Whitepaper 1.1

Translation of the Whitepaper V1.1 from Chinese is under way...

Note:
This whitepaper is subject to future editing.
Should there be any inconsistency, the Chinese version shall prevail.

I. Antshares in General

Antshares and the Blockchain

What is Antshares?

Antshares is a decentralized and distributed ledger protocol that digitalizes real-world assets into digital ones, enabling registration, deposit, transfer, trading, clearing and settlement via a peer-to-peer network.

Antshares keeps records of the transfers of digital assets with e-contracts. In Antshares, digital tokens generated by e-contracts function as general underlying data and could be used for recording rights and assets like equities, creditor's claims, securities, financial contracts, credit points, bills and currencies, and could be applied for areas like equity crowdfunding, equity trading, employee stock ownership plans, P2P financing, credit points, funds and supply-chain finance, etc.

What is the 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 refers to the historical transaction data of bitcoin. The majority of the subsequent crypto-currencies named their folder of transaction data as blockchain as well, so this term began to refer to the historical transaction data of crypto-currencies.

Since 2015, mainstream financial players started to look into systems like bitcoin, ethereum and Ripple. These financial institutions took 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 as the *blockchain technology*. The blockchain technology is the combination of cryptography, network topology, consensus algorithm and game theory, etc, with technical modules like Proof of Work, Proof of Stake, Smart Contract, Lighting Network and Side Chain atop.

The Technological Core of the Blockchain
We consider the technological core of the blockchain is about how to reach consensus on a distributed basis, i.e. by what mechanism, nodes in a network of no center node (or multiple center nodes) reach consensus on all transactions within the network. This consensus includes elements like the contents, the validity and the chronological order of transactions.

•Reaching distributed consensus on contents and validity via digital signature

In traditional paper-based systems, contents, or transaction instructions and authentication information (sign and seals) are stored separately. E.g. a withdrawal at a bank counter, the application signed by the client and the transaction ledger of the banking system are stored separately. This poses difficulties to people outside of the bank in authenticating these transaction instructions.

Transaction instructions and authentication information in a blockchain system are stored in bundles. A centralized database is not required for nodes, but with the digital signatures, to perform self-authentication on the integrity (not-tampered) and validity (accessible to the signer) of the transaction instructions, thus ensuring consensus on the content and its validity on a distributed basis.

•Reaching distributed consensus on the chronological order of the contents through a consensus mechanism

Due to the high-latency nature of a P2P network, the chronological order of transactions observed by different nodes may not be necessarily consistent with each other. Thus, a mechanism is required in the blockchain system to reach consensus on the chronological order of transactions. This particular algorithm of reaching consensus on the chronological order of transactions in a given time window is called the consensus mechanism, such as:

oProof of Work: Bitcoin, Ethereum(present)

oProof of Stake: Peercoin, NXT, Ethereum(future)

oDelegated Proof by Stake: BitShare, Crypti, Lisk

oUNL/Quorum Slice：Ripple, Stellar

oPractical Byzantine Fault Tolerance：Antshares(delegated Byzantine Fault Tolerance, or dBFT), Hyperledger Fabric

•Reaching distributed consensus on the historical data with hashing algorithm

Blockchain systems create a chain structure via citing the hash value of the previous block, like a cross-page seal. Tampering any content of any particular transaction may invalidate the bundling digital signature while tampering against the chronological order of transactions may change the hash values of blocks, i.e. the cross-page seal becomes inconsistent on both pages. That is to say, any node, without a central node, could perform authentication on the validity of all transaction history, hence a consensus is reached among nodes.

•Reaching distributed consensus on the computation with Smart Contracts

Originally proposed by Nick Szabo in 1993, the concept of Smart Contract had come to existence long before the blockchain. Scripts of bitcoin basically realized the concept of Smart Contract while Ethereum have had great progress from there, creating a more flexible, Turing-Complete Smart Contract platform. Addtionally, Hyperledger also achieved Smart Contract based on a vessel technology (what it calls a chainnode).

We consider the Smart Contract in a blockchain system is a re-consensus reached on the computation outcome of data input from the basic consensus on the contents, validity, chronological order and historical data.

Apart from the aforementioned consensus, blockchain may integrate technical modules far beyond the distributed-consensus-related, such as the Lightning Network, Side Chain, Cross-Chain Transaction, Stealth Address and Confidential Transaction.

Design Goals
The mission of the Antshares is about *digital assets for everyone*. Bitcoin wants to create a financial system parallel to the existing ones whereas Antshares is about building a financial system bridging the real-world assets. Meanwhile, the user-base of the Antshares is the great majority of Internet users, not just for Libertarians, Geeks and developers. To reach this goal, Antshares takes a very different underlying design.

Linking the Real-World with Compliance

•Replacing Tokens with E-Contracts

The common practice when it comes to digitalizing assets is tokenizations. That is to say, user may issue s customized token and claims its binding assets. Then, this kind of tokens may be transferred and traded among users just like the bitcoin.

However, tokenization is flawed in terms of the existing laws. The transfer of tokens is much like the transfer of money, that is, the tokens could be transferred from the sender to the receiver with or without the latter's consent. This kind of transfer is fine with currency, which does not carry obligations, not with assets like stock equities and creditor's claims that do carry complicated rights and obligations. Thus, the transfer on Antshares is conducted in the form the e-contracts. In most cases, the transfer of assets requires the digital signatures signed with the private keys from both the sender and the receiver. In certain cases, an extra signature from the issuer of the asset is required. Recording transfers of assets on the Antshares is merely an onchain solution of the transfer of offchain assets. There are no new legal relationships that parties could enter into, so unlike the tokenization, flaws in laws are eliminated.

•User-Controlled Identity Authentication

Real-world identity information is fundamental to confirm rights on real-world assets. In most circumstances, legally binding contracts require signature with autonyms as well. Users should be able to authenticate with their true identity when required by the parties involved in a trade or by the laws of the jurisdiction of the trade. Meanwhile, the range of publication of such identity information should be user-controlled. Any third party outside of the trade should not be able to acquire such information. Moreover, Identity authentication should be made optional, rather than mandatory. When parties involved in a trade do not require autonyms from the counterparty, users should not bear the hassle.

Antshares employs digital certificate to perform user identity authentication. Users (individuals or institutions) may apply for digital certificates from the certificate authority (CA) to prove the correlation between the identity and the public key controlled. CAs will not be appointed by Antshares, but freely chosen by the parties of a trade. For example, Chinese users may choose any one of the 38 CAs recognized by the MIIT, or choose the company who registered the equity to be the CA, to perform identity authentication and issue the certificate.

Rather than the X.509 digital certificate solution, Antshares employs blockchain to maintain the certificate revocation list and is set to gradually develop a blockchain-based digital certificate and identity authentication solution.

Meeting the Demands of Financial Trades
•Certainty Bookkeeping without Forks

We consider the existing blockchain consensus mechanisms can be categorized into:
a) One Man Bookkeeping and b) Joint Bookkeeping

Blockchains like Bitcoin, Ethereum and BitShares employ the One Man mode. In this mode, a single node, under certain rules (computing power in its possession, stakes, ballots), could perform the bookkeeping of a single block. Other nodes may add new blocks after this block to show their recognition. Adding blocks is like voting on the versions of the history. When a fork takes place, the version of history that received most votes (the longest chain) becomes the consensus.

Transaction confirmation under the One Man mode is actually an expression of probability. For example, the likelihood of a transaction that received 1 confirmation to become the historical consensus is 98%, the ones that received 2 confirmations (1 block added after the block containing the transaction in question) have a 99% consensus probability, while 6 confirmations will make it 99.9999999%. But in theory, even 10,000 confirmations may allow the existence of a minimum probability that everything turns upside down. Blockchains like bitcoin could avoid such an extreme scenario because they basically buried long-past history through adding manual checkpoints.

Should the One Man mode be considered post-event voting (adding blocks) thus to achieve consensus, the Joint mode is about pre-event decision to generate bookkeeping nodes with certainty. No post-event voting, no uncertainty. In a public blockchain, this kind of pre-set decision could be made with an onchain election. The elected bookkeeping nodes may perform joint-signature on every new block generated. That is to say, in the post-event voting scenario, more confirmations, higher the probability, whereas in the pre-event decision mode, confirmation leads to the ideal simultaneous finality of a trade.

In the One Man mode, post-event voting (adding blocks) is about voting on the content of the block, not about the generator of the block, making it suitable for a public blockchain with no identity information. However, in the One Man mode, the finality of a trade is rather weak, making it inappropriate for financial trading. On the other hand, the Joint mode introduces weak trust on the bookkeeping nodes, i.e. to believe that no major (1/3 or more) number of the bookkeeping nodes may gang up and do evil. This requires identity authentication of the controlling parties of the bookkeeping node to some extent, for one thing, to judge on their reputation and technological capacity, for another thing, should the nodes do evil, cryptographic evidence will be available for investigations. This leads to the conclusion that Joint Bookkeeping is suited for public blockchain with identity information or for Consortium/Private blockchains.

The One Man mode is generally recognized with sound usability, i.e. in a world where Internet is segregated into different areas (e.g. the connection from one country to another was completely cut off.), the network will remain resilient. However, this usability is only available to nodes that followed the longest chain. When the segregated Internet comes back in one piece, history observed by the nodes that followed the shorter chain will be rewritten by the longest chain. For nodes that followed the shorter chain, this is some delusional usability that comes with the price of consistency.

We could conclude that the One Man mode chooses Anonymity, and is trust-free on any node. But that comes with the price of consistency and finality. While the Joint mode is advantageous over consistency and finality, it requires nodes to authenticate themselves to achieve a weak trust from other nodes.

We Use Fiat Currency

The core functions of a currency can be summed as: a) medium of exchange, b) bookkeeping unit and c) value storage. Crypto-currencies like bitcoin could deliver a sound function as the medium of exchange, i.e. users may transfer assets globally via bitcoin. However, inflexible supply of crypto-currencies makes them highly volatile in price and jeopardizes their capacity to function as bookkeeping units and value storage. BitShare and Nubits tried to be designed as stable cryptos that are anchored with fiat currencies. But their narrow application speaks for their failure.

This is to say, while ANS is the stake and ANC is the gas, fiat currency can be directly used as currency on the Antshares Blockchain.

The Division of Labor of Nodes and their Professionalization

Nakamoto had a flat design of bitcoin. All nodes take part to update the ledger (mining), store complete historical data and broadcast transactions. There is supposedly no division of labor with professionalization. However, with its development, we do have specialized labor division now. Bookkeeping (minging) is now far beyond Nakamoto's One-CPU-One-Vote envision, but with GPU, FPGA and ASIC mining devices. These days, it is economically impossible to run any computing device other than ASIC miners. We now have complete professionalization of bookkeeping nodes with bitcoin.

Moreover, several dozens of Gigabytes of historical data of bitcoin in the past 7 years have become a storage burden. Ordinary users are no longer willing to run a full node that stores all the historical data; rather, they have turned to web wallets, off-chain wallets, etc. Though advocates call for more full nodes, its number is now on a constant decrease.

With Antshares, our design goal is to have a clear division of the system's workload. Bookkeeping nodes are at the center of the Antshares Blockchain. They are trusted by the holders of Antshares in reaching consensus and generating new blocks. Full nodes are critical participants of the Antshares network. They are run by service providers to store complete historical data and detect and relay transactions. Ordinary users run light nodes or simply access the network with their client. An ordinary user may access service providers in the Antshares eco-system via a web-browser or a mobile App to synchronize and store data that are only relevant to the user in question. The Antshares Blockchain adopts the weak-trust-based Joint Bookkeeping mode, that is to say, digital signatures of the bookkeeping nodes are included in blocks. Users do not have to download full historical data to verify the current block. We consider this conducive to our mission, *digital assets for everyone*.

Highly Scalable Frame Design
Low Latency, High Throughput and Pluggable

When competing with traditional technology solutions, scalability is the handicap of blockchain technology. In order to have a censorship-immutable and trust-free system, bitcoin chose the Proof of Work consensus mechanism, compromising in latency and throughput. Antshares's consensus mechanism depends on weak trust, granting it with low latency and high throughput. This consensus mechanism ensures a list of bookkeeping nodes in a small range with certainty and proficiency. Thus it's low in latency and high in throughput.

At the moment, the block generating rate is manually set at 15 seconds. With low enough latency in inter-nodes connection in the future, most blocks will be generated by every 1 second. With the bandwidth at 100Mbit/t and external cryptographic computing hardware, the Antshares Blockchain is capable of handling thousands, if no tens of thousands, of transactions per second.

Meanwhile, Antshares adopts a pluggable modular design. Users may employ their own consensus mechanism, ECC/Hasing Algorithm, P2P network protocol, etc. Antshares is easy to be reconstructed into a consortium/private blockchain with Antshares being viewed as the consortium's/company's voting power. Proof-of-concept trails can be performed on the public chain of Antshares by businesses while a quick shift and reconstruction to consortium/private chain is within the reach. Also, businesses may run Antshares-deprived consortium/private chain and shift it to the Antshares public chain without the hassle of rebuilding peripheral systems.

Hierarchical Design and Superconducting Transaction

A hierarchical design is indispensable to support sound scalability while maintaining multiple types of assets and transactions. Yet it is missing in blockchains with decentralized exchanges like Ripple, BitShare and NXT. These blockchains perform order-book-keeping and order-matching by themselves, with bids, cancels and matching operations all recorded onchain. This design is flawed as follows:

•Bids and cancels wait for block confirmation, resulting in high latency and poor user experience

•Miner fees are required for bids and cancels, with excessive storage and bandwidth consumption

•Chronological order of transactions is critical. However, placing the order-book-keeping and order-matching records on the underlying layer of the blockchain empowers bookkeeping nodes with greater privilege. The empowered nodes could rank orders based on their preference, granting them front-running capability.

Though onchain asset exchange is supported by Antshares, the Antshares Blockchain itself does not provide functions like order-book-keeping and order-matching. It performs merely the execution and clearing&settlement of the trades. Our hierarchical design places the order-book-keeping and order-matching functions on the second layer while achieving the full trading capacity through a mechanism called *superconducting transaction*.

Parties involved in a superconducting transaction do not need to escrow their assets through a middleman (traditional exchange). Users send private-key-signed orders to the exchange while the latter completes the order-matching, then broadcast it onchain, then the clearing&settlement. Assets, all along the way, are within the control of the users, eliminating the moral risks of traditional exchanges. With the superconducting mechanism, exchanges perform merely the order-matching.

With the superconducting transaction mechanism, users enjoy absolute control. They can actively launch double-spending attack to avoid the order in question being settled. Exchanges, on the other hand, may blacklist the user as punishment and deterrence.

Application Scenarios

CrowdFunding and Trading of Stock Equities

Though the funding procedure may still be done through multiple crowdfunding platforms, companies could take advantages of the irrevocability of the Antshares Blockchain. They can store public documents concerning the funding onchain. Upon completion of the funding, companies may register the stock equities on Antshares and issue them to the investors, cutting the red tape of documentation and back-office labor. Stock equity on Antshares is an asset with certain liquidity. Users may perform peer-to-peer transactions of these equities through Antshares. Compliant exchanges may be connected to Antshares and provide equity transaction of un-listed companies. With Antshares, start-ups could acquire a market evaluation and liquidity of their equities while the users are granted with an exit mechanism, which is the pain point of stock equity crowdfunding.

Moreover, Antshares is efficient in crowdfunding amount management. During recent years, many countries have come up with laws and regulations over stock equity crowdfunding. These laws and regulations specify the eligibility and investment amount of investors. For example, in the U.S., JOBS Act Title III, effective since April, 2016, specifies that the amount of investment from a single investor may not exceed 100,000 U.S. dollars per year. Antshares can be applied by the regulators for an easy management over these amounts.

ESOP and Cap Table Management

Antshares is ideal for companies that are in need of an employee stock ownership program or cap table management. Certain firms in the U.S. have already adopted centralized service provider like eShares for their digitalized cap table management. However, the flaws of a centralized system are needless to say. For example, eShares is the single point of failure in question: once its server goes down or get hacked, all the equity data of its client companies are endangered.

Blockchain-based Antshares is far more economical and secured than a centralized system. No single point of failure, no FUD for client companies. Also, the Smart Contract functionality of Antshares provides companies with flexible control over equity transfers. Companies may set a limit that stock equities can only be held by designated employees or investors, or set a limit on the proportion of the equities transferrable or tradable. For example, an employee may be limited that only 10% of his/her shares can be traded per year.

For the time being, ESOP solution consultancy firms provide paper-based plans. With Antshares, they can provide a powerful digitalized management solution to their client companies.

P2P Financing
The Antshares Blockchain addresses multiple existing problems with P2P financing platforms, such as the lack of information transparency, insufficient credit investigation and poor liquidity of creditor claims.

For the moment, claim confirmation can only be resorted to the internal data repositories of these P2P financing platforms. In cases of hacking, data loss and platform going bankrupt, creditors can hardly prove their claims. In the 2015-2016 cascades of collapses of Chinese P2P financing platforms, this risk has been fully exposed. Some P2P platform performed exit scams, with their creditors subsequently discovering that the websites have gone dark and themselves in the dilemma of proving their claims.

Moreover, for a P2P platform, the credit control over the debtors is restricted to its own database. For example, a platform sets a 100,000 yuan loan repayment capacity on a debtor through credit investigation. The debtor in question then has a 100,000 yuan cap of fiduciary loan on this particular platform. However, this debtor may borrow from multiple (n) platforms and enters into n*100,000 debts. The general ledger nature of the Antshares allows platforms to share the credit information on a single debtor. This is of the same principle with which crowdfunding platforms uses Antshares to control investment amounts.

Lastly, Antshares-registered claims became transferrable, eligible for mortgages, and even programmable. Claims may circulate beyond a single platform, thus adding liquidity. Long-term claims may subsequently become attractive. Users can be assured to purchase long-term claims with high interest rates without worrying about emergency monetization. With Antshares's trading function, long-term bonds can be monetized under discount or mortgaged. Additionally, companies that utilized Antshares for their equity management can mortgage their equities to issue their own company bonds.

Credit Point Management

Airlines, telecom operators, banks and hotels have already been issuing their own credit points. Issuing credit points to customers is a nice way to retain them and encourage repeated consumption.

However, the databases of these issuing bodies are information silos. Company A cannot acquire information on Company B's issuance, making the credit points of A and B impossible to interoperate. But credit points issued on the Antshares Blockchain can be openly, transparently and confidently checked by anyone. This shall contain the issuer's spamming incentives. Users' transaction demands and market makers' profit-seeking will forge a new market of multiple kinds of credit points, activating a large sum of sleeping points.

Supply Chain Finance

Supply Chain Finance may include multiple business modes and segments, ranging from factoring, trade finance, warehouse receipt finance, accounts receivable finance to corporate notes and credit financing in the supply chain. A blockchain-based distributed irrevocable business information platform provides authentic, effective and low-cost solutions to segments like participant verification, transaction validation, timeliness validation, bank due diligence and corporate financing documentation, thus enhancing the general efficiency of the supply chain finance.

Others

With its asset issuance functionality, Antshares can be utilized for issuance of fund shares and asset vouchers. Meanwhile, Antshares's digital contract functionality can be applied for evidence storage and financial contracting. Also, its decentralized transaction functionality has potentials in commodity exchanges and foreign exchange tradings.

Legal Status
To be edited...

> 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.

II. Economic Model

Built-in Assets and Fees

There are two built-in assets on Antshares: the Antshares and the AntCoins. The Antshares represent ownership of the Antshares Blockchain and are used for elections, bookkeeping and generating AntCoins as dividends. While on the other hand, the AntCoins are about the right of using the Antshares Blockchain and are used to pay systemic fees.

Systemic Fees

Systemic Fees are required in the form of AntCoins as payment for writing data into Antshares Blockchain. They can be categorized into:

a) Accounting Charge Collected by Bookkeepers

To write a transaction onchain, a certain number of AntCoins will be charged as accounting fees, which goes to the bookkeepers to compensate their expenditures in storage, connection and computing resources.

The rate of accounting charge or whether to charge it at all is collectively determined by all bookkeepers. As long as more than 2/3 of the bookkeepers are willing to, a transaction can be free of charge when writing into the Antshares Blockchain. Thus, organizations using Antshares in bulk could pay the bookkeeper offchain with fiat currency without further the hassle of paying AntCoins onchain.

b) Extra Service Charge Collected by Antshares Holders

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 be written into the corresponding addresses of the Antshares proportionally in real-time. Antshares holders may claim the AntCoins registered in their names anytime they wish to.

Antshares (ANS)

100 Million Antshares exist, representing All of the ownership of the Antshares Blockchain. These 100 Million ANS will be created at once in the Genesis Block and distributed based on certain plans. The total number of Antshares is set at 100 Million, no alteration. The minimum unit of the ANS is 1 Antshares, no further division.

ANS are used for

•Bookkeeper Election

•Acquiring AntCoins generated by new blocks

•Acquiring Extra Service Charge in the form of AntCoins

•Voting over major issues concerning the protocol of the Antshares Blockchain

AntCoins (ANC)

100 Million AntCoins could be generated, representing ALL of the right of using the Antshares Blockchain. ANC will be generated by every new block. With the set slowly-decreasing pace of generation, ANC will be generated from 0 to 100 Million within approximately 22 years.

ANC are used for

•Accounting Charge payment

•Extra Service Charge payment

•Bookkeeper Nominee Deposit as collateral

Distribution and Issuance

Distribution of Antshares

Before running the Genesis Block to create all the 100 million ANS, the Antshares team shall set certain rules on the distribution of these ANS.

Approximately 10% of the ANS have been designated to early supporters of the Antshares, in exchange of 600,000 yuan of seed fund. 400,000 yuan of the seed fund was from several individual investors under an overall valuation of 5 Million. 200,000 yuan of the seed fund was from a VC, PreAngel, under an overall valuation of 10 Million. It is worth noting that individual investors have contributed voluntarily in full-time or part-time.

Approximately 17% of the ANS have been designated to participants of the ICO Phase I, which took place in October, 2015, in exchange of 2,100 bitcoins. About 1,200 bitcoins were from individual investors while 900 bitcoins from one institutional investor.

Approximately 23% of the ANS will be designated to participants of the ICO Phase II, which is about to be launched in August, 2016. This ICO has no pre-set price or cap, but it does come with a refund mechanism. See details in the ICO CrowdFunding Draft.

All the remaining 50% of the ANS will be hold by the Antshares team. They will be locked for 1 year via a smart contract after the Antshares MainNet launch. After the 1-year locking, these ANS will be allocated for supporting the long-term operations of the Antshares.

ANS designated to early supporters, ICO 1 participants and ICO 2 participants will be in place after the official launch of the MainNet of the Antshares Blockchain. The MainNet is expected to be online in the 4th quarter of 2016.

Issuance of AntCoins

AntCoins are generated with every new block. The initial amount of ANC is zero while it will grow to 100 million after 22 years. The generation gap of every other block is 15 seconds, so it takes 1 year for 2 million blocks to generate.

In the first year (Block No. 0-No. 2,000,000), 8 ANC will be generated by every new block. In the second year (Block No. 2,000,000-No. 4,000,000), 7 ANC will be generated by every new block. With this pace of decrease (-1 ANC per year), in the 8th year, only 1 ANC will be generated by every new block. This 1-block-1-ANC pace will continue since then, till the 44,000,000th block in the 22nd year, fulfilling the 100 million total sum of ANC. ANC shall cease to be generated after that.

With this pace, 16% of the ANC will be created in the 1st year, 52% through the 4th year while 80% through the 12th year.

ANC will be written into the corresponding ANS addresses proportionally. ANS holders could claim these ANC to their ANS address anytime they wish to. For example, a shareholder who has 1% of all the ANS could acquire 8*0.01=0.08 ANC in every block of the 1st year, meaning 460.8 ANC everyday.

to be continued...