XinChain White Paper

V0.1.0

Feiyang Tan
2020

Xinchain provides low-cost information recording services to individuals, enterprises and organizations through blockchain technology, so as to achieve the abilities for notarization, announcement and so on.
Xinchain Ecosystem also provides free and convenient information verification services to all users, so as to achieve the abilities for verification and checking.

Note: Yellow information is undecided, red information is unresolved problem, green information is problems solved. The red and green messages are the author's self-question and answer, readers can choose to ignore, it will not be affecting the mechanism of understanding the Xinchain.

Background:

In 2009, Satoshi Nakamoto released bitcoin and initialized the starting point of the blockchain era. At the same time, it opened the Pandora's box that the decentralized system is feasible for the world. In the following time, more people inherited the concept of decentralization, and with the emergence of Ethereum, EOS, Hyperledger and other projects, the entire blockchain technology is rapidly moving towards to a more popular, more diverse and more powerful Direction development. Here I deeply salute all technical personnel, supporters and users who participated in the development of blockchain technology.

One of the most essential characteristics of the blockchain is its unchangeable, which leads a very important point for the future value network. But until now, due to various factors, in many cases it is still inefficient, difficult, or even impossible to judge the authenticity of information. The Xinchain will be able to solve this problem for us.

At today, the application of blockchain technology in many aspects still faces many obstacles, one of which is the high threshold and high cost of using blockchain. With the rapid development of blockchain technology, the difficulty of developing a public chain or building an enterprise-level alliance chain at this stage is much lower than before. But even so, for the vast majority of individuals and companies, blockchain technology still represents the need to invest a lot of manpower, time, and money.

Xinchain will lower the threshold for all demanders to use blockchain technology and realize that a blockchain can effectively solve and a large number of problems required: information verification.

Brief Introduction of Xinchain:

Xinchain provides significant low-cost information recording services to individuals, enterprises and organizations through blockchain technology, so as to achieve the functions of notarization and announcement. Xinchain Ecosystem also provides free and convenient information verification services to all users, so as to achieve verification, query and other functions.

The SinChain has the ultra-high performance of theoretically unlimited TPS and has very good scalability.

The Xinchain community will exist as a incompact center of the Xinchain, and it is more of a symbol center, only to solve problems outside the chain more efficiently, and does not have the ability to change the chain.

Xincoin is a special account book that is recorded on the Xinchain together with other information by default. The function of the letter currency is to record the information on the Xinchain.

The Xinchain has two different ways of recording information. One is irrevocable and the other is revocable. The revocation mechanism is mainly used for services that need to be revoked or updated with new information, such as property rights certificates.

The information on the Xinchain will be stored in units of years. The user can adjust the length of time the information needs to be recorded by selecting the amount of payment credit.

60% of the credits spent will be paid to the miners who package the block, 20% will be paid to the nodes participating in the verification, and 20% will be used as the cost of community operations.
How does the verifier participate? How to determine and prove whether you have participated? How to pay?

Xinchain realization:

1. Mining:

In order to reduce meaningless computing power competition and maximize TPS, Xinchain uses DPOS as a consensus mechanism.
How to ensure that the node equipment maintains a certain competitive relationship under the DPOS mechanism, so as to ensure that the node hardware equipment standard is high enough? Make certain modifications to the DPOS mechanism

Rate all nodes:
Asset * ln (Asset holding time)

The top 20 nodes of the entire network will be used as super nodes and have the right to mine. All super nodes will allocate a section of the winning hash value range for the fair selection of mining nodes based on the ratio of their scores to the total score. Such as:
20 nodes, the scores are: 1, 2, 3 ..., 19, 20. Total score 210 points
Then:
The hash range of the middle dart of node one is: 0x00000000000000000000000000000000 ~ 0xffffffffffffffffffffffffffffffff * 1/210
The hash range of the middle dart in node two is: 0xffffffffffffffffffffffffffffffff * 1/210 ~ 0xffffffffffffffffffffffffffffffff * 3/210
And so on

After each round of block confirmation, the central node will sign the hash value of the block, and the range of the signed hash value will determine the next mining pre-selected super node.
What should I do if there is a fork in the block? The fork is mainly caused by the instability of the network and the malicious operation of malicious nodes. The possibility of malicious operation motivation in the Xinchain: 1. Increase the probability of own mining and obtain the processing fee. 2. For the operation of a node. 3. Other malicious. Forking will inevitably happen. The Xinchain will adopt a chain priority mechanism, and if a node discovers the

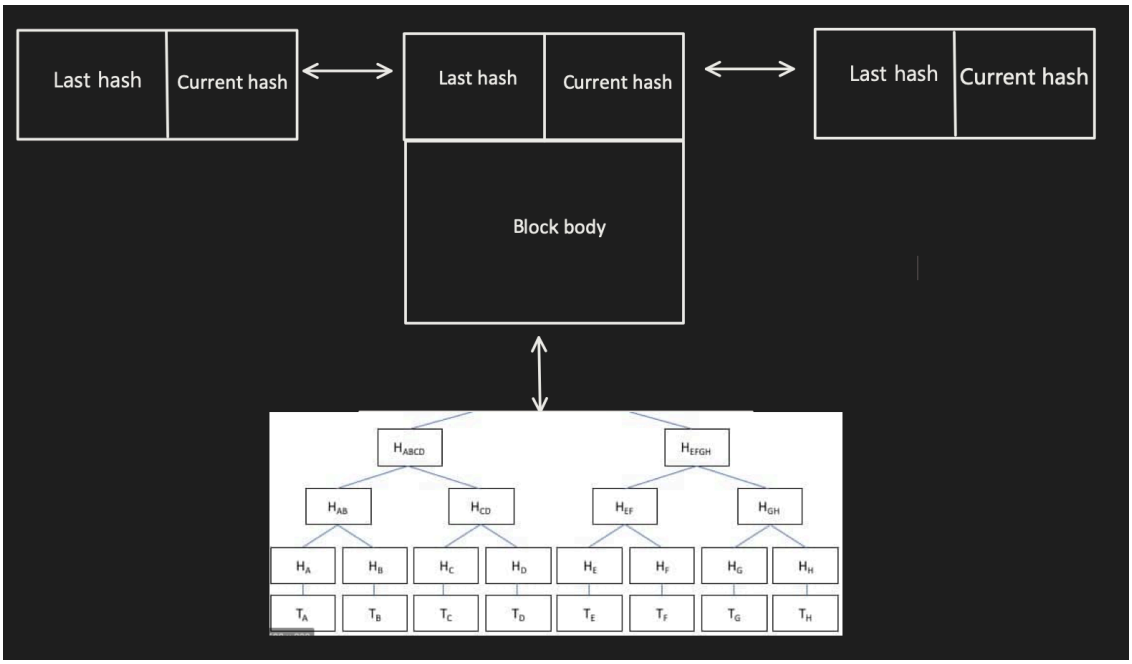
presence of other nodes in the network, it will use a certain rule to prioritize the two chains. Select the block with high priority; How to design the priority mechanism?
What should I do if the central node is disconnected? Standby central node, broadcast at the same time as the central node; what if the central node maliciously does not broadcast the result to the winning node? After receiving the information, other nodes broadcast each other again (the broadcast cannot be falsified because it contains signed content); what if the central node maliciously does not receive the response information of the winning node? The winning node broadcasts the whole network and broadcasts each other again; what if the winning node is malicious or non-malicious and does not receive the broadcast? If the whole network does not receive a response, choose another node; how to choose another node fairly?

The results of mining will be announced by the entire network, and the nodes will automatically collect legal new blocks.
What if I receive multiple copies of legal block broadcasts? : The legal block broadcast needs to be signed by the private key of the currently designated mining node (confirmed), so if multiple legal broadcasts are received, the private key of the mining node is lost, or the mining node has issued two broadcasts . Each mining node can only broadcast once. What happens if there are two broadcasts?

2. Block:

In the Xinchain, blocks are generated every 30 seconds (considering the time-consuming of various network protocols, as short as possible). The block information is divided into block information and block additional information. The block information mainly saves a "folder hash" information, and the block additional information is the hash of each file saved in the block.
The maximum size of each block: 37KB.
Block header (32B): pre-hash value (16B), hash value (16B)
Block body (56B): version (2B), height (6B), miner public key (32B), folder hash (16B)

The blockchain only retains the header hash of the Merkle Tree folder, and the contents of the folder itself and other hash values of Merkel Tree will remain outside the blockchain. Folder information
File (72B): Operation sequence (1B), operator public key (32B), file hash (16B), operator signature (16B), reserved (7B)
The number of files contained in the folder corresponding to each blockchain is an adjustable number, which is determined according to the current network busyness.
How to ensure that the mining node will not wait for more transactions, resulting in the risk of delaying block generation?



Information about the number of folders corresponding to the blockchain:

Number of files	512 （2^9）	4096 （2^12）	32768 （2^15）	524288 （2^19）
Merkel Tree required hash	510	4094	32766	524286
Total size	45KB	0.361MB	2.75M	44M
TPS	17+	130+	1000+	17000+

3. chain:

The information storage of XinChain is in units of years (525600 blocks). Before adding a new block, the 525600th block will be deleted and the automatically renewed blocks will be repackaged.

Continuously updating blocks can ensure that the meaningless information in the chain is filtered out, so that every data in the entire chain has the necessary meaning.

Xinchain still uses the hash connection of front and back blocks to form a chain. Its security mainly comes from the unforgeability of the signature of the mining node and a certain amount of proof of work.

4. The Modified DPOS:

In order to ensure that each node has a certain degree of power to upgrade the node hardware, it can also increase the difficulty of modifying the chain by a certain amount of work. Every time a mining node mines, it will try to arrange it in a different order, and finally release the Merkel tree head node must be less than a certain range to become a legal block. The range will be adjusted in some way.

Is it really necessary? How to adjust?

5. TheState of the world:

The world state of the Xinchain will record all file hashes and the guidance of the hash. The canceled file and its two indexes will also be saved in the world state, which is convenient for certain queries.
The world state of Xinchain will also record the current account asset information file. The file stores the public keys and balances of all accounts with coins. The information of this file will be stored in the No. 1 file of each block of Xinchain by default.

6. Credit:

The Xincoin will be stored in a different way from other digital currencies. All account numbers and account balance information will be recorded in a text file in a certain format. The file will be recorded in each block as the number one file. This file represents the balance information of all accounts after the second block. And is retained by the node as the world state.
Credit is not an orthodox decentralized digital asset. Cryptocurrency is not the focus of CryptoChain. Cryptocurrency is more like a purchased service. Therefore, Sinco will be issued and managed by the SinChain community. The letter currency can use some kind of legal currency as the main body. Or use virtual currency as the theme.
Credit usage: usage records will be stored in each number one file.
Cryptocurrency transfer: Cryptocurrency transfer will also be saved in file No. 2 through a certain format file.
How?

Cryptocurrency issuance / purchase: Cryptocurrency will be issued in a fixed amount through some mechanism.
What mechanism? 1 Investors have a certain return before market stability is guaranteed. 2 Make sure that there is no loss in the center.
Credit recycling: a certain amount of official recycling mechanism.
What mechanism? 1 To a certain extent, guarantee the lowest price of the second-level market price. 2 Ensure that the official does not have funding problems.

It takes 1 credit to save irrevocable information every year, and can pay n credits, which is automatically updated n-1 times. It takes 1 credit to save the revocable information every year. It can also pay n credits and update it automatically n-1 times. The revocable information needs to add 4 credits as a deposit. All 4 credits will be returned after the information expires . Revoking revocable information will cost 1 credit and return 4 credits.

7. First internal document:

The number one file is the file that records the credit balance, and its recorded content is
Public key: ox00000000000000000000000000000001
Current balance: 30.0
This transaction: -1

8. Second internal document:

Document No. 2 and record of credit transfer records:
Transfer account public key: ox00000000000000000000000000000001

Account collection public key: ox0000000000000000000000000000002
Transfer amount: 1
Transfer account signature: ox0000000000000000000000000000003

9. node:

Light node: user terminal, used to verify the authenticity of information, store, purchase, transfer credits. The light node only saves the information of the block header on the chain. The size of the light node increases by 32B every 30 seconds, and the full chain size: 32M.
Full node: the right to verify and candidate mining. The full node saves the block, block additional information, and the current number one file and number two file. The size of the full node will depend on the busyness of the Xinchain. In the case of 1000 + TPS, the full node increases 45KB every 30 seconds, and the full chain size is 45G.
Unlimited nodes: have the right to dig. The super node will save all the blocks, additional information of the blocks, the first file and the second file. The Xinchain community will also retain the complete unlimited nodes.

10. The user terminal:

Client: mobile APP, web page, desktop port.
Each time you open the client, update the latest to the latest block first.
In the verification process, the user only needs to enter the information (text, pictures, files) that need to be verified, the client will send the hash value of the information to request verification, and the verification will be sent to n full nodes, and the full node will find the hash value If it does not return false, if there is information other than the returned block height and Merkel tree header hash of the block body, it is necessary to convert the other hash of the Merkel tree header hash. If the response received by the user terminal is all false, it means that the information to be verified does not exist. If the verification information is received, the Merkel tree header hash is calculated, and then the hash of the block is calculated to compare the block with the local block The hash value of, indicates that the information that needs to be verified exists.
How to ensure that information such as files and pictures is not affected by changes in software, systems, and the environment?

There is no cost for verification.
How to assign tasks to full nodes? How to choose a full node? How to reward full nodes for helping verification?

11. Xinchain Community:

The Xinchain community will serve as the Xinchain publicity agency and code management agency.
The SinChain community will be set to a replaceable mode, and the SinChain community can be replaced without affecting the operation of the SinChain. Or tolerate the form of multi-community centers.

12. Anonymous and real name:

XinChain, users can freely choose to create an account, and an account needs to be traded to be recognized by the entire network.
Accounts are free to choose anonymous and real names. The real-name system is mainly for binding the main body behind the account, and most of the information can only have its value if there is a binding main body. It also provides the main body for the necessary information to prevent counterfeit records.
The real-name system cannot retrieve the private key or revoke the operation.
Anonymity management requires a set of operational details.

13. Replaceability:

Xinchain will use pluggable design in many places to facilitate the replacement and replacement of some technologies, and also ensure the decentralization of the structure
The signature method, the use of hash equations, the interaction between this structure and the Xinchain will be set to an alternative mode. That is to say, within the feasible range, users and nodes can use different encryption methods, and ICT tolerates multiple encryption equations. It is conducive to adapting to the laws and regulations of different countries and regions, and also enables the decentralized upgrade of the encryption method of the Xinchain ecology.
In detail?

The replaceability of the trust chain ecological structure enables the trust chain to tolerate the replacement of the trust chain community, or tolerate the multiple trust chain community. It can tolerate the existence of an indefinite number of super nodes.
In detail?

14. Information format:

The stored information will be suggested in a certain format. To avoid confusion, misunderstanding and collision of information.
The collision information will not be recorded.

Summary of advantages:

The affordable TPS is very high, and the ultimate limit of TPS comes from the speed of network information transmission.
The block size is fixed, but the record information that can be included can be superimposed arbitrarily.
The essence is service, there is no resistance and gray area of government.
The business value is considerable.
Information can be withdrawn.
Easy to use.

Application scenario:

Need to prove the authenticity of a certain information:

School graduation certificate, after the student provides the graduation certificate, the employer / inspector can check on the chain

Hospital patient information on the chain, the patient provides identity, check the authenticity of the unit chain query

Proof of ownership of the government ’s on-chain property, provided by the owner, and on-chain inspection by the inspector

Property rights on-chain property rights certificate, the owner provides a certificate, inspection and put on the chain query

Information for opening to the outside world (and to ensure that it cannot be changed after opening):

Collective, public welfare, charity funds
French, regulations, rules
Contract, contract
Cheng Ruo, Statement
Reward and punishment

No external information:

The node and the chaining process do not require the information itself to be saved. All the saved information is not empty, nor can it be obtained through the Xinchain.

Information transfer:

When saving information, in addition to the hash of the information, there is a default 7B reserved size information that can be customized. As information completion, transfer, encryption, etc.