Messages sent between accounts are defined by the pattern of consensus status. This architecture allows for seamless conversion of messages between binary and JSON formats.

Schema-defined database

The database state is also similar to the above model definition.

Separating authentication from applications

To reduce resource consumption, the VOIDCHAIN operating system separates the authentication from the application program. The verification logic is divided into three phases: 1. The confirmation message is internally consistent; the internal consistency does not require access to the blockchain state and the external is read-only. . Can be done in parallel. 2. Verify that all preconditions are valid; the same preconditions are also read-only and can be parallelized.

3. Modify the application state. Here is the write operation. Each program is processed serially.

Before the transaction enters the block, authentication is required, but once the transaction is included in the blockchain, the authentication operation is no longer required.

Virtual Machine Independent Architecture

The virtual machine currently being evaluated:

1, Wren

Wren(http://wren.io (https://link.jianshu.com?t=http://wren.io)) is a small, fast, category-based programming language. The Wren language and virtual machine were chosen because of its short and slick codebase and ease of documentation and understanding. It also has very good performance and can be easily embedded in C++ applications

in.

2. Web Components (WASM)

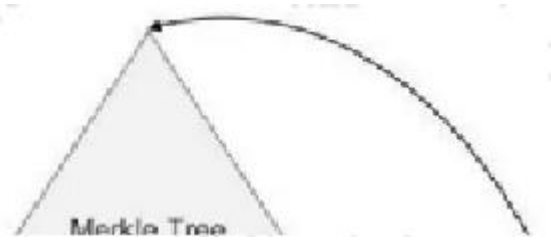
WASM is an emerging Web standard for building high-performance Web applications that can be clearly defined and sandboxed with a small amount of adaptation. The benefits of WASM are widely supported in the industry, so it is possible to develop and develop smart contracts in familiar languages, such as C or C++.

3, Ethernet virtual machine (EVM)

This virtual machine has been used for most existing smart contracts and can be used on the VOIDCHAIN system blockchain. It is conceivable that in the VOIDCHAIN operating system blockchain, EVM contracts can be run in an internal sandbox, and only a small amount of adaptation is required to interact with other VOIDCHAIN applications.

Cross-chain interaction

The VOIDCHAIN operating system supports the promotion of cross-chain interactions between blockchains. This is achieved by simplifying message existence proofs and message sequence verifications. But for the developer to hide the details of cross-chain interaction and validation.



VOIDCHAIN cross-chain interaction

The Merkel Certificate (LCV) for Light Client Authentication

For the client, to be light, that is to say not concerned about all transactions, more concerned with their own related transactions, the same for the exchange, the maintenance of the lightweight Merkel deposit in their own chain In this case, there is no need to rely on full-node miners, which will save more resources.

Therefore, one of the goals of LCV is to produce a relatively lightweight proof of the existence of the transaction. The second goal is that the proof can be verified by others by tracking a lightweight data set. In other words, the purpose is to prove that a particular transaction is included in a particular block, and this block is included in the verified blockchain history.

Then take a look at how Bitcoin did it.

Bitcoin's SPV is a complete record of all nodes reading block header data, and the block header data grows by 4MB per year. Suppose 10 transactions are generated per second, a valid proof requires 512 bytes, and the block out time is 10 minutes, which is each The block contains 6000 hash values. For VOIDCHAIN blockchains with a block time of 3 seconds are inefficient. The VOIDCHAIN operating system's LCV only needs to verify the header data of a certain transaction. Using the hash chaining table structure, the size of the data set can be kept within 1024 bytes, which can prove whether any transaction exists. This

It is based on the fact that the verification node retains all the block header data of the previous day (2 MB in size) and then proves that these transactions require only 200 bytes of proof data.

It can also be further optimized according to the application scenario. If all the header data is needed, then there is only 420 MB/year of data. The general situation can find the right balance between the time and quantity of the used block header data

point. The same blockchain can lazily record only the hash value of past data as evidence of previous data.

After a certain density of correlations between chains and chains. They will become more and more efficient. A chain may contain the entire history of another chain, so there is no need to prove each other. From a performance point of view, this will greatly reduce the frequency of interchain certification operations.

Cross-chain communication delay and completion

certification

In cross-link communications, miners must wait for irreversible confirmation of other blockchains before accepting them as valid inputs. But using VOIDCHAIN system software, relying on DPOS and 17/21, the confirmation time is only 45 seconds. This will happen when the miners on one chain have not fully confirmed the completion. VOIDCHAIN only has to wait. VOIDCHAIN operation

The system avoids this situation by assigning a sequential identification number to each message that arrives at the account (proving that there is no missing between historical transaction data). The user can use these labels to prove that all messages to this account have been processed and are It is processed sequentially.