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)

Metaverse is a decentralized open platform based on public blockchain technology that encompasses Digital Assets and Digital Identities. By building a general technology platform that can be utilized by enterprises and individuals, Metaverse digitizes assets (conceptually similar to asset securitization) such as rare goods (artwork/antiques), intellectual property, and rights to returns from financial instruments in order to improve market efficiency. Through the provision of smart contracts and digital identities, Metaverse connects standalone stores of value to form an internet of value.

MVS hopes to develop iteratively by working closely with businesses. Hence, each version of MVS will support a different degree of functionality, with successive updates responsive to market feedback. The initial version of MVS will be released with a minimal set of operations. This will subsequently be expanded using Bitcoin as the foundation to provide additional functions such as Digital Identity and Digital Assets.

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

1 Overall Background of MVS – Blockchains

1.1 About Blockchain

Blockchain technology originated from the Bitcoin system. Because of the technology's decentralized nature and its immutable ledger, Bitcoin provides a solution for problems such as trading fraud and double spending. It is widely believed to be the first application of blockchain technology.

Bitcoin is a sophisticated online payment system first invented by Satoshi Nakamoto, who defined Bitcoin as a Peer-to-Peer Electronic Cash System. In the past seven years, despite the initial misgivings, Bitcoin has ascended to prominence and now boasts a market cap of over USD $100 billion.

Many acknowledge 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 convincingly proved that physical assets can and will be digitized. As a decentralized system, blockchain uses cryptography to maintain an immutable ledger, allowing all parties to freely transfer value and conduct transactions in a trust-free environment. This has wide-ranging implications for industries such as banking, insurance, healthcare, logistics and media.

1.2 A Brief History of Blockchain

The development of blockchain technology and its concepts follow the deconstruction and reconstruction of the Bitcoin system. Namecoin and Peercoin made landmark contributions in the process of moving from cryptocurrencies to the blockchain concept, while Bitshares and Ethereum furthered our understanding of the blockchain.

- **Namecoin and Peercoin**

Namecoin is the first application forked from Bitcoin. It was designed and implemented to add the concept of "decentralized domain name" to Bitcoin's original electronic cash system (this can be 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 shared a PoW algorithm with known mining centralization issues and had to deploy mining hardware as full nodes in the network, blockchain technology would lag years behind its current state of development. Peercoin came up with a different consensus mechanism, 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 mechanism also continuously drove the development of blockchain technology.

- **Bitshares**

Bitshares improved on PoS by implementing the Delegated Proof-of-Stake (DPoS)

consensus protocol. Bitshares constantly put forward new concepts such as Keyhotee, a project that gave digital identity more prominence. Furthermore, it introduced multiple types of transactions to simplify asset registration and issuance. Crucially, Bitshares introduced a Decentralized Asset Exchange. To provide a better user experience, it modified its block creation rate to be one every few seconds; however this came at the sacrifice of some system stability.

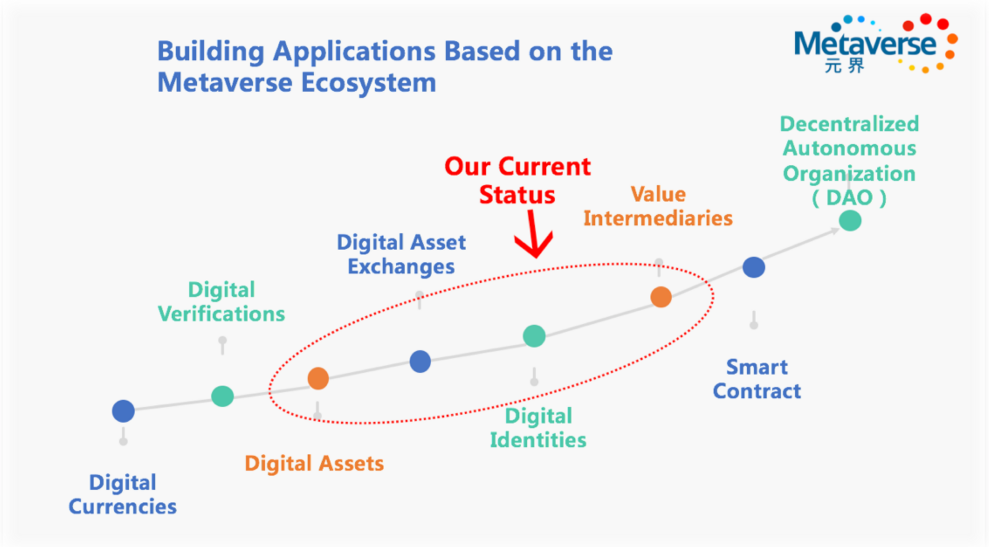
- **Ethereum**

Unlike Peercoin and Bitshares, Ethereum uses the PoW consensus protocol to secure its network in its early stages and will transition to a PoS consensus protocol by forking. This design primarily considers the system's safety during its initial stages. In addition, Ethereum implemented the concept of smart contracts, its most important contribution apart from its enhancement of block creation characteristics and reward mechanisms. 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 and Permissioned Blockchains**

The difference between public and permissioned blockchains 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 required to select the node responsible for recording a transaction. On the other hand, permissioned blockchains only grant access to whitelisted nodes, and may establish a strict firewall. Therefore, a public blockchain's trust mechanism is targeted at the general public and has a broad scope – all parties who use the public blockchain or record transactions on it are within the scope of trust. However, permissioned blockchains only trust permissioned nodes and hence have relatively small scopes of trust.

- **Blockchain Roadmap**



Bitcoin, Bitshares and Ethereum are currently in the digital currency/digital notarization, decentralized exchange, and decentralized organization stages respectively. Looking at the current status of blockchains today as illustrated above, it is clear that blockchain technology is still developing. Hence, our goal of building a blockchain ecosystem containing diverse applications built on a value transmission network featuring a comprehensive basic infrastructure layer still requires a gargantuan effort.

2 Why Metaverse Was Established

2.1 The Virtual World Has Become A Reality

The term ‘Metaverse’ first appeared in Neal Stephenson’s 1992 science fiction novel Snow Crash, where humans controlled avatars in a virtual reality world known as the Metaverse. Through avatars, one could interact and form relationships with other electronic agents.

Modern life is just like the world described by 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: an increasing number of digital assets transfers will take place online, and Avatars (Digital Identities) and intermediary Oracles will become the new mainstream economic model.

The name Metaverse Project was inspired by Neal Stephenson’s Metaverse.

3. Metaverse Economic Model

3.1 The Metaverse Token – ETP

- *ETP*

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

ETP is not a new form of digital currency – instead, it represents the rights and interests of Metaverse. Hence, the price of ETP will not be anchored on any fiat money 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 assets and identities on Metaverse) must be paid in ETP.

- *ETP Distribution Mechanism*

(1) ICO and community building

In the blockchain industry, ICOs are common and are 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, Lisk and the controversial The DAO project that followed all launched their ICOs in 2016. Domestically, NEO also successfully crowdfunded 2,100 and 6,119 Bitcoins in October 2015 and September 2016 respectively.

Metaverse Project has distributed 25 million ETP in its first Initial Coin Offering (ICO). Another 25 million ETP will be used to set up the Metaverse Foundation to support blockchain ICO projects that benefit the Metaverse community, facilitate investment activities that enhance Metaverse's ecosystem and reward major contributors to the community.

(2) PoW and PoS mining

Additionally, about 30 million ETP will be distributed as block rewards through the PoW mechanism to those who help maintain Metaverse's system, through a process known as mining.

The block difficulty of Metaverse will adjust to match the network's computing power. The

targeted block generation time is 24 seconds; the actual block time at the time of this writing is 33 seconds. The initial reward for mining each block is 3 ETP and block rewards decrease by 5% every 500,000 blocks. Hence, setting block time and block reward as standard parameters, we can obtain 1) a graph showing amount of ETP mined against time in years, and 2) the decay diagram of the total reward obtained every 500,000 blocks against time in years.

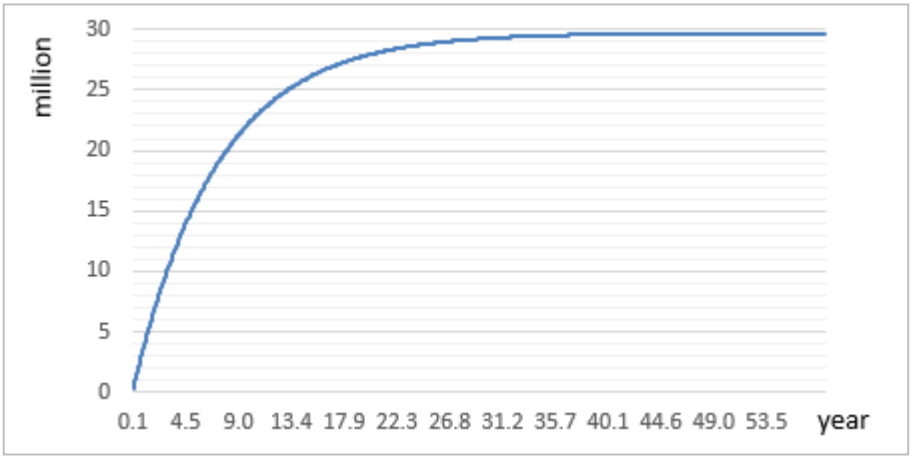


Figure 1: Amount of ETP mined against time in years

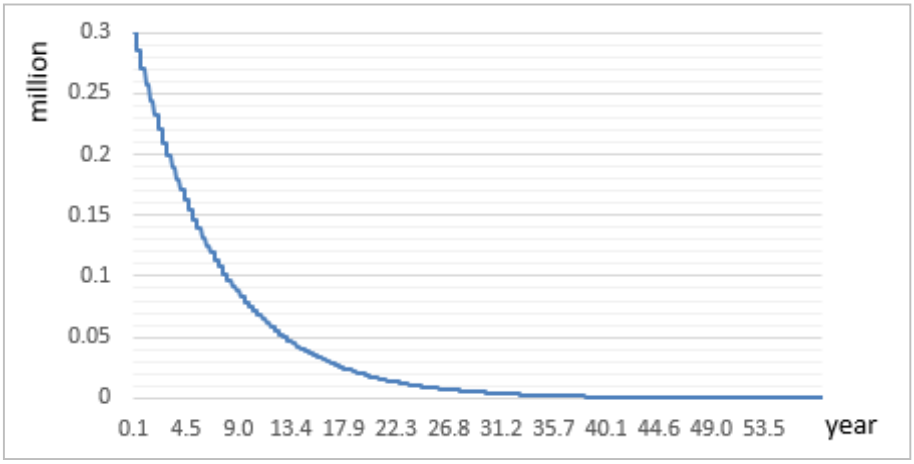


Figure 2: Total reward obtained every 500,000 blocks against time in years

(3) Coinlock and Coinlock Rewards

Metaverse incorporated a paid coinlock function at the system level while designing ETP's economic model. This design is the first of its kind – it can be thought of as the tokenization of coin age, and it paves the way for a PoS-based economic model in the future as well as financial applications derived from the coinlock function.

To obtain ETP rewards, users must take the initiative to use the coinlock function. This reward will be sent together with the principal amount to the user's coinlock address through a coinbase transaction once the locking period ends.

Reward details are specified below:

H + block height	25,200	108,000	331,200	655,200	1,314,000
Reward rate	0.10%	0.67%	3.20%	8.00%	20.00%

- **H + block height**: Assuming the current block height is 'H', users must lock their ETP for 25,200 blocks (till block height = H + 25200) to obtain the lowest-tier coinlock reward.
- **Reward Rate**: Assuming that users lock 100 ETP and choose the fourth-tier coinlock reward (requiring H + 108000 blocks), their address will reflect a balance of 100 x (1+0.67%) = 100.67 ETP after the 112,696th block has been created.

The initial design provides five reward tiers, but the block height required for each tier does not scale linearly. If we convert the block time to days (using the actual block time of 33 seconds for calculations), we can estimate the time required for each coinlock tier:

H+ block height	25,200	108,000	331,200	655,200	1,314,000
Estimated Time (In Days)	**10**	**41**	**127**	**250**	**502**

(The numbers above are computed values. Reward rates are correct to two decimal places; estimated times have been rounded to the nearest integer. Specific reward rates and unlocking times will be determined by actual block times.)

This table presents the tier rewards in a more intuitive manner. Users will naturally compare and contrast them with rates of return available elsewhere, since interest rates and rates of return form the backbone of the financial industry. 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 the development of its ecosystem.

This is a bold design that attempts to create interest rates native to the blockchain ecosystem and community, instead of depending on interest rates set by external central banks. However, the initial implementation of this design is not ideal because the interest rate is not dynamic or adjustable, let alone capable of reaching the true market rate through decentralization and game theory mechanisms.

As Metaverse progresses, we will further promote the degree of activity of ETP in both centralized and decentralized trading markets. ETP trading pairs in these markets will serve as key data points to determine ETP interest rates; they will be used as input parameters to influence ETP's

economic model either through voting or by directly obtaining data from the decentralized market. The volume of ETP transfer activity, the number of accounts, special transactions (to be developed) and other blockchain parameters may also be incorporated into this model.

3.2 Micro-Inflation Model

ETP is the token representing the rights and interests of Metaverse's Democratic Autonomous Organization (DAO). 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 forgotten passwords, carelessness or death. As such, the issue of there being insufficient ETP in circulation will steadily worsen. 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 we have designed requires the introduction of micro-inflation to fill the demand for ETP circulation. We have distributed a total of 50 million ETP through ICOs and the Metaverse Foundation, and a further 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 specific reward amounts determined by the total amount of coins deposited and the locking period chosen. ETP inflation rates will be fed back into the algorithm determining coinlock reward rates, allowing it 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 environment 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 with 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. This design runs counter to intuition.

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 native digital token ETP will use Bitcoin's UTXO (Unspent Transaction Output) model 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 will be testing the use of the Account model to handle smart assets. This can help reduce system complexity while retaining the benefits of the UTXO model.

The result of this design is that digital assets can be sent and received easily on Metaverse, just

like Bitcoin. Smart contracts will only be required when the demand for more complex transactions 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 timestamped, append-only public data store that does not allow past records to be altered or deleted (note that it is "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 individuals with special permissions could interfere with the blockchain).

This property fulfills the design requirements of registration functions – they are public, unique and trustworthy. Hence, registration on the blockchain need not be limited to just Smart Assets. Any data that has value has a reason to seek ways to be stored on the blockchain.

(2) How should the Smart Asset registration function be designed?

When we mention "registration", what we actually refer to is the act of describing something 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 requirements:

A. This descriptive set of data should be reusable, or its design would have failed and be ineffective.
B. Considering potential future applications, it should be accompanied by a set of query, addition, calculation and verification functions.

Considering that "Assets" usually have relatively simple generic attributes and well-differentiated special attributes and that 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 Asset Field	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 satisfying the basic information structure requirements outlined above, we must next consider how this information will be used. Bitshares attempted to issue assets on the basis of market functions, but this method produced numerous limitations including complex over-collateralization, anchoring and price feed mechanisms. Because the underlying financial infrastructure was incomplete, the market was unable to make full use of these applications on a large scale.

Blockchain systems such as BitShares and Ethereum have also begun exploring the feasibility of the Proof of Assets (PoA) protocol. On BitShares, if the authenticity of smart assets can be verified by alternative means such as posting one's private key 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, and furthermore users lack an incentive to issue their blockchain assets within a less liquid market.

In Ethereum, smart contracts seem to be able to handle all problems, including defining tokens. Some tokens can actually be regarded as smart assets because they store value and are editable. Smart contracts can theoretically support any wild business model, giving rise to projects such as Digix. It cleverly engaged third parties (gold exchanges, accounting firms, custodians) to provide a series of asset certifications forming a chain of evidence recognized by markets. This evidence is 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 took the following items into consideration:

A. The legitimacy and reasonableness of registration fees. Registration fees are undoubtedly legitimate, because they create 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. However, what would be an appropriate amount for a registration fee? Presently, this has yet to be determined. No one can predict 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 Metaverse's developer community, with the remainder 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; others 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"). Value attributes are reflected by constant trading and changes in the asset's market value. Editable attributes will apply constraints

placed on asset circulation in the real world to smart assets registered on the blockchain through various technical means (including smart contracts based on virtual machines and business-based scripting languages).

Metaverse will mainly focus on developing smart assets using the PoA model. Hence, its design will pay special attention to helping users easily provide PoA. In addition to those above, Metaverse also raised the following points:

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 pair of symmetrical transactions, Oracles can carry out asset authentication through the process illustrated below.

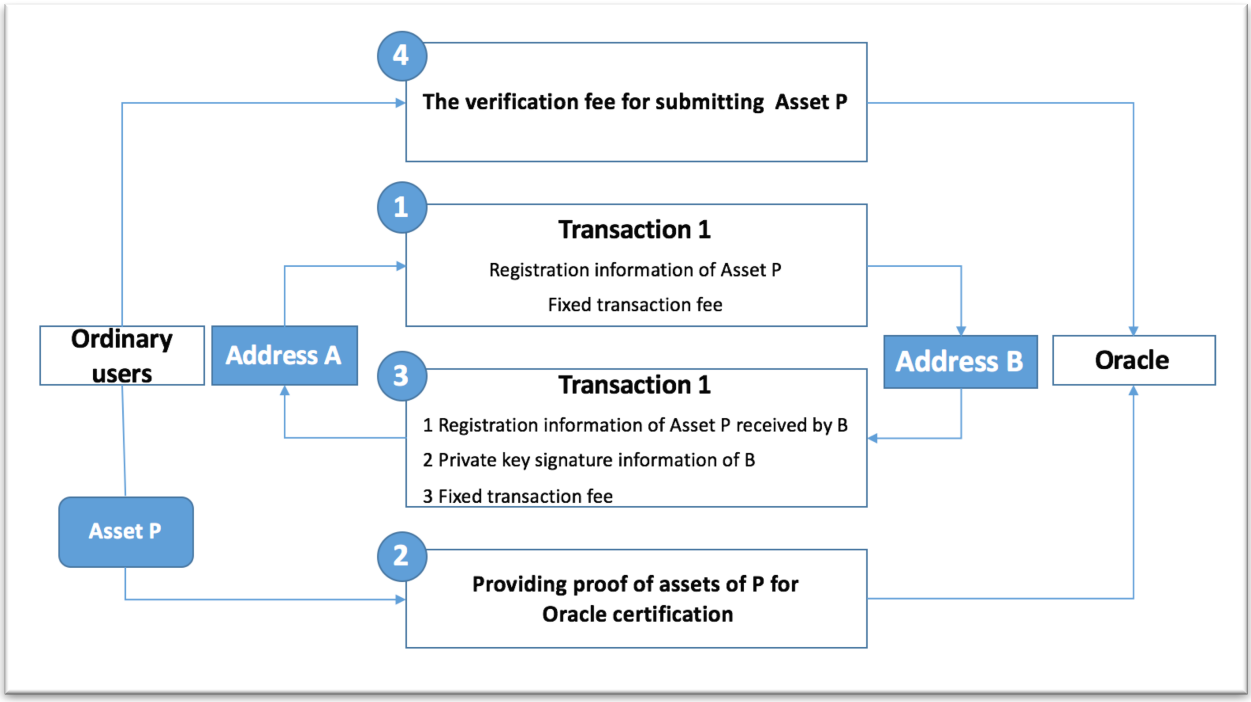


Figure 3

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

We are unable to take physical possession of smart assets the way we would physically possess tangible assets such as gold. Instead, smart assets are owned by individuals through digital

identities. In turn, these digital identities are secured through mathematical concepts to ensure they 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 Avatar involves far more than just giving your public key an alias, just as ID cards and mobile numbers are not an alias for your name. Other pieces of data with application value will be attached to each Avatar's unique index and secured through cryptography to protect 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 be able to access an Avatar's data regardless of whether it has been encrypted. Here, zero-knowledge proofs and homomorphic encryption play a vital role in 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 anonymously using public and private keypairs, most activities in the real 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 artificial intelligence (AI), machines in the Internet of Things (IoT), companies or organizations.

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 appear more complex, but more accurately reflect what ownership looks like in the real world. These relationships are authenticated and secured on Metaverse through cryptography.

There are plenty of specific (financial) use cases built on smart assets, including trading, borrowing, leasing and mortgaging to name a few.

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

The digital identity information held applications is a subset of the digital identity information available on the client end, which implies 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 ultimately belongs to the client. (2) A portion of the data dictionary must be shared between the client and application, or some intersecting data fields cannot be matched and the intersection will be left empty.

As for (1), the basic idea is to protect the client's identity information-related interests from being violated by the application. Users are responsible for declaring ownership of their digital identities through active management methods such as "timely identity creation", "status updates" and "seeking certification". Alternatively, users can obtain services from the application by selectively authorizing some information while still retaining absolute ownership over it. 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

As we all know, asymmetric encryption uses public keys for encryption and the corresponding private key for decryption, allowing information to be privately transmitted. Additionally, digital signatures made with private keys allow users to prove their identity through the corresponding public key. 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 information provided by person A is consistent with the plaintext corresponding to the ciphertext registered on the blockchain.

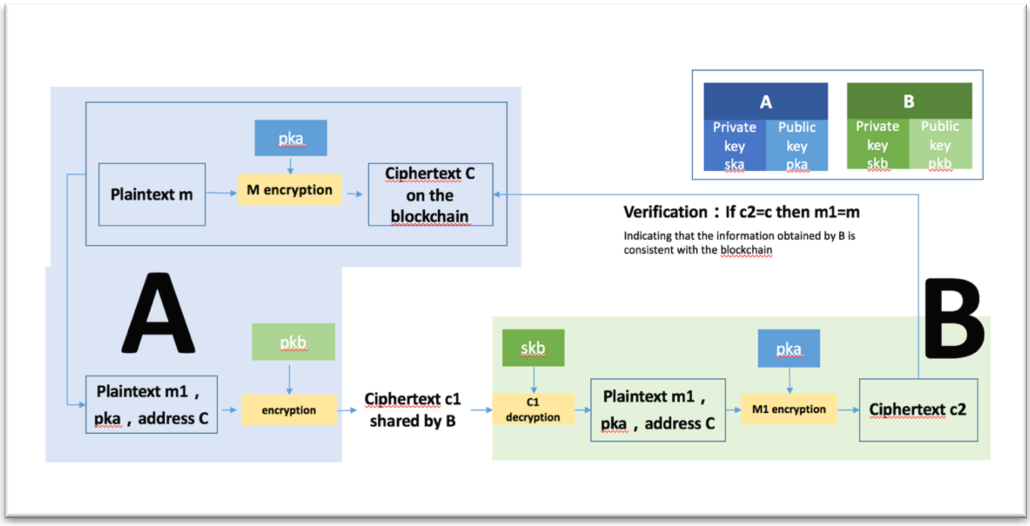


Figure 4

However, this construct is unable to solve problems outside the scope of the three goals outlined above. 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 create 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 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, and should form a special asset class. The exposure of identity information in 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 will 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 such as verification codes and passport numbers. Thus, users will 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. This will be elaborated on 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 email addresses and mobile phone numbers
(2) Customizing other personal information by defining field names and field values. For example, "City", then "Shanghai".
(3) If you do not wish to be registered on the blockchain immediately, your information can be stored locally and modified at any time.
(4) For the information to become an immutable record, users must pay a small fee in ETP to create a digital identity and issue the transaction on the blockchain.

Using this digital identity on Metaverse will require the following steps:

(1) Application service providers will submit requests for data; this data can be shared as per Figure 4.
(2) Request for an Oracle to verify the digital identity you have just registered. These Oracles may include banks, the public security system, or friends who have already been verified.
(3) A timeline of your personal resume will be generated. The effects of this simple application are more apparent after a number of years - you will find a pristine record of your life journey that has not been modified by unscrupulous service providers.

3.5 Oracle – Value Intermediary

Using the example of Alice and Bob, how many Oracle intermediaries are required in a simple New York weather forecast contract? The answer is three: one to input weather 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 act as wormholes between the virtual and physical worlds – without intermediaries, communication between these worlds will be hindered. Presently we lack a way to quantify the value perception and logic of these two worlds in code, let alone in practical application.

Unlike the slogan of "cutting out the middleman", Metaverse will reserve a position on the blockchain for value intermediaries, otherwise known as Oracles. Custodian Oracles can take custody of physical assets and issue them as smart assets on the blockchain, while identity verification Oracles can provide proof for personal information related to Avatars. Regulatory Oracles (such as government departments regulating special transactions) can also provide services such as proof of transaction authenticity and proof of compliance. Many other Oracles can provide similar services on Metaverse.

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

After Metaverse distributes 30,000,000 ETP through PoW mining, DPoS mining rewards will mainly be sourced from transaction fees. Metaverse has designed a number of native functions for the value intermediary ecosystem based on information registration, certification and other transaction types. In turn, each transaction type supports various applications related to digital identity and smart assets. We foresee that the the total amount of transaction fees, as well as the added value created by them, will increase.

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 meet business needs and inject a constant stream of value into the network, incentivizing miners and nodes to support the distributed ledger. Re-examining this problem, when transaction fees are charged not just for transactions but also for blockchain services (such as value intermediary services or smart contract activation), then the value of a blockchain will no longer 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 obtain a larger cut from service fees with higher profit rates. In the past, these services were conducted offline and neither used the benefits of blockchain technology (except to record the transaction) nor contributed back to the blockchain system (except for the transaction fee). Recording these 'transactions' feels somewhat pointless. All services will be priced in tokens at the market rate based on their 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.

- **Blockchain bloat**

Bitcoin's blockchain grows by about 1 MB every ten minutes (1GB weekly), noticeably increasing the cost of running a full node. Bitcoin has seen a decline in the total number of full nodes globally, 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 bloat, a problem that might be exacerbated by Metaverse's use of the UTXO model. This issue is well documented in Ethereum's White Paper – in the early stages it will be addressed by miners, since they must operate full nodes to mine.

- **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 produces fresh problems such as mining centralization and the potential threat of a 51% attack.

Mining centralization produces extremely undesirable results in the Bitcoin industry and led to the gradual erosion of 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 until the system migrates to the HBTH-DPoS consensus algorithm.

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

If Metaverse achieves business success, it will face a new wave of risks. When 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 an exchange. Thus, the total value of the digital assets on Metaverse is a function of the cost of maintaining / attacking the system (during the PoW stage, this refers to the cost of mining). Ideally, the total value of the digital assets should not exceed five times of the cost of mining.

4. Metaverse Design Principles

4.1 Minimalist Design Principle

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

4.2 Stable Evolution Principle

During the evolution of Metaverse, only two situations require MIPs:

- Enhancing core functions
- Repairing security issues

Regardless of the situation, we 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 process of implementing Metaverse, the multitier architecture model should be used. Functions should be split into modules and the level of coupling between modules should be reduced.

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 primarily provide functions such as digital identities, digital asset registration and transfer, simple built-in scripts and datafeeds and credit ratings. Metaverse can be used to support all consortium blockchains, forming an open platform ecosystem.

In the second phase, Metaverse will transit to a DPoS-based enhanced consensus algorithm (HBTH-DPoS). Building upon the ecosystem developed during the first phase, we will extend smart contract functions and provide complete Oracle services.

The following section will mainly discuss Metaverse's technology selection and architecture.

5.1 Technology Model Selection

For the first phase, there were three technical solutions to choose from: the Bitcoin, Ethereum and Bitshares systems. Amongst these three, Ethereum's code system updates iterations more quickly and comes with the EVM (Ethereum Virtual Machine). Considering the limited resources and time available to Metaverse during its initial development (low-level reconstruction), Ethereum's system may not be suitable.

The entry point for Metaverse is digital identity and digital assets. Metaverse once considered an extremely idealized Bitshares system. However, due to its "anchoring mechanism" and non-UTXO model, we can only subtract from their code. Due to code reusability principles, the risk and difficulty of subtracting code far outweighs that of adding code. Thus, Metaverse finally selected Bitcoin's technology system.

Within Bitcoin's technology system, Metaverse's main code uses Libbitcoin as the framework to design its own Hierarchical Deterministic (HD) account system. Ethereum's Ethash algorithm was integrated to design a variety of asset transaction types.

Advantages of choosing Libbitcoin:

1. Metaverse is not just an altcoin. The integration of digital assets and digital identity requires code to be highly modular. Studying versions 0.8 and 0.12 of the Bitcoin code, we believe the degree of coupling in Bitcoin Core's code is relatively high, which is not conducive to the development and maintenance of Metaverse.
2. In terms of code structure, some historical problems with Bitcoin Core (e.g. mixing C++ templates and macros) hinder debugging. Unclear class inheritance structures also hinder reconstruction.
3. Bitcoin Core's code does not support Unicode.

After comparing Libbitcoin and Bitcoin Core's code, we found Libbitcoin to be more advantageous, especially in the areas of readability and module coupling.

Disadvantages of choosing Libbitcoin:

1. Missing important modules such as miner, account and json-rpc;
2. It contains more bugs related to block synchronization and establishing network connections;
3. As a result of using the boost-asio library, Libbitcoin designed a large number of handlers to achieve the asynchronous effect, complicating the tracking and debugging of underlying modules;
4. Huge amounts of code (the module design and forced code style required extra coding).

5.2 Basic Architecture

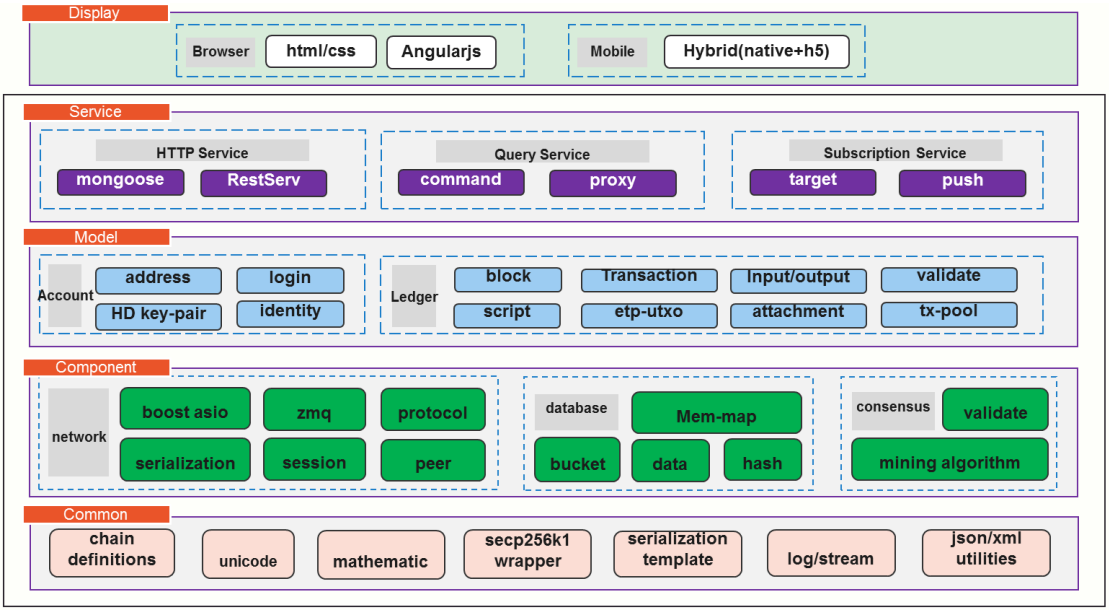


Figure 5: Architecture Diagram of v0.3

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

Common Layer

This layer is a basic storage layer containing a number of definitions for basic classes, configuration inheritances, math libraries, flow processing libraries and other general functions. This common layer is composed of small functions, basic classes and C + + templates and also contains important libraries such as secp265k1 and zmq and implements a large number of primitive types, such as:

bc::wallet::script – transaction scripts
bc::wallet::payment_address – transaction address

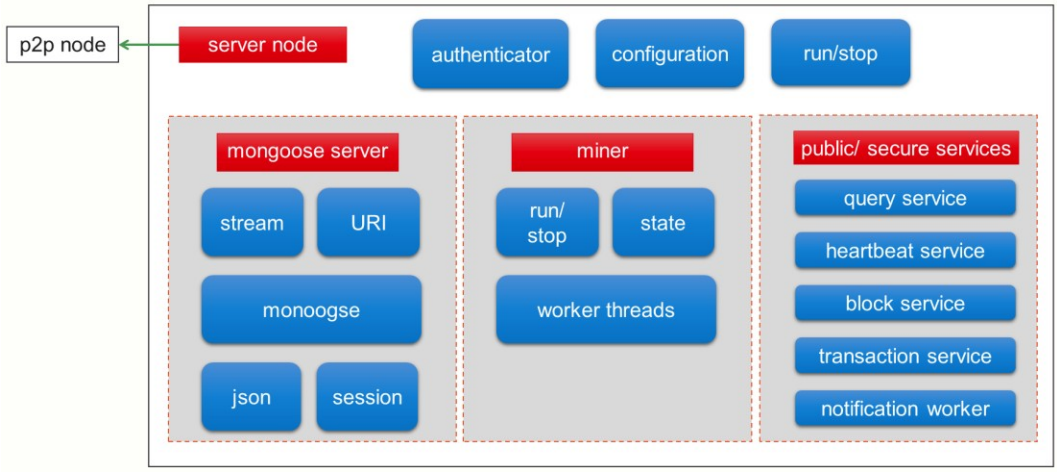
Component Layer

The component layer contains the core components of a blockchain: network communication (network), block persistence (database) and consensus processes (consensus). The entire blockchain is dependent on the network module for survival.

- Network

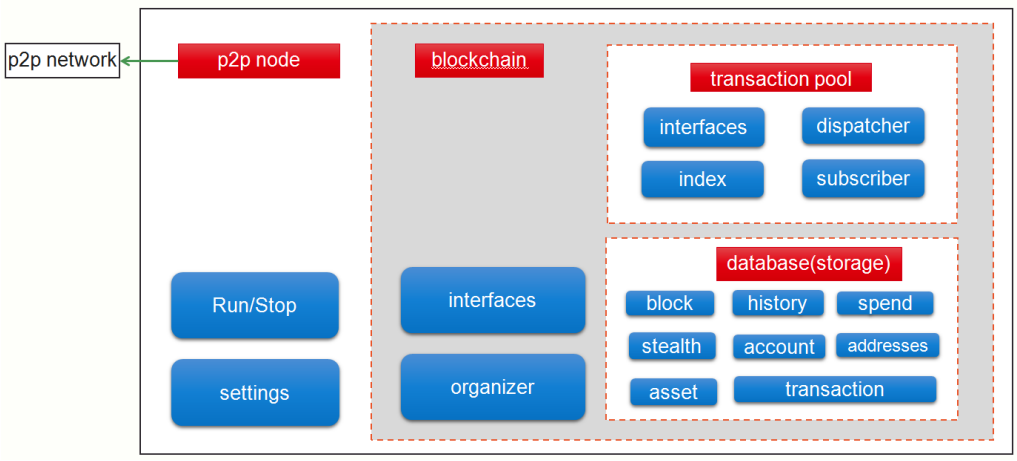
The P2P network, PoW mechanism and verification have been included in this layer. The bottommost layer is used to support P2P network modules for all network messages (it does not support LAN penetration). The consensus module contains functions related to mining, block verification and network difficulty adjustment.

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



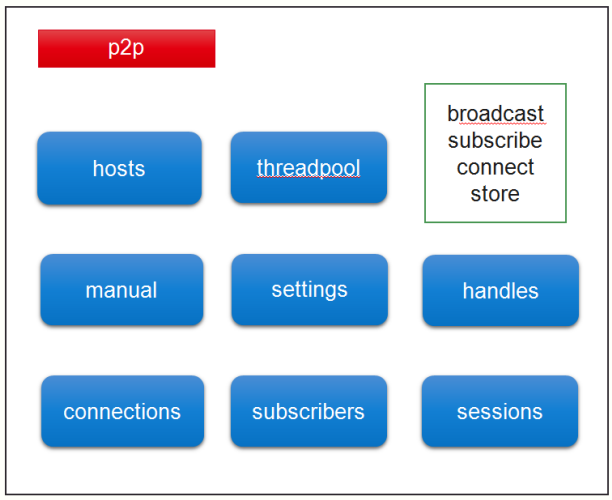
- Mongoose server is a http server;
- Miner refers to the consensus module;
- The public query provides an open, encrypted query interface (binary system);
- server_node is derived from p2p node.

p2p node is described below.



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

Again, p2p network is described below.



In other words, the entire inheritance level also reflects how the network module 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 low-level module.

- **Database**

Storage (database) is not a traditional database, but rather a small local embedded database. At present, SQLite and LevelDB are the available mainstream options.

Early on in the technical 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. The advantages of this method are superior speed and performance and easy access to memory-pool. However, it lacks extensibility, 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 architecture diagram for v0.3, we can see that Model layer contains two core elements: Account and Ledger.

- **Account**

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

- **Ledger**

Based on the UTXO model, we designed an extended transaction that is different from ETP transactions. These extended transactions categorized under: digital identity ledger, digital asset ledger and data-feed off-chain data reference ledger.

The following diagram illustrates Metaverse's implementation of different transaction types.

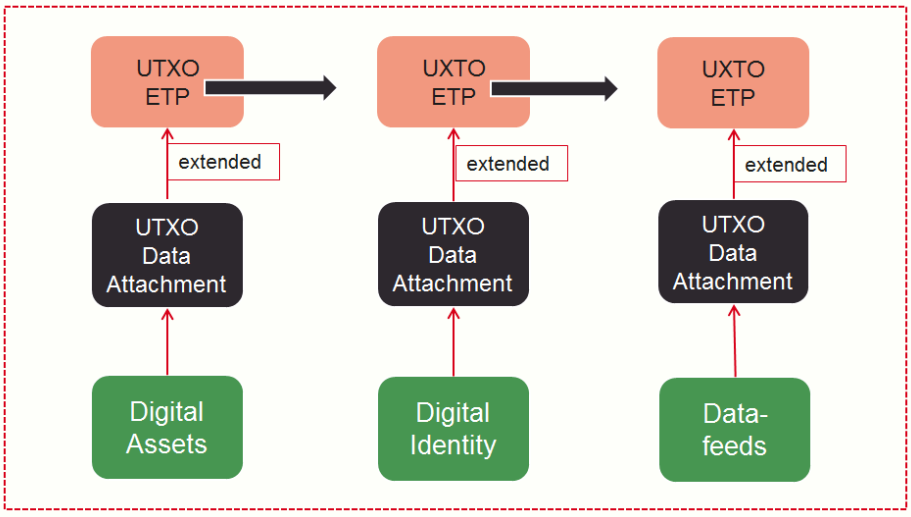


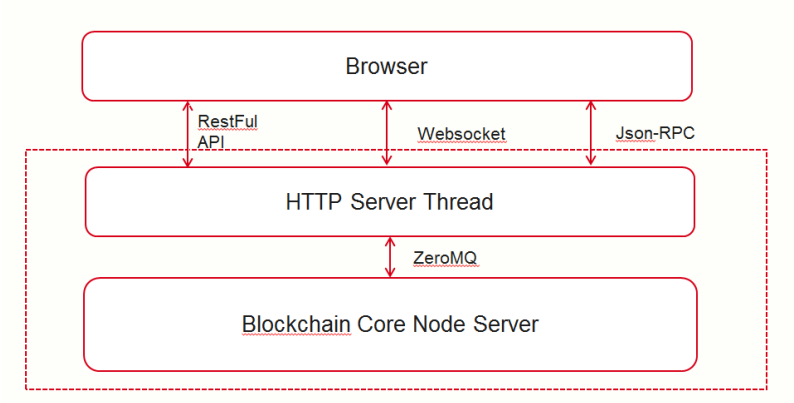
Figure 6: Transaction implementation

Service Layer

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

All services are provided to users with HTTP Server as the interface gateway and are used by calling commands.

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



- **HTTP Server – mongoose**

Mongoose is an HTTP Server with small concurrent volume, based on select / epoll (optional). Considering Metaverse is a user-facing program, the main consideration is for ease of use rather than concurrent volume.

- **Users'** 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 computations, 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, mixed development methods will be used to build a light payment client.

5.3 Envisioning the Metaverse Blockchain as a service

5.3.1 The internet of information and the internet of value

A property of the internet of information is that businesses and technology can be decoupled via multilayered architectures that separate business layers from technical layers.

The properties of the internet of value are: it has an exclusive nature, and comes with a financial system. When separated from this financial system, it becomes a classic distributed system and cannot be called 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 these limits 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, these solutions use multi-instance architecture. For example, Company A and Company B both purchase the same product F. However, the companies will eventually run completely different instances of product F. There is normally no direct relation between these companies, apart from arbitrary connections through third party financial institutions such as banks or securities companies.

In contrast, on the internet of value, A and B should run different subnets on the same instance of application F. There is a direct rather than indirect link between A and B; in other words, some services provided by third party financial institutions such as payment functions will become unnecessary (since blockchains are intrinsically equipped with a payment system).

Metaverse hopes to establish an internet of value through the provision of these basic services.

5.3.2 Blockchain service

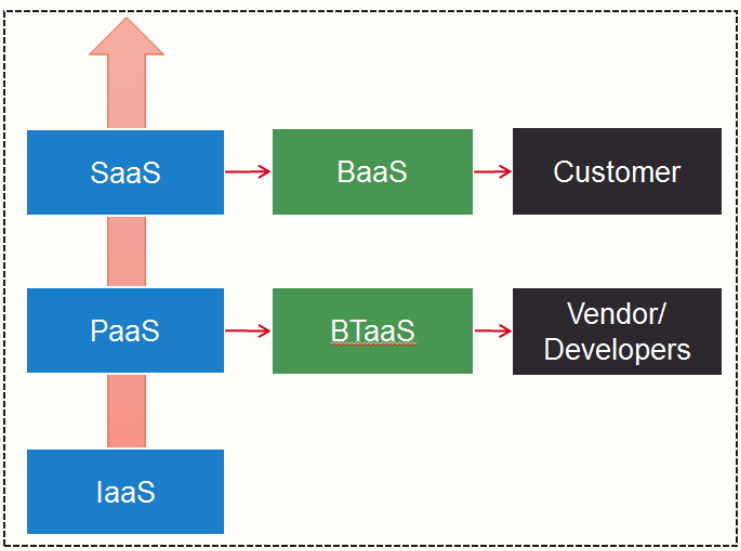
Blockchain as a Service (BaaS) refers to using data generated by blockchains to provide a series of blockchain-based operational services such as searches, queries and data submission.

In the blockchain sector, block explorers, digital currency trading platforms and applications derived from public chains such as document storage (Factom) and digital identity (uPort) all currently fall under the umbrella of blockchain services.

These applications share one feature: they are based on existing public blockchains, and exhibit or strengthen the existing functions of public blockchains rather than use blockchain technology to create a private service.

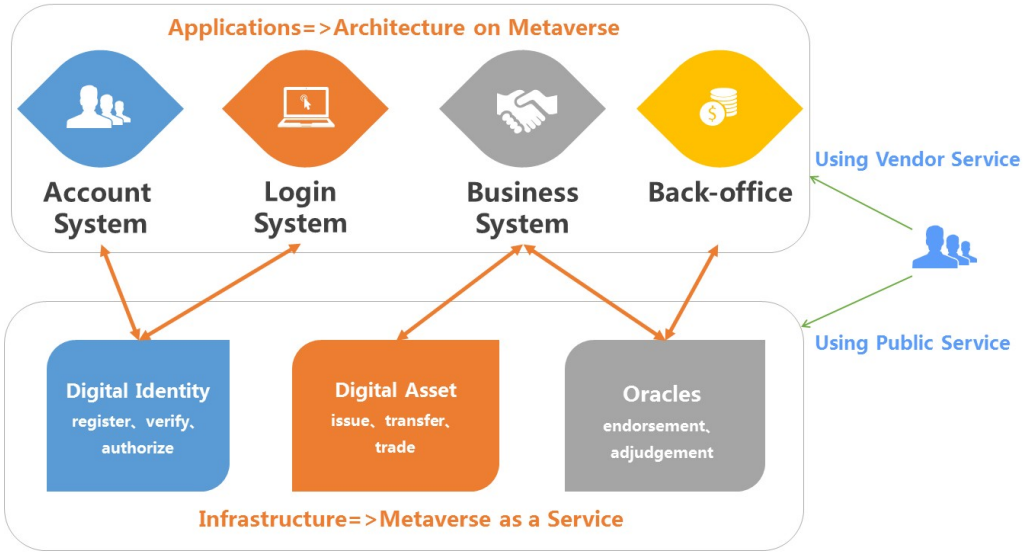
Extending the SaaS / PaaS concept from cloud computing to blockchains, we gain two new service types:

- BaaS – a variant of SaaS – **BaaS (Blockchain As A Service)**
- BTaaS – a variant of PaaS – **BTaaS (Blockchain Technology As A Service)**



BaaS caters to ordinary users, while BTaaS caters to vendors and developers.

5.3.3 Metaverse Blockchain as a service



The Metaverse public blockchain is capable of providing infrastructure services (BaaS) for all IT systems and devices. The system can be compatible with privately-owned IT systems using digital identity as the primary entry point.

The Metaverse public blockchain provides identity verification and authentication in addition to asset query and trading functions. Data on the blockchain is 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 blockchain consensus process refers to the process of objectively recording the entire network's transaction data and making it immutable. This consensus process is implemented 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 termed "economic" algorithms because they allow the cost of cheating the system to be calculated. They ensure that cheating is unprofitable by making the cost of cheating much greater than its reward. Through this, they create an algorithm that makes use of economic games between nodes to tend towards a stable equilibrium.

Correspondingly, we also have distributed consistency algorithms in the field of computing such as Paxos and Raft. These can be called classic distributed consistency algorithms.
The biggest difference between distributed consistency algorithms is their reliability when faced with the Byzantine Generals Problem, otherwise known as Byzantine fault tolerance (PBFT is Byzantine fault tolerant). Both Paxos and Raft are theoretically susceptible to getting stuck in an dead loop with no possibility of passing through via the voting system (although this probability is extremely small). However, both algorithms meet the safety requirement, just that the liveness requirement is relaxed. PBFT is similar in this regard.

The similarities and differences between traditional distributed consistency algorithms and the blockchain consensus process are outlined below.

Similarities

- Append only
- Emphasis on sequencing
- The principle of the minority obeying the 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 consistency algorithms do not take Byzantine fault tolerance into account (except for Byzanetine Paxos). They assume that all nodes only meet non-man-made problems such as crashes or network malfunctions, and do not consider the problem of malicious nodes tampering with data.
- Traditional distributed consistency algorithms cater to logs (databases), are more general situation, whereas the blockchain consensus model caters to transactions. Strictly speaking, traditional distributed consistency algorithms hence belong to underneath the layer containing the blockchain consensus model.

Metaverse is a public blockchain. Several prominent consensus algorithm designs used in public blockchains include Proof of Work (PoW), Proof of Stake (PoS) and Delegated Proof of Stake (DPoS) pioneered by Bitcoin, Peercoin and BitShares respectively, as well as several other Byzantine fault tolerant (BFT) protocols.

Most cryptocurrencies choose to ignore Byzantine fault tolerant algorithms as they fail to resolve token distribution issues. Although Metaverse's ETP is not a currency, it will be distributed to nodes as repayment for their contribution to network safety.

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

As the project matures in the future, the ETP distribution used to provide mining rewards will draw to a close and Metaverse will switch over to an improved DPoS consensus algorithm. This algorithm will consider "Token Height Destroyed" in its design.

First Phase: PoW Mining

In the first few years of the Metaverse system's operations, GPU mining and a decentralised timestamp server system will be employed to secure the system. We are still looking into Metaverse's mining algorithm, but will avoid Bitcoin's SHA256 and Litecoin's scrypt algorithms to avoid 51% attacks from Bitcoin and Litecoin mining pools.

Second Phase: HBTH-DPoS

Although PoW mining can help safeguard Metaverse's system security in its initial years, it has flaws such as energy waste and the tendency for mining centraliztion.

The DPoS mechanism pioneered by Bitshares is 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 a large number of tokens in a short time, attackers can interfere by voting for or opposing important proposals to manipulate the token price for short-term profit. In the current Bitshares system, it is estimated that only USD $3 million of tokens is required to manipulate voting results.

Secondly, voter apathy: voters (users) are often uninterested in the state of a system. Once they have chosen a delegate, most voters are unlikely to make a switch even when the delegate turns out to be malicious. In the past three months, only 1% of voters changed their delegate.

Metaverse improved the DPoS consensus protocol by adding the concepts of Token-Height and HeartBeat. The basic model is as follows:

- Token-Height (TH) originates from the concept of Bitcoin Days Destroyed;
- Bitcoin Days Destroyed = number of Bitcoins in a transaction * number of days since the

Bitcoins were last spent;

- TH = number of ETP in a transaction * number of blocks since the ETP was last spent * Metaverse constant

By using TH to weight votes in DPoS, Metaverse aims to avoid financial interference issues. If attackers were to temporarily acquire large amounts of ETP to influence voting, their TH value would be very small and thus they would hold little influence over the voting process. To achieve their goal, attackers must either acquire more ETP from the market or hold the ETP for a sufficient amount of time to gather TH. Both methods significantly increase the cost of an attack.

In the DPoS phase, Metaverse will distribute ETP to ETP holders based on their prevailing stake, similar to other systems utilizing the PoS consensus protocol. However, the difference is that ETP holders will not receive ETP passively. Rather, they must send a “HeartBeat” to the system to indicate that they are still active. At the same time, this HeartBeat is equivalent to a digital signature from the owner's private key. Lastly, ETP holders must choose to either replace or maintain their delegate when sending the HeartBeat.

There are two advantages to designing the HeartBeat: firstly, it motivates users to check their delegates, alleviating though not fundamentally resolving the voter apathy problem. Secondly, the system will not allocate new ETP to inactive holders, exerting a dilution effect on their holdings.

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

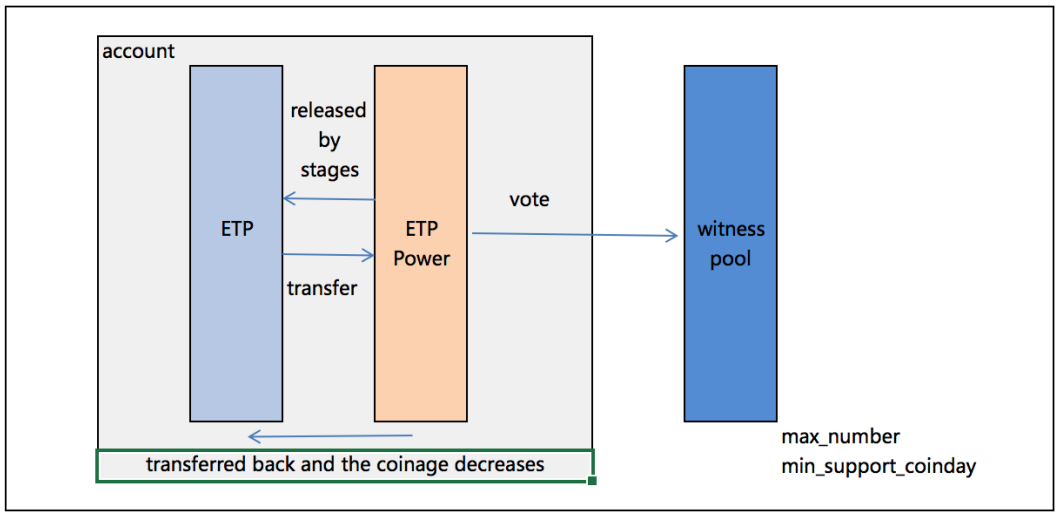


Figure 7: Power-DPoS

The model’s specifications are as follows:

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

2) The concept of coinage is defined as the accumulation of stake over time. This forms

unforgeable “evidence”, similar to PoW. Considers that staking is the price and sacrifice paid by holders, just as the verification of mathematical functions with CPUs or GPUs requires miners to incur the cost of electricity and computing power. The formula for calculating coinage is as follows:

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

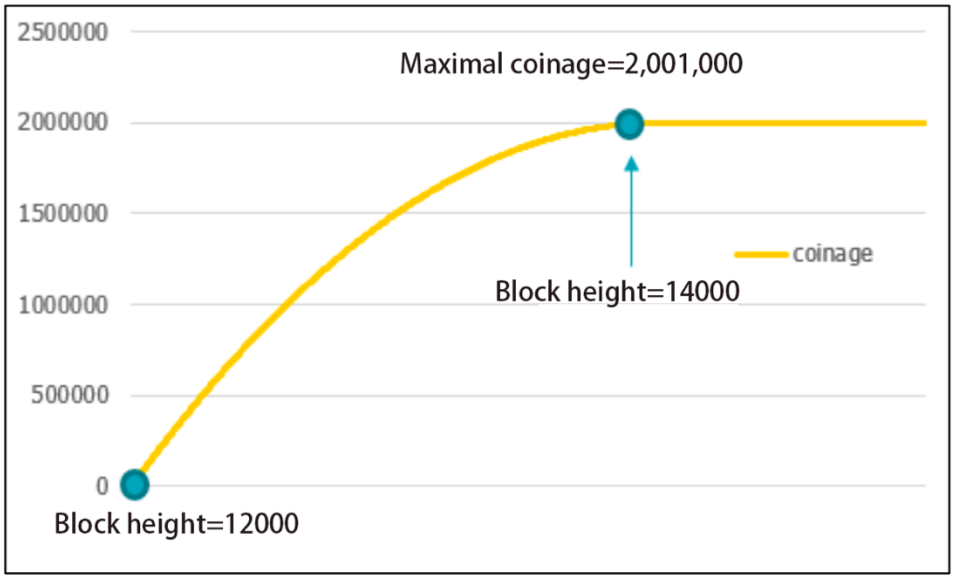
$$f(h) = \begin{cases} \dfrac{H-h}{a} & ,h \le H \ , \ H = h_1 + max; \\ 0, h > H. \end{cases}$$

- Locked(ETP) is the number of ETP locked in a special address prior to voting;
- f(h) is a time density function related to height.;
- h_1 refers to block height at the beginning of the locking period, h_2 refers to block height at which the ETP is unlocked;
- H is the maximum height at which ETP locking can generate coinage. When this limit is exceeded excess height will not generate new coinage ;
- max refers to the number of blocks that can generate coinage;
- a is an arbitrary conversion parameter.

Assume h_1 = 12000, current h = 14500, max h = 2000, the conversion parameter a = 5000 and locked(ETP) = 5000. If the ETP is unlocked at this point, then h_2 = h = 14500. But if H = h_1 + max = 14000 < h_2, then coinage generated by the locked ETP would be:

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

The graph is as follows:



In this case, if the block time is about 15 seconds, then it takes about 8.33 hours to generate 2000 blocks. Attackers only need to lock their ETP for a short time to obtain the maximum voting weight, which poses a large risk. Max can be adjusted to change this time.

3) Coinage and power are linearly correlated. The ratio is defined as ratio(CoinageToPower).
4) ETP generates power according to the following process:

Local client: normal address (ETP for power) → Local client: voting address (ETP for power) → Locking is completed through the transaction between addresses; the ETP is locked once the transaction is completed → when the ETP is unlocked, calculate the coinage → unlock; unlocking is the reverse of the locking transaction, but unlocking does not occur instantly. The conditional function for unlocking is:

The first 100 blocks unlock 0.01% of the locked ETP. This number increases by 10% every 100 blocks, i.e. the next hundred blocks unlock 0.01% * (1 + 10%) of the locked ETP, until all blocks are unlocked. Density and cumulative functions for the amount of ETP unlocked every 100 blocks are shown below:

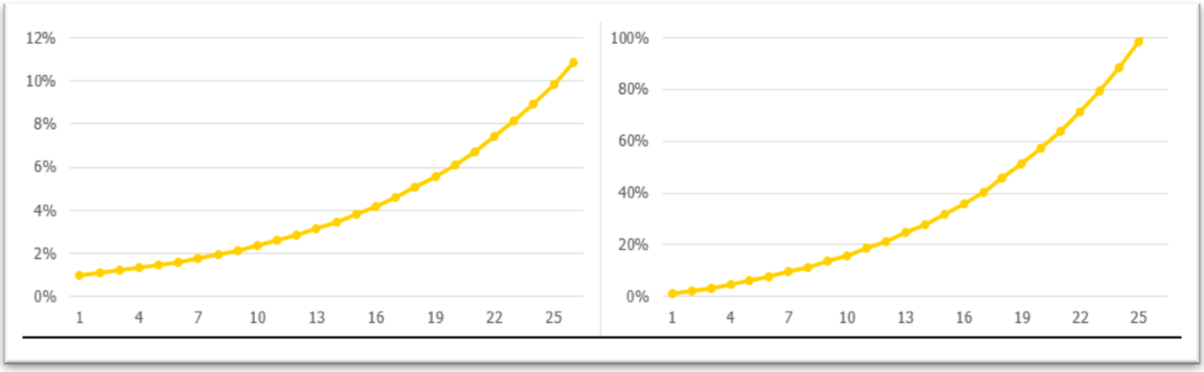


Figure 8: Left – density function, Right – cumulative function

From the graphs, one can see that unlocking speed is relatively slow at first, but will increase. Under this assumption, it takes about 2400 blocks to complete the unlocking process. If block time is 15 seconds, it takes about 10 hours for unlocking to complete. Furthermore, the amount of ETP unlocked in the first 5 hours accounts for only about 20% of the total. If the total time needs to be adjusted, the height interval to increase the amount of ETP unlocked can 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 decrease.

Other unlocking models are also available. The one used here is the simplest, a geometric progression.

6.2 Transaction Type

Besides the coinbase transaction, there is only one other type of transaction in bitcoin, 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) to execute such transactions. Although Ethereum's team invested large amounts of effort to simplify the coding, such as allowing functions to be written with just a few lines of code, the need to write code to use smart contracts will alienate many businesses and users.

There are many transaction types on Metaverse. They were designed with efficiency and ease of use in mind, and will resemble neither Ethereum's one-contract-fits-all model, nor BitShares which defined a large number of transaction types. After ETP trading, smart asset issuance and digital identity registration are the highest-priority transaction types. Ethereum-style smart contract transactions will then be added to the Metaverse system.

6.3 Ledger Model

Metaverse will use a hybrid combining Bitcoin's UTXO model and the balance-based Account model.

- The UTXO model will be used for ETP
- The Account model will be used for user-defined digital assets

For more information about the UTXO model, interested readers can consult the Bitcoin developer documentation.

6.4 Digital Identity and Data-feed

Metaverse will consult and integrate the zk-SNARK (Zero-Knowledge Succint Non-Interactive Argument of Knowledge) scheme proposed by Zcash to protect users' digital identity and privacy.

Data-feed is another important function in Metaverse. Unlike Ethereum, Metaverse's data-feed will largely be handled by Oracles. Their credibility will be based on two factors: 1) valid credentials provided by the Oracle, and 2) their records on Metaverse.

The market will provide feedback on their credibility in several ways. Firstly, data-feed users will "vote" on their credibility through their transaction records. If users vote correctly, they will be rewarded (similar to rebates for leaving reviews). Suggestions for rules to determine voting outcomes and rewards will be disclosed in later versions. Secondly, inappropriate votes will be decided through the voter's motivation and their influence on the outcome. These actions will be penalized – they will be recorded on Metaverse regardless of the voting outcome, and Avatars and Oracles can choose to consider or ignore these records when transacting with digital identities.

The reason for this is because business logic should not be hardcoded into Metaverse. All blockchains are bound by their basic function: consensus. For data-feeds, malicious behavior will only impact their effectivess, rather than consensus in Metaverse. Actions that use data-feeds "for evil" must pay the price to Metaverse's consensus, but these defenses must be implemented in the Oracle or business application layers. Even so, the team designing Metaverse still hopes that there can be a healthy data-feed model. As such, we will give suggestions for rules.

6.5 Cross-platform

Metaverse will be compatible with Windows/Linux/MacOS platforms in its initial stages. As Metaverse develops, we will consider transplanting Metaverse to ARM or other embedded platforms to facilitate asset digitization 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