AiotCoin White Paper

Revision history

Edition	Describe	Author	Date	Email
V1.0	first draft	Stephen	20170715	Stephen.sevenT@viewfin.com

Contents

Abstract

AiotCoin Project （abbreviated as ATC).

ATC is a centralized platform based on the public chain technology system, covering digital assets and digital identity. ATC through the construction of a universal 2B2C technology platform, will be equipped with intelligent digital assets, through contracts and digital identity, enhance the efficiency of market operation, will connect the island a value into the value of the Internet.At the same time as the upgrading of the consumption value of the road, clearing medium distributors level things, namely consumer investment, under the background of 3.0 blockchain technology becomes feasible.

ATC hopes to conduct iterative development by closely combining the reality of business, so for ATC, we support different functions in different versions, ATC development will be based on market feedback iterative updates. So in the initial version of ATC, technically we retain only minimization operations available public area blockchain set, currencily as the basis for the reconstruction of development by bitcoin\litecoin, increase the digital identity and digital assets etc..

ATC was originally developed and maintained by the Seven-T anonymous organization, and ATC is based on the AGPL3.0 license agreement. ATC source code in the future on line, open source, open source address or:
https://github.com/ATC-live/AiotCoin

ATC White Paper

1 ATC background - technique of blockchain 3.0

1.1 About blockchain

The source of blockchain technology it is due to the characteristics of this technology to the center, The characteristics of a book cannot be changed, the bitcoin system have the ability to solve some problems, such as transaction fraud, honeysuckle etc.. Many people believe that bitcoin system is the first application of blockchain technology.

Bitcoin system is undoubtedly an ingenious invention, and behind the mysterious anonymous creators, Nakamoto (Satoshi), the bitcoin system has been defined as a peer to peer electronic cash system". In the past seven years the subtle, bitcoin ecosystem surrounding growing up from the doubts, the total market value of bitcoin has more than $45 billion.

As we all know, bitcoin is not just a new cash system, it also has blockchain attributes, and through blockchain technology to protect bitcoin to the central book. More importantly, bitcoin systems make us confident that physical assets can be digitized. Blockchain as a decentralized system, in order to maintain a way of cryptography can not be tampered with the books, so that many of the value of freedom of interaction or transaction without the need to build trust in the environment, this model can bring significant changes to the banking industry, insurance industry, medical industry, logistics, media industry and other industries.

1.2 History of blockchain

The development of blockchain and concept is accompanied by the deconstruction and reconstruction of the bitcoin system. All from the digital encryption currency to blockchain concept in the process of major milepost, we found that the domain name coins, made very little money based contributions, and bits of shares and Ethernet respectively brought two times square concept more influence upgrade.

1.2.1 Domain name coins (NMC)and PPCoin coins(PPC)

The NMC is the first application of project money branching off from bitcoin, it is the design and implementation of the concept of "objective is added to the center of the domain name in the electronic cash system in the original (can be regarded as the predecessor of digital identity, and take safety) and bitcoin mining method with node network securit.

If all the blockchain needs to design a new POW mechanism of mining algorithm, or need to share a set of existing problems mining center POW mechanism, and the need to deploy hardware as the network node of the whole machine, so the development of the blockchain will lag for many years now. A different concept of consensus algorithm proposed by PPC, then very famous POS proof of interest mechanism, after the proposed POS scheme, a new block chain system to try to continue to emerge in the way of low cost, the new minimally invasive consensus mechanism continues to push the development of blockchain technology.

1.2.2 Bit shares(BTS)

BTS is a project that grew up on the shoulders of the giant POS consensus mechanism, and later improved the consensus mechanism as a DPOS equity representative. On the BTS, new concepts have been put forward, including more prominent digital identity of the project Keyhotee, and through the definition of a variety of transaction types, you can more easily register, publish digital assets. BTS mainly to the concept of centralized exchange, and in order to achieve a good trading experience, to re improve the speed of fast, outs of the block can be secondly, and accordingly also sacrificed some of the stability of the system.

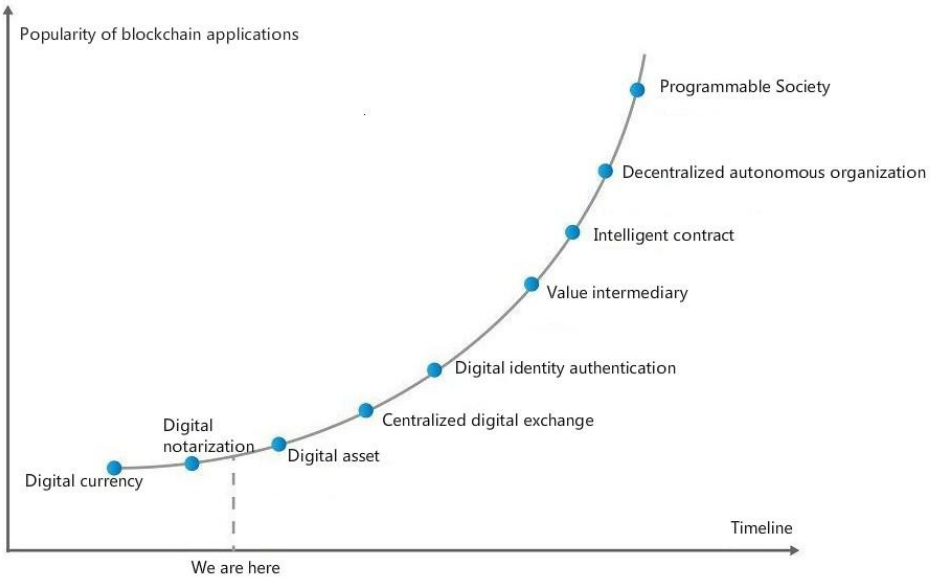
1.2.3 Ethereum

Unlike PPC and BTS, the ETH project adopted POW consensus mechanism in the early stages to protect the network from being attacked, and in the near future, it will be transformed into a POS consensus mechanism via forking. Such a design is primarily concerned with the overall security of the initial system. In addition the ETH concept in the practice of intelligent contract, this is in addition to the improvement of their ETH public block chain block characteristics and reward system, the most important contribution, through smart contracts and specially developed EVM, expand the blockchain of ETH treatment to type, all types of transaction is through the contract form.

1.2.4 Public chain and License chain

The difference between the public blockchain and the license blockchain mainly embodies two aspects: the attitude towards the node and the scope of trust. In the public block chain, node access threshold is very low, we generally consider that each node is not credible, so we need to prove some mechanism (POW, POS or their modified) to select the entry node, and the nodes on the list of license chain only authorized access to, and can set up a strict firewall. It is for the public trust mechanism of public blockchain, a wide range of public participation of all blockchain bookkeeping and the use scope of trust, and the trust chain permission scope only exists between the permit node, a relatively small range.

Blockchain development roadmap:



Bitcoin is in digital currency and digital notary, and the BTS are near the central exchange, The ETH square is located in the centering organization. In fact, the blockchain and the actual contact point are still in the icon position. Therefore, the blockchain is still growing, we want to build a fully equipped value transfer network, and the upper application of rich block chain ecology, still need to make great efforts.

2 Value orientation of ATC

2.1 Internet of things and Consumption investment

The word "Aiot" stands for A (league alliance) or A (AD Advertisement), Iot stands for (Internet of things).

Our modern life and work increasingly rely on the Internet, people have a lot of time online and offline, changes the communication between people, the frequency of more frequent than before, in the near future, we can foresee people experiencing the transition from the Internet to the information value of the Internet, intelligent transfer more and more assets will take place online, Avatar (digital identity) and intermediate Oracle will become the mainstream of economic mode at that time. At the same time, each individual will be popular in the network background, has become a gateway in the network, at the same time as disseminators and participants, the dual identity of consumers and investors, ATC is committed to becoming the gateway with settlement, the value of the return, consumption and investment settlement of bridge.

3 Economic model of ATC

3.1 Token of ATC —Tip

3.1.1 Tip

The time slot (Tip) concept is the smallest time gap in the universe, and it will be used as a token for AiotCoin, abbreviated as TIP. The total circulation of AiotCoin in block ICO and POW mining is 168 million, the smallest unit of AiotCoin is 10-8, namely ten decimal decimal, similar to the design of bitcoin, Wright currency. AiotCoin can transfer and deal on the public chain, and the incentive mode adopts the dual mode of POW and POS reuse, and the security of AiotCoin is guaranteed by the elliptic curve digital signature algorithm (ECDSA).

AiotCoin is not a new form of digital currency, it will be independent as an individual in the era of new Internet of things, IP will become a contributing clearing medium for gateway nodes. Therefore, the price of AiotCoin will not anchor any legal currency or encrypted currencies, such as bitcoin\litecoin, but depends on the ecological development of AiotCoin and the market demand of AiotCoin.

AiotCoin will be used to measure the value of the smart asset on the new block3.0. When using the AiotCoin system, the independent IP creates a new smart asset, registers a Avatar, and tags itself as a Oracle.

3.1.2 Community construction and ICO

In the block chain domain, the ICO distribution mechanism is a common and default way of token distribution. In 2014 January, the project start BTS for a period of 200 days of ICO; after July, the ETH project initiated by a staggering 25000 square bitcoin ICO; after the 2016 DigixDAO project and Lisk project were also launched ICO, and the controversial TheDAO project.

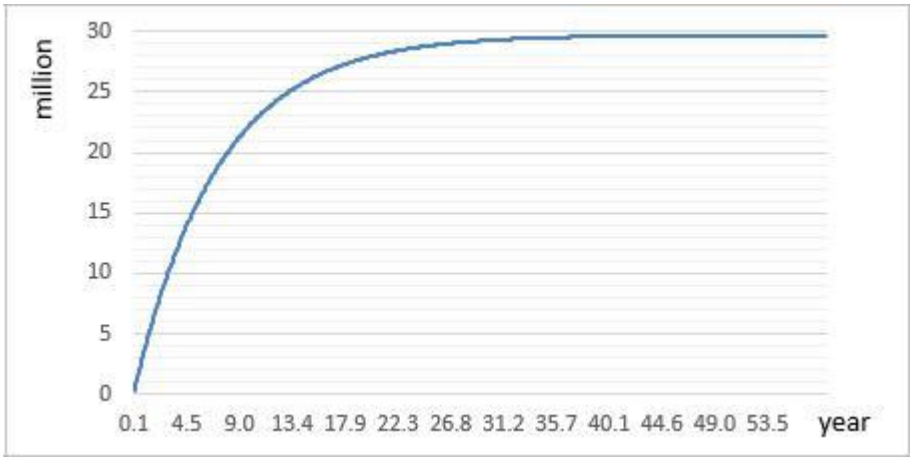
TIP of AiotCoin will be used as the final token, block IP community promotion user independent asset settlement subject matter for settlement marks early development of community member dynamic static assets, when the number of TIP reached 10% of the total AiotCoin. Later, TIP will be converted to AiotCoin at a rate of not less than 1:1.

3.1.3 POW+POS of Mining mechanism

1.68 hundreds of millions of AiotCoin will be distributed to the maintainer on the block via the POW+POS mechanism as a block reward.

AiotCoin block difficulty will be adjusted as the force changes by block, the target block time is 23 seconds; each block of reward is 3 AiotCoin. This time block and block reward as the standard parameters can be obtained, the amount of AiotCoin issued by POW mining changes with time and each of the one hundred thousand blocks total reward attenuation curve:

Attenuation diagram of reward for each one hundred thousands blocks:



3.2 Micro inflation model

TIP is the equity token of AiotCoin, the DAO (Democratic, Autonomous, Organization, democratic autonomous organization). TIP is not a currency, so TIP should not have inflation; but considering all tokens of natural loss in the process of using, including accidental loss, forget the password, or the holder of a natural death, this will cause the TIP stock shortage problem has become increasingly serious. Take the white book of the ETH square for example, Vitalik Buterin proposed a token loss rate prediction, which he thinks will lose about 1% a year.

Taking into account the loss of a portion of TIP, in the process of circulation and loss fraction, may be a lot of pledge and exchange hoarding, we design the TIP economic model requires the introduction of micro circulation demand to compensate for inflation TIP. Prior to the official implementation of the ICO, TIP will be released as a POW+POS model in the community membership promotion, and the dynamic IP individual contribution to make DPOS reward.

3.3 Avatar Digital identity

One cannot hold like gold in real life that physically hold the smart cable on assets, ownership of assets held by the individual needs of intelligent control of digital identity and digital identity in mathematics by unforgeable way. As a symbol of online identity, Avatar can represent people holding intelligent assets on the blockchain.

Create a Avatar far more than to your public key with an alias, like identity cards, mobile phone number is not your name, alias, and other valuable information will also be attached under the unique Avatar index, and cryptography way to protect privacy information, in addition to all non authorized Avatar access to information (such as the provision of private key signature information, launched special transactions, or in an intelligent way of contracts), otherwise unable to obtain a Avatar encrypted or unencrypted information. Here, zero knowledge proof, homomorphic encryption and other technologies will play a huge role. Avatar does not need to display the content of the information, it can achieve matching, verification, credit evaluation and other services. In the bitcoin system we can hold by the private key to anonymous bitcoin, but in real life, most of the activities we need to provide various levels of personal information, for example, if you need to add a female entrepreneurs club, you need to provide the age and sex of the two basic information.

Behind Avatar may be a real person, or AI, or a machine in the Internet of things (IOT), or a company or an organization.

Avatar can have multiple types of intelligent assets, and an intelligent asset may also be owned by multiple Avatar, and Avatar and smart assets are many to many relationships. This relationship seems complicated, but this is the real ownership relationship in real life, and in the AiotCoin block chain, these relationships are indeed right and secured by encryption technology.

Built on top of intelligent assets, specific (financial) application scenarios can be plentiful: transactions, loans, leases, and mortgages.

3.4 Value intermediary of Oracle

Take the examples of Alice and Bob to show how many Oracle agents are needed in a simple forecast for New York weather contracts The answer is at least 3: a weather data entry Oracle, a panel arbitration Oracle, and a secured Oracle.

Blockchain technology claims to be disintermediation, or "the elimination of middlemen", is still a myth at the moment. The intermediary of value still plays an important role, and the future still has a long time to play an important role. They are like the virtual and real time parallel wormhole, leave them, two of the world's communication obstacles will appear, because so far, two of the world's standard of value judgement and logic is not all quantitative written code, not to mention the actual application.

Unlike the slogan "destroy the middleman", AiotCoin keeps the location of the block chain for the value broker, which we call Oracle. Oracle can keep the physical custody of assets, then the issue of intelligence assets in the chain, Oracle can provide proof of identity authentication between personal information and Avatar in the chain, regulatory Oracle (such as the regulation of specific transactions in government departments) can provide the authenticity of transactions, proof of compliance in the chain..... There are many other Oracle that can provide such services on AiotCoin.

After the AiotCoin POW way to distribute 16 million 800 thousand AiotCoin, DPOS mining reward will be the main source to the transaction fee (transaction fee), AiotCoin for the ecological value of intermediary design information registration, certification and other types of transactions of the primary function based on different applications, each type of transaction but also support digital identity, intelligent assets etc. the direction, we can foresee the added value and the total transaction fees will be raised.

We always discuss how to reduce the bitcoin bitcoin as a payment system or network transaction fees (Fees), while expanding the block volume and block speed, meet the needs of the business on the one hand, on the other hand to make the value of Everfount injection system for miners, accounts nodes have enough incentive to: now we can revisit this issue, when the fee is no longer just because the transfer payment, but

in exchange for the blockchain more services (such as the purchase value of intermediary services, start smart contracts) the value chain, the block will no longer rely solely on a block of capacity and speed, and can transfer to improve the type and quality of the service, which will bring new opportunities.

The incentive model about the accounting people will reach a new equilibrium, get more people into account will be higher rate of profit from service fees, while in the past this service is completely offline, they did not use the blockchain technology value (except the transfer records), there is no feedback to blockchain system (except for more transfer fee). This "transaction" records a maiduhuanzhu feeling in the block chain, all services will be based on the scarcity and importance of characteristics in the market to block chain tokens for these services pricing.

3.5 Potential risks and considerations of AiotCoin

Blockchain technology is still in the early stages of development, and its maturity is still in the process of continuous research. Block chaining technology comes from bitcoin systems, so it will inherit the advantages of bitcoin systems as well as some drawbacks.

3.5.1 Increasing block size

The total data volume of the bitcoin block chain will increase by about 1MB every 10 minutes, equivalent to 1GB per week, so the cost of running a full node will increase significantly. Globally, the number of bitcoin nodes dropped from more than 10 thousand in the second half of 2013 to more than 5500 in July 2016. The block data volume of the Ethernet square is increasing by about 2GB per month, and the growth rate is still increasing. The AiotCoin block chain will also face the growing problem of data on blocks, which may become more complex because of the design of AiotCoin using the UTXO approach. In the ETH white paper elaborated on this problem, this problem will be early miners to solve, because they need to run the whole mining node.

3.5.2 The problem of mining - Center

Mining is a double-edged sword, on the one hand, mining system can guarantee the protected resources, on the other hand, because mining produced some new problems, such as the problem of mining center and the potential threat of attack force is 51%.

In the bitcoin industry, mining center is a very annoying result, in the face of the center of the etheric Fang mining is gradually losing the initiative.

AiotCoin hopes to optimize the mining algorithm, although it can not guarantee to avoid the mining center of the problem, but can ease the process, until the whole system migration from POW to HBTH-DPOS consensus algorithm.

3.5.3 The failure of business success

If AiotCoin is commercially successful, this will pose a new risk. When the total value of digital assets on AiotCoin rises to a level, attacks that destroy the AiotCoin system and shorting digital assets on the exchanges will become profitable. Therefore, the total value of digital assets on the AiotCoin is a maintenance / attack system cost function (especially in the stage of POW mining cost). Ideally, the total value of digital assets should not exceed the cost of mining 5-10 times.

4 Design principle of ATC

4.1 Minimum design principle

In high-level design, the core function module is the core, and it doesn't make too many complex designs on the basic function, so it can be extended only when necessary.

4.2 Evolutionary stability principle

In the course of AiotCoin evolution, only two kinds of TIP are needed:

4.2.1 Enhancement and expansion of core functions

4.2.2 Security bug fixes

Neither form of TIP should have a major impact on the underlying architecture

4.3 Compatibility principle

The version of AiotCoin must be compatible and support full platform operation.

4.4 Modular design principle

It is divided into modules to reduce the coupling between modules, and libbitcoin\liblitecoin is used as the main part of the code.

5 Architecture design of ATC

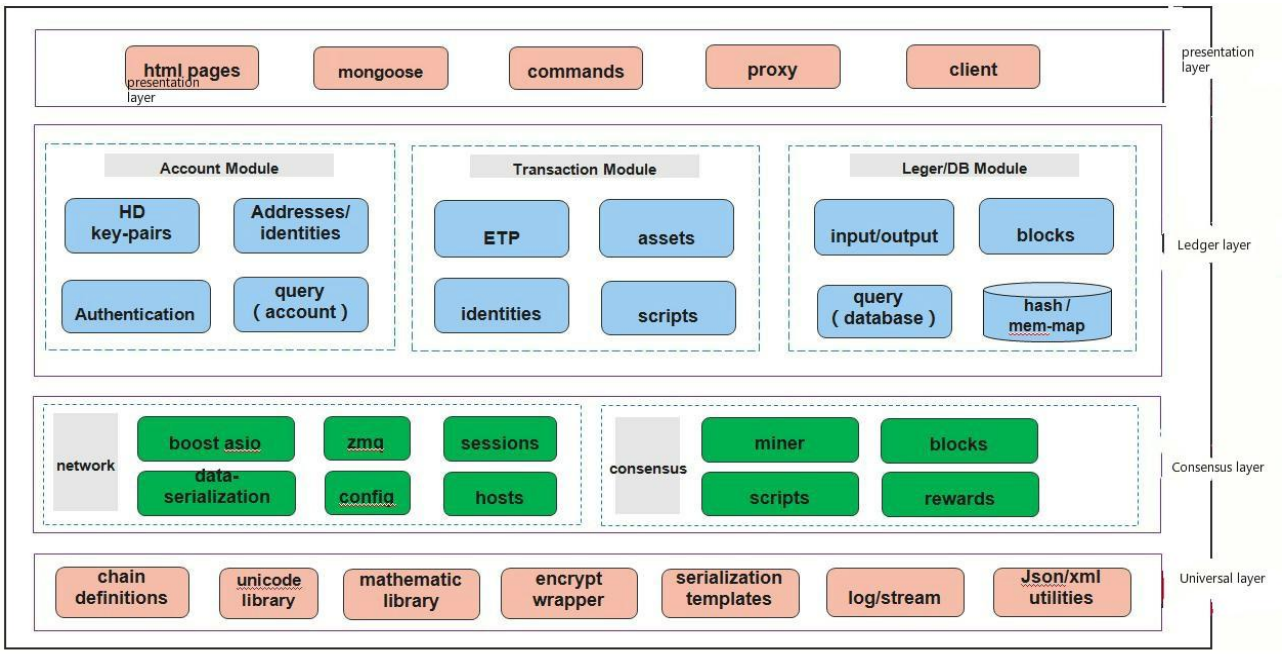
In the development plan of AiotCoin, we divided the development of AiotCoin into two stages:

In the first stage, AiotCoin will be based on the POW consensus algorithm, mainly providing digital identity, digital asset registration and transactions, simple built-in scripts, simple datafeed and credit evaluation functions. AiotCoin can be used to support all chain chains to form an open platform ecosystem.

In the second stage, AiotCoin will move to the DPOS based consensus algorithm, which will extend the intelligent contract function of AiotCoin and provide complete Oracle services with the help of the first phase of ecological accumulation

5.1 Infrastructure

5.1.1 Infrastructure diagram:



html pages: The front page of the AiotCoin is primarily for browsers;

mongoose：The HTTP server side of AiotCoin is a very lightweight http library;

commands：The set of AiotCoin interactions is the basis for access by all users;

proxy/client：In order to separate the presentation layer from the ledger layer, proxy and client primarily provide the proxy execution of the command;

Account: HD key-pairs based implementation of the local account system, in the future will expand the digital identity function;

Transaction：And transaction related parts, currently the main realization of the digital assets and TIP core functions;

Leger/DB：The Transaction primarily provides the underlying data structure, such as input/output, as well as local storage functions, and provides transaction pool capabilities;

network：Is the underlying core module for all AiotCoin network services;

consensus：Including the block and block validation function, and comes with a solo function;

Common layer: library collection that provides basic functionality for all modules.

5.1.2 Presentation layer

The presentation layer contains the user command line interface and a lightweight HTTP server - mongoose. The command line interface is a set of interactive actions that extend about more than 40 extensions commands based on the libbitcoin\liblitecoin native command, AiotCoin. Mongoose integrates the functions of Json-rpc and Restful API, and provides a user-friendly WebUI interface. Users can access the AiotCoin client via API or through a browser.

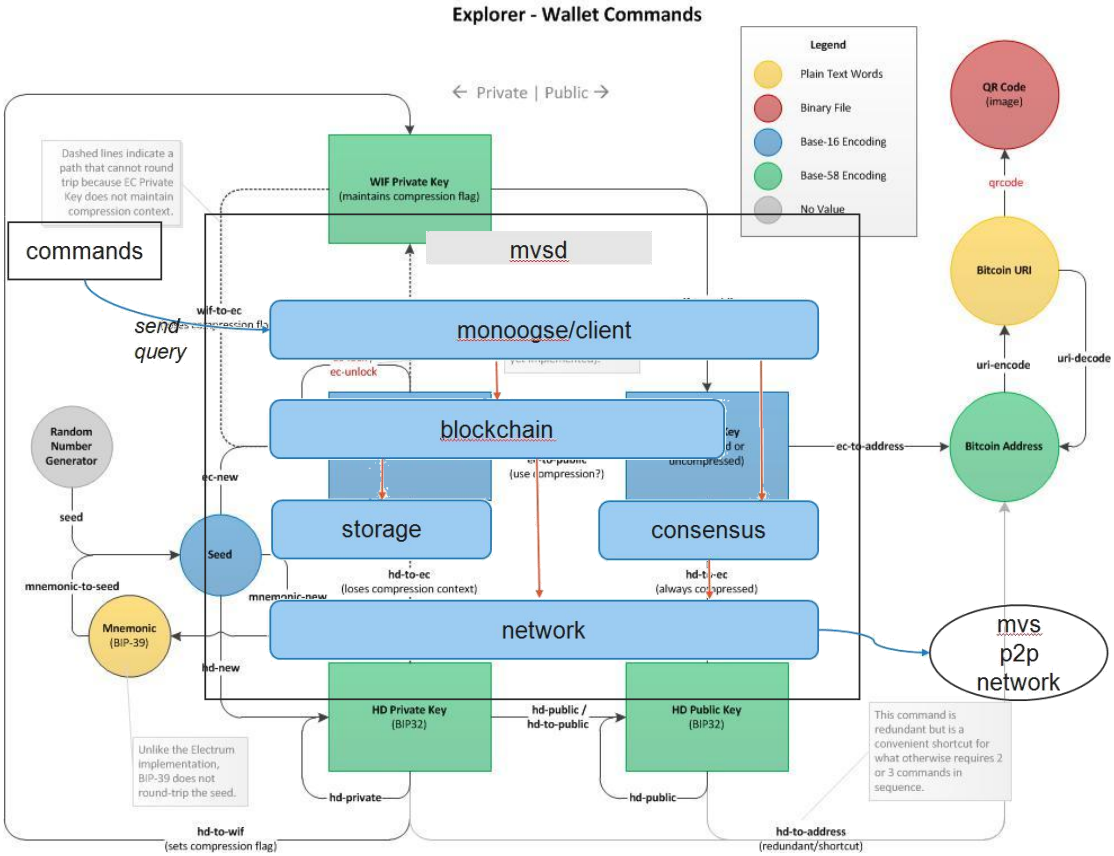
The whole presentation layer is divided into two parts, the first part is the mongoose server, the second part is the command set.

Among them, Json-rpc and websocket are recommended ways to use, Restful API because of the realization of the command relationship, temporarily unable to do Restful.

According to the type of command can also be divided:

Wallet Commands	**Encoding Commands**	**Messaging Commands**
ec-new	address-decode	message-sign
ec-to-address	address-embed	message-validate
ec-to-public	address-encode	**Transaction Commands**
ec-to-wif	base16-decode	input-set
hd-new	base16-encode	input-sign
hd-private	base58-decode	input-validate
hd-public	base58-encode	script-decode
hd-to-ec	base64-decode	script-encode
hd-to-public	base64-encode	script-to-address
mnemonic-new	base58check-decode	tx-decode
mnemonic-to-seed	base58check-encode	tx-encode
qrcode	wrap-decode	tx-sign
seed	wrap-encode	**Online Commands**
uri-decode	**Hash Commands**	fetch-balance
uri-encode	bitcoin160	fetch-header
wif-to-ec	bitcoin256	fetch-height
wif-to-public	ripemd160	fetch-history
Key Encryption Commands	sha160	fetch-public-key
ec-to-ek	sha256	fetch-stealth
ek-address	sha512	fetch-tx
ek-new	**Math Commands**	fetch-tx-index
ek-public	btc-to-satoshi	fetch-utxo
ek-public-to-address	cert-new	send-tx
ek-public-to-ec	cert-public	send-tx-node
ek-to-address	ec-add	send-tx-p2p
ek-to-ec	ec-add-secrets	validate-tx
token-new	ec-multiply	watch-address
Stealth Commands	ec-multiply-secrets	watch-tx

The following figure shows the relationship between native commands:



As we can see, we can rely on most of the native commands to assemble the key-pairs and transactions we want. But for users, this is very unfriendly, so we added an account concept at the ledger layer to simplify the command, that is, to extend the command - extension commands.

5.1.3 Ledger layer

As the core layer of the blockchain, the account book takes on most of the business process flow of AiotCoin. The diagram below is a simplified schematic of the process:

All the command processing through public inquiry service by mongoose and forwarded to the mvsd, a sub service public inquiry service of blockchain, according to the type of command, processed, send the results and return the results to the user.

At the ledger level, according to the overall architecture diagram, we can see that there are three core modules: account, transaction, storage.

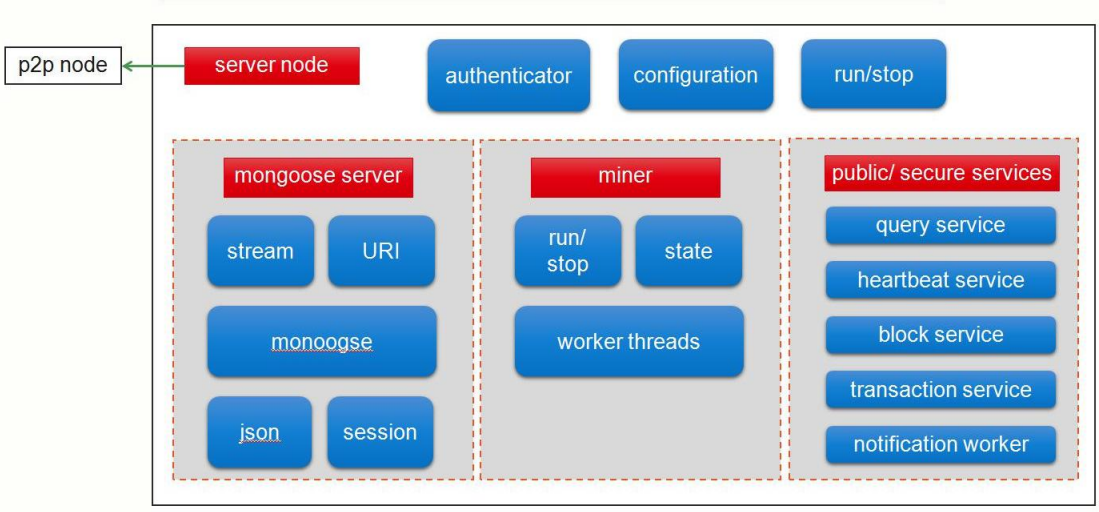
Considering the performance of Sqlite, and the replacement brings the complexity of technology, we retained the Libbitcoin design of the original hash-memory-map mode at present, the advantage of this approach is the speed and performance is very

good, easy access to the memory-pool, the expansion of the disadvantage is insufficient, and the cost of learning a certain.

5.1.4 Consensus layer

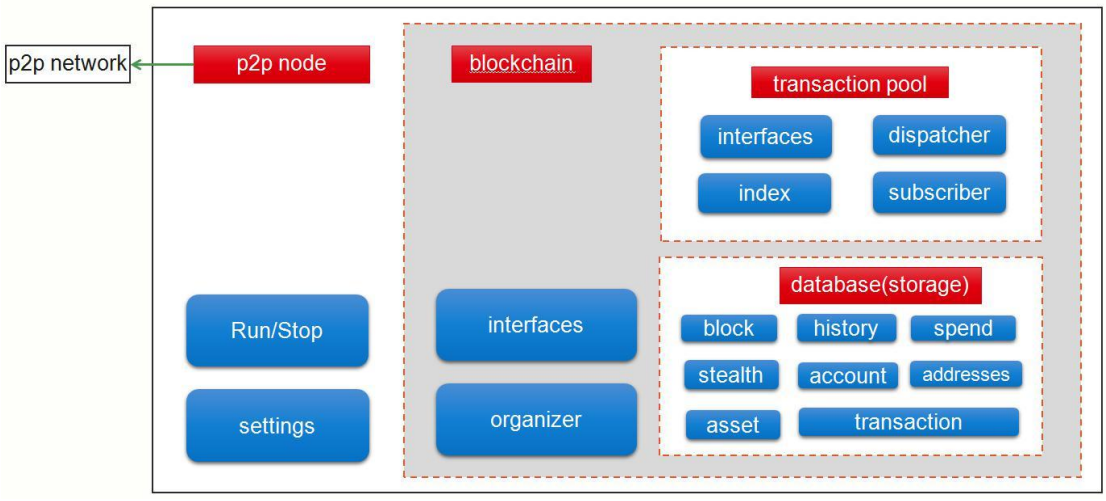
Consensus layer is the underlying module for the whole block chain, In understanding, I incorporated P2P-network as well as workload verification and validation into this layer, and at the bottom was the P2P network module that supports all network messages (not supported by LAN penetration). The second is the consensus module, including mining, block network card and the difficulty of adjustment and other functions.

Now let's consider the entire whole node, which contains the members as shown below:



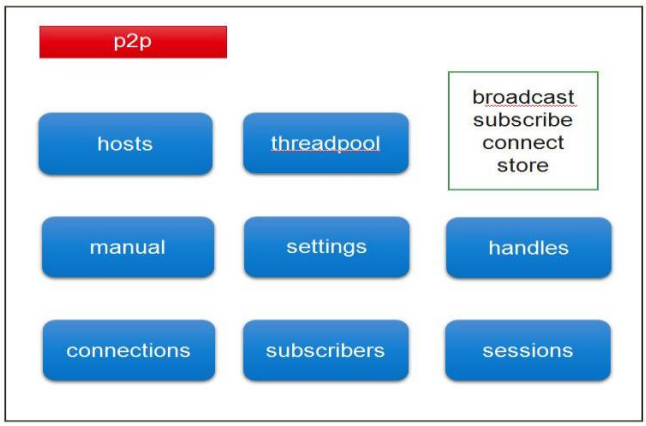
A public query is an open and encrypted query interface (binary); Server_node is derived from P2P node.

The P2P node contains the following diagram:



P2P node contains the main blokchain services, blockchain is mainly composed of transaction-pool and database, and P2P node is also derived from P2P network;

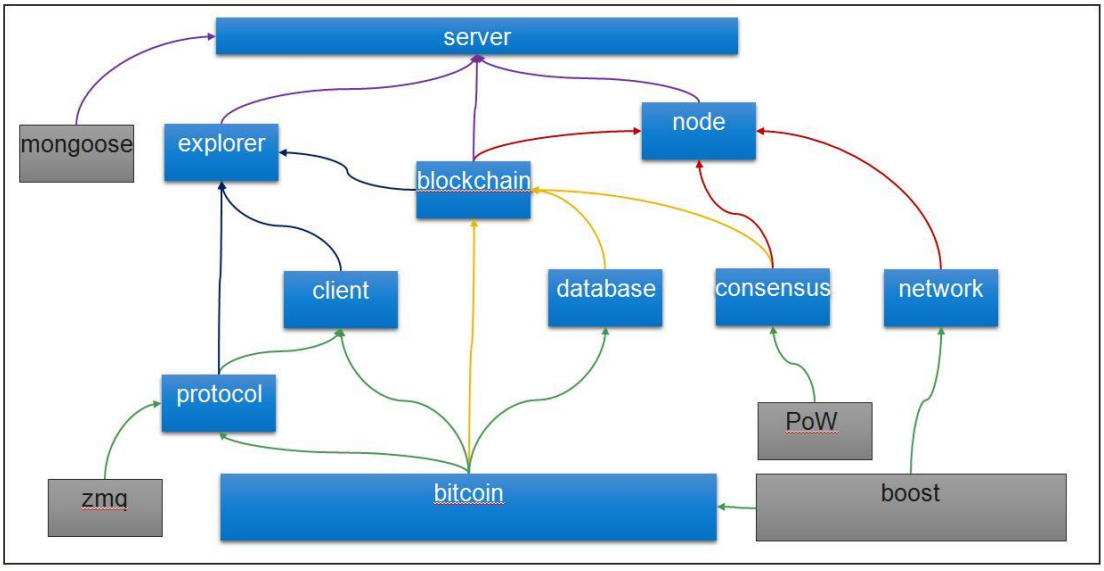
And the P2P network contains the following:



That is to say, in the whole hierarchy also reflects the network module is the basis of the blockchain, while the consensus validation portion of the content through the miner (consensus) module to the server_node, a module is at the bottom.

5.1.5 Universal layer

Universal layer is a base layer, which contains some basic definitions, the configuration of inheritance, the math library, according to the current processing base, and other common functions, is a small function, a large number of base classes, and the general template composed of the underlying C++. This layer contains important libraries such as speck265k1/zmq, as well as implements many classes, and the following is the dependency of each library of AiotCoin:



6 Reward model of ATC

6.1 Consensus Process

The so-called block chain consensus process refers to how to objectively record the whole network transaction data and can not be tampered with. At present, the "big three" respectively use different consensus algorithm (Consensus Algorithm), the use of bitcoin (Proof of Work PoW proof of work), will be converted into the etheric Fang (Proof of Stake PoS proof of interest), bit shares use authorization that DPoS (Delegated Proof of rights Stake).

The above algorithm called "economics" algorithm, called economics algorithm, refers to the cheating cost can be calculated, and the cost is often much larger than to cheat cheating benefits, namely cheating unprofitable, through this thought to construct a node for the game between the algorithm and the direction of a stable equilibrium.

Correspondingly, we also have distributed consistency algorithms in the computer domain, such as Paxos and Raft, which I also call traditional distributed consensus algorithms.

The biggest difference between them is the reliability of the system under Byzantine Generals (Byzantine Problem), Byzantine fault tolerance (PBFT algorithm supports Byzantine fault tolerance). However, both the Paxos and Raft algorithm, the theory may enter a cycle of death can not vote (although this fact the probability is very low), but they are to meet safety, just relax the requirements of liveness, PBFT and so.

AiotCoin is a public blockchain,block design public consensus algorithm of several outstanding, including the bitcoin system pioneered by POW (proof of proof of work mechanism of work), created by the little coin system rights proof mechanism of POS (proof of stake), by a representative of the interests of the first bit shares that the mechanism of DPOS (delegate proof of stake), in addition to some other mechanism of Byzantine fault tolerance (BFT, Byzantine fault tolerant, Byzantine Fault Tolerance).

Most cryptographic currencies are selective in ignoring Byzantine fault-tolerant algorithms, because this algorithm does not solve token distribution problems. Although AiotCoin is not a currency, AiotCoin will be distributed to these nodes as a feedback to the network security contributing nodes.

With the future of the project maturity increases, for mining reward AiotCoin distribution near the end, DPOS will switch to an improved consensus algorithm, this algorithm will consider the currency block height destruction "is an important design index.

In the AiotCoin system a few years ago the running time, will use GPU mining to ensure the system security, and a decentralized time stamp service. In mining AiotCoin algorithm comparison and study, but will use bitcoin SHA256 and scrypt algorithm of litecoin, the reason is to avoid bitcoin or litecoin currency pool 51% attack is mine.

Although the POW proof of work mechanism of mining can help AiotCoin system security in the first few years, but POW mining also has some problems, such as waste of energy, mining center development trend and so on.

In the DPOS phase, AiotCoin, like other systems using the POS consensus mechanism, distributes the AiotCoin to different equity holders based on the prevailing rights and interests. However, the difference is that the AiotCoin system will not receive equity holders in a passive way to get new AiotCoin tokens, but need to holders of the system sends a "heartbeat" to prove that the equity holders or active. At the same time, the heartbeat is equivalent to a digital signature from the owner's private key, and the holder chooses to change or maintain his or her rights while sending the heartbeat.

There are two advantages of this design heart: the first is to encourage people to check their own interests, although not fundamentally solve the problem of voter indifference, but played a role in mitigation; second is the new AiotCoin system will not be distributed to the stock right up has been inactivated, and the dilution effect on inactivation of equity.

In the DPOS phase, we will also consider using the Power-DPOS improved algorithm.

6.2 Type of Transaction

In addition to the transaction type of Coinbase, there is only one transaction type on bitcoin, namely bitcoin transfer from sender to recipient.

Another type of transaction called "contract" has been introduced into the ETH square system, and the contract will be used to divide all other types of transactions, such as the issuance of assets, into the transactions of the "super money". ETH users need to know some square code to complete this operation, although the ETH team put a lot of effort to make the ETH code easier, for example, just a few lines of code can achieve some functions, but the concept of writing code for common operations or make a lot of business customers at a distance.

There are many kinds of AiotCoin in the transaction type, transaction type design taking into account the two efficiency and availability, is not like that a contract through the ETH to adapt to all types of transactions, also won't like BTS as defining many types of transactions. The issuance of intelligent assets and

registration of digital identities are the two highest class of transaction types other than AiotCoin transactions. Later, transaction types like Ethernet Fang smart contracts will also be added to the AiotCoin system.

6.3 Account model

AiotCoin will mix bitcoin's UTXO account model and the balance based model. For AiotCoin, we use the UTXO model for user defined digital assets, and we use the base balance account model. For the UTXO model, the reader can refer to the bitcoin developer document.

6.4 Data feed and ID

AiotCoin will reference and integrate the Succinct Non-interactive ARguments of Knowledge (zk-SNARKs) proposed by Zcash (zero-knowledge) to protect the privacy of users' digital identities.

Data-feed is another important feature of AiotCoin, unlike the idea of the etheric square, where AiotCoin's data-feed is largely assumed by a Oracle - based role.

The market will provide feedback on the credibility, is data-feed users through consumption records "vote" on the appropriate voting results will enable voters rewarded (similar to the evaluation on the voting behavior, rebate) rules and reward model suggestions will be disclosed in subsequent versions; inappropriate vote by vote the motivation and influence on the results to determine, this behavior is going to pay first, regardless of the voting results will be faithfully recorded in AiotCoin, followed by the other Avatar or Oracle, can choose how to deal with this record digital identity according to their own preferences.

The reason for the rule is that the business level rules should not be written into AiotCoin in a hard coded way. No block chain can do more than its core business (consensus) business design. For data-feed, if there are destructive attacks, will only affect the effectiveness of data-feed, without affecting the AiotCoin consensus, any behavior by data-feed "evil" still need to pay the cost of the AiotCoin consensus, but their aggressive behavior is the need for defense in the Oracle or BAPP level; even so, AiotCoin the designers still hope to have a healthy data-feed mode, so the rules will give suggestions.

6.5 Platform of all

Windows/Linux/MacOS will initially be compatible with platforms of AiotCoin. With the development of AiotCoin, AiotCoin is also considered to be ported to embedded platforms such as ARM, enabling the IOT.

At the same time, with the development of the times, AiotCoin will be compatible with mobile platforms, carry out third party wallet private key management mechanism to adapt to the great development of the IOT era.

Reference

1. Bitcoin Whitepaper ——Satoshi Nakamoto http://bitcoin.org/bitcoin.pdf

2. Namecoin: https://namecoin.org/

3. Bitshares whitepaper——Daniel Larimar http://docs.bitshares.org/bitshares/papers/index.html

4. Ethereum WhitePaper——Vitalik Buterin: https://github.com/ethereum/wiki/wiki/White-Paper

5. Smart Contract ——Nick Szabo http://szabo.best.vwh.net/idea.html

6. Smart Property —— https://en.bitcoin.it/wiki/Smart_Property

7. Blockchain— from Digital Currency to Credit Society ——ChangJia, HanFeng and etc. ISBN：9787508663449

8. Snow Crash——Neal Stephenson 1992

9. Metaverse——https://en.wikipedia.org/wiki/Metaverse

10. Tim Swanson ——http://www.coindesk.com/smart-property-colored-coins-mastercoin/

11. Coin Days Destroyed ——https://en.bitcoin.it/wiki/Bitcoin_Days_Destroyed

12. http://blockchaindev.org/article/consensus_introduction.html

13 ZeroCash——http://zerocash-project.org/paper