AntShares White Paper 1.1

This documentation is a work in progress. You can view other documents on the Github wiki or visit our official website.

This is an open source community project. You can contribute to the development of the documentation at github.com/AntShares/docs. Thanks for visiting.

Overview of AntShares

AntShares and blockchains

What is AntShares?

AntShares is a smart asset platform and the first open source public blockchain project in China. Smart assets are the combination of smart blockchain contracts and digital assets, making registering, distributing and trading digital assets more intelligent.

Digital assets are assets stored in the form of electronic data with blockchain technology to achieve features such as decentralization, trustless, traceability, transparency and so on. The AntShares blockchain supports a variety of digital assets, allowing users to register, distribute, freely trade and circulate assets. Digital certificates can solve the issue of trust on the blockchain. Through digital certificates, user-issued assets can also enjoy the protection of the law. For business scenarios with complex logic, users can use smart contracts to enhance the functionality of assets, or create asset-independent business logic.

The Smart Contract was first proposed by the cryptologist Nick Szabo in 1993, and is almost the same age as the Internet. According to Szabo's definition: When a pre-programmed condition is met, the smart contract executes the corresponding contract terms. Blockchain technology gives us a decentralized, immutable, highly reliable system in which smart contracts are very useful. AntShares has Turing-complete smart contract capabilities, which are executed in the AntShares Virtual Machine (AVM), and has many advantages such as being deterministic, having termination, resource control, concurrency, fragmentation and scalability.

AntShares combines a range of technologies such as point-to-point network, Byzantine Fault Tolerance, digital certificates, smart contracts, superconducting transactions, and cross-chain interoperability protocols, allowing you to manage your smart assets quickly, efficiently, safely and legally.

What is a blockchain?

The term blockchain originates from Bitcoin. In his bitcoin whitepaper, Satoshi Nakamoto proposed the term *chain of blocks* while in his following release of the original Bitcoin program, the folder keeping transaction records was named *blockchain*. Originally, blockchain merely referred to the historical transaction data of bitcoin. The majority of the subsequent cryptocurrencies named their folder of transaction data as blockchain as well, so this term began to refer to the historical transaction data of cryptocurrencies.

Since 2015, mainstream financial players have started to look into systems like Bitcoin, Ethereum and Ripple. These financial institutions have taken a separate view on the underlying technology and the upper-level business of systems like Bitcoin. They have been calling the combination of these underlying technologies *blockchain technology*. Blockchain technology is the combination of cryptography, network topology, consensus algorithm and game theory. With technical modules like Proof of Work, Proof of Stake, Smart Contract, Lighting Network and Side Chain.

The Core of the Blockchain

We believe that what's at the heart of blockchains is how to achieve a distributed consensus - that is, in the absence of a central body or a network with multiple centers, how each node processes all transactions that occur within the network to achieve a common consensus. This consensus includes elements such as the content, validity, and chronological order of the transactions.

- Effectively reaching a distributed consensus of transactions using the digital signature of the contents

In the traditional paper system, the transaction content (transaction instructions) and authentication information (signature and seal) are stored separately. For example, in bank withdrawals, the user-signed application forms and the transaction records are stored separately. In this way, it is difficult for people outside the bank to verify the authenticity of these transactions.

The blockchain system binds and stores the transaction content and authentication information together. Each node does not require a central organization but rather performs the authentications itself to verify the integrity of the transaction instruction (without tampering) and validity (the signer has the authority) based on digital signatures, thus realizing the distributed consensus on the content and validity of the transaction.

- Achieving a distributed consensus on the order of affairs through a consensus mechanism

Due to the high network latency in point-to-point networks, the order of transactions observed by each node may be inconsistent. Therefore, the blockchain system needs to design a mechanism to agree on the order of the transactions that occur within a certain period of time. This algorithm for the order of the affairs of a time window is called a "consensus mechanism". Common consensus mechanisms include:

```
* Proof of Work: Bitcoin, Ethereum (now)
* Proof of Stake: PeerCoin, NXT, Ethereum (future)
* Delegated Proof of Stake: BitShares, Crypti, Lisk
* UNL / Quorum Slice: Ripple, Stellar
* Byzantine Fault Tolerance: AntShares, Hyperledger Fabric
```

- Achieving distributed consensus on historical data through hashing algorithms

The blockchain system typically constructs a chain structure by referencing the hash value of the previous block (hash) to achieve an effect similar to "riding a seam". Any tampering on a single transaction will result in the failure of the bound digital signature; any tampering of the order of the transaction will cause a change in the hash value of the block, causing the "saddle" to fail. Therefore, any node does not need to rely on a central organization to verify the validity of all the historical transactions in order to reach a consensus.

- Achieving a distributed consensus on the results of the "smart contract"

Nick Szabo presented the concept of Smart Contract in 1993, much earlier than the emergence of blockchains. The script system of Bitcoin was the first basic realization of the concept. Ethereum built upon that foundation to achieve a more flexible Turing complete smart contract platform. In addition, Hyperledger has also implemented a container-based smart contract (which is called a chaincode).

We believe that the smart contracts on the blockchain are about reaching another distributed consensus of calculated results using affirmed data as inputs such as transaction content, validity, order, history and so on.

In addition to the above consensus details, the blockchain technology also includes lightning network, side chain, cross-chain transactions, hidden address (Stealth Address), confidential transactions, etc. and is not limited only to the distributed consensus technology.

Design goals

The mission of the AntShares is "Digital Assets for Everyone". Bitcoin and other blockchains hope to build a parallel to the real world financial system. AntShares wants to build a financial system that can bridge the gap to real world assets. At the same time, the AntShares target audience consists of mainstream Internet users, not just liberals, geeks and developers. In order to achieve this vision, AntShares needs to use different designs on the base level.

Compliance with the Physical World

- Replace the token with an electronic contract

The practice of digitizing assets in the blockchain world is called "tokenization". That is, the user issues a custom token and declares that the tokens represent an asset. Then this token can be traded and exchanged similarly to a Bitcoin.

However, there are many flaws in the legalization of the token. The circulation of the token is similar to a transfer - the token can be transferred from the sender to the recipient without the consent of the recipient. This circulation is only suitable for assets of simple rights and without obligations (like money), and not applicable to equity, claims and other assets with complex rights and obligations. In AntShares, in order to complete the transfer of assets using electronic contracts, most of the cases will require the sender and recipient to sign with their respective private keys. In some cases, asset issuers are required to participate in the signature. Using electronic contracts to record the transfer of assets on the AntShares blockchain is merely another way to transfer offline assets and does not create any new legal relation, solving the legal flaws of tokenization.

- Account Authentication

Real name identity information is the basis of a large number of real world assets. In most cases the legal contract (legally binding contract) also requires real-name signature. When the legal conditions of the exchange or transaction participants have real name requirements, the user should have the ability to prove their true identity. At the same time, the disclosure of such information should be controlled by the user. A third party outside of the transaction should not receive user identity information. At the same time, identity authentication is only an option, not mandatory. If the transaction participants do not require each other's real names, the users do not need to authenticate.

AntShares uses digital certificates to implement user authentication. Users (individuals or organizations) can apply for a digital certificate from the certificate authority (CA) to prove the correspondence between the public key and the identity they control. AntShares does not specify a CA, but instead the transaction participants choose a self-approved CA. For example, a Chinese user may choose any of the 38 CA agencies certified by the Ministry of Industry and Information, or may choose a company that is registered on the exchange to be the CA to verify and distribute the certificate.

Unlike the X.509 digital certificate implementation scheme, AntShares plans to use the blockchain to maintain the certificate revocation list and gradually form a set of digital certificate systems and identity authentication schemes based on blockchain technology.

Fulfilling the needs of financial transactions

- Non-breaking deterministic billing

We believe that the existing consensus mechanism of the blockchain can be divided into two categories: "single bookkeeping" and "joint accounting".

Bitcoin, Ethereum, BitShares, etc. utilize the "single bookkeeping" model. In "single bookkeeping" model, a single node complying with certain rules (such as the power, interest, ballot) is able to complete a single block of accounting work. The other nodes express the recognition of the block by appending a new block after this block. The action of appending blocks is equivalent to them voting on history. When the bifurcation occurs, which history with more votes (longer chain), becomes the consensus.

Transaction confirmation under the "single bookkeeping" model is a probabilistic function. For example, the probability that a transaction (a transaction is included in a block) becomes a historical consensus is 98%, and the probability of becoming a historical consensus after two confirmations (including the transaction Of the blocks are added after a block)is 99%, while the six confirmations may be 99.999999%. But theoretically, there is a small chance of failure, even after ten thousand blocks. Bitcoin and other blockchain solves the issue by adding a manual checkpoint that fixes the history, to avoid such extreme cases.

If the "single bookkeeping" model is agreed by way of voting post transactions (additional blocks), the joint accounting model generates a deterministic billing node by means of prior resolution, thus avoiding post-event voting and obtaining certainty. In the public chain, this prior decision can be a chain vote. After selecting a group of billing nodes, each new block is signed by these billing nodes. In this way, the model of "vote later, confirmation probability increases with votes" is changed to the model of "vote first, confirmation is final", and the ideal transaction fineness is obtained (finality).

Post-voting (additional blocks) in the "single bookkeeping" model is a vote on the block content rather than the block builder, so it is suitable for the public chain without identity information. However,under such a model, the final confirmation is weaker and not suitable for financial transactions. The joint accounting model needs to introduce a weak trust in the billing node, ie, it is believed that there will not be a large number of (usually 1/3 or more) of the billing node colluding. Then it is necessary to understand the identity of the controller of these billing nodes so that: firstly, one can determine the reputation and technical ability, and secondly, if colluding occurs, one can use the cryptographic evidence to follow up. So the joint bookkeeping is suitable for the public chain and affiliate / private chain with identity information.

It is generally believed that the "single bookkeeping" model is more usable, that is, it is still able to work when a network split occurs (such as a country's Internet connection with another country). But this usability is only applicable to nodes that follow a longer chain. When the network partition is restored, the history of the node following the shorter chain is rewritten by the long chain. For a node that follows a shorter chain, this is an illusory usability created by sacrificing consistency.

It can be said that the "single bookkeeping" model has chosen anonymity, to achieve no need for any node trust, but at the expense of consistency and finality; the joint accounting model chose consistency and finality, but the identity of the billing nodes is required in order to obtain weak trust of the other nodes

- Use fiat currency as currency

There are three core functions of money: exchange medium, accounting units and value storage. Bitcoin and other encrypted digital currency is a good exchange medium, users can, through Bitcoin, engage is global circulation of value. However, the general inelasticity of encrypted digital assets brings high volatility, thus failing to realize the full currency function of the accounting unit and the value store. BitShares, Nubits and other systems are trying to design a stable encrypted digital currency that is anchored by fiat currency, but it is not very successful and has a narrow range of applications.

AntShares will use fiat as its internal currency.

- Node division and specialization

In the original design of the original Bitcoin is flatness. All nodes are involved in: accounting (mining), storage of complete historical data, broadcasting transactions. There is no division of labor. However, in practice, specializations in Bitcoin slowly appeared. Accounting (mining) evolved from the idea of the "one CPU one vote" to the use of GPU, FPGA (ready-made programmable gate array) and ASIC (ASIC) of the mining machine. At present, devices other than ASIC computing devices can not economically carry out mining. The accounting node has been fully specialized.

The historical data of the past seven years amounting to dozens of GBs has also become a storage burden. Many ordinary users are no longer willing to store full historical data of the whole node, but instead use the web wallet, off-chain wallet and so on. Despite the various calls to run the whole node , the number of nodes continues to decline.

In AntShares, our design goal is to make the whole system to have a clear division of labor. The accounting node is most important role of the AntShares blockchain, tasked by AntShare holders to produce blocks and reach a common consensus. Full nodes form the main part of the AntShare blockchain network, usually ran by companies providing external services. These nodes save the complete historical data, listen to and broadcast transactions. Ordinary users are running light nodes or act as clients. Ordinary users ,through the browser or mobile app, can access the eco-system of AntShare service providers, only to synchronize and save their own data. Since the AntShares blockchain uses a weak trust-based joint accounting system, every block contains the digital signature of the billing node. Ordinary users can check the current block without downloading full historical data. We think that this model is condusive to the realization of "everyone's digital assets," the AntShares vision.

It should be noted that the weak trust is not the trust of a single accounting node, but trusting that the group of nodes will not collude; This is not trusting a shifting centralised body, but rather, a decentralised way of independently voting who to trust.

Highly scalable architecture design

- Low latency, high throughput, pluggable

Scalability is a major factor in the fight between blockchain technology and traditional methods . In order to achieve design goals of anti-audit and trustless, Bitcoin selected Proof of Work as its consensus mechanism. However, this also brought high latency, low throughput performance problems. AntShares uses a consensus mechanism that relies on weak trust and also creating specialized accounting nodes, ensuring low latency, high throughput. The consensus mechanism of the

AntShares guarantees to a large degree, the list of professional accounting nodes, thus achieving low latency and high throughput.

At present, block time of AntShares is manually limited to 15 seconds. In the future, when the latency between the billing nodes is low enough, most of the blocks are expected to be completed in 1 second. With about 100Mbit / s bandwidth and specialized hardware for cryptographic calculation, AntShares is able handle thousands of thousands of transactions per second.

In addition, AntShares is designed to be modular. Users can change the consensus mechanism, ECC / hash algorithm, P2P network protocol and other modules. At the same time, by viewing AntShares as voting rights in a organization, AntShares can be easily transformed into enterprise / private chain. Business organizations can conduct proof-of-concept on the AntShares public chain and, if necessary, quickly migrate to the enterprise / private chain model; conversely, the businesses can start using AntShares in a private chain and if needed, quickly migrate onto the public chain without repercussions.

- Hierarchical design and superconducting transactions

In order to support a variety of assets, multi-type transactions at the same time to achieve good scalability, layered design is essential. Ripple, BitShares, NXT, etc all are blockchains of decentralized functionality but without layered design.The blockchain itself acts as the ledger and transaction matcher. In such a blockchain, pending orders, withdraw orders, matching and other operations are recorded on the blockchain. This design has many drawbacks:

- Pending orders, withdrawal orders need to wait for block confirmation, this large delay results in a poor experience
- Pending orders, withdrawal orders need to pay transaction fees and also increase the storage and bandwidth consumption
- Due to the it existing on an exchange, the order of transactions becomes extremely important. By aligning the order book and the transaction matching at the blockchain level, the accounting node is given larger power. The accounting node can sort the trade, choose, and have the front-running capability according to its wishes.

Although AntShares support the exchange of assets on the chain, the blockchain itself does not provide order book and order matching functionality. The chain is only responsible for the execution and settlement of the transaction. Our hierarchical design puts the order book and matching function on the second layer, through a mechanism called "superconducting" to achieve a complete transaction function.

Under the superconducting transaction, the two parties do not need to host the property to an intermediary (traditional exchange). Users only need send to the exchange an order signed with their private keys. After the exchange matches the buyer and seller orders and broadcast transactions is the transaction complete. From beginning to end, property does not leave the user's control, putting an end to the traditional moral hazard. Exchange under the superconducting trading mechanism only plays the role of information matching.

In the superconducting trading mechanism, because the user has absolute control, so the user can take the initiative to double the order so that it cannot be resolved. This problem can be settled by the exchange blacklisting the user as a way of punishment and deterrence.

Applications

Crowdfunding and equity trading

The AntShares blockchain can be used for crowdfunding. The company raising funds can still go through various fund-raising platforms to complete the fund-raising, but the it can utilize the immutability of AntShares blockchain publish its public documents. After the crowdfunding, the company can use the AntShares to distribute the shares to the large number of investors, avoiding cumbersome paper instruments and offline labor. The share on the chain a liquid asset, the user can carry out point-to-point equity transactions through AntShares. Compliant trading exchanges can also utilize AntShares, providing non-listed companies equity trading services. Through AntShares, start-up companies can obtain market valuation, equity liquidity,users obtain access to the exit mechanism to solve the difficult problems of exiting an crowdfunding.

In addition, the AntShares can also facilitate the management of the amount of money raised through crowdfunding. In recent years, countries have introduced the relevant laws and regulations on crowdfunding. These laws and regulations tend to restrict investors in eligibility, investment and other specific provisions. For example, the JOBS Act Title III, which came into force in April 2016, provides for a maximum of $ 100,000 for a single investor's maximum annual investment share. Through the AntShares can facilitate the regulation on the total amount of limited control.

Employee holdings and capital structure management

Companies that use the Employee Stock Ownership Plan (ESOP) and who needs cap table management can use AntShares to carry out equity management. Some of the companies in the United States have already purchased a centric service provider like eShares to carry out the electronic management of the cap table, but the centralized system has many drawbacks. For example, eShares is a single point of failure.If ever eShares service is down or blacklisted, then the equity information of companies using eShares is at stake.

Block-based technology is more economical and more secure than such a central system. There is no single point of failure, thus companies using it do not have to worry. The smart contract function gives the company a flexible to transfer control or ownership. The company can limit the equity to be held only by designated by the employees and investors, you can set the flexibility to allow the transfer of shares or the proportion of transactions. For example, you can set up to allow employees to transfer up to 10% of their own shares each year.

At present, the solution for the consulting firm that provides ESOP solutions is still accomplished through paper instruments. Through AntShares, such consulting firms can provide customers with a powerful tool for digitally managing equity.

P2P loans

P2P loan platform using AntShares can solve many existing problems such as information opacity, incomplete information, debt liquidity and so on.

First of all, the existing model of P2P loan platform internal database is the creditor's only source of claims, in the event of hacker tampering, data corruption, platform collapse and other events, it is difficult for creditors to prove their case. In the 2015-2016, the wave of collapses of China P2P lending platform has exposed this risk. Once creditors find that out that the platforms are unavailable, they are in the situation where they are unable to prove their claims.

Second, the P2P loan platform for the borrower's credit limit is often limited to the platform itself. For example, a platform, through the credit process, finds out that the borrower's repayment capacity of 100,000 yuan, then the borrower's credit limit on the platform is 10 million. But this can not prevent the borrower in the n platform for borrowing, bear n x 10 million in debt. The general ledger feature of AntShares blockchain allows the P2P loan platforms to share the borrower's credit line. This is similar to how AntShares can be used to control the amount of equity an investor can buy.

Finally, by using AntShares to record P2P loan claims, the claims become transferable, collateral, and even programmable. Creditor's rights can not only be transferred within the platform, but also cross-platform, increasing it's liquidity. With creditor's rights becoming transferable, long-term debts become more attractive. Users buy long-term debt without worries, enjoy high interest rates, without fear of emergency. Through the transfer function of AntShares , long-term bonds can be discounted or mortgaged.

In addition, the use of AntShares to manage the equity of the enterprises can even use the AntShares to mortgage equity or issue corporate bonds.

Points management

Airlines, operators, banks, restaurants and many other commercial institutions will issue their own points. Through a point system, companies encourage the retention of users and multiple consumption.

The database of issuing organizations are data silos (information silo). Organization A can not obtain information of the points system of another organization in a trustless manner, so it is difficult to achieve points interoperability between the two. The distribution of points through the AntShares blockchain can be disclosed transparently and is credibly accessible by anyone, limiting the powers of the issuer. The user's exchange needs and the market maker's profit-making will form a variety of points in the trading market, activate the hidden potential in this system.

Supply chain finance

Supply chain finance covers a wide range of business models and links, from the factoring, trade finance, warehouse receipts, accounts receivable financing to the supply chain of corporate bills, corporate credit financing and other financial business links. Based on the blockchain technology to provide distributed, non-tampering business information recording platform, you can participate in certification, transaction verification and timestamp verification, bank financing survey, corporate financing materials and other links to provide a true and effective, low-cost solution, thereby enhancing the overall effectiveness of supply chain finance.

Others

Digital asset functions can also be used distribute shares, financial proofs, etc .; digital confirmations can be used as receipts, agreements; Decentralizaion functions can be used for large-scale commodity exchanges, and foreign exchanges.

Legal Status

(To be revised)

AntShares do not have a universal payment in terms of an original currency. An AntShare is not a kind of digital currency, but a blockchain agreement, [Edit: this is confusing: so there is no monetary legal dispute, not five ministries "on the prevention of bit currency risk notice" refers to the virtual currency, with banks, payment agencies]

Individual users and organizations can be certified by the government-authorized CA certification body. The equity registration on the chain chain is electronically signed by a company certified by real name. The transfer and trading of the shares are made by the assignor, the assignee and the company. Before the signing of the three parties, the Company has the obligation to ensure that the transfer and transaction of the shares are in line with the provisions of the Company Law, which are required to obtain the original consent of the original shareholders, the original shareholders' right of subscription and the limitation of the number of shareholders. The nature of the equity transfer and the transaction is an electronic contract in which the parties are engaged in electronic signatures.

Ants built-in KYC (user identity) and AML (anti-money laundering) interface program. Third-party payment, bank and other financial institutions can be used to comply with the agreement. Taking into account the possibility of missing the key, the AntShares also designed an asset recovery mechanism - immediately you lost an address of the corresponding private key, you can still without the help of a third party, you can retrieve the assets.

Economic model

System assets and fees

There are two built-in system assets: AntShares and AntCoins. AntShares represent the ownership of the blockchain, which is used for electoral accounting, to obtain AntCoins dividends, etc. AntCoins represents the right to use the blockchain, and are used to pay fees of various systems on the chain.

System cost

Writing data to the blockchain requires paying a small amount of AntCoins as the system cost, which is divided into two categories:

- The bookkeeping fee charged by the accountant

When writing a transaction to the blockchain, the transaction generally requires some AntCoins as an account fee. The accounting fee is charged by the accountant to subsidize the storage, bandwidth, and expenditure of the accounting node.

Whether the collection fee is collected, and how much is collected is determined by the accountants. A transaction can be free, as long as more than 2/3 of the accountants are willing to write the transaction. Therefore, organizations using AntShares in bulk can pay the bookkeepers with currency offchain, reducing the need to pay with AntCoins.

- Additional charges for holders of AntShares

Additional service charges refer to the cost of using AntShares blockchain to complete certain advanced functions and is paid with AntCoins. The types of transactions that currently require additional service charges are: asset creation, candidate registration. Additional premiums will be required for future upgrades such as asset changes, asset write-offs, and asset freeze.

Additional service charges will be recorded according to the proportion of AntShares held immediately to the address of AntShares holders. AntShares holders can claim the coins registered in their names at anytime.

AntShares

AntShares, abbreviated as ANS.

A total of 100 million AntShares, representing the ownership of the chain. 100 million will be created in the Genesis Block and distributed accordingly. The total amount of AntShares shares are constant at 100 million and can not be increased. The smallest unit of the AntShares is 1 AntShares and can not be divided.

The main use of AntShares shares:

- Vote to choose the accountant
- Get AntCoins generated by new blocks
- Obtain additional service charges for AntCoins
- Vote to decide the matter of the AntShares blockchain

AntCoins

AntCoins, abbreviated as ANC.

A total of 100 million ANC will be produced, representing the right to use the chain. The AntCoin will be generated with the formation of each new block, in accordance with a decreasing rate of generation, it will take around 22 years for the amount of ANC to grow from 9 to 100 million.

The main purpose of AntCoins are:

- Pay the payment fees of the AntShares blockchain
- Pay an additional service fee for the small block area chain
- As a deposit for the deposit of the candidate

Assignment and distribution

The distribution mechanism of AntShares

100% of the total amount of AntShares shares in the creation of a block was created. Before the creation of AntShares the team set certain rules on the distribution of AntShares shares.

About 10% of the AntShares shares were allocated to the early supporters of AntShares in June 2014, earning $600,000 in seed funding. Of which 400,000 yuan by a number of individuals after a 5 million overall valuation of investment and 200,000 yuan by the venture capital institutions Ra Li capital after a 10 million yuan overall valuation of investment. Individual contributors also provide all kinds of support in full time or part-time free of charge.

Approximately 17% of the AntShares shares were completed in October 2015 for ICO 1 and assigned to the participants, earning more than 2100 bits. Of which about 1,200 bits are from individual investors and about 900 are from a single institutional investor.

Approximately 23% of the AntShares will be allocated to participants in ICO 2 launched in August 2016. The ICO does not set the price and ceiling, but the design of the return mechanism, see ICO rules.

The remaining 50% of the AntShares shares held by the AntShares team, will be in the AntShares net after the use of AntShares smart contract locked for 1 year. 1-year lock-up period, this part of the AntShares will be used to maintain the long-term development of AntShares.

Early supporters, ICO 1 participants, and the AntShares shares assigned by ICO 2 participants will be available immediately after the operation of the small-ants blockchain. The small nest blockchain is expected to run in the fourth quarter of 2016.

The release mechanism of AntShares

AntCoins are produced with the generation of each new block. The initial amount of AntCoins is zero and it grows until the total limit of 100 million after about 22 years. The interval between each AntShares block is about 15 seconds, about 2 millions blocks are generated in a year.

In the first year (Block No. 0-No. 2,000,000), each block will generate 8 ANC; In the second year (Block No. 2,000,000-No. 4,000,000), each block will generate 7 ANC; the amount of ANC generated decreases by 1 each year till year 8 where each block generates only 1 ANC. From then on, the rate is kept constant until about 22 years at the 44 million block, the total amount of ANC reaches 100 million, at which point ANC will stop being generated.

According to this curve, 16% of ANC will be created in the first year, 52% will be created by the end of the 4th year, 72% of the ANC by the end of the 8th year..

These small coins will be distributed proportionally to corresponding ANS addresses. AntShare holders can claim these ANC anytime. For example, if someone holds 1% of the whole net, the user will be able to get 8/100 = 0.08 AntCoins per block for about 460.8 AntCoins a day.

Technology Architecture

User

Private key, public key

Private key: A 256-bit hash generated by the user to be kept and not exposed. The private key is the proof of ownership of the user account and the ownership of the asset in the account.

Public key: Each private key comes with a matching public key. Public keys in AntShares are generated by the private key through the ECC (Elliptic Curve Cryptography) curve algorithm. The algorithm used by AntShares are secp256r1 and SM2 (Chinese commercial cryptographic algorithm).

Script, address

Script: AntShares uses an OP_CODE scripting system similar to Bitcoin. The OP_CODE in AntShares is a Turing-complete set of instructions. For example, the following two scripts can be used to verify multiple signatures

```
OP_M (public key list) OP_N OP_CHECKMULTYSIG
```

```
OP_PUSHBYTES M (public key list) OP_PUSHBYTES N OP_CHECKMULTYSIG
```

Address: The address is the hash value of the script. The form of the address is as follows:

```
AM2Y8aSWh3LTwQBoZCNSVNCF9eqVt2vmVX (secp256r1 / SHA256 algorithm)
SSYfWvN36FsWejmGXyhBtP5iKq9EGuaEPr (SM2 / SM3 algorithm)
```

The hash algorithm supported by the AntShares is SHA256 and SM3 (Chinese commercial password algorithm)

Account and account address

An account is a combination of a number of (1-16) public keys. The most basic account consists of a public key whose account address is its 1-of-1 multi-signature address.

In more advanced designs, the account can be composed of two public keys, generated by the 2-of-2 multi-signature address for the account address. Of the two public keys, the one with the smaller value becomes the payment key the larger one becomes the query key. The query private key allows the user to read the balance of the asset and the historical transaction information that can be controlled by the account. Holding both private keys gives the user complete control over all assets in the account. Combined with AntShares' stealth addressing system, users can provide the outside world with a fixed address as a point of entry without sacrificing privacy.

In the wallet client, the private keys are used for separate functions. The interface will be similar to online banking, using one private key to login and using the payment private key to confirm transactions.

Authentication

The user (person or organization) may apply for identity authentication to the CA certification authority to provide true identity information to other transaction participants in the transaction. When applying for authentication, the user provides the CA with the public key and identity documents signed with the corresponding private key. After verification, the CA issues a digital certificate to the user, which is signed by the CA, which contains the user's public key and identity information. The digital certificate proves the one-to-one correspondence between the public key and the user identity.

When a user uses AntShares, the transaction is signed with the private key corresponding to the public key. The signature is in accordance with the definition of "reliable electronic signature" in China's "Electronic Signature Law" and is legally binding.

Privacy Protection

There are some contradictions within blockchain regarding the need for openness and privacy, but through some cryptography techniques, we can solve the privacy protection problem.

The privacy protection scheme of AntShares combines the multi-signature concealment address, the addition of homomorphic encryption and other leading cryptography techniques. Other than the direct participants of the transaction, other third parties can verify the validity of the transaction, but can not know the participant's identity and transaction amount.

Transaction data under multiple signatures are still publicly available, but there is no analytical linkability between each transaction. Even if the same person sent you a number of transactions, these transactions will be scattered across a number of unrelated addresses, no one other than yourself will be able to discover or prove that these addresses belong to you. AntShares builds upon the work done on BIP63 and adds in multi-sig and stealth addressing functionality, creating a multi-sig stealth address feature. This will be explained in detail in another paper.

Multiple signature stealth addresses can include user identities but can not protect transaction amounts. AntShares uses additive homomorphic encryption means to hide the transaction amount, yet allowing the nodes in the network to verify the validity of the transaction. The other nodes in the network can verify that the balance of the asset in the entire network is unchanged after the transaction of an asset is completed, thus verifying the validity of the transaction without knowing the specific transaction amount.

Assets

The assets of the AntShares block can be divided into system assets and user-issued assets. The system assets are the represent the rights in the AntShares agreement. The user's assets represent the rights of assets outside of the AntShares blockchain.

System assets

System assets include AntShares and AntCoins. AntShares represent system ownership, AntCoins represent the right to use the system. The specific form of AntShares and AntCoins has been described in the chapter "(b) the economic model" and will not be repeated.

User-issued assets

Any user can issue assets. Assets are created and distributed in two steps. After creation, the assets are registered in the blockchain but are not actually generated to any address; after the distribution, the assets actually enter the address.

Currency: The AntShares block-chain agreement introduces the external currency in the form of a gateway. Currency transfer does not require a recipient signature.

Equity Assets: Equity assets are used as shares of a representative company (or stock company stock) to issue assets. The transfer or transaction of an equity asset requires the signature of the recipient.

Creditor's rights Assets: Creditor's rights are used as monetary liabilities representing individuals or organizations.

Other assets: other types of assets, assets founders can customize.

Trade

A transaction is a matter that invokes or changes the rights of any asset on the chain. There are a number of types of transactions designed in the system, each containing an input list, an output list, a signature list, and specific data related to the transaction type.

Asset-related transactions

Asset creation: used to create a new user to issue assets. The user can define the type, name, total, etc. of the asset and specify the administrator account of the asset. The creation of assets requires the consumption of a certain number of registration vouchers as an additional service charge.

Assets Distribution: Within the limit of the total amount set by the asset creator, the asset is created at the address specified by the issuer. Asset allocation can be completed at one shot or done in batches.

Asset change, cancellation, freeze: Not yet supported, will be supported in future releases.

Asset transfer related transaction

Contract Agreement: Specify all participants of the transaction and determine whether they are required to confirm acceptance based on the type of asset involved in the transaction. The recipient can choose to accept (signature) or reject (ignore).

Commissioned transactions: do not specify the recipient, but specifies an agent. The agent is responsible for matching the recipients. "Superconducting transactions" is done through such methods. The transaction structure of the superconducting transaction is as follows:

```
public class Order // order
{
    public UInt256 AssetId; // Asset
    public UInt256 ValueAssetId; // Unit Price
    public UInt160 Agent; // agent
    public Fixed8 Amount; // Total amount of transactions
    public fixed8 Price; // transaction price
    public UInt160 Client; // client
    public transactionInput[] Inputs; // transaction input
    public byte[][] Scripts; // signature list
}
```

Accounting related transactions

Registration, withdrawal of Candidate: The user who wishes to register as a candidate accountant is required to pay an additional service fee and at the same time freeze a registered voucher at the account address. Candidates can use the frozen coupons at any time, but if so, they will be disqualified and need to be re-registered as a candidate. The user should be prepared to participate in the accounting prior to registering as a candidate. Candidates may be elected as official accounts at any time.

Election account: see the accounting mechanism

Transaction fees

Transaction costs are divided into accounting fees and additional service fees, are paid in AntCoins. Specific in the "(b) economic model" chapter to be explained, not repeat them.

Accounting mechanism

Blockchain

AntShares uses a block-like chain similar to Bitcoin to record data.

The blockchain can be imagined as a book, and each block is a page of accounts in the book. Each page contains transactions for a preset period of time. The AntShares blockchain generates a block every 15 seconds. The new block is attached to the previous block and forms a chain structure. Each block contains transaction information that occurs within 15 seconds, as well as other necessary retrieval and verification information.

The block data structure of the small-ants block is shown as follows:

```
public class Block // block
{
     public uint Version; // version
     public UInt256 PrevBlock; // linked block
     public UInt256 MerkleRoot; // The hash value of the transaction list
     public uint Timestamp; // timestamp
     public uint Bits; // keep fields
     public ulong nonce; // random number
     public UInt160 NextMiner; // next block
}
```

For more information on the consensus mechanism, please refer to the AntShares consensus White Paper