SANCHAIN Whitepaper

Decentralize Everything

V2

- Content

- Architecture

    Consensus mechanism

    Publishing Algorithm,

    Smart Contract,

    Performance and Scalability,

    Security and Privacy

- Service ecology

    Dapp

    DAO

    Asset Issuance

- Summary

- Conclusion

- Abstract

Sanchain aims to establish a distributed block chain collaboration network and makes the corresponding contribution to the whole block chain network from the bottom right node—nodes to the application layer—

DAPP, so as to realize the blockchain all distributed collaborative network.

- Background

Blockchain technology is the result of bitcoin launched in the 2008, since then, 'Decentralize Everything' has become a concept of the block chain world, individuals or organizations in minimizing intervention achieve social cooperation coordination, people from all walks of life provide a variety of efforts.

Although 'Decentralize Everything' has all kinds of difficulties, Openbazzar、bitshare and so on　had opened a door to 'Decentralize Everything', sanchain will realize the dream of Decentralize Everything more from the bottom to the application layer.

- Blockchain application

A successful blockchain application platform should meet the following requirements:

support millions of users;

provide computing storage capabilities;

software upgrades and bug recovery

low latency

- Structure

design idea

Sanchain is a shared open-book, including records of account and general ledger balances. Anyone can read the general ledger and also read all the transaction records in the sanchain network. All the nodes in the network through a mechanism named "consensus" which every parties should abide. The network can reach a consensus in a matter of seconds. The mechanism of the consensus is a technical breakthrough, it can do a quickly, security and distributed transactions in the network. Decentralized network is more efficient than centralized network in many aspects, and because there is no single point of failure in decentralized network, it is more reliable. In addition because the fully open source, it will be more secure.

The localization of sanchain is to achieve a block chain platform which is lightweight, low cost, safe and reliable, easy to use, easy to expand. Domains include: de centralized applications, decentralized autonomous organizations, digital asset management, and intelligent contract platforms

- Consensus mechanism

We studied the bitcoin and Ethereum that is on the basis of PoW (Proof of Work), its main advantage is completely t decentralized and the defect is blocks of time is too long, the transaction processing ability is too weak. We also discussed the way represented by Ripple that validator vote to reach a consensus to generate block, this approach improve the processing ability of the transaction, but it is at the expense of decentering in absolute sense.

Finally we research the DPoS(Delegated Proof-of-Stake) mechanism represented by Bitshares which through the method of voting makes all users have the opportunity to participate in the consensus's structure and reduces the computation and communication cost in the consensus process, so as to get the ideal block formation rate and transaction processing capabilities.

On the basis of the above consensus forms, we designed a consensus mechanism called SPOS (Sanchain Proof of Stake improved ownership certificate mechanism) certificate mechanism. It is based on the equity certificate mechanism and makes special improvements.

The main features of SPoS are as follows:

1. Nodes which generated by minority voting nodes and often held lots of SAN themselves and are widely recognized by the network generate blocks. For these nodes, the benefits of their positive work will be far greater than the benefits of fraud. The result of less generation of nodes is to speed up the generation of blocks and the ability to process transactions. The speed of block generation in Sanchain is set to 3seconds, for small transactions, it can be considered as being dealt with on time.

2. Through the smart contract to increase the scalability of the system. In the process of sanchain's consensus，it will actively deal with various smart contract, smart contract can help users to construct every kind of application in sanchain network to satisfied different demand of different users.

- Publishing Algorithm

   As sanchain is used more and more widely, the demand for SAN will be getting greater and greater. And according to the law of economic operation, the total amount of economy is also increasing continuously. We designed a reasonable publishing algorithm to

accommodate this change in economic growth and usage. Attract more people to actively use the sanchain network, participate in the construction process of sanchain network, in the beginning of the protocol been created, system will issue 30 million SAN, its total amount is limited, in the later process of block generated, we will carry out incentive according to certain rules, and according to the definition of sanchain, could not produce any excess San.

- Smart Contract

  Sanchain provides rich smart contract interface, users can create various types of smart contract applications flexibly on the blockchain. The sanchain will provide abundant interface, as long as there is plenty of imagination, its potential is infinite.

- Performance and Scalability

  Thanks to the SPOS mechanism, the concept of mining is completely different from the PoW mechanism of bitcoin, the nodes dig block is elected by the algorithm instead of produced by competition by many nodes. The speed of block generation in Sanchain is 3 seconds each. That has a great advantage over 10 minutes of

bitcoin and 2.5 minutes of litecoin. Even compared to the speed of Ripple and Bitshares of about 10 seconds, it is also greatly improved

Therefore, sanchain's transaction processing capability has several orders of magnitude improvement compared with bitcoin, and it is expected that the throughput capacity can reach at least visa and MasterCard levels, or even higher in the future.

Scalability, Sanchain is a completely decentralized application, anyone can run their own nodes to join the network. By adding new nodes, you can improve the responsiveness of sanchain, so sanchain has unlimited scalability.

- Security and Privacy

The same as bitcoin, the whole system of sanchain is built on the cryptography system which is proved by mathematical theory, So we have every reason to believe that sanchain can reach the security level at least bitcoin level.

Transactions on sanchain networks are anonymous, so there's no need to worry about exposing personal

information on your account through transaction records.

For data on block, we provide encryption options to ensure that only the parties to the transaction can get the specific content of the transaction, the nodes on the network verify only the legality of the transaction without having to understand the details of the transaction, this fundamentally satisfies the user's privacy needs.

- Service Ecology

Dapp(Decentrallized App)

The system is dedicated to support centralized applications from a technical level, to make different Dapp producibility so that ordinary Internet users can really feel the value of blockchain technology.

DAPP applications for different industries, you can bring the blockchain technology to more users and industries. Including decentralized social networking, decentralized storage and decentralized domain name services, decentralized computing services, and so on. Through the introduction of incentive mechanism, the concept of shared economy will be further used to change the existing app market and business model.

DAO(Decentralized Autonomous Organization)

The concept of common sense "Decentralized Autonomous Organization" refers to a virtual entities that has certain quantity of members or shareholders, such as relying on 67% mostly decided to spend money and modify the code. The members collectively decide how the organization will allocate the funds. The method of allocating funds may be a reward, salary, or more attractive mechanism, such as a reward with internal money. This merely uses cryptography and blockchain technique to fundamentally replicate the legal significance of traditional companies or non-profit organizations to enforce them. Thus much of the discussion surrounding the Dao revolves around a "capitalist" model of a "decentralized autonomous cooperation(DAC)" with accepted shareholders and tradable shares. As a replacer, an entity that is described as "decentralized autonomous community" will enable all members have the same rights in decision-making and request majority consent of 67% when increasing and decreasing members. The rule that everyone can only have a membership needs to be enforced by the group.

- Asset Issuance

The governance of sanchian is decided by its community discussion, the whole community makes its own suggestions and contributions to matters such as collaboration and upgrading. Typically, communities achieve autonomy and, when there is a serious disagreement in the community, the community has the right to say "no", thereby ensuring that the entire community will not be divided.

- Summary

The sanchain team believes that the social cooperation in future will be a big bottom, which provide cooperation technical support for the various division of the society, so as to realize the cooperation of decentralize everything, after the founding team opened the sanchain, subsequent development and iterations will coordinate the upgrade iterations for the San community. Throughout the collaboration, the community follows the blockchain spirit —the code is law.

SanChain open source community