Metaverse

White Paper

Revision Timeline

Version		Author	Date	Email box
V0.1	First draft	Eric Gu	Augest,2016	eric.gu@viewfin.com
V1.2	Revision	Chen Hao	September,2016	hao.chen@viewfin.com
V2.0	Revision	Michael Jiang	October,2016	youming.jiang@viewfin.com
V2.1	Revision	Michael Jiang	Feburary,2017	youming.jiang@viewfin.com
V2.12	Revision	Chen Hao	201707	hao.chen@viewfin.com

CONTENTS

Abstract

Metaverse Project (MVS or Yuanjie in Mandarin)

Metaverse is a decentralized open platform based on public blockchain technology that encompasses Digital Assets and Digital Identities. By building a 2B2C general technology platform, Metaverse digitizes assets (similar to asset-backed securities) such as rare goods (artwork and antiques), intellectual property, and rights to earnings from financial instruments to improve market efficiency. Through the provision of smart agreements and digital identities, Metaverse connects separated stores of value to form an internet of value.

MVS hopes to develop iteratively by working closely with businesses and responding to market feedback; hence different versions will support different levels of functionality. The initial version of MVS will be released with a minimal set of operations and be built up over time using Bitcoin as its foundation, with the added functions of Digital Identity and Digital Assets.

The software of Metaverse is distributed under the terms of the AGPL3.0 licensing agreement and was developed and maintained by Viewfin's development team. Metaverse will be releasing its source code to open source development. Open source address: https://github.com/mvs-org/metaverse

Metaverse White Paper

1 Overall background of MVS - Blockchain

1.1 About Blockchain

Blockchain technology originates from the Bitcoin system. Because of the technology's decentralized nature and its immutable ledger, Bitcoin has the ability to solve certain problems such as trading fraud and double spending. Bitcoin is widely believed to be the first application of blockchain technology.

Bitcoin is an undoubtedly sophisticated online payment system first invented by Satoshi Nakamoto, who once defined Bitcoin as a Peer-to-Peer Electronic Cash System. In the past seven years, from the initial misgivings, Bitcoin have been lifted with its market cap exceeding $10 billion USD to date.

It is widely acknowledged that bitcoin is not just a new cash system; it also possesses blockchain attributes and guarantees the security of its distributed ledger via blockchain technology. More importantly, Bitcoin convinced us that physical assets can and will be digitized. As a decentralized system, blockchain uses cryptography to maintain an immutable ledger, allowing multiple parties to engage in free value interactions or transactions in an environment that does not require trusted institutions. This brings about major changes to industries, such as banking, insurance, healthcare, logistics and media.

1.2 A Brief History of Blockchain

The development of blockchain technology and its concepts are accompanied by the deconstruction and reconstruction of Bitcoin system. Namecoin and Peercoin made essential contributions to the process of developing the cryptocurrency concept into blockchains, while Bitshares and Ethereum both had a major impact on the way we understand blockchains.

- **Namecoin and Peercoin**

Namecoin is the first application derived from Bitcoin. It is designed and executed to add the concept of "decentralized domain name" to Bitcoin's original electronic cash system (which is considered the predecessor of digital identities). Namecoin also introduced merged mining, allowing the simultaneous mining of Namecoin and Bitcoin to guarantee the security of the node network.

If all blockchains needed to design a new Proof-of-Work (PoW) algorithm, or needed to share a set of PoW with known centralized mining drawbacks and deploy mining hardware as full nodes of the network, then blockchain development would have algorithm, the well-known Proof-of-Stake (PoS) algorithm. The release of the PoS algorithm created a low-cost way to develop blockchains, leading to large numbers of new blockchain attempts. Micro-innovations of the consensus protocol also continuously drove the development of blockchain technology.

- **Bitshares**

Bitshares improved on the PoS consensus protocol by implementing the Delegated

Proof-of-Stake (DPoS) consensus protocol. Bitshares constantly put forward new concepts including Keyhotee, which gave more prominence to digital identity. Furthermore, it introduced multiple types of transactions to simplify the registering and issuance of assets. Bitshares' Decentralized Asset Exchange modified its block creation rate to be one every few seconds to provide a better user experience; however, the stability of some of its systems was sacrificed.

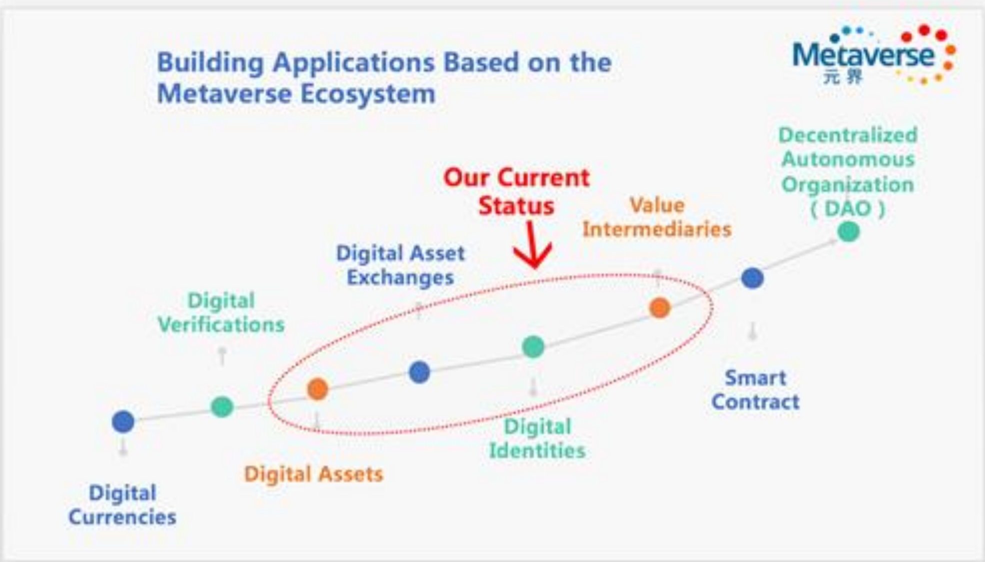
- **Ethereum**

Unlike Peercoin and Bitshares, Ethereum uses the PoW consensus protocol to secure its network in the early stages and will transition to a PoS consensus protocol by forking. This design is mainly for the security of the whole system. In addition, Ethereum implemented the concept of smart contracts, which is its most important contribution apart from the enhancement of its block features and its reward mechanism. Through smart contracts and its specially-developed EVM, Ethereum expanded the range of transaction types that could be handled by blockchains, with the downside that all transaction types on Ethereum must be implemented in the form of contracts.

- **Public Blockchain and Permissioned Blockchain**

The difference between public and permissioned blockchain lies mainly in their attitude towards nodes and their scope of trust. Public blockchains have a low threshold for node access and generally treat all nodes as not credible, hence some certification mechanism (PoW, PoS or their variants) is needed to select the node responsible for recording a transaction. On the other hand, permissioned blockchains only allows access to whitelisted nodes, and may establish a strict firewall. Therefore, a public blockchain's trust mechanism is wide-ranging - all people involved in the public blockchain ledger and its users are within the scope of trust. However, permissioned blockchains only trust permitted notes and have relatively small scopes of trust.

- **Blockchain Roadmap**



Bitcoin is currently at the "digital currency "and "digital notarization" stage, while Bitshares is closer to the stage of "decentralized exchange". Ethereum is located at the stage of “decentralized organization”. Looking at the current status of blockchains today as illustrated above, it is clear that blockchain technology is still growing, and MVS is aiming to build a value transmission network with a complete infrastructure. Constructing an ecosystem with many diverse blockchain-based applications ultimately still requires a gargantuan effort.

2 Why to Establish Metaverse

2.1 The Virtual World is A Reality

The term ‘Metaverse’ appeared in Neal Stephenson’s 1992 science fiction novel Snow Crash (Xuebeng in Mandarin) in which humans possessed avatars, through which they interacted with each other in a VR-based world and even formed relationships with electronic agents.

Modern life is just like the world described in Neal Stephenson’s novel. As our work and life become increasingly dependent on the Internet, people spend more time online rather than offline. The way people communicate has also changed, with communication occurring more often and at higher intensity. In the near future, we foresee a transition from the internet of information to the internet of value: more digital assets transfers will happen online, causing Avatars (Digital Identities) and value intermediary Oracles to become the new mainstream economic models.
The name of MVS is inspired by Neal Stephenson’s Metaverse.

3 Metaverse Economic Model

3.1 The Metaverse Token - Entropy

- **Entropy**

The token used by Metaverse is called Entropy (ETP). A total of 100 million ETP will be issued through a combination of Initial Coin Offerings (ICOs) and PoW mining; similar to Bitcoin, the smallest unit of Entropy is 1 x 10^{-8} ETP. ETP can be transferred and traded on Metaverse and will be an important factor deciding the miner of each block after MVS transitions to the PoS protocol. The security of ETP is guaranteed by the ECDSA (Elliptic Curve Digital Signature Algorithm).

ETP is not a new form of digital currency – instead, it represents the equity of Metaverse. Therefore, the price of ETP will not be anchored on any legal currency or cryptocurrency such as Bitcoin, but will depend on the demand for ETP as well as the development of Metaverse's ecosystem.

ETP will be used to measure the value of smart properties in Metaverse or as collateral in financial transactions. Additionally, fees applied on Metaverse (to create new smart properties, register a new Avatar, designate yourself as an Oracle or invite trusted institutions to verify the assets and identities on Metaverse) must be paid in ETP.

- **ETP Distribution Mechanism**

(1) ICO and community building

In the blockchain field, ICOs are common and the default method of token distribution. In January 2014, Bitshares launched an ICO lasting 200 days. Ethereum launched an ICO which raised a staggering 25,000 Bitcoin in July 2014. DigixDAO and Lisk also launched their ICOs in 2016, as did the controversial TheDAO project. NEO also successfully raised 2,100 and 6,119 Bitcoins in October 2015 and September 2016 respectively.

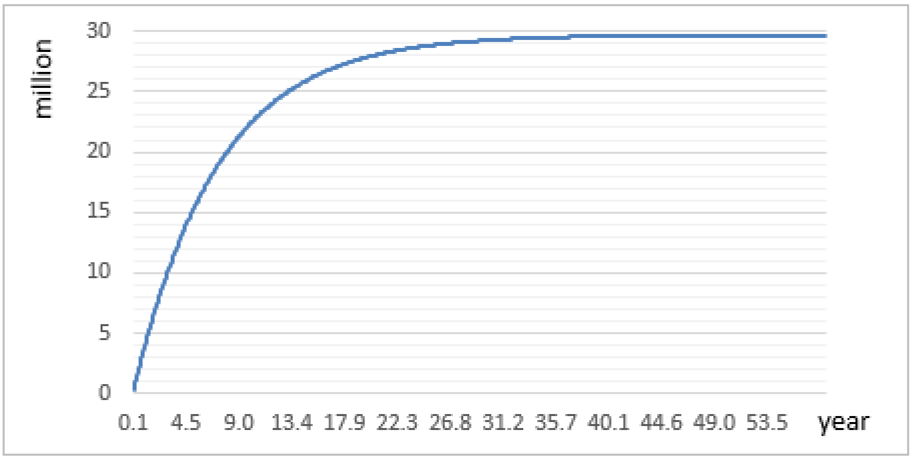
Metaverse Project has distributed approximately 22.6 million ETP in its first Initial Coin Offering (ICO). Another 27.4 million ETP will be used to set up Metaverse Foundation to support blockchain ICO projects conducive to the Metaverse community, facilitate investment activities that benefit Metaverse's ecosystem, as well as to reward major contributors to the community.

(2) PoW and PoS mining

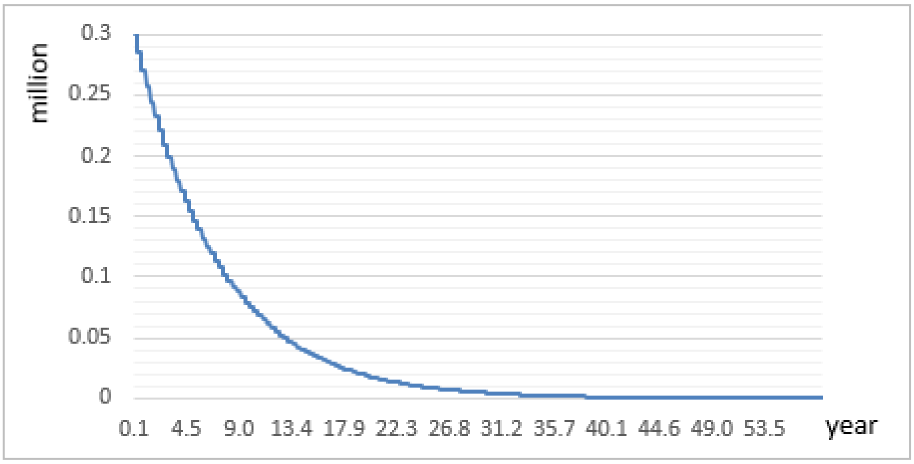
Additionally, about 30 million ETP will be distributed as block rewards to those who help maintain Metaverse's system through PoW mining, which is also called ETP mining.

The block difficulty of Metaverse will adjust to match the network's computing power. The targeted block generation time is 23 seconds and the reward for mining each block is 3 ETP. Block time and block reward are set as standard parameters; below is a graph of the amount of ETP that can be obtained through PoW mining over time in years.

The graph of the amount of ETP that can be obtained through PoW mining over time.



The decay diagram of the total rewards every hundred thousand blocks over time.



(3) Coinlock and Coinlock Rewards

Metaverse incorporated a paid coinlock function into the system level while designing ETP's economic model. This is the latest development in blockchain economic systems. In summary, it tokenizes coin age, paving the way for a future PoS-based economic model based as well as financial applications derived from coinlock.

To obtain ETP rewards, users must take the initiative to use the coinlock function. This reward will be sent to the user's coinlock address through Coinbase (a new transaction type) once the locking operation is completed.

Reward details are specified below:

H+block height	26295	112696	345600	683687	1371130
Reward rate	0.10%	0.66%	3.23%	7.98%	20.00%

H + block height: Assuming the current block height is 'H', users need to secure 26,296 blocks (till block height = H + 26296) to obtain the lowest-tier coinlock reward.

Reward Rate: Assuming that users lock down 100 ETP and choose the fourth tier coinlock reward (requiring H + 112,696 blocks), their address will reflect a balance of 100 x (1+0.66%) = 100.66 ETP after the 112,696th block is secured.

The initial design has a total of five reward tiers, but the block height required for each tier does not scale linearly. If the expected block creation time (23 seconds) is counted in days, we shall have the conclusion as below:

H+ block height	26295	112696	345600	683687	1371130
Time needed	7 days	30 days	92 days	182 days	365 days

This table presents the tier rewards in a more intuitive manner that users will naturally compare and contrast with other available rates of return. Similar to how investors consider an investment's returns, users will also consider the opportunity cost of obtaining coinlock rewards, i.e. ETP's price fluctuations and its ecosystem development since interest rates and rates of return form the backbone of the financial industry.

This is a fairly bold design that attempts to create interest rates dependent on blockchain ecology or the blockchain's community rather than a central bank. However, the initial implementation of this design is not particularly ideal because the first version's interest model is not designed not to be dynamic and adjustable, let alone capable of reaching the true market rate through decentralization and economic games.

As Metaverse progresses, we will further promote the degree of activity of ETP in the central and decentralized trading markets. The volume of ETP transactions will serve as a key data point to determine ETP interest rates, and is also an input parameter that influences ETP's economic model via voting or directly obtaining data from the decentralized market. The volume of ETP transfer activity, the number of accounts and special transactions (to be built) and other blockchain parameters may also be incorporated into this parameter.

3.2 Micro-inflation Model

ETP is the equity token of Metaverse's DAO (Democratic Autonomous Organization). Because ETP is not a currency it should not be subject to inflation. However, token loss may occur for a number of reasons such as accidents, carelessness or death, hence insufficient ETP in circulation becomes a more serious problem. In Ethereum's white paper, Vitalik Buterin predicated an annual loss rate of 1%.

Considering that token loss may occur and the possibility that a large amount of ETP may be pledged or hoarded, the ETP economic model requires micro-inflation to make up for this loss so that sufficient ETP remains in circulation. We have distributed a total of 50 million ETP through ICO and Metaverse Foundation, and another 30 million ETP will be distributed through the mining process. We will continue to release small amounts of ETP in an orderly fashion through coinlock rewards, with the specific reward amount determined by the total amount of coins locked and the time limit chosen. ETP inflation rates will be fed back into the coinlock algorithm, allowing coinlock rewards to be dynamically adjusted.

This feedback mechanism enables the system to self-adjust and recover and will be upgraded with subsequent versions of Metaverse to be more robust. Our end goal is to realize more intuitive economic models and a more effective economic ecology on the Metaverse platform.

3.3 Smart Assets

Bitcoin's Wikipedia page wrongly credits the concept of "smart assets" to Nick Szabo's 1997 study – more accurately, Szabo defined a class of assets embedded within smart contracts to execute certain contract terms.

The Ethereum project overemphasizes the concept of smart contracts such that the existence of digital assets is dependent on smart contracts, though this is an anti-intuitive design.

In Metaverse, we want to re-emphasize the importance of digital assets. Smart contracts should be dependent on digital assets, not the other way around. Using the object-oriented programming model as an analogy, digital assets would form a class, whereas contracts are methods contained within the class.

Unlike Ethereum, Metaverse's digital token ETP will follow Bitcoin's UTXO (Unspent Transaction Output) system in which all transactions are defined by a set of inputs and outputs, and contain the private key signatures of all current and previous owners of the ETP. These elements come together to form a new UTXO. Separately, we attempted using the Ledger Model to handle smart assets because it helps reduce system complexity and retains the benefits of the UTXO system.

The result of this design is that the digital assets on Metaverse can be easily sent and received, just like Bitcoin. Smart contracts will only be required when more the demand for more complex transaction patterns arise.

3.3.1 Registration of smart assets

To register Smart Assets, we first take several questions into consideration:

(1) Why do we register Smart Assets?

One of blockchain's benefits is that it offers a data store that can be publicly shared, and is append-only with timestamps. It does not allow previously recorded transactions to be altered or deleted (note that it says “not allowed”rather than “not possible”, since in reality it is possible for previously recorded transactions to be altered and deleted because a blockchain’s ability to resist attacks is imperfect and the blockchain could face also interference by people with special permissions).

This property fulfills the design requirements for registration: transactions are public, unique and trustworthy. Hence, registration on the blockchain need not be limited to just Smart Assets - all valuable data has a good reason to seek schemes allowing them to register on a blockchain.

(2) How should the functionality to register Smart Assets be designed?

The concept of “registration” refers to the act of describing some item with data. As such, the first step to registering Smart Assets is to find a set of data that describes an asset, taking special note of two key design characteristics:

A. This descriptive set of data should be reusable, if not the function would be ineffective and a failure.
B. It should consider potential future applications and have a complete interface that supports querying, addition, calculation and verification.
“Assets” usually have relatively simple generic attributes and well-differentiated special attributes. Additionally, since the important data is generated during the asset transfer process, smart asset registration can be described as filling out a form similar to the below.

Category	Smart Assets	Explanation
Generic attributes	Identification	A string of characters that uniquely identifies an asset
	Inventory	A basic attribute required to verify the validity of asset transfers.
	Minimum units	
Special attributes	Description	The location where special attributes are stored.

After fulfilling the basic information structure requirements outlined above, we must consider how this information will be used next. Bitshares attempted to issue assets on the basis of market functions, but this method produced numerous limitations including complex over-collateralization, anchoring and feeding mechanisms. Because the market’s underlying financial infrastructure has yet to mature, it is unable to fulfil market functions when asset values grow.

Blockchain systems such as Bitshares and Ethereum have also begun exploring the feasibility of the Proof of Assets (PoA) protocol. If the authenticity of smart assets can be verified by alternative means such as by posting a note containing one’s private key digital signature on forums or by providing an asset certificate tied to your account’s credit, it can be valued in the open market by those who recognize the asset. The issue with this method is that it is inconvenient to provide such verifications on the Bitshares blockchain, and furthermore users lack an incentive to issue their blockchain assets in a less liquid internal market. In

Ethereum, smart contracts seem to be able to handle all problems, including defining tokens. In fact, some tokens can actually be regarded as intelligent assets because store value and are editable. Theoretically, smart contracts are capable of supporting wild business models, allowing projects like Digix to exist. It cleverly seeks third parties (gold exchanges, accounting firms, host providers) to provide a series of asset certifications forming a chain of evidence recognized by markets. This evidence is also recorded on the blockchain rendering the asset's registration tamper-proof (of course, this scenario doesn't consider artificial hard forks).

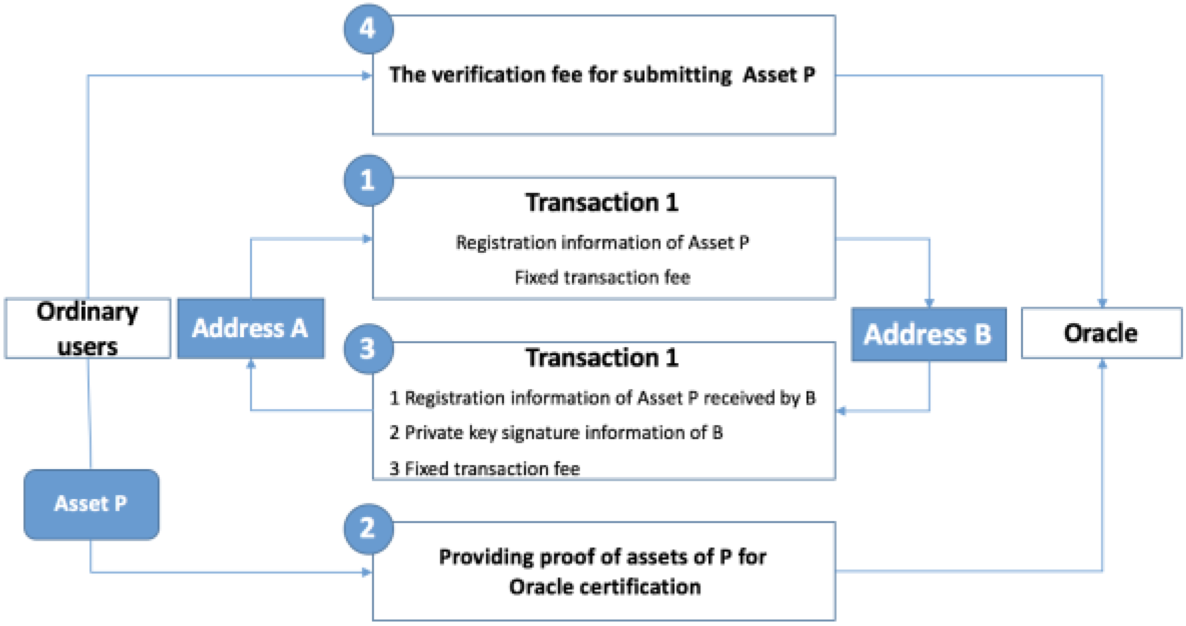
The second step incorporates registration fees into the design of Metaverse's economy. Metaverse takes the following items into consideration:

A. The legitimacy and reasonableness of registration fees. Registration fees are undoubtedly justified, because it forms a self-protection mechanism for the system. When smart assets can be registered with zero or low costs, the system becomes vulnerable to DDoS attacks. Presently, an appropriate registration fee has yet to be determined. No one can determine what the value of an ETP token, which fluctuates by design, will be. Hence, we are inclined to deploy a fee model that uses a weighted algorithm.
B. This fee is not a traditional transaction fee because the transaction is not a transfer, but rather a new transaction type with specific functions. A portion of all transaction fees generated by these new transaction types will be sent to a special system address to support the development of Metaverse's community, and the remaining will be allocated to nodes that generate blocks.

(3) What can be done after a Smart Asset is registered?

The registration of smart assets on the blockchain does not occur in isolation; it implies that other must recognize it through the PoA protocol before it gains the attributes of an asset, otherwise it is a meaningless string of data. Once recognized, Smart Assets have two types of attributes: value attributes and editable attributes (or attributes "worth editing"). Its auditability will be reflected by constant trading and changes in market value. Through technical means (based on a virtual machine's smart contract or a business's scripting language), its editable attributes will reveal that the constraints placed by society on normal asset circulation also exist for Smart Assets registered on-chain.

Metaverse will mainly focus on developing the PoA model of smart assets, hence its design will pay special attention to helping users easily provide PoA. Additionally, Metaverse also raised the following : (1) using the datafeed provided by Value Intermediaries (Oracles) to prove an asset's value. From this point of view, each third party in the Digix project is an Oracle instance. (2) a credit transfer model based on blockchain transactions. By constructing a symmetrical transaction, Oracles can carry out asset authentication through the process illustrated below:



It is simpler to safeguard ordinary users and Oracle from fraud; further elaboration can be found in the Oracle section below.

3.4 Avatar-Digital Identity

Unlike assets such as gold, we are unable to take physical possession of smart assets. Instead, the ownership of smart assets is controlled by individuals through digital identities and secured through mathematical concepts that ensure these identities cannot be forged.

As a symbol of one's online identity, Avatars can be used to represent oneself and hold smart assets on the blockchain.

Creating an alias for your public key is the first step in the creation of an Avatar. Similar to how identification and mobile phone numbers are not an alias for your name, various pieces of valuable information will be attached each Avatar's unique index and encrypted to ensure data privacy. Unless the Avatar's owner grants authorization (by providing the private key signature, initiating a special transaction or via smart contracts), users will not have access to both its encrypted and unencrypted information. Hence, zero-knowledge proofs and homomorphic encryption play a vital role allowing Avatars to retrieve information such as credit scores and validation results without revealing the contents of a message. Although the Bitcoin system allows one to hold Bitcoin using public and private keypairs, most offline activities in the offline world require us to provide some form of personal information: for example, you must provide your age and gender to join a young female entrepreneur's club.

Avatars can be held by a real person, but can also be held by AI (artificial intelligence), a machine in the IoT (Internet of Things), a company or an organization. A single Avatar may hold multiple types of smart assets, and a single smart asset may also be owned by multiple Avatars. Thus, there is a many-to-many relationship between Avatars and smart assets. Many-to-many relationships appears more complex, but more accurately reflect what ownership looks like in the offline world. These relationships are authenticated and secured on Metaverse through cryptography.

There is a diversity of specific (financial) use cases built on smart assets: transactions, borrowing, leasing and mortgages to name a few.

3.4.1 {Digital Identity s.t.app} ⊆{Digital Idental s.t.client/address}

The digital identity information held in Metaverse is a subset of the digital identity information available on the client end, which means that: (1) the client retains absolute ownership and usage rights over its identity information. Although the application has a temporary right to use this information, its ownership ultimately belongs to the client. (2) A portion of the data dictionary must be shared between the client and application, or the data within some intersecting fields cannot be matched and the intersection will be left empty.

As for (1): the basic idea is to protect identity-related information on the client side from being violated by application side. Users are responsible for declaring ownership of their digital identities by"timely creating identity", "updating status","seeking certification" etc. Alternatively, users can obtain services from the application by delegating some authority while still retaining absolute ownership over their information. This issue will be discussed later in this white paper.

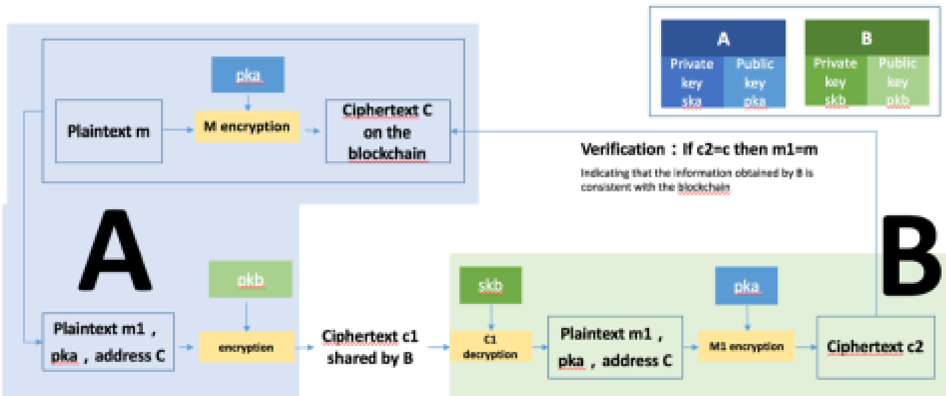
As for (2): the basic idea is to allow the client limited freedom to define field names. This issue will also be discussed later.

3.4.2 Confidentiality and information sharing of Avatar

As we all know, asymmetric encryption uses public keys for encryption and the corresponding private key for decryption, allowing information to be securely transmitted. Private keys can also be used to make digital signatures, thereby allowing users to self-authenticate with their public keys. Keypairs achieve the following goals:
(1) person A can encrypt all his digital identity information from the beginning

(2) person A can disclose a portion of his digital identity information without revealing his/her private key.

(3) person B can verify that the plaintext information provided by person A is consistent with the ciphertext registered on the block chain.



However, this construct is unable to solve the problems outside the scope of (1) - (3). For example, person B could still leak the personal information he has obtained from A, compromising A’s privacy.

Furthermore, since transactions on the blockchain are accompanied by digital signatures, transactions that share identity-related information and transactions that creates the digital identity generally originate from the same account. This removes the need to include A’s digital signature within ciphertext c1. However, if these two transactions are initiated by different accounts, A must provide the digital signature of the account that created the digital identity to prove that A does in fact own that digital identity.

3.4.3 The ideal of data sovereignty

Today, our right to create and manage our own digital identities has been given up to various service providers. Once a digital identity is stored on their servers, it becomes almost impossible to retain sovereignty over one’s personal information.

Metaverse believes that digital identities should be classified as a form of intellectual property (one of the previously mentioned “special assets”). The exposure of plaintext usually implies a violation of intellectual property rights, but this action of “sharing” demonstrates the changing nature of ‘value’. It remains to be seen whether users will derive benefit or harm from this change.

Metaverse provides a platform where anyone can register a personalized "resume": in exchange for a small information storage fee, users will possess a customized, tamper-proof resume. Timestamps and public/private key encryption jointly protect one’s information ownership rights. Although names and mobile phone numbers can be misappropriated by malicious individuals, they are unable to provide stronger evidence chains that include a user’s verification code and passport number. Thus, users simultaneously own the earliest, most complete and latest version of their digital identity which will belong exclusively to them. The authentication mechanism for digital identities on Metaverse is similar to that of smart assets and will be provided by Oracles; again, this will be described later in the Oracle section.

Creating a digital identity on Metaverse involves the following steps:

(1) Providing personal information that can be strongly verified such as P.O and mobile phone numbers

(2) Customizing other personal information by defining field names and field values, for example "city" and "Shanghai".

(3) If you do not wish to register immediately on the blockchain, your information can be stored locally and modified at any time.

(4) To create an immutable record, pay a small fee in ETP for digital identity creation and confirm the transaction. Using this digital identity on Metaverse will require the following steps:

(1) Application service providers will submit a data request. Please submit the requested information following the instructions in 3.4.2 .

(2) Request for an Oracle to verify the digital identity you have just registered. These Oracles may be banks, the public security system, a friend who has been certified etc.

(3) A timeline of your personal resume will be generated. The effects of this simple blockchain application are more apparent after a number of years - you will be amazed to find a pristine record of your life's journey that has never been modified by unscrupulous service providers.

3.5 Oracle – Value Intermediary

Using the example of Alice and Bob, how many Oracle intermediaries are needed in a contract regarding a simple forecast of New York's weather? The answer is three Oracles: one for imputing data and one for group arbitration with the third being a guarantor.

Blockchain technology claims to do away with trusted intermediaries ("cutting out the middleman"). At the moment, this seems like a fantasy. We believe that intermediaries will continue play an important role for some time to come. They function as wormholes between the virtual and physical worlds and allow them to communicate since we presently lack a way to quantify critical thinking and value perception in code, let alone in practical application.

Unlike "destroing the middleman", Metaverse will reserve the position for them on the blockchain, which we call it Oracle. Hosting Oracles can store physical assets and then issue smart assets on the blockchain. Authentication Oracles can provide proof of personal information and correlation with Avatar. Supervision Oracles (for example, government departments that regulate special transactions) can provide proofs, such as transaction authenticity, compliance proof. There are many other Oracles alike that can provide such services on Metaverse.

On the macro level, Oracles also serve to enrich the types of transactions available, adding value to blockchains.

After MVS distributes 50,000,000 ETP by PoW mining, DPoS mining rewards will mainly be sourced from transaction fees. MVS has designed a number of functions specifically for the value intermediary ecosystem based on information registration, certification and other transaction types. Each transaction type supports various applications related to digital identity and smart assets. We foresee that the added value and total amount of transaction fees will be increased.

The issue of how transaction fees (usage fees) can be reduced within payment networks such as Bitcoin is a constant topic of discussion among us. At the same time, increasing block size and creation rate would help with meeting business needs and injecting a constant stream of value into the network, incentivizing miners and nodes to support the distributed ledger. However, if we re-examine the problem, charging transaction fees not just for transactions but also in exchange for blockchain services such as value intermediaries or the creation of smart contracts), allows the value of a blockchain to not be solely reliant on its block capacity and creation rate. Blockchains could create value by enhancing service quality and increasing the types of services available, ushering in new opportunities.

The incentive model for miners will also reach a new equilibrium since they will derive more benefit from services with high transaction fee rates. In the past, these services were conducted offline and did not utilize the benefits of blockchain technology (except to record the transaction). Similarly, they did not feed back into the blockchain (except for the transfer fee). Recording these ‘transactions’ feels somewhat pointless. All services will be priced in blockchain tokens based on their market value, scarcity, importance and other characteristics.

3.6 Potential Risks and Considerations

Blockchain technology is still in the early stages of development and will mature as research efforts progress. Blockchain technology originates from the Bitcoin system, hence it will inherit both its flaws and merits.

- **The increasing capacity of blockchain**

Bitcoin’s blockchain grows by about 1 MB every ten minutes (1GB weekly), causing the cost of running a full node to increase notably. Bitcoin has seen a decline in the total number of full nodes running from about 10,000 in late 2013 to roughly 5,500 in July 2016. Ethereum’s blockchain grows at a rate of 2GB per month and is picking up speed. The Metaverse blockchain will eventually face this problem, which is exacerbated by Metaverse’s use of the UTXO system. This issue is well documented in Ethereum’s White Paper and was solved a while back by miners who must operate full nodes to carry out mining operations.

- **The problem with mining centralization**

Mining is a double-edged sword. On one hand, it guarantees that the system is protected by computing power, but on the other hand it produced fresh threats including mining centralization problems and the potential threat of a 51% attack. Mining centralization leads to extremely undesirable results in Bitcoin’s industry sector and has gradually eroded Ethereum’s first mover advantage.

Although we cannot guarantee that this problem will be avoided, Metaverse hopes to slow down its progress sufficiently (by optimizing the mining algorithm) so that the system can transit to the HBTH-DPoS consensus algorithm.

- **Potential failures brought about by business success**

Looking to the future, the success of Metaverse will bring new risks. Once the total value of digital assets on Metaverse reaches a certain level, it becomes profitable to attack the Metaverse system and short its digital assets on the exchange. Thus, the total value of the digital assets on Metaverse is a function of the cost of maintaining / attacking the system, (specifically the cost of mining during the PoW stage). Ideally, the total value of the digital assets should not exceed five times of the cost of mining.

4 Metavesre Design Principles

4.1 Minimalist Design Principle

The core concept of blockchains are ledgers, and the core function of a ledger is to keep records. MVS will center the design of its digital asset and digital identity ledgers around ledgers, and will not consider precipitating application content on top of basic functions. We will strive to keep all functions as simple as possible and expand on the underlying infrastructure by using Metaverse Improvement Proposals (MIP). We call this the minimalist design principle.

4.2 Stable Evolution Principle

During the evolution of MVS, only two situations required MIP:

- Enhancing core functions.
- Repairing security issues.

Regardless, MIP should ensure that the Metaverse blockchain operates in a stable manner.

4.3 Compatibility Principle

MVS versions must be backward compatible and support all operating platforms including desktops and mobile devices.

4.4 Modular Design Principle

In the MVS implementation process, a hierarchical module-submodule structure was used to reduce the level of coupling between modules.

5 Metaverse Architecture Design

Metaverse development is divided into the following two phases:

In the first phase, Metaverse will be based on the PoW consensus algorithm. It will mainly provide digital identities, digital asset registration and transfer, simplified built-in scripts, simple datafeed, and credit evaluation functions. Metaverse can be used to support all consortium blockchains, forming an open platform ecosystem.

In the second phase, Metaverse will transit to a modified DPoS-based consensus algorithm (HBTH-DPoS). Building upon the ecosystem consolidated in the first phase, we will extend the functionality of smart contracts and provide complete Oracle services.
The following section will mainly discuss how Metaverse chose its technologies and their architecture.

5.1 Technology Model Selection

There are three possible options for the first phase: Bitcoin, Ethereum or Bitshares system. Amongst these three, Ethereum's coding system updates most quickly and incidentally comes along with an EVM (Ethereum Virtual Machine). Considering the limited development resources and time available to Metaverse, low-level reconstruction may not be suitable.

The entry point for Metaverse is digital identity and digital assets, and Metaverse once aimed for an extremely idealized Bitshares system. However, due to the "anchoring mechanism"and UTXO model used by Bitshares we could only subtract from their code. Due to the principle of code reuse, the risk and difficulty of subtracting code far outweighs that of adding code. Thus, Metaverse finally settled on Bitcoin's technology system.

Within Bitcoin's technology system, MVS chose to base its main code on the Libbitcoin library to design its own Hierarchical Deterministic (HD) account system. Moreover, Metaverse combines Ethereum's Ethash algorithm to design a variety of asset transaction types.

Advantages of choosing Libbitcoin:

1. Metaverse is not a simple altcoin. The integration of digital assets and digital identity requires code to be highly modular. By studying versions 0.8 and 0.12 of the Bitcoin code, we believe the coupling of Bitcoin Core is relatively high, which is not conducive to the development and maintenance of Metaverse.

2. In terms of code structure, some of the historical problems faced by Bitcoin Core such as C + + templates and macros also plague Metaverse debugging. The class inheritance hierarchy is unclear, which causes problems for reconstruction.

3. Bitcoin Core's code does not support Unicode.

After comparing Libbitcoin and Bitcoin Core's code, we found Libbitcoin to be superior in the 3 areas mentioned above, especially in terms of readability and module coupling.

Disadvantages of Libbitcoin:

1. Missing important modules such as miner, account and json-rpc;

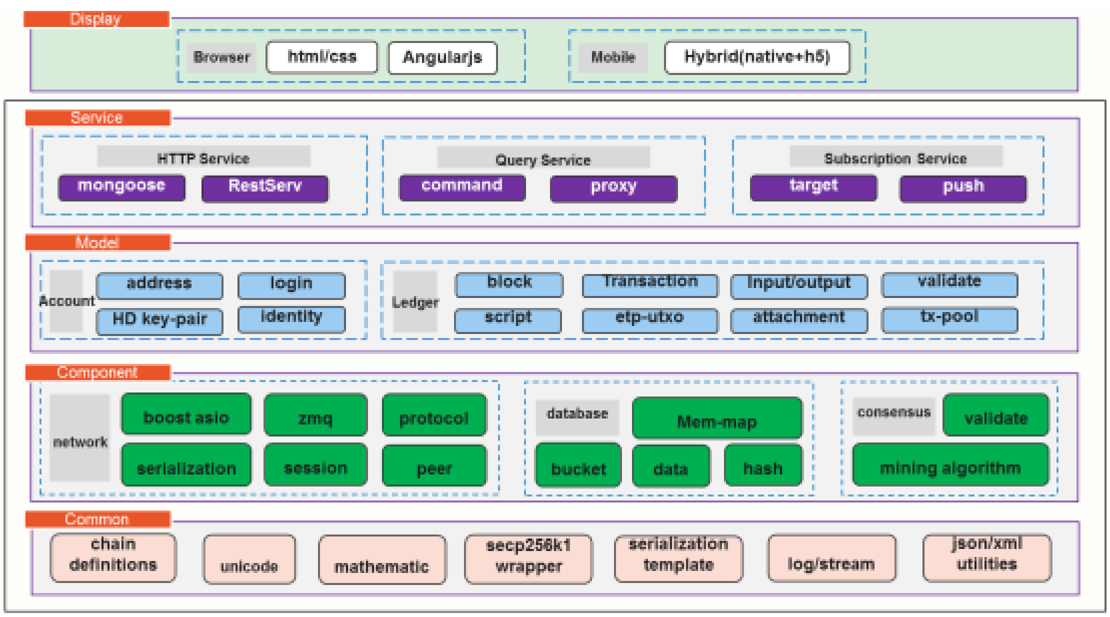
2. It produces more bugs when trying to establish a network connection for block synchronization.

3. As a result of using the boost-asio library, Libbitcoin designed a large number of handlers to achieve the asynchronous effect, causing problems for underlying module tracking and debugging.

4. The amount of code is huge. A lot of extra work must be done to achieve clear module design and to meet mandatory code requirements.

5.2 Basic Architecture

The architecture diagram of v0.3 is shown below



During the first phase of MVS, we designed the following five layers for the Metaverse client.

Common Layer

This layer is a basic one containing a number of common functions including the definitions of foundation classes, configuration inheritance, math libraries, flow processing libraries and other general functions. This common level is composed of small functions, foundation classes and C + + templates and also contains important libraries,

such as speck265k1/zmq, and a large number of classes.
bc::wallet::script------transaction scripts
bc::wallet::payment_address----transaction address

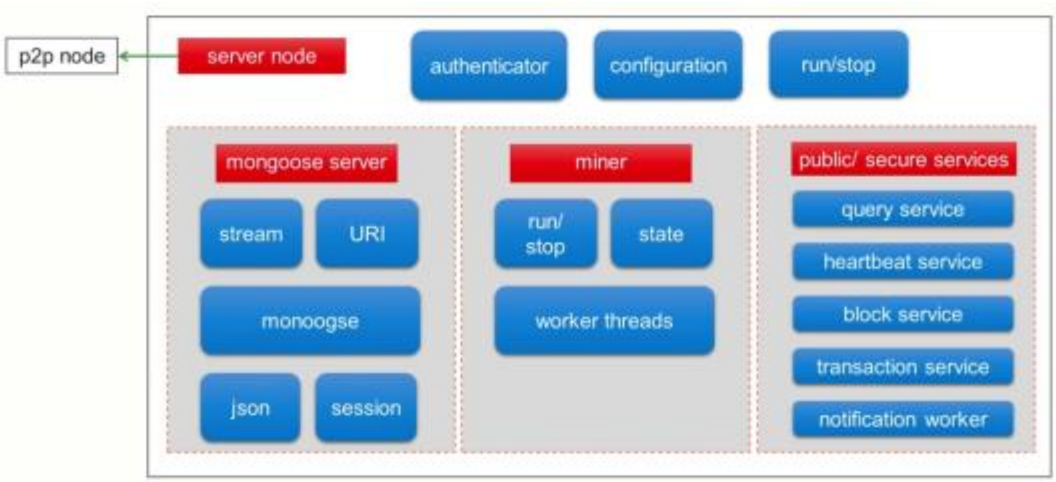
Component Layer

The component layer contains the core components of a blockchain: network communication, blockchain database persistence and consensus processes. The Network module in particular is an underlying module that the entire blockchain lives and dies by.

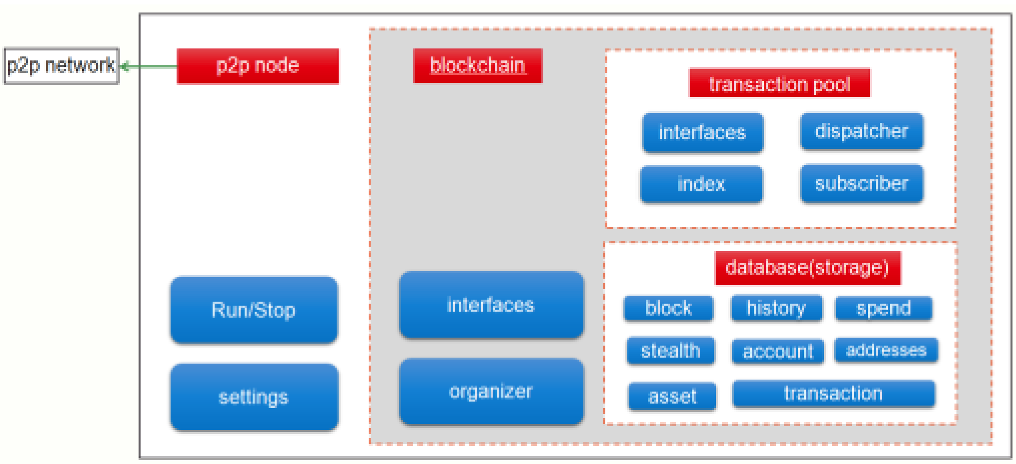
- **Network**

The P2P-network, PoW mechanism and its verification are included in this layer. The bottommost layer is used to support the P2P network modules to receive all network messages (it does not support LAN penetration). The consensus module contains functions related to mining, blockchain verification and network difficulty adjustment.

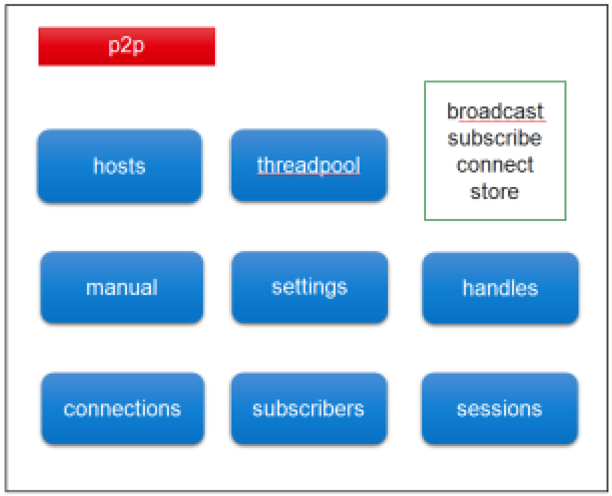
Now we consider the full nodes. In terms of inheritance levels, we have server_node structure of the bottom, which contains the following elements:



Mongoose's server is a http server;
Miner refers to the consensus module;
The public query provides an open and encrypted query interface (binary);
And server_node is derived from the p2p node.
The p2p node is demonstrated as follows.



p2p node contains the main blockchain services, and blockchain is mainly composed of transaction-pool and database.
p2p node is also derived from p2p network;
p2p network contains the following contents:



In other words, the entire inheritance level also reflects how the network module's forms the basis of the entire blockchain;

The contents of the consensus verification portion are integrated into server_node through the miner (consensus) module, which is also a module in the bottom layer.

- **Database**

Unlike traditional databases, this storage database is a relatively small locally embedded database. At present, Sqlite and Leveldb are the available mainstream options.

Early on in the technical module selection process, we considered using Sqlite in place of Libbitcoin's native key / value hash-memory-map file storage method.

Taking Sqlite's performance and the technical complexity of replacing Libbitcoin's existing code into account, we decided to retain Libbitcoin's original hash-memory-map approach. This storage method has superior speed and performance and can easily access memory-pool. However, it lacks extendibility, and has a certain learning cost.

- **Consensus**

The Consensus module mainly provides the ETHASH consensus algorithm, stand-alone CPU mining module and transaction verification module.

Model Layer

According to the overall structure diagram of v0.3, we can see that ledger layer contains two core elements: account and ledger.

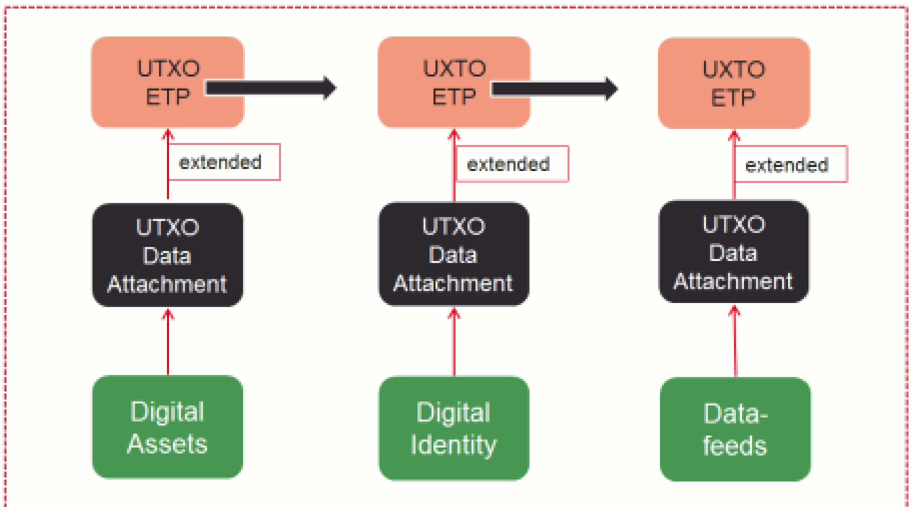
- **Account**

Based on the HD key-pairs, we designed a two-tier HD account.
The concept of the account will be extended to form digital identities in the application layer;

- **Ledger**

Based on the UTXO model, we designed an extended transaction that is differs from ETP transactions. These can be further extended into three categories: the digital identity ledger, digital asset ledger and data-feed data reference ledger.

The following figure illustrates MVS's implementation of different transaction types:

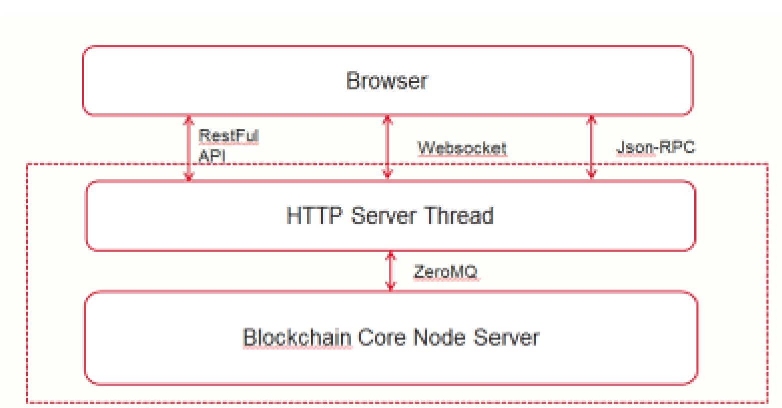


Service Layer

The service layer contains two types of interfaces: a Query Service and a Subscription Service. Query services can be implemented in three interface formats: RestFul API, Websocket and Json-RPC; subscription services can be implemented through Websocket.

All services are provided to the user with HTTP Server as the interface gateway, and the user uses both services by calling commands.

The following figure illustrates the relationship between the service layer and other layers:



- **HTTP Server —— mongoose concurrent volume mongoose**

Mongoose is an HTTP Server with small concurrent volume, based on select / epoll (optional). Considering Metaverse is a user-facing program, its usability rather than concurrent volume is the main concern here.

- **Uses' command set**

The command set can be divided into two categories:
Online commands refer to those that will interact with the blockchain, such as the getbalance command.
Offline commands refer to commands that purely perform calculations, such as the getaccount / fetch-tx command;

Display Layer

The display layer is a human-machine interface (HMI). Currently, we have established an AngularJs library for the desktop version that interacts with the core of the Metaverse Wallet. For mobile devices, a mixed development method will be used to establish light payments on the client side.

5.3 Blockchain is the Assumption of Service

5.3.1 The internet of information and the internet of value

A unique feature of the internet of information is that businesses and technology can be decoupled via multilayered architectures that separate data access layers from business logic layers.

On the other hand, the internet of value features an exclusive nature and often intrinsically contains financial systems. When separated from this financial system, it becomes a classic distributed system and cannot be called as an internet of value.
On the internet of information, the typical product separating business and technology is cloud computing.

Today, cloud computing has gradually expanded beyond its typical applications and is attempting to penetrate multiple verticals and industries to provide better technical solutions. A common example would be financial services solutions hosted on the cloud;

However, regardless of the fact that these cloud-based solutions are applied to financial services, they can be replicated in all kinds of industry. For instance, Company A and Company B both purchase the exact the same product F. However, product F may completely serve as different application at Company A and Company B. There is usually no direct relationship between them apart from a small connection between them and a third-party intermediary such as a bank or a securities company.

To achieve the Internet of value, A and B could run different subnets on the same instance of application F and hence be directly connected; in other words, some of the services provided by third party intermediaries O such as payment functions (which blockchains are intrinsically equipped with) are no longer necessary.

Metaverse hopes to establish the internet of value via the provision of this basic service.

5.3.2 Blockchain service

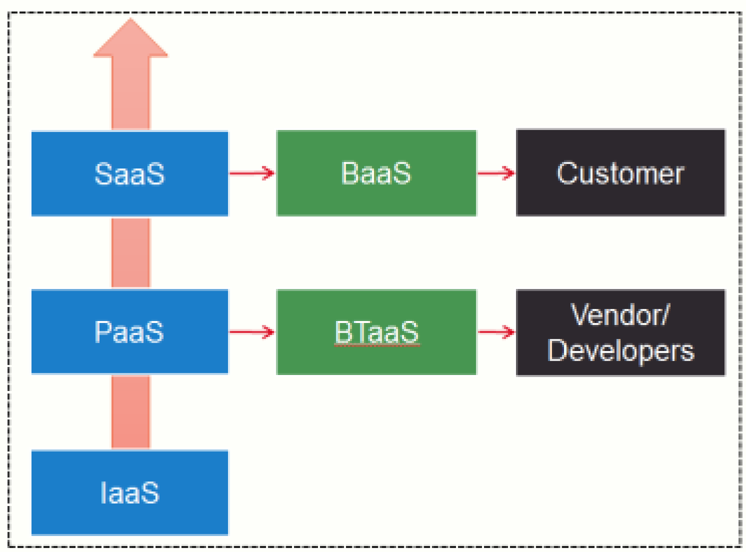
Blockchain as a Service (BaaS) refers to using data generated by public blockchains to provide a series of operational services including blockchain-based querying, transactions and data analysis.

In the blockchain sector, blockchain explorers, digital currency trading platforms and other applications derived from public chains such as certificate-Factom and digital identity-uPort all currently fall under the umbrella of blockchain services.

These applications share one feature: they are all based on existing public blockchains to develop or strengthen their existing capabilities, rather than merely use blockchain technology to create a private service.

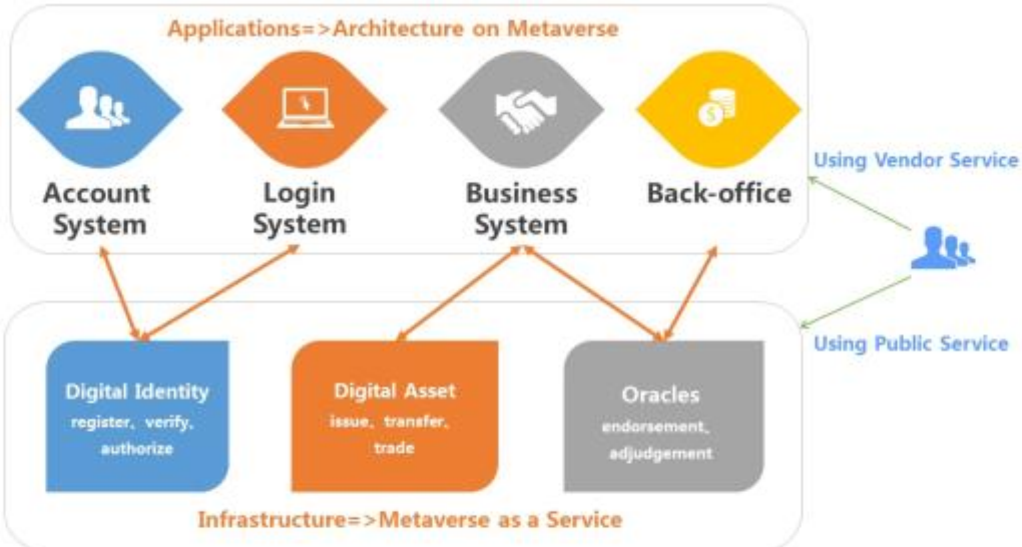
Extending the SaaS / PaaS concept from cloud computing to blockchains, we acquire two new service types:

- BaaS——the variant of SaaS——**BaaS (Blockchain As A Service)**
- BTaaS——the variant of PaaS——**BTaaS (Blockchain Technology As A Service)**



BaaS targets at ordinary users, while BTaas targets at vendors and developers.

5.3.3 Blockchain provides service



Metaverse blockchain is capable of providing infrastructure services (BaaS) to any IT system or device. The system can be compatible even with privately-owned IT systems using digital identity as the primary entry point.

The Metaverse public blockchain provides identity appraisal and authentication functions in addition to asset querying and performing transactions. The data on the blockchain is sheerly immutable and reliable, and services provided by external operators are supervised by users through the Metaverse public blockchain.

6 MVS Consensus Algorithm and Token Model

6.1 Consensus Process

The so-called block chain consensus process refers to the process of objectively recording the entire network's transaction data of such that it is immutable. This consensus process is realized in practice through consensus algorithms.

Currently, several mainstream consensus algorithms exist. These include the PoW (Proof of Work), PoS (Proof of Stake) and DPoS (Delegated Proof of Stake) mechanisms used by Bitcoin, Ethereum and Bitshares respectively.

These algorithms are generally credited to the field of economics, because they calculate the cost of cheating the system. They ensure that cheating is unprofitable by making the cost of cheating much greater than its reward. Establishing an economic game between nodes based on these algorithms hence allows the system to have the tendency of a stable equilibrium.

Correspondingly, we also have distributed consensus algorithms in the field of computing such as Paxos and Raft algorithms; these can also be called classic distributed consistency algorithm.

The biggest difference between these two classes of algorithm is their reliability under the Byzantine Generals Problem Scenario; specifically, the PBFT algorithm supports Byzantine fault tolerance. On the other hand, both the Paxos and Raft algorithms are theoretically susceptible to getting stuck in an endless loop with no possibility of passing through via the voting system (although this probability is extremely small). However, both algorithms meet the safety requirement, although they relax the liveness requirement. PBFT is similar in this regard.

The similarities and differences between traditional distributed consensus algorithms and the blockchain consensus process.

Similarities

- Append only
- Emphasis on serialization
- The principle of the minority following majority
- The problem of separate coverage: blocks in longer chains override the shorter ones, and multi-nodes override the logs generated by smaller numbers of nodes

Differences

- Traditional distributed consensus algorithms do not take Byzantine Fault Tolerance (except for Byzanetine Paxos) into account and assume that all nodes only meet non-man-made problems such as computer or network failures. They do not consider the problem of malicious nodes tampering with data.

- Traditional distributed consensus algorithms are log-oriented (database), which could be used in common cases. However, the blockchain consensus model focuses on transaction. Thus, strictly speaking, traditional distributed consensus algorithms belong to underneath the layer containing the blockchain consensus model.

Metaverse is a public blockchain. Several prominent consensus algorithm designs for public blockchains currently exist including the PoW (Proof of Work), PoS (Proof of Stake) and DPoS (Delegated Proof of Stake) mechanisms used by Bitcoin, Peercoin and Bitshares respectively. Various other forms of Byzantine Fault Tolerant (BFT) mechanisms exist.

Most cryptocurrencies today choose to bypass the BFT algorithm as it fails to resolve the issue of token distribution.

Although Metaverse's ETP is not a currency, it will be distributed to nodes that made contributions to network security.

The total amounts of full nodes is inadequate in the early phases of any blockchain projects, making it more difficult to guarantee the entire system's network security. Through the introduction of PoW, Metaverse will distribute ETP to mining nodes as block rewards, allowing the system to attract a large number of full nodes that can secure the network at early stage.

As the projects mature in the future, the ETP available as mining rewards will dwindle and Metaverse will transit to an improved DPoS consensus algorithm. This algorithm will consider "Token –Height Destroyed" as a performance indicator.

First phase: PoW mining

During the first few years of the Metaverse system's operations, GPU mining will be employed to ensure network security and implement a decentralised timestamp server system. We are still looking into Metaverse's mining algorithm, but will avoid the SHA256 and scrypt algorithms to avoid facing the possibility of a 51% attack.

Second phase: HBTH-DPoS

Although PoW mining can help safeguard Metaverse's system security in its initial years, it has limitations such as energy waste and mining centralization.

The DPoS mechanism pioneered by Bitshares is even more robust and decentralized than PoW and PoS. More importantly, each participant in its system is a qualified voter.

However, there are 2 design flaws within the DPoS consensus mechanism. Firstly, financial interference: by acquiring the majority of tokens, delegates can interfere by supporting or opposing important protocols to manipulate the token price for short-term profit. In the current Bitshares system, it is estimated that only $3 million USD worth of tokens is required to manipulate voting results.

Secondly, voter apathy: As voters (users) often lack of interest in the state of a system, most transfer their votes to delegates and are unlikely to monitor potentially malicious delegate behavior.

Metaverse solves these problems through a modified DPoS consensus protocol by adding the concepts of Token-Height and HeartBeat.

Token-Height is similar to the concept laid out in Bitcoin Days Destroyed, which measured the transaction volume of Bitcoin.

The number of Bitcoin Days Destroyed is the number of Bitcoins in a transaction multiplied by the number of days since those coins were last spent.

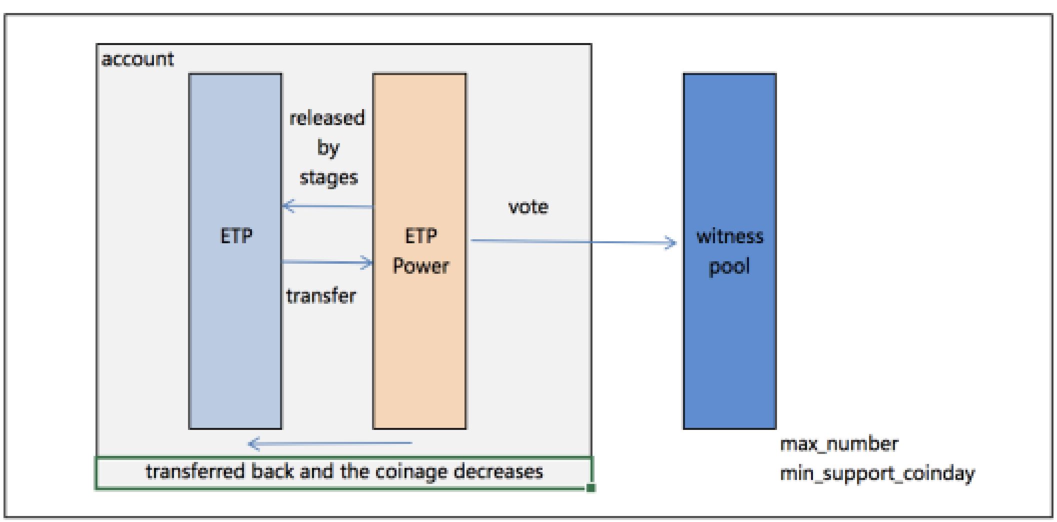
Similarly, Token-Height in Metaverse is calculated as the number of ETPs multiplied by the number of blocks since those tokens last spent.

By weighting the voting power in DPoS in such a way, Metaverse significantly lowers the likelihood of financial interference by reducing the voting power of attackers who acquire large amount of ETPs from the market. To accumulate enough voting power to make an impact, would-be attackers would either have to acquire much more ETP than a 51% attack would have required, or hold the ETP for a long period of time to increase its voting power, ensuring that the opportunity cost of such an attack is prohibitively high.

In the DPoS phase, Metaverse will distribute ETP to equity holders based on their prevailing equity holdings similar to other systems utilizing the PoS consensus protocol. However, the difference is that the equity holders of Metaverse will not acquire the new ETP passively by receiving tokens. Rather, the holder needs to send a HeartBeat to the system to prove that he/she is active. At the same time, this HeartBeat is equivalent to a digital signature from the owner's private key. Lastly, the equity holder must choose to either replace or maintain his / her delegate when sending his heartbeat.

There are advantages to designing the Heartbeat in this way: firstly, it motivates users to check their delegates, alleviating though not fundamentally solving the voter apathy problem. Secondly, the system will not allocate the new ETP to inactive users, exerting a dilution effect on their equity holdings.

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



The model's specifications are as follows:

(1) Separate voting attributes and transaction attributes of ETP and define built-in tokens for voting known as power. Define coinage as the basis of calculation of valid votes, which can prevent voting attacks carried out by obtaining large numbers of ETP from the trading market.

(2) Define the concept of coinage (equity accumulation over time) . This forms "evidence" that can't be forged, similar to PoW. Consider how the price of holding and locking down equity is borne by holders, just as how using a computer's CPU or GPU to verify a consensus algorithm's mathematical function costs electricity. The formula for calculating coinage is as follows:

$$Coinage = \sum_{h=h_1}^{h_2} Locked(ETP) * f(h)$$

$$f(h) = \begin{cases} \dfrac{H-h}{a} & ,h \leq H \ , \ H = h_1 + max; \\ 0, h > H. \end{cases}$$

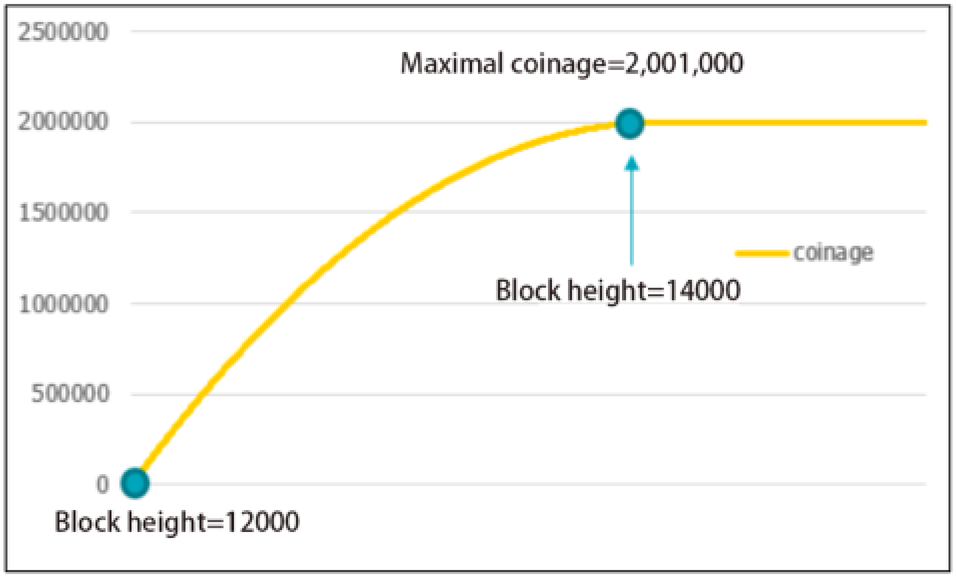
- Locked(ETP) is the number of ETP locked on the special address before voting
- f(h) is the time density function relevant to height.
- h1 is the height at the beginning of the locking period, h2 is the height when the ETP is unlocked
- H is the maximum height of coinage that can be achieved by ETP locking; when this limit is exceeded excess height will not generate new coinage records.
- max refers to the number of blocks that can generate coinage.
- a is conversion parameter with no special meaning.

Assume that h1=12000, current h=14500, max h=2000, the conversion parameter a=5000 and the number of locked (ETP) is 500. In this case, if the ETP is unlocked immediately, then h2=h=14500. But if H = h1 + max = 14000 <h2, locked ETP can generate coinage:

$$Coinage = \sum_{12000}^{14000} 5000 * f(h) = 2{,}001{,}000$$

.

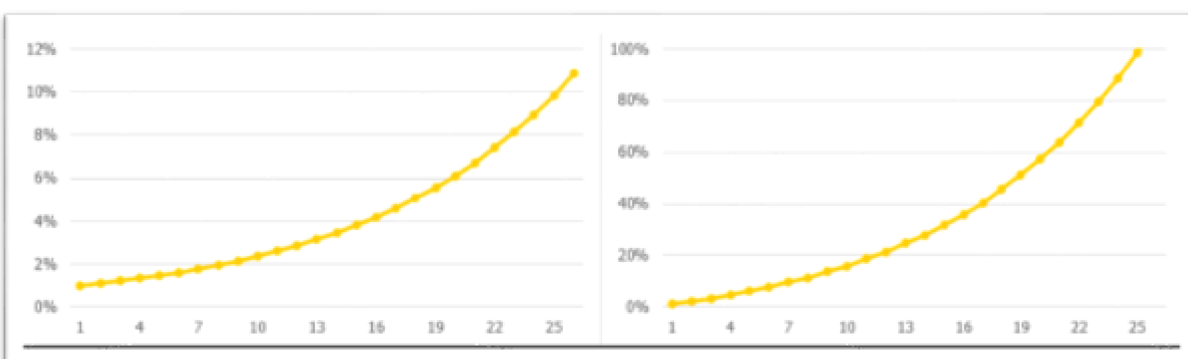
The figure is as follows:



In this case, if the block creation speed is about 15 seconds, then it takes 8.33 hour to generate 2000 blocks. Attackers need only to lock their ETP for a short time to obtain all voting-weights, a risky prospect. One can simply adjust max to change this time.
(3) The mathematical relationship between Coinage and power is linear function, defined ratio for the ratio (Coinage To Power).
(4) ETP generates power as follows:

Local client: conman address (ETP for power) -> Local client: voting address (ETP for power) -> Locking is completed through these transactions within addresses; and the ETP is locked at the moment the transaction is completed. -> when the unlocking happens, calculate the coinage-> unlock; unlocking is the reverse of the locking transaction, but this process doesn't happen instantly. The unlocked conditional function is:

Each of the first 100 blocks unlocks 0.01% ETP. This number increases by 10% for every 100 blocks, i.e. each of the second hundred ones unlocks 0.01% x (1 + 10%) ETP, until all blocks are unlocked. The density functions and the cumulative functions for the unlocking of ETP are as follows:



From the graphs, it is apparent that although unlocking speed is relatively slow at first, but will increase. Under this assumption, it takes about 2400 blocks to complete unlocking. If the block creation speed is 15s / block, it takes about 10 hours to unlock all the ETP, and the number of ETP unlocked in the first 5 hours accounts for only about 20% of the total amount. If the total time needs to be adjusted, the height interval required to increase the amount of ETP unlocked must also be modified. For example, if the interval is increased to 200 blocks, the time required doubles.

To change the unlocking speed while preserving the shape of the curve, the rate at which the number of blocks unlocked increase (increase ratio) should be adjusted. For example, if the ratio is adjusted to 5%, the unlocking speed will be decreased.
Other unlocking models are also available. The one used here is the simplest, an equal proportional model.

6.2 Transaction Type

Besides the coinbase transaction type, there is only one other type of bitcoin transaction left, which is the transfer of coins between sender and receiver.

With smart contracts, Ethereum greatly expanded the types of transactions that can take place on the blockchain to include transactions such as asset issuance. However, users must be familiar with Solidity (the language used to code smart contracts on Ethereum) in order to execute such transactions. While relatively simple for trained developers and coders, the need to learn Solidity has alienated no small number of business users. Bitshares, on the other hand, uses an intuitive design to enable multiple types of transactions; its architecture, however, is complex and inefficient.

In Metaverse, we seek a balance between efficiency and user experience. Neither the one-contract-fits-all (Ethereum) nor the half-dozen contract type (Bitshares) model are best for the types of transactions our platform emphasizes from the outset: smart property issuance and digital identity registration. An Ethereum-style transaction type will be added to Metaverse in the future.

6.3 Ledger Model

Metaverse combines the Bitcoin UTXO model and the balance-based model.

The UTXO model will be used for ETP while the balance-based model will be used for user-customized digital assets.

For more information, interested readers can study the Bitcoin developer documentation.

6.4 Digital Identity and Data-feed

Metaverse will deploy the zero-knowledge verification protocol developed by Zcash known as zk-SNARKs in order to secure users' digital identity and privacy.

Data-feed is another important function in Metaverse. Unlike Ethereum, in Metaverse a large portion of data-feed responsibilities will be handled by Oracles. Their credibility will be based on two factors: (1) their valid credentials; and (2) their records on Metaverse.

The market will provide feedback on their credibility in several ways. Firstly, data-feed users will “vote” through their transaction records. Appropriate votes will accumulate, providing rewards for voters similar to evaluation rebates. Suggestions regarding decision rules and reward models will be released in subsequent versions. Secondly, inappropriate votes will result in negative implications for voters that will be determined according to the voting mechanism.

The reason for this feedback mechanism is that business-level rules should not be hardcoded into Metaverse. All blockchains are bound by their basic function: consensus. For data-feeds, malicious behavior will affect the business itself but not the Metaverse consensus mechanism. Indeed, malicious behavior that utilizes the data-feed will incur costs due to MVS consensus but must be defended from the Oracle or BAPP layers. Even so, the people behind MVS’ design hope that there can be a healthy data-feed model that can provide new rules and suggestions.

6.5 Cross-platform

Windows, Linux and MacOs platforms are compatible with Metaverse in its incipient phase.
Metaverse will consider transplanting MVS to ARM and other embedded platforms to assist in the digitalization of assets in the Internet of Things and Energy Internet.

References

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