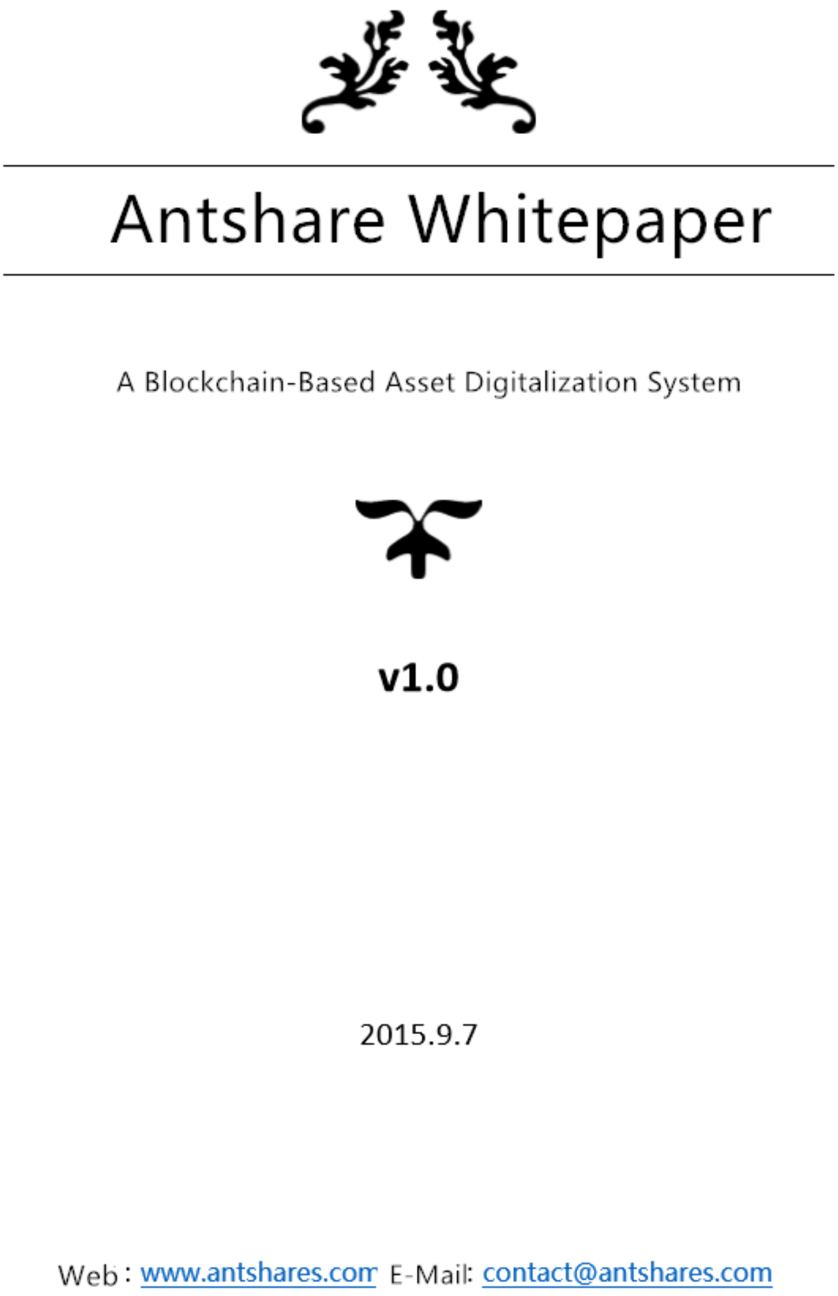
# Whitepaper 1.0

https://github.com/cmptrx/AntShares/wiki/Whitepaper-1.0



## Antshare Whitepaper

A Blockchain-Based Asset Digitalization System

**v1.0**

2015.9.7

Web：www.antshares.com E-Mail: contact@antshares.com

A newer version of this paper is under revision. The link is Whitepaper 1.1.

Introduction

Charpter 1 Overview is a generalized description of Antshares, for all readers.

Charpter 2-7 comprises logical description of the Antshares techlogocial solution, for readers with background knowledge of the blockchain.

As an open-source project in compliance with the MIT open-source protocol, Antshares source codes are stored at https://github.com/Antshares/Antshares

# Table of Contents

#1 Overview

##1.1 What is the Antshares?

Antshares is a blockchain-based decentralized network protocol, capable of digitalizing real-world assets and rights and, via a peer-to-peer network, enabling financial services including registration, issuance, tranfer, trade, clearing, and settlement.

Antshares could be applied to stock equity crowdfunding, p2p finance, digital asset management and smart contracts, etc.

##1.2 What is the Blockchain?

Blockchain is a type of data structure based on cryptography. It organizes and maintains large sum of data in a decentralized fashion. Blockchain is best-suited to function as the ledger of e-cash, or, digital assets.
All data on the Blockchain are attached with relevant digital signatures, providing immutability.

Meanwhile, blockchain carries merits like full-openness, high reliability, real-time settlement and trust-free, etc. A blockchain-based financial system is overwhelmingly better than a traditional and centralized one. We believe the Blockchain could become the mainstream underlying technology for financial networks.

##1.3 Application Scenarios of the Antshares：

###1.3.1 Stock Equity CrowdFunding

Antshares can be applied to stock equity crowdfunding. Upon completion of the crowdfunding, start-ups could use Antshares to manage the equities held by various shareholders. Stock equity trades could be available with the Antshares-enabled decentralized trading mechanism. While start-ups acquire a market valuation and liquidity, their users would be offered with an exit mechanism. By registering stock equities on the Antshares Blockchain, start-ups may acquire funding in a *Blockchain-IPO* fashion.

###1.3.2 P2P Finance

P2P Finance sector may utilize Antshares for registering creditor's claims, making them transferrable and tradable, thus increasing the liquidity. They may reach users beyond its own clientele. Users, on the other hand, can be assured to purchase long-term claims with high interest rates without worring for an emergency monetization. With Antshares's trading system, they may monetize their long-term bonds under discount.

Additionally, companies could utilize Antshares for issuing their own company bonds.

###1.3.3 ESOP, Employee Stock Ownership Plan

Companies with ESOPs may use Antshares for management of the employee shareholders. Instead of developing its own system, simply utilizing the Antshares would be a much more economical and secured approach. Antshares, by design, offers flexible stock transfer control to client companies. A company may, for example, set a limit that only designated employees may hold company stocks, or, set a proportion on the stocks transfferable and tradable, say, only 25% of the stocks held by an employee could be traded every year.

###1.3.4 E-Contract

Unlike blockchain-based payment systems like the Bitcoin, Antshares is rather an e-contract system. Users sign the contracts with their own private keys for the exchange of digital assets. In fact, Antshares can be deployed for signing any kind of e-contract. If the subject matter of the contract are registered digital assets on the Antshares Blockchain, the contract will be automated onchain to a programmed delivery and execution. However, if the assets in quetion are offchain, parties involved may execute on their own. Even in the latter situation, Antshares could have cut off the red tape of signing and storing large sum of papers. Also, digital signatures will ensure the non-repudiation of the contracts.

###1.3.5 Others

Antshares users could issue their own assets, including credit points, shares of a fund and property certificates, etc. Further, the e-contract funcionality of Antshares is suited for storage of evidence and financial contracts while the decentralized exchange function could be applied for commodity and foreign exchange markets.

##1.4 Behind the Design

###1.4.1 Decentralization of Power vs. Decentralization of Transaction

It is a power to control properties and it is autonomy and decentralization that we pursue. Bitcoin, via its public key system and PoW consensus mechanism, have successfully achieved the autonomy and decentralization of property rights.

However, a complete decentralization is not necessary when, with certainty and in an accountable way, conducting simple transactions without discretion. For example, an open-source project does not require everyone to code independently. Compiled versions are there for downloading, while just a handful of people may be actually doing the validation.

If the accounting mechanism of the blockchain were to be designed for simple transactions that are with certainty, without discretion and accountable by cryptographic evidence, greater efficiency could be achieved in lieu of a complete decentralization.

Bookkeepers of Antshares enjoy much lesser power than Bitcoin miners. In this context, bookkeeping becomes exactly a simple transaction. With this design, Antshares is capable of a settlement window of about 15 seconds.

###1.4.2 Settlement Blockchain vs. Log Blockchain

Ripple, Bitshares and Counterparty are all Log Blockchains, documenting all user behaviors. For example, to send a bid instruction in the Counterpary, which is based on Bitcoin Blockchain, you have to wait for 10 minutes to have a successful bid placed (not deal). Moreover, the fees you have to pay for a bid is higher than the regular transfer fee.

Antshares, on the contrary, is designed as a Settlement Blockchain. That is to say, log transactions like bids and cancels will not be written onto the blockchain. Antshares Blockchain is solely for registering transactions within which asset changes take place. Settlement Blockchains, sacrificing some non-essential information logs, could achieve better throughput, flexibility and user experience. Also, deprived from it, a brand-new type of decentralized transaction mode we call Super-Conducting Transaction emerged.

###1.4.3 Parallel-to-Finance vs. Bridging-the-Finance

The PoW mechanism, which is adopted by the Bitcoin, provides great censorship resistance. Anonymity is enjoyed by users (in transfers) and miners (in bookkeeping) alike. However, censorship resistance poses difficulties in compliance issues. Bitcoin has created a financial system parallel to the existing ones in the real world. But we believe parallel systems are difficult to bridge real-world assets. Stock equities and creditor claims bound by real-world laws are difficult to be bridged onchain with compliance.

The target clientele of Antshares is the entire existing Internet-financial eco-system, so large sum of real-world financial assets will be bridged onchain. On that account, the design of Antshares has taken into consideration of compliance issues, and has defined itself as a blockchain financial system bridging the real-world.

##1.5 Characteristics of the Antshares
###1.5.1 Bridging Real-World Finance with Compliance

Antshares is after the compatibility with the real world.

Antshares provides Chinese-law-recognized identity authentication solutions for both individual and corporate users. Digital signatures of the authenticated accounts will be recognized and protected by the *Law of Digital Signature* of China, and function as regular signs and seals. It is worth noting that identity Authentication is optional, not mandatory.

Transfers and trades of assets like stock equities are in fact multi-party-signed e-contracts, so they are recognized and protected by the *Contract Law* of China.

###1.5.2 Decentralized "Super-Conducting" Transactions

Superconducting transaction is a unique feature of Antshares. Users will be able to have an experience greater than what centralized exchanges could offer, and concludes decentralized transactions. Also, users do not need to deposit in advance to place bids. When deals are made, exchanges will broadcast them on the Antshares network before they are written onchain.

For example, a user A sells equities of a certain company via the superconducting transaction. User A does not need to deposit the equities into the exchange in advance. He signs the bid with his private key locally. When the deal is made with a counterparty, fiat currency (in this case, RMB) of the counterparty will be transferred to the wallet of User A, no need for a relay through the exchange.

Superconducting exchanges do not manage the properties of their users. There will be no deposits or withdrawls. This contributes to simplified operational procedures and increased user trust. Anyone, an institution or an individual, could be a superconducting exchange, as long as hardwares for a stable matching service are provided.

Superconducting transaction creates a new form of trading: Exchanges do matching while the blockchain delivers properties. Superconducting exchanges have no special powers, because they do not do escrow, and all transaction instructions are served with cryptographic evidence. Given that, regulators may not implement pre-approval on these exchanges. We believe, with the blockchain technology becoming the mainstream, superconducting model would prevail in the mainstream financial markets including the Chinese A-share market.

###1.5.3 Familiar User Experience:

Ordinary users are not necessarily ANS/ANC holders. And there are two "passwords" for query and payment respectively.

Tradings on the Antshares are performed via superconducting exchanges. AntCoins are not charged for bids and cancels. When a deal is made, the exchange will pay the ANC for writting information onchain. This experience is just like traditional stock markets in that users do not necessarily hold ANS/ANC. Moreover, by design of the Antshares protocol, the client of the software adopts two passwords (private keys), one for query and the other for payment. This provides a user experience similar to traditional e-banks, reducing the learning cost of users while maintaining sound security.

###1.6 Legal and Regulatory Compliance

A universal natural currency capable of payment and pricing does not exist in the Antshares; rather, fiat currencies like the RMB are introduced through gateways. Antshares itself is NOT a digital currency, but a blockchain protocol, eliminating currency-related legal issues and excluding it from the definition of a digital currency in the *Notification on Preventing the Risks Posed by the Bitcoin* published by 5 ministries of China. Antshares, by its nature, can enter into cooperation with banks and third-party payment providers.

Individual and institutional users of Antshares could perform real-name authentication through government-authorized CAs. Also, stock equity registration on the Antshares is signed with the digital signatures of real-name authenticated companies. Every trade and transfer of equities will be signed by the transferor, the transferee and the issuing body. This is to say, before every transfer and trade of equities, the issuing company who shall later be engaged in the signing, will be obligated to ensure the trade is in compliance with the *Company Law*, concerning consent from at least half of the original shareholders, pre-emptive rights, and limit on the number of shareholders. Transfer and trade of equities on the Antshares is essentially an e-contract digitally signed by parties involved.

Antshares has built-in KYC and AML APIs. Third-party payment providers, banks and other financial institutions may utilize the Antshares protocol with compliance. For the sake of lost private keys, Antshares has an asset-retrieving mechanism in place, i.e. even if you lose the private key to a certain address, assets within it are still retrievable without helps from a third party.

#2 User System
##2.1 Private Key, Public Key, Address, Account and Acccount Address

Private Key: A 256-digits nonce, kept by the user privately. The private key proves the right to use its corresponding account as well as the ownership of assets inside.

Public Key: Every private key comes with a corresponding public key. ECC public key are generated via one-way certainty algorithms.
Possible candidates: secp256r1 (international standard), secp256k1 (Bitcoin) and SM2 (Chinese standard).

Address: Scripts from ordered arrangement of a public key, generated by one-way certainty algorithms.
Currently supported scripts include:

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

Addresses are like:

AM2Y8aSWh3LTwQBoZCNSVNCF9eqVt2vmVX (secp256r1)
36wgQd5KunzhDbgF7eNhm7J5paCWzY2ghj (secp256k1)
SSYfWvN36FsWejmGXyhBtP5iKq9EGuaEPr (SM2)

The support on which one or all three depends on the solutions provided by the digital certificate and identity authentication partner. We are sured to support at least secp256r1 (international standard) for now.

Account and Account Address: An account is a combination of public keys of a certain number (1-16).
A basic account comprises one public key, making its account address a 1-of-1 multisig address.
In advanced designs, an account could comprise 2 public keys, making its account address a 2-of-2 multisig address. For these 2 public keys, the one lesser in value will be the payment public key while the other one the query public key. With the corresponding private key (query private key), the holder may access information on the balance and history that is in control of the account. With both private keys, the holder may control the assets that are in control of the account. With Antshares's privacy address solution, users could have a permanent account address for payment information and list it in the public without jeopardizing the privacy.

In the design of the wallet client, query private key and payment private key could be encrypted by query password and payment password respectively. The user experience here is similar to a e-bank, that is, to log in with the query password and pay with the payment password.

##2.2 Identity Authentication
Users (individual or institutional) may apply for identity authentication from a Certificate Authority, thus to enable them to provide identity information to the counterparty. When applying for the authentication, users shall provide public keys and identity papers with private key signatures. When checked, CA will issue a digital certificate to the user that had been signed by the CA and includes the user's public keys and identity information. This very digital certificate proves the correlation between the public key(s) and the identity of the user. (See Figure 1) With Antshares, users sign with the corresponding private key. This signature is within the defition of a "reliable digital signature" of the *Law of Digital Signature* of China, making them legally enforceable. (See Figure 2)

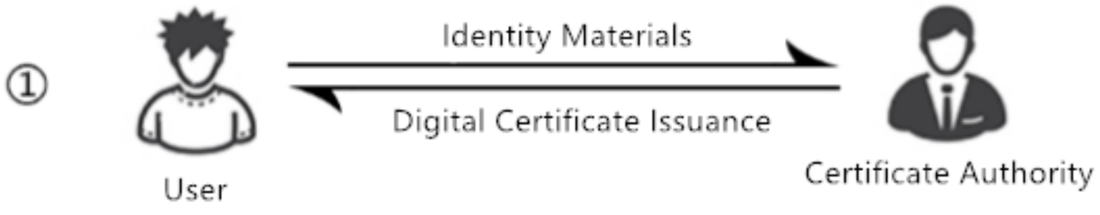


Figure 1: Identity Authentication

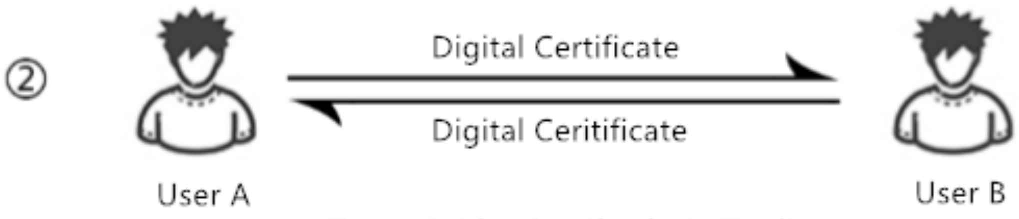


Figure 2: Identity Checks in Trading

Digital certificates containing user identity information will be kept by the user, not stored onchain. Given that, unless the user voluntarily provides the certificate to others, any third party will not be able to acquire his/her identity information. Unless vonluntarily provided, the user's identity finds no correlation to the public key.

##2.3 Privacy Protection—Open Address vs. Privacy Address
Data openness seems to contradict with privacy protection. However, Antshares tackles this issue with a multisig-based Stealth Address privacy address protection soluition. When using a privacy address, no one will be able to learn about the identities of the parties involved other than themselves.

Transaction data under privacy addresses are still in the open. But analyzable correlation between every other transaction does not exist. Even if someone send you multiple transactions, these transactions will be separated into multiple non-related addresses. Nobody other than yourself could find out or prove that these addresses are in your control.

Bitcoin has a BIP63 proposal on the Stealth Address solution. From there, Antshares had expanded it with features like multisig and query private key, thus forming its own privacy address solution.
The details will be elaborated in another article.

#3 Assets
Assets on the Antshares can be categorized into: a)Natural Assets and b)User Issued Assets.
Natural assets are the vehicles of Antshares protocol's internal rights and interests.
While on the other hand, user issed assets are the vehicles of assets or rights&interests beyond the Antshares protocol.

##3.1 Natural Assets

These include: Antshares and AntCoins.

###3.1.1 Antshares (ANS)

In total, 100 million Antshares would represent all of the ownership of the Antshares protocol. In the Genesis block, 100 million ANS will be created. Then, these ANS will be distributed under certain plans. The total amount of ANS is capped. ANS provides rights and interests like:

a) Bookkeeper Election
b) Acquiring AntCoins as dividends
c) Voting power over major issues of the Antshares protocol

###3.1.2 AntCoin (ANC)

In total, there would be 100 million AntCoins, accurate to 10-8. ANC represents the rights to use the Antshares protocol. ANC will be, under certain mechanism, distributed to ANS holders. ANC is capped as well.

Distribution of ANC can be calculated as follow:

Issued Amount at Current Block Height=(Total-Issued Amount at Last Block Height) x 2.4297257e-7

ANC is for:

a) Extra Service Charge Payment
b) Basic Byte Fee Payment
c) Bookkeeper Nominee Deposit as collateral

##3.2 User Issuance

Any user can issue assets. Assets are generated through creation and distribution.

###3.2.1 Currency

Antshares bridges external currencies through gateways.
Transfer of currencies does not require the receiver signature.

###3.2.2 Stock Equities

Stock equities represent stocks of a limited company (or a joint-stock company).
Transfer or trade of stock equities requires receiver signature.

###3.2.3 Bonds

Currency debts of an individual or an institution.

###3.2.4 Others

Custom-definition available for the creator of an asset.

#4 Transactions

This refers to transactions within which rights and interests of assets, or that of the Antshares protocol, change. Antshares's design covers many types of transactions. For every transaction, an input list, an output list and a signature list and certain data associated with the transaction classification always exist.

##4.1 The Asset-Related

###4.1.1 Asset Creation

This is to create a type of user-issued asset. User could define the classification, name and total amount of the asset and designate an administrator account of the assets.
Creation consumes some ANC as extra service charge.

###4.1.2 Asset Distribution

Within the total amount of the asset, a distribution from the scratch could be conducted by generating the asset into the creator-designated address. The distribution could be done once and for all, or, in anytime, in any order.

###4.1.3 Asset Alteration, De-Listing and Freezing

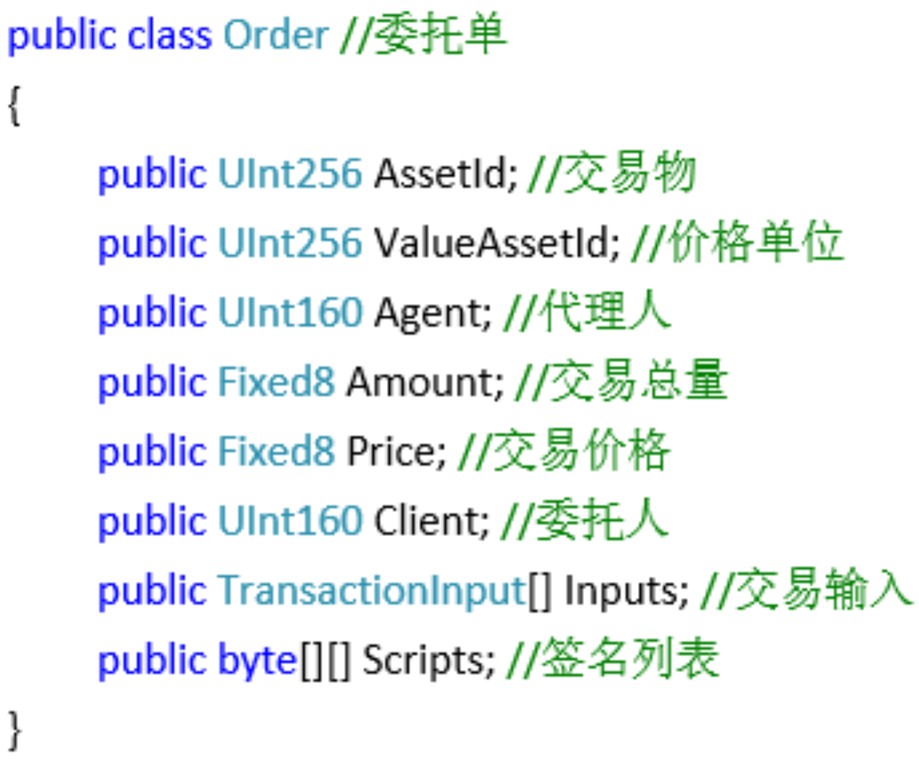
Coming Soon.

##4.2 The Asset Transfer&Exchange-Related
###4.2.1 Contract Trading

Designated counterparties. May implement a confirmation on the counterparty based on the type of asset in question. The counterparty may confirm to accept(sign) or refuse(ignore).

###4.2.2 Trust Trading

Counterparties un-designated but an agent designated. The agent will be matching trades.
Superconducting transaction is about this kind of trading, whose data structure is like:



```
public class Order //委托单
{
        public UInt256 AssetId; //交易物
        public UInt256 ValueAssetId; //价格单位
        public UInt160 Agent; //代理人
        public Fixed8 Amount; //交易总量
        public Fixed8 Price; //交易价格
        public UInt160 Client; //委托人
        public TransactionInput[] Inputs; //交易输入
        public byte[][] Scripts; //签名列表
}
```

##4.3 The Accounting-Related
###4.3.1 Bookkeeper Nominee Registration and Quitting

Users who wish to be registered as bookkeeper nominees need to pay an extra service charge and freeze certain amount of ANC to the bookkeeper address. Should the nominee move the frozen ANC, the candidacy will be revoked and a re-registration would be required. Users should be technologically-prepared before registering the candidacy. The bookkeeper nominee could be elected formal bookkeeper anytime.

###4.3.2 Electing the Bookkeepers

See Accounting Mechanism.

##4.4 Transaction Fees

Transaction fees are basic byte fees and extra service charge, both paid in ANC. While the latter one will be destroyed and then become the undistributed, for future re-distribution, the basic fees will be paid to the bookkeeper as economic reward.

###4.4.1 Basic Byte Fee

This is for bandwidth and blockchain bytes. It is proportional to the bytes used in a transaction, and collected by the bookkeeper. The bookkeeper may decide to charge this fee or not and how much in detail.

###4.4.2 Extra Service Charge

Extra Service Charge is the fee paid by AntCoins for advanced functionalities of the Antshares Blockchain. For the time being, extra service charge is required for Asset Creation and Registration for Bookkeeper Nominees. In the future, Altering, Writing-off and Freezing of Assets may require extra service charge.

Extra service charge will not be collected by anyone, but destroyed immediately and back to undistributed status. Through the distribution of ANC, they will ultimately be re-distributed to all ANS holders proportional to their shares.

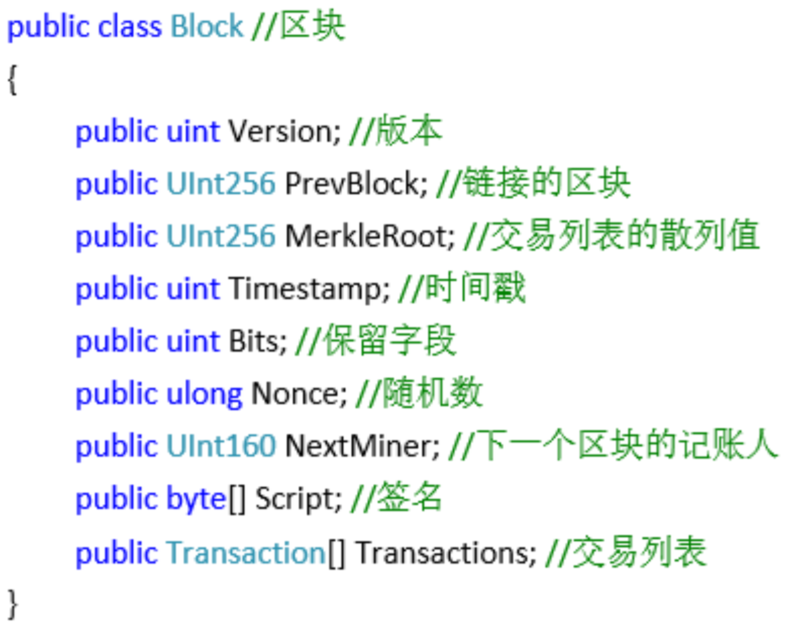
#5 Accounting Mechanism
##5.1 The Blockchain

Antshares keeps records of data in a way similar to the Bitcoin Blockchain.

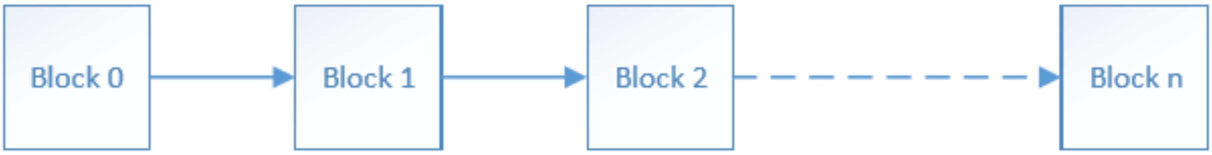
Blockchain can be seen as a ledger while every block is like a page of the ledger. On every page, all transactions in a pre-set time window are included.

For about every 15 seconds, a new block is generated on the Antshares Blockchain. Every new block comes after the one before it, forming a chain-like structure. All transaction information within 15 seconds are included in that block, along with other necessary index and validation information.

Bellow show the block data structure of Antshares:



```
public class Block //区块
{
        public uint Version; //版本
        public UInt256 PrevBlock; //链接的区块
        public UInt256 MerkleRoot; //交易列表的散列值
        public uint Timestamp; //时间戳
        public uint Bits; //保留字段
        public ulong Nonce; //随机数
        public UInt160 NextMiner; //下一个区块的记账人
        public byte[] Script; //签名
        public Transaction[] Transactions; //交易列表
}
```



A complete blockchain comprises of all transaction information since the Genesis block. So, by executing all these transactions, you get all the status and ownership of currently existing assets.

The decentralization nature of blockchain technology ensures the system to be strong and secured. The Openness nature brings to the system transparency and auditability. Antshares blockchain is capable of handling the equivalent amount of work of a traditional
centralized database with much smaller costs.

##5.2 Consensus Mechanism－Neutral Bookkeeping
Consensu mechanism is about how the nodes running the Antshares protocol reach consensus
on the status of the blockchain.

Antshares, through ANS holders' voting, decides the choices of bookkeepers and the number of them. The chosen bookkeepers shall reach consensus on the contents of blocks and decide on the transactions they should include.

###5.2.1 Characteristics of Neutral Bookkeeping

The accounting mechanism of Antshares is called Neutral Bookkeeping.

PoW, PoS and DPoS are about "who has the right to do bookkeeping." While neutral bookkeeping is about "how to limit the powers of bookkeepers". In such a consensus mechanism, bookkeepers can decide on whether or not to participate, but enjoy no power over transaction data alteration, manual exclusion of certain transactions or manual ranking of them.

With neutral bookkeeping, Antshares is capable of: a) a new block every 15 second, even 5 second after some optimization
b) a single bookkeeper cannot exclude a transaction from a block
c) every confirmation is done by all bookkeepers, 1 confirmation=full confirmation
d) with superconducting transactions, bookkeepers cannot do front-running by making up transactions.

###5.2.2 Electing the Bookkeepers

ANS holders may initiate a transaction of "bookkeeper election", and vote for any number (11024) of nominees. We believe bookkeepers should be identity-authenticated, so nominees would have to use other channels (say, a campaign website) to provide digital certificates that can prove their true identity.

Antshares shall collect all the votes in real time and have a list of bookkeepers and a number of bookkeepers needed. The latter number is calculated through: rank all nominees based on votes they receive, weighed by ANS holdings, pick out the 50% in the middle and get an arithmetical average. When the elected bookkeerps are below the minimum threshold, back-up bookkeepers of the system would be activated.

When confirmed on the number of bookkeepers needed, such a list would be generated by ranking votes. 1 ANS for 1 nominee equals 1 vote; 1 ANS for multiple nominees, they all get 1 vote respectively.

###5.2.3 Consensus on the Nonces
Before the generation of every new block, bookkeepers need to generate a block nonce collectively. Antshares adopts Shamir's Secret Sharing Scheme for this delibration. SSSS solution is generally used for sharing passwords. With SSSS solution, N pieces of encrypted text can be generated through text S. And with K pieces of them, text S can be reconstructed.

Say, N+1 bookkeepers could reach consensus on the nonce with 3 steps. Step1, pick a nonce and generate N piece of the nonce via SSSS solution, then encrypt with the public key along with other N bookkeepers and broadcast.

Step2, upon receiving the broadcast from other N bookkeepers, decrypt the part you can and broadcast.

Stpe3, upon receiving at least K pieces, the nonce is decrypted; with the nonces from all bookkeepers, merge them and you have a block nonce.

Block nonce is collectively generated by all bookkeepers. So, just one honest bookkeeper is enough to make this nonce impossible to predict or make-up, even if all the other bookkeepers have gone rogue.

###5.2.4 Consensus on Block-Included Transactions

In the aforementioned Step 1 broadcast of block nonce generation, bookkeepers also broadcast hashes of transactions they deem that should be included in this block. Upon detecting this broadcast, other bookkeepers may check that whether or not they have the corresponding transaction data of the broadcasted hashes. If no, then request them from other nodes.

When the block nonce has been generated, every bookkeeper must merge all transactions in the step1 broadcast (excluding transactions with only hashes, no matching data), and sign. A 2-of-3 signature from bookkeepers would complete this block, otherwise, this round of consensus of this block fails, everything back the step1 of 5.2.3 and try again.

###5.2.5 Consensus on the Distribution of ANC

Other than user-initiated transactions, in every block, another special transaction will be used for distributing ANC to ANS holders. This algorithm is based on block nonce and weighed by shares held and ANC will be randomly sent to ANS holders. ANC distributed in every block can be calculated in the way introduced in 3.1.2.

#6 Distribution Mechanism
##6.1 Distribution of ANS

ICO, exchange, OTC. ANS represents ownership of the network.

##6.2 Distribution of ANC

Nobody holds ANC in the Genesis block. Given time and certain algorithms, ANC will be distributed to ANS holders in every block proportional to their part of the share. See 3.1.2.

#7 The Eco-System
##7.1 Exchange

ANS and ANC will be listed on centralized exchanges like Huobi, OKCoin, BTCC, BTC38 and so on. Or, they can be traded on the Antshares Blockchain in the form of superconducting transactions. Exchanges spend too much on the deposits and withdrawls of assets and currencies. Superconducting exchanges do not need to be engaged with the delivery issue, thus cutting off operational costs significantly. See 1.3.2.

##7.2 Wallet

Wallet providers may, by default, encourage ANS holders to vote for them to become bookkeepers. Bookkeepers could receive ANC (basic byte fee) as economic reward. This is yet another economic drive for wallets to provide better wallet serive.

##7.3 CrowdFunding and P2P Finance

China's regulators had explicitly banned crowdfunding platforms from operating their own
stock equity exchanges. Instead, they can use Antshares as the management system. This meets
the needs of transfer and trading from the users in compliance.
For the same reason, P2P Finance platforms could use Antshares as the creditor claims management system.

#8 Conclusion
Antshares utilizes the Blockchain Technology to conduct registration, transfer, trading, clearing
and settlement. By digitalizing assets, any real-world property right would become programmable.
With the atom-level trading and real-time delivery natures of the blockchain, the operational costs
of securities trading, along with its eco-chain, could be significantly shortened. We believe
that Antshares is not only overwhelmingly superior to traditioanl financial systems, it could create
a brand-new digitalized financial eco-system.