Metaverse 元界

# The New Reality

***Version: Gravity (v3.0)***

*SuperNova drives low entropy to higher entropy via gravity.*

Hao Chen, Eric Gu, Youming Jiang

May 2018

# Abstract

Metaverse is a blockchain project that provides a foundational infrastructure for social and enterprise needs. Our goal is to construct a universe where digital assets (Metaverse Smart Token, or MST) and digital identities (Avatar) build the basis for asset transactions with the help of a value intermediary (Oracle), thus establishing a new blockchain ecosystem that will transform human society and allow us to enter the New Reality.

Unlike other blockchain projects that use technology as an entry point, Metaverse started from an enterprise value creation perspective, with the relationships between people, people and assets as the core foundations of our project. We describe this relationship through the use of BISC (Built-in Smart Contract), which can reduce the technical risks of commercial applications during development and usage.

Through BISC, Metaverse provides functionalities in digital assets (MST), digital identities (Avatar), Oracles, and MST exchanges. Through the use of MST, users reap the advantages of blockchain technology, such as the power to generate and distribute their own cryptocurrency. The digital identity Avatar reflects the relationship between people, people and assets, and this Avatar can be linked to MST. Through the use of Avatars, anyone can become value intermediary Oracles, and Oracles can help construct an immutable decentralized system (Reputation). MST can resolve fundamental liquidity issues in asset trading, thus solving a critical problem in any financial system.

MST and Avatar are utilized under blockchain technology that is fundamentally integrated with IT systems. This process can be described as BaaS (Blockchain as a Service). BaaS is a quick and convenient way to build blockchain applications.

## 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 wider blockchain concept, while Bitshares and Ethereum furthered our understanding of the blockchain.

- Bitcoin

Blockchain technology is derived from the Bitcoin system. The Bitcoin system is a very modern innovation created by a mysterious figure named Satoshi Nakamoto, who defined Bitcoin as a "Peer to Peer Electronic Cash System." The Bitcoin system seamlessly integrates workflow verification mechanisms, token incentives, cryptography, peer to peer networking, and UTXO technologies. This system has been operating safely for close to a decade.

Bitcoin also introduced a new type of currency - cryptocurrency, and in recent years cryptocurrency has become the most prevalent type of application in the blockchain industry. At the same time, the emergence of cryptocurrency has driven people to explore more forms of blockchain applications, such as Coloredcoin and Namecoin. Then came technical advancements such as smart contracts, with blockchain technology developing through these innovative projects.

- Namecoin

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.

- Peercoin

Peercoin introduced the Proof of Stake (PoS) consensus mechanism. If all blockchains needed to implement a Proof-of-Work (PoW) consensus mechanism, which requires intense resource consumption due to the deployment of costly mining equipment, blockchain technology would lag years behind its current state of development. After the PoS consensus mechanism was proposed, the innovation of different consensus algorithms has become a constant topic of discussion in the industry.

- Bitshares

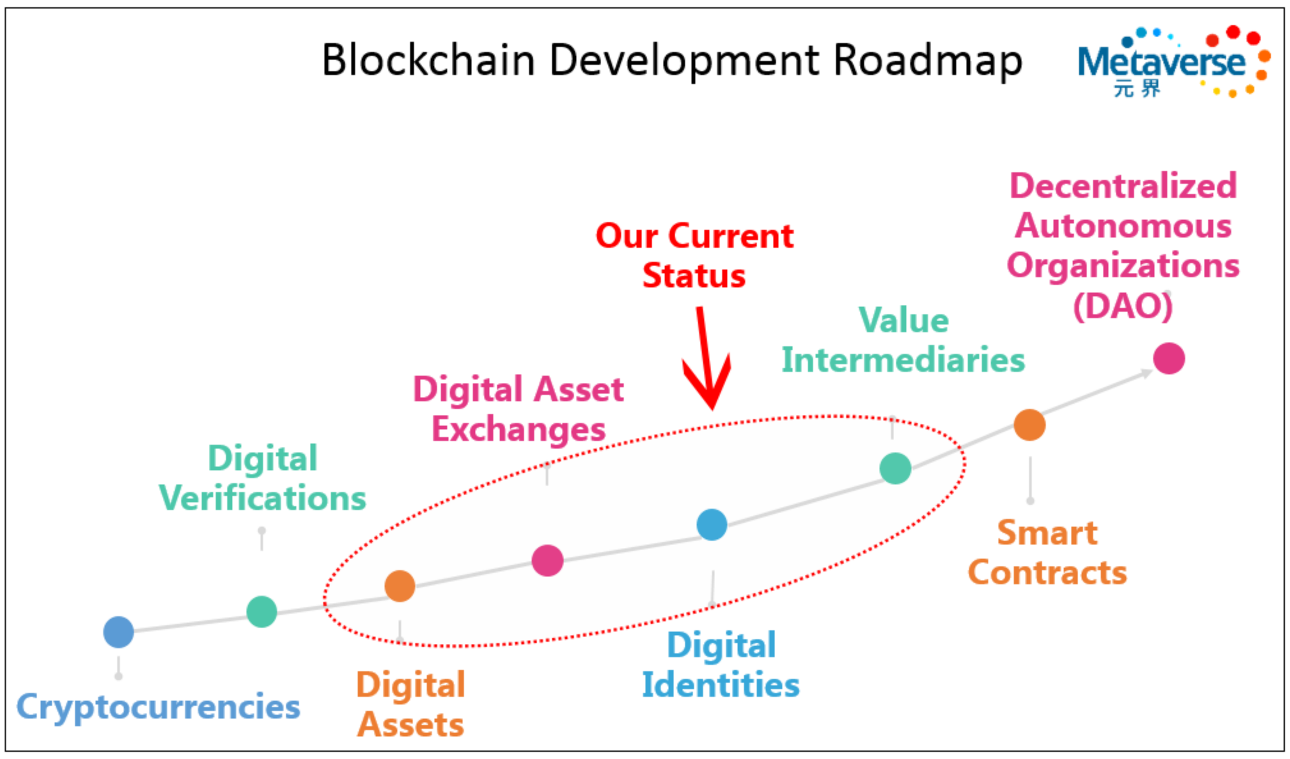
Bitshares expanded on PoS by implementing the DPoS (Delegated Proof of Stake) mechanism, which achieves block confirmation in mere seconds. DPoS is not just a technical consensus algorithm since it also provides a community governance mechanism. Bitshares is also a decentralized exchange platform, where new concepts are put forward continually, such as a digital identity project called Keyhotee. By defining multiple transaction types, Bitshares allows for easy asset and identity registration, which further promotes the distribution of digital assets and other features.

- Ethereum

Ethereum's most important contribution to the blockchain field is the smart contract, an all inclusive tool that describes business logic. The smart contract and its features such as the virtual machine (EVM) greatly reduces the barriers for people to develop blockchain applications. Aside from smart contracts, Ethereum also has a more efficient P2P network protocol, such as the KAD algorithm, the Uncle Block - which reduces the risk of mine pool centralization, the Casper consensus mechanism, and the ERC20 token standard. All of these features vastly promoted the development of the blockchain industry.

## Blockchain Development Roadmap

The development of blockchain is traceable. For example, in the 1990's designing artificial intelligence might have seemed unattainable and far from reachable. However, with the popularity of Internet applications and the development of algorithms and chips in recent years, artificial intelligence has entered into the view of the world. The development of blockchain technology can be traced in the same way. If we want to step into DAO (Decentralized Autonomous Organization), there are a lot of conditions that must be met. We sum up these conditions in the following figure:



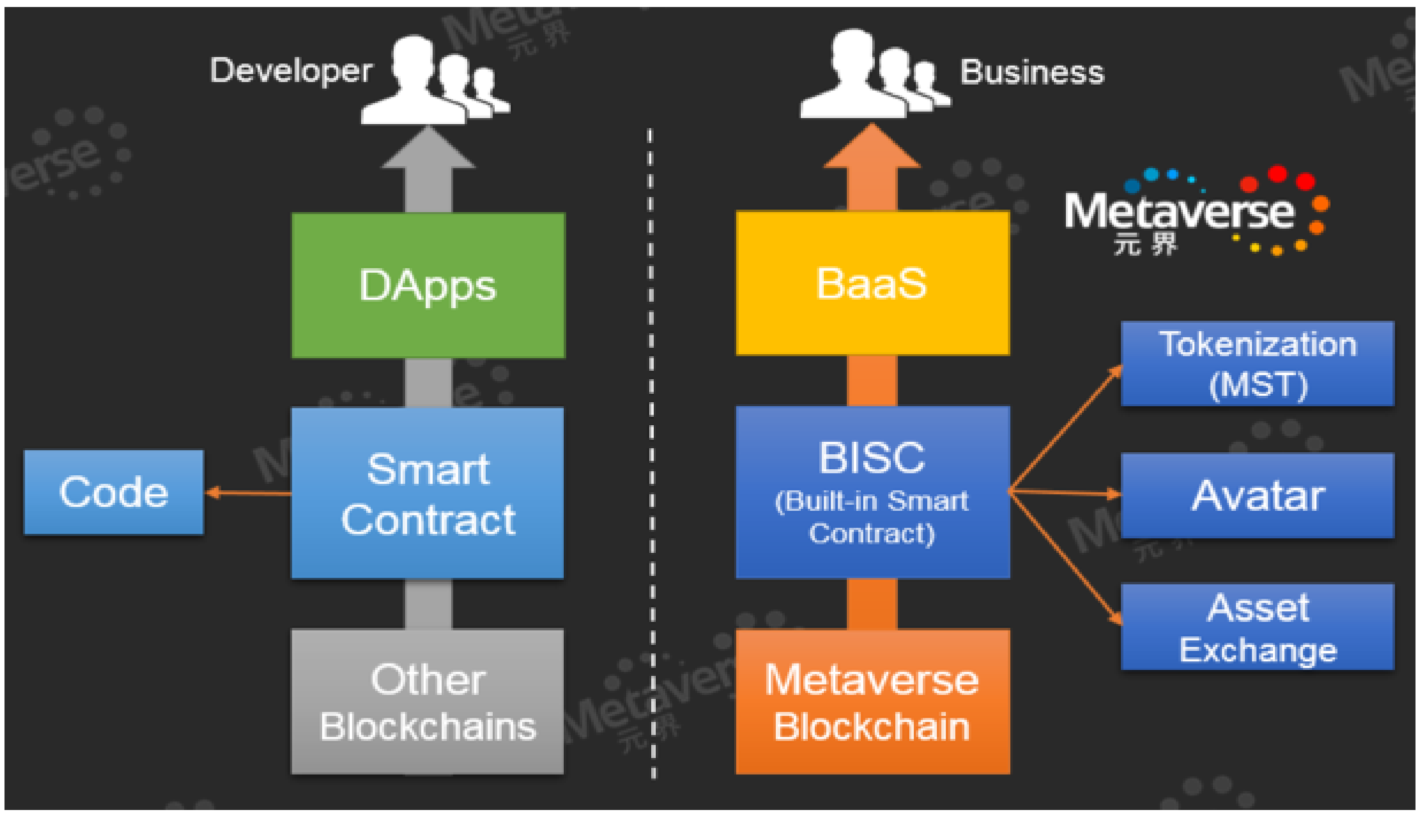
Bitcoin operates in the "Cryptocurrencies" and "Digital Verifications" stages, Bitshares in the "Decentralized Asset Exchanges" sector, and Ethereum in the "Smart Contracts" stage. For Metaverse, the bridge between blockchain and real world applications lies in the circled region. Metaverse is aiming to build an ecosystem that concentrates around these elements.

# Metaverse: The New Reality

The term Metaverse first appeared in Neal Stephenson's 1992 science fiction novel "Snow Crash". In the world depicted in the novel, humans control their own Avatars, and these Avatars in turn communicate with each other and with electronic agents in a virtual reality world. The name "Metaverse" was inspired by the world created in Neal Stephenson's novel.

The world we live in today is similar to the one described in "Snow Crash". Our work and life increasingly rely on the internet, as people spend more time online rather than offline. The way people communicate with each other has also changed, with most communication taking place through the internet. In the near future, we foresee a transition from the internet of information to the internet of value. More and more digital asset transfers will take place on the blockchain through Avatars (Digital Identities) and Oracles (Value Intermediaries). This paradigm of digital value will shape a new economic model.

Metaverse differs from other blockchain projects that use technology as their entry points since Metaverse focuses on creating value for enterprises. We summarize the relationship between people and people as well as the relationship between people and assets. From this information, we can create a model from the ground up that is convenient to use. We call this BISC (Built-in Smart Contract), and BISC can reduce the technical risks of enterprise applications during development and usage. The picture below shows this relationship: on the left are other smart contract blockchain projects, and on the right is Metaverse's system.



Through BISC, Metaverse provides digital assets MST, digital identities Avatars, Oracles, and asset exchange functions. MST allows users to enjoy the benefits of peer to peer asset operations enabled through blockchain technology, and  MST gives people the ability to distribute their own "Bitcoin". Avatars embody the relationship between people and assets and can be linked to MST. Through Avatars, any person can become an Oracle, and an Oracle can help people build an immutable decentralized system of reputation. Asset exchanges can solve fundamental liquidity needs for MST.

Metaverse's core developers and its community will build BISC together. Users do not need to pay specific attention to the technical details to conveniently enjoy BISC. BISC is not limited to decentralized applications creation, as it can be integrated into traditional IT solutions, described in the above picture as BaaS (Blockchain as a Service). BISC, through BaaS, creates value for enterprise applications on the blockchain.

The new world described above can be difficult to imagine and will fundamentally change the way we live, work, and learn. We call this change The New Reality.

# ETP (Entropy)

## ETP (Entropy)

Entropy is Metaverse's token and is abbreviated as ETP. This name draws from the second law of thermodynamics, which describes the degree of chaos in a system's microscopic particles.

The total number of ETP's in circulation is 100 million, and the smallest denomination of ETP is 10^-8. ETP can be transferred and traded on Metaverse and will be an important factor to select who will be bookkeepers after Metaverse transitions to the PoS consensus protocol. The security of ETP is guaranteed by the Elliptic Curve Digital Signature Algorithm (ECDSA).

ETP is not a new form of cryptocurrency. It represents the utility of the Metaverse Blockchain. Therefore, ETP's price is not anchored to any fiat currency or cryptocurrency like Bitcoin. The price of ETP depends on the development of Metaverse ecosystem and market demand.

ETP can be used to measure the value of digital assets (MST), or it can be used as a collateral in financial transactions. Additional, fees applied on Metaverse and must be paid in ETP. Those fees are not paid to the Metaverse Foundation because Metaverse is a not-for-profit project. These fees are paid to the developers in charge of maintaining the Blockchain and miners. Examples of transactions with fee include: to create digital assets, register a new Avatar, designate oneself as an oracle, or invite trusted institutions to verify assets and identities on Metaverse.

## ETP Distribution Mechanism

ETP is distributed through the following ways:

**(1) ICO and Community**

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

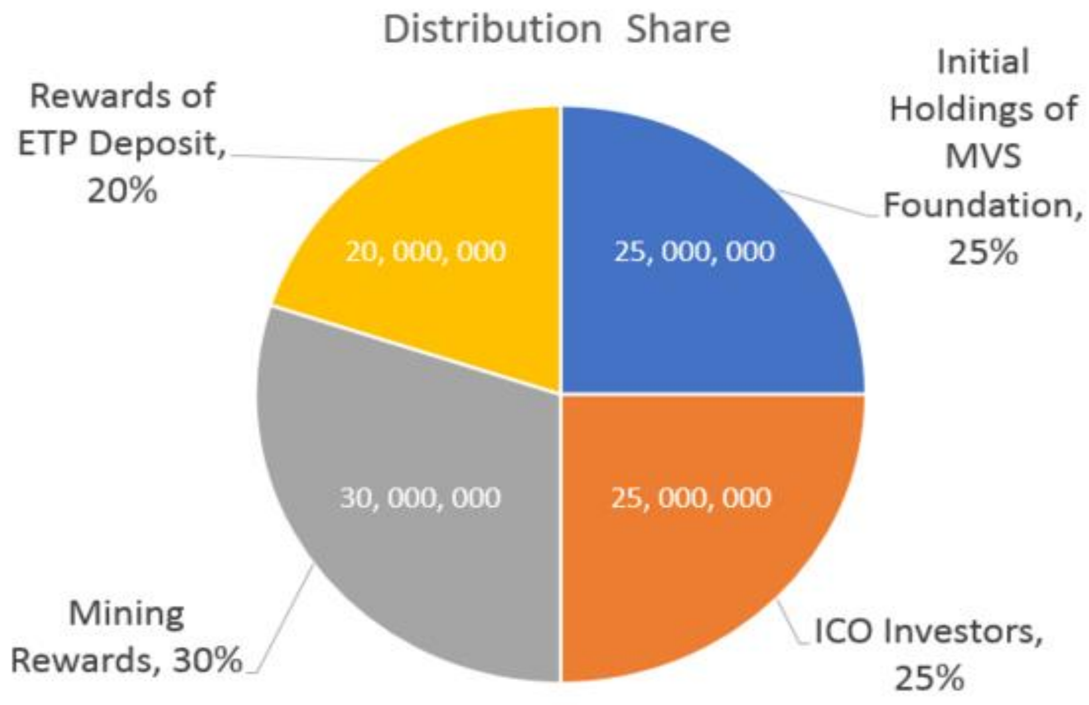
**(2) PoW Mining Rewards**

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

**(3) Deposit Interest Rewards**

Users can initiate ETP deposit rewards by locking their ETP for a period of time. The system will display the principal and interest reward, and these are given to the users in normal transactions. The total amount of ETP reserved for deposit rewards is 20 million

ETP Distribution Diagram:

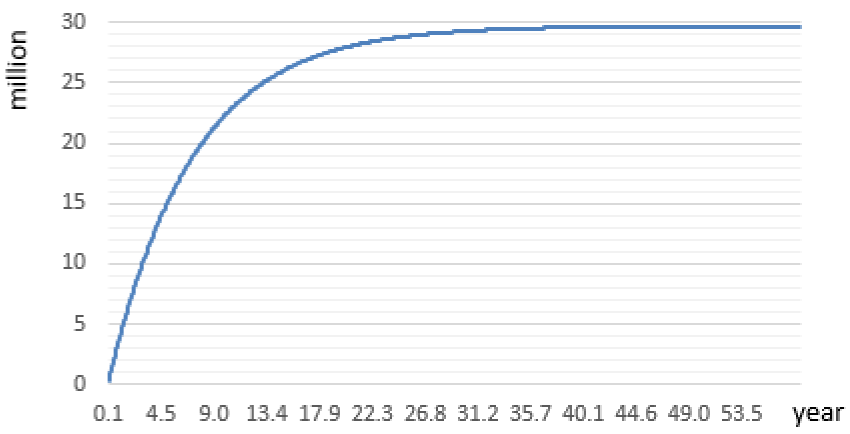


### PoW Distribution Mechanism

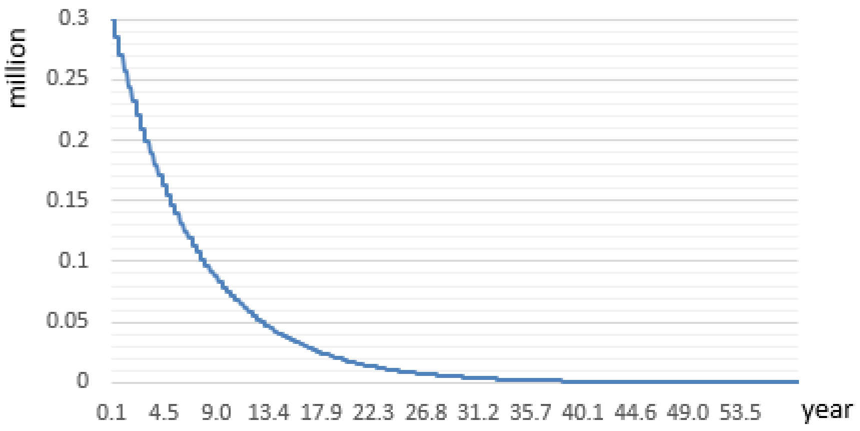
In theory, mining a block on the Metaverse blockchain should take an average of 24 seconds. The initial reward for mining each block is 3 ETP, and block rewards decrease by 5% for every 100,000 blocks mined. The relationship is shown in the equation below:

$$Total\,PoW = \lim_{n\to+\infty}\sum_{0}^{n} 0.95^{n} * 500000 * 3 = 3000000$$

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 rewards per 500,000 blocks against time in years)*

### ETP Deposit and Deposit Reward Distribution

Under ETP's economic model, we have added in a built-in ETP lock function on the blockchain that rewards depositors. This concept is a new design that will help Metaverse migrate to the DPoS consensus mechanism and will help the development of financial applications based on the deposit lock function.

To obtain ETP rewards, users must take the initiative to use the deposit lock function. This interest reward will be sent with the principal amount to the user's digital wallet once the transaction is confirmed.

The deposit lock reward details are specified below:

| Number of Blocks X | 25200 | 108000 | 331200 | 655200 | 1314000 |
|---|---|---|---|---|---|
| Reward Interest Rate | 0.10% | 0.66% | 3.23% | 7.98% | 20.00% |

**Number of Blocks X:** Assume that the current block height is "H", and after initiating the coin deposit transaction, the rewards will be given out but frozen. Users must wait until the X amount of blocks is reached to get their ETP principal and reward. The minimum number of blocks that must be frozen is 25,200.
**Reward Interest Rate:** If a user locks up 100 ETP and chooses the 20% reward interest rate, then the user will receive 100(1+20%) = 120 ETP, but will have to lock up the tokens for 1,314,000 blocks.

Since locking up ETP generates interest, this will allow the total circulation of ETP to surpass 100 million. The MIP-2 calculated time to surpass this mark is roughly 14 years, and the Metaverse community has recently come up with proposals to cap the total circulation at 100 million ETP.

The ETP locking mechanism is by nature a bold design, since an internal, original interest rate exists that does not depend on the central banks' rates. The first implemented version, however, was unsatisfactory because this version did not design the model dynamically like in real life adjustable interest rate situations. Also this first version was not essentially decentralized, and game theory was applied to generate the market interest rate.

Further, we are about to promote ETP trading activity in centralized and decentralized marketplaces. "ETP trading pairs" in these markets will provide an important database for ETP interest rates. Through voting or direct information gathering of decentralized market data, community members can influence ETP's economic model and adjust the parameters. ETP's on-chain transfer activity, number of accounts, special transactions (to be built), and other parameters can be included in this economic model.

## Micro-inflation Model

ETP is the token representing the utility of Metaverse. ETP is not a currency, so it should not be subject to inflation. However, token loss may occur for a number of reasons such as accidental loss, forgotten passwords, carelessness, or death. As such, the issue of declining ETP in circulation will steadily worsen. In Ethereum's white paper, Vitalik Buterin predicated an annual loss rate of 1% for crytocurrency tokens.

Taking into consideration the fractional losses of ETP during circulation and the possibility that a large amount of ETP may be pledged or hoarded by exchanges, we have designed the ETP economic model to require the introduction of micro-inflation to fill the demand for ETP circulation.

Between the ICO and the Metaverse Foundation, we have distributed 50 million ETP. Through the mining process we will distribute another 30 million ETP, and we will continue to release small amounts of ETP in an orderly fashion through locked deposit rewards, with specific reward amounts determined by the total amount of coins deposited and the chosen locking time period. At the same time, the ETP inflation rate will be used as a parameter to reference the adjustment of the ETP deposit reward rate mechanism.

This system of feedback mechanisms enables economic self-adjustment and repair (mainly through the ETP deposit reward tool). The system will be upgraded with subsequent versions of Metaverse to be more robust. Our end goal is to realize intuitive economic models and a more effective economic environment on the Metaverse platform.

# Consensus Mechanism

Metaverse's consensus mechanism can be split into two stages. In the first stage we employ the conservative and safe PoW mechanism to guarantee the growth of our ecosystem.

In the second stage, as the Metaverse ecosystem develops to support higher transaction output and as the ETP distribution for mining nears the limit, we will consider switching to a DPoS or PoS consensus mechanism or a consensus mechanism similar to the combination of ETHASH-Casper.

**First Phase: Proof of Work (ETHASH)**

In the first few years of the Metaverse system's operations, GPU mining will be employed to secure the system. We will avoid Bitcoin's SHA256 and Litecoin's scrypt algorithms to avoid 51% attacks from Bitcoin and Litecoin mining pools.

Considering ASIC's centralized mining pool, we chose the ETHASH algorithm as the mining algorithm for Metaverse. The PoW mechanism will be maintained for some time. When a new consensus protocol appears that is stable and safe, we will switch over to this new consensus protocol. We have also designed an improved version of the DPoS algorithm as an alternative to the second stage.

**Second Phase: HBTH-DPoS**

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

The DPoS algorithm implemented from Graphene can contribute to a high performing blockchain system. However, there are two flaws in the design of the DPoS consensus mechanism:

1. Financial interference: by acquiring a large number of tokens in a short amount of time, attackers can interfere by voting for or against 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 are required to manipulate voting results.
2. 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. We estimate that 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. As explained by the following model, Token-Height (TH) stems from the concept of token destruction:

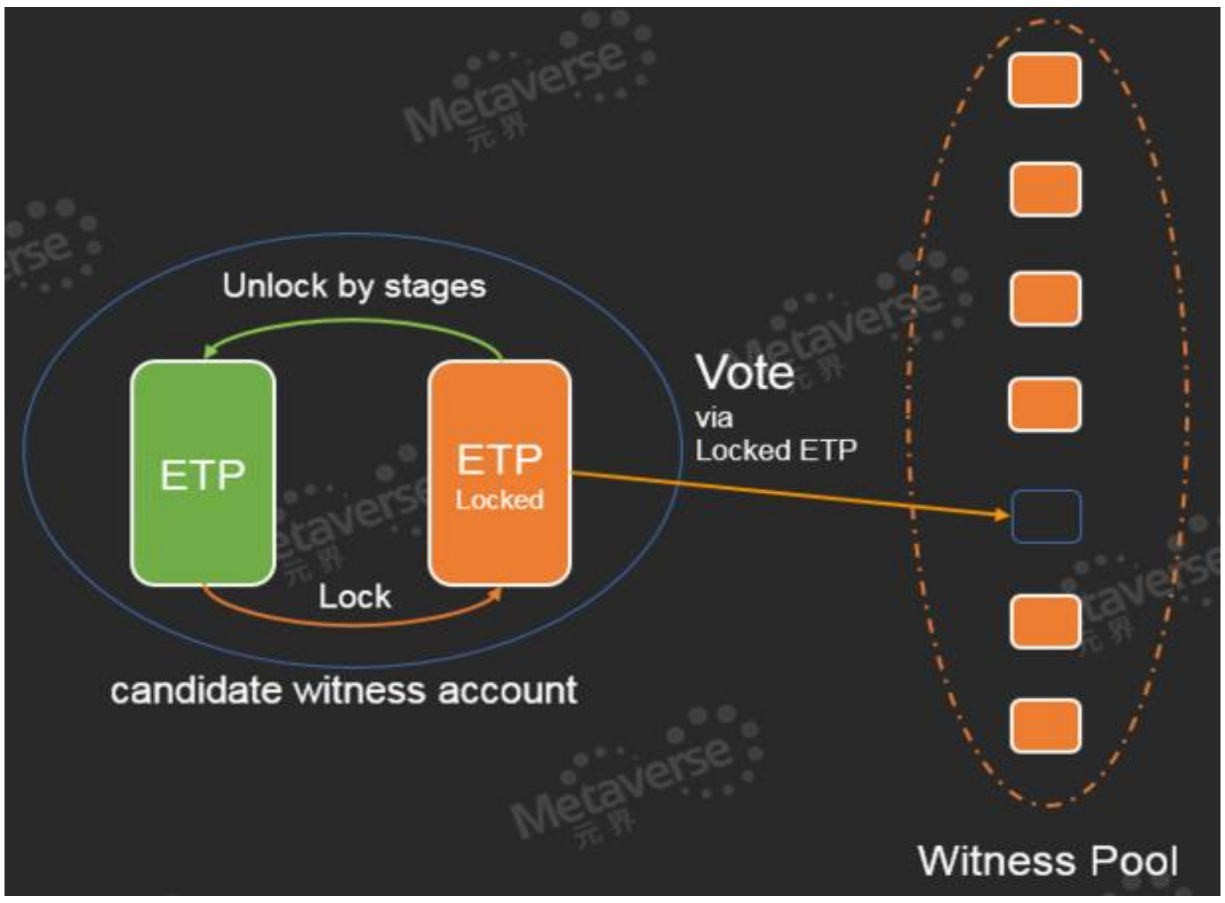
**CoinDays = Number of coins * Number of days since the coins were last spent**
**TH = CoinDays * Metaverse Constant**

By using TH to weigh 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 using the PoS consensus protocol. However, the difference is that ETP holders will not passively receive ETP. Rather, they must send a "HeartBeat" to the system to indicate that they are still active. This HeartBeat is equivalent to a digital signature from the owner's private key. ETP holders must choose to either replace or maintain their delegate when sending the HeartBeat.

There are two advantages to implementing the HeartBeat. Firstly, this system 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 HBTH-DPoS phase, we will consider using a model as below:



The model specifications are below:

1. Separate ETP's voting and transaction attributes, and define built-in voting tokens as locked ETP. Define coinage as the basis for calculation of 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 rights and interests over time. This forms unforgeable "evidence," similar to PoW. Consider that holding these rights and interests represents the cost and sacrifice paid by holders. The computer's CPU or GPU performs the verification of the mathematical function similarly to how the miner pays for the electricity cost and the computing cost. The formula for calculating coinage is below:

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

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

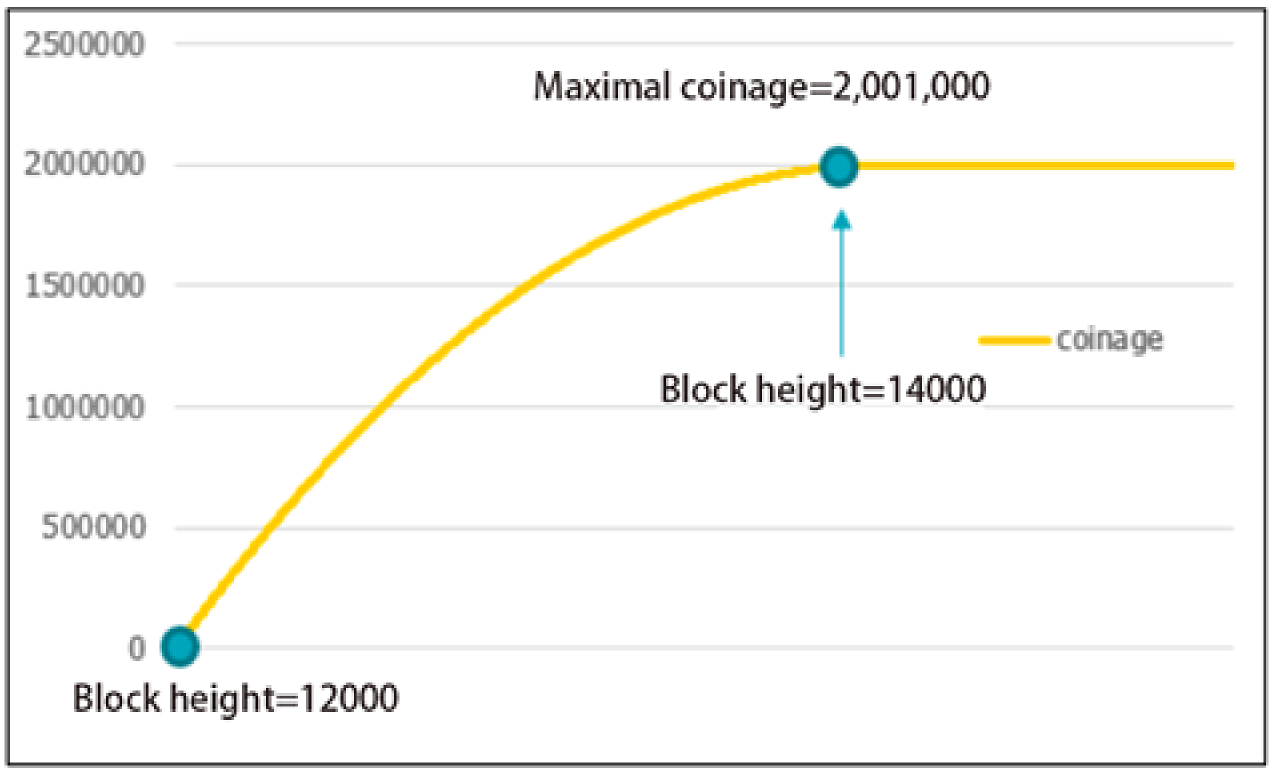
(coinage is equal to coindays.)

- *Locked(ETP)* is the number of ETP locked in a special address prior to voting;
- *f(h)* is the time density function dependent on height;
- *h1* is the block height at the beginning of the locking period, *h2* is the block height after 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* is the number of blocks that can produce coinage;
- *a* is a conversion parameter and has no special significance;

Assume *h1* = 12000, current height *h* = 14500, *max* = 2000, conversion parameter *a* = 5000, *locked(ETP)* = 5000, if the ETP is unlocked at this point, then *h2* = *h* = 14500. But if *H* = *h1* + *max* = 14000 < *h2*, then the coinage generated by the locked ETP is:

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

Schematic diagram below:



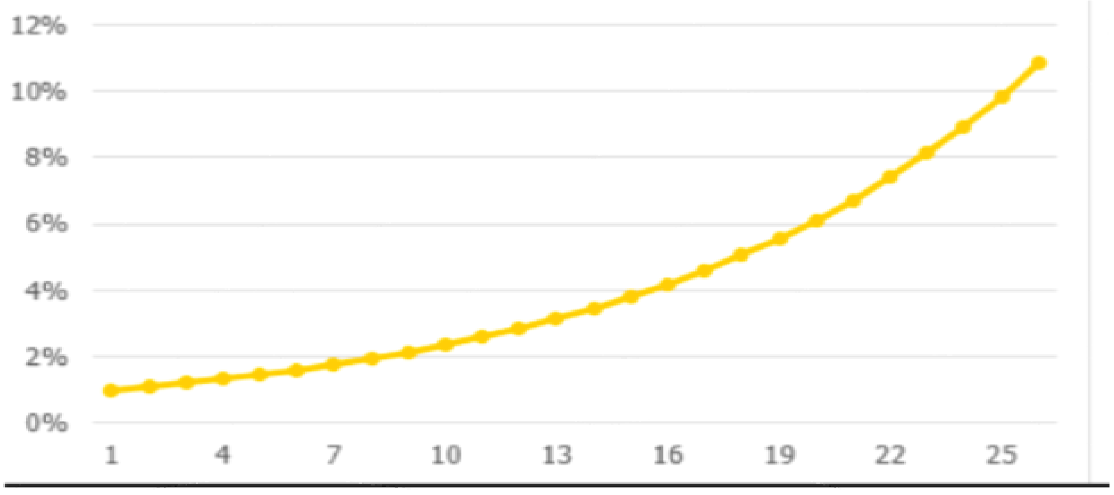
In this case, if the block time is about 15 seconds, then it takes about 8.33 hours to generate 2000 blocks. Attackers only need to lock their ETP for a short time to obtain the maximum voting weight, which poses a large risk. *Max* can be adjusted to change this time.

3. The mathematical relationship between coinage and locked ETP is a linear function, defined as a ratio(coinage to locked ETP).

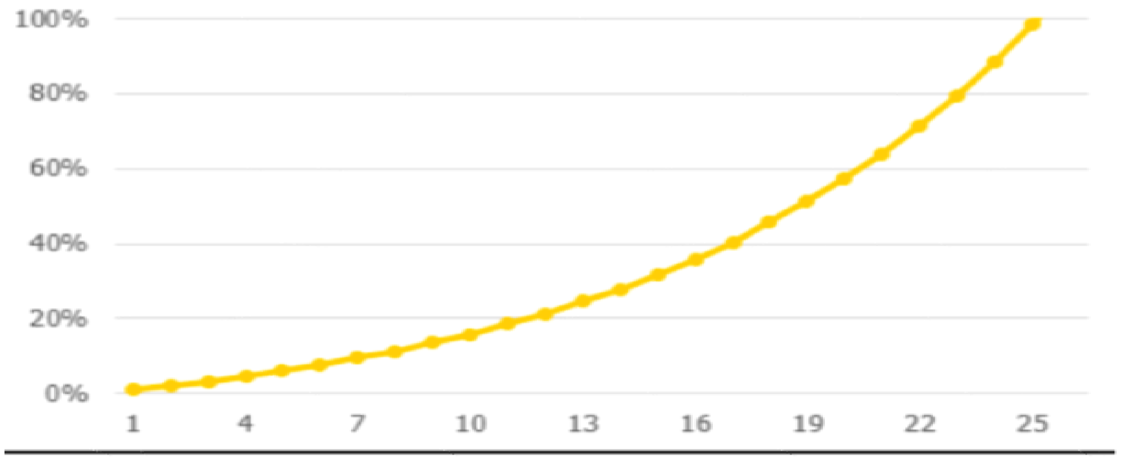
4. ETP generates locked ETP as follows:

Local client: normal address (ETP for lock) -> local client: voting address (ETP for lock) -> locking is completed through the transaction between these addresses, ETP is locked once the transaction is completed -> when the ETP is unlocked, calculate unlock (height(unlock-lock)), calculate coinage -> unlock, unlocking is the reverse of the locking transaction, but unlocking does not happen instantaneously. The conditional functions for unlocking are:

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 unlocked ETP's are shown below:



*(ETP Unlocked for Every 100 blocks density function)*



*(ETP Unlocked for Every 100 blocks cumulative function)*

Unlocking speed is relatively slow at first, but will increase over time. Under this theory, 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 can be modified to increase the amount of unlocked ETP's. For example, if the height interval is increased to 200 blocks, the required time to unlock doubles. To change the unlocking speed while preserving the shape of the curve, the rate of unlocking blocks (increase ratio) should be adjusted. For example, if the ratio is adjusted from 10% to 5%, the unlocking speed will decrease. Other unlocking models are also available, but the one used here, a geometric progression, is the simplest.

# Digital Asset - MST

Bitcoin's Wiki entry mentioned that Nick Szabo in 1997 researched and put forward a concept called "smart property". In reality, Szabo simply defined a class of assets embedded with smart contracts that execute certain contractual terms.

The Ethereum project overemphasizes the concept of smart contracts such that the existence of digital assets is dependent on smart contracts. This design is counterintuitive. The typical standard is the ERC20 token. Although ERC20 allows users to easily transfer and store tokens, some problems exist with the Ethereum contract accounts. For example, when the target account code is incompatible, or when an exception is triggered during the token transfer process, these situations cause accidental token loss. Ethereum community developers therefore proposed the ERC223 token. Although this standard upgrades the security of the digital assets, this switch corroborates the fact that the use of smart contracts to implement digital assets is a counter-intuitive design.

The emergence of the ERC20 token also standardized the ICO market. Before ERC20 came out, ICO's lacked a formal process, and new online token trading platforms needed a long time to prepare from a technical perspective. With ERC20, the only requirement is to provide the contract account address to an Ethereum supported platform.

Therefore the standardization of the blockchain token is inevitable, and this standardization for both platforms and applications will enhance blockchain potential and bring about considerable economic efficiencies.

Digital assets on Metaverse can be characterized as the **Metaverse Smart Token**, or MST. MST reemphasizes the importance of digital assets, that for smart contracts to work, they need digital assets and not the other way around.

Currently, Metaverse has made technical extensions to Bitcoin's UTXO model. Bitcoin's UTXO features will be added to MST, including security, traceability, and ACID features. MST gives everyone the ability to issue Bitcoin at the same price. MST can be used for peer-to-peer payments and also supports a variety of financial instruments such as asset additions and asset replacements.
Note: The original version of the Metaverse white paper labeled digital assets as Smart-Property.

## Designing MST

### Asset Registration (Issuance)

The first step in designing MST is referred to as the "registration" operation and entails finding a set of data that describes an "asset." Examples of these data sets are equity registration, game property registration, and consumption points registration.

The concept of "registration" is meant to describe an object with formatted data and has two key design characteristics: firstly, this set of data description should be reuseable and be difficult to tamper with. For example, the total amount of released assets must be conditionally modified. Secondly, the design needs to provide convenience, accurate queries, additions, and verification of interfaces.

The generic nature of an "asset" and its varying attributes is relatively simple to understand. Asset registration can be generally described by a form similar to the following table:

| Category | Digital Asset Field | Explanation |
|---|---|---|
| Common Attributes | Identification | A property that uniquely identifies the asset |
| | Total Amount | Fundamental attribute of verifying asset validity at the time of transfer |
| | Minimum Unit | After decimal point can be customized 1~8 decimal places |
| | Special Rights（Asset Certificate） | Places where special rights are stored, such as distribution rights |
| Custom Attributes | Custom Data Fields | Place of storage for the custom attribute |

Important data points come from asset transfers. After MST satisfies the design of the basic information structure, we need to consider how to use this information.

Bitshares tried to issue assets based on market functions, but this method produced numerous limitations including complex overcollateralization, anchoring mechanism, price feed mechanism, etc. This practice has proved very limited because the underlying financial infrastructure was incomplete, and the market was unable to make full use of these applications on a large scale.

A new generation of blockchain systems such as BitShares and Ethereum have explored the design and feasibility of the Proof of Assets (PoA) protocol.

On BitShares, the authenticity of digital assets can be verified by alternative means such as posting one's private key signature on forums or providing an asset certificate tied to one's account credit. These digital assets can be valued in the open market by those who recognize the assets. The issue with this method is that it is inconvenient to provide such verifications on BitShares, and furthermore users lack an incentive to issue their blockchain assets in a low liquidity market.

On Ethereum, smart contracts seem to be able to solve all problems, including defining the ERC20 token. Some tokens can be regarded as digital assets because they store value and are editable. Theoretically, smart contracts can support any business model, which gave rise to projects such as Digix. Digix cleverly sought out third parties (gold exchanges, accounting firms, custodians) to provide a series of asset certifications that formed a market-approved evidence chain. This evidence is recorded on the blockchain, which makes the asset's registration tamper-proof.

### What MST Can Do

Asset registration is only the beginning, as others then need to recognize the asset (PoA) to form its attributes. Otherwise there is just a bunch of meaningless data. Once the market recognizes MST, the digital assets represented by MST will have two attributes: value attributes and operational attributes.

Value attributes are continuously reflected by trading and market price changes. MST will implement operational attributes through technical means (virtual machine-based smart contracts or enterprise-based scripting languages, etc.). Operational attributes can add real world asset flow constraints to digital assets registered on the blockchain.

Metaverse will focus on developing a PoA model for MST, so our design will pay special attention to using the Metaverse digital identity to help users provide proof of assets. We propose:

(1) Value intermediaries, or Oracles, can use their off-chain data feed as evidence of asset value. From this viewpoint, third parties in the Digix project are all examples of Oracles.

(2) Credit scores for digital identities can be transmitted through blockchain transactions. When there is enough proof on the blockchain, the data on the chain can prove itself. We call this phenomenon "bootstrap proof".

Once we have a recognized MST, it means that we have "assets". The transfer of assets on the blockchain means that asset liquidity can be guaranteed through the blockchain, so asset transfer is the most basic function of MST.

MST transfers are "lodged" in ETP transactions, so using ETP to pay for transaction fees is very natural. One can think of a small ETP transfer as part of the MST transfer. Metaverse is not compatible with Bitcoin technology standards, unlike the Bitcoin compatible token Coloredcoin. This allows us to have a greater degree of freedom in expanding the Bitcoin technology stack.

### Payment Fees

We believe it is justifiable to require users to pay registration fees since this is a mechanism for the system to protect itself. If there are no costs (or negligible costs) in registering MST, the system will be vulnerable to DDoS attacks. We stipulate that any type of MST transfer must have ETP as a fee.

So the next question is, what is the appropriate fee to charge? Presently no one can deduce how much a token is worth in Metaverse. In terms of design, this fee may be variable, so the fee model will use a weighted system.

For now, all of the transaction fees generated by the new transaction types on Metaverse will be aggregated to an address managed by Viewfin, the company developing Metaverse, to support the development of the Metaverse community, and the remaining ETP is rewarded to miners. As a reminder, Metaverse Foundation is a non-profit organization and does not perceive any of the fees charged on the platform.

## MST's Basic Features

### Global Uniqueness of MST

The smart contract Token does not have global uniqueness, which might make it inappropriate to use in the financial sector. Usually we require the Token's symbol to be unique rather than the Token's receiving address. If the contract's asset symbol can be repeated, fraudsters can construct tokens with the same symbol, so users will be unable to quickly and accurately differentiate the Token from the legitimate address of a smart contract.

Therefore, Metaverse must construct a globally unique Token system. The Token's symbol has the following two properties:

1. Rarity of the Unique Symbol
2. A first come first serve system, with unique token symbols requiring registration

Taking into account the globally unique symbols, and to facilitate easier differentiation for users, upper and lower case letters will be insensitive.

The above two points will propagate a Token symbol trading market, much like domain name exchanges. Therefore MST must have the following features:

1. Symbol ownership can be transferred
2. The right to use the symbol (name right) may be granted to others

MST splits right to use and right of ownership. This is a feature not currently available in any smart contract Token systems.

### MST Domain Name Space

When designing the Token symbol, we reserved dot(.) as an allowable character.
This trait can describe an affiliation for the asset. For example SONY.GAME or SONY.PICTURE. This decreases the scarcity of sought after symbols. For example, MVS issues BTC symbols, and then VIEWFIN.BTC is issued, which makes the latter more reliable.

Due to the presence of dot(.), the naming rights of the symbol become tradable in the symbol market. For example, if you want to use the VIEWFIN prefix, you can contact VIEWFIN's developer privately to make a purchase.

### MST's Multiple Operating Paradigms

MST supports the issuance of globally unique tokens, and these tokens can perform the same payment function as Bitcoin. On a broader scale, however, operating just as a payment function is insufficient. We describe what we mean below:

1. Total token circulation amount cannot be modified after the intial release, which is unsuitable. There is a need for incremental issuance.
2. In economic activities, sometimes there is a need to freeze assets. However, the existence of a freeze asset function on the blockchain represents a platform tool to help complete transactions, rather than an economic model.
3. Asset freezing is accompanied by unlocking. The unlocking conditions represent the true meaning of a smart contract. Metaverse will enforce the arbitration clause when the unlocking conditions are not met.
4. Swap is the basic requirement of an asset that MST must fulfill.
5. Assets need to be destroyed on specific occasions.
6. Exchange is an advanced requirement between assets that MST must fulfill.

Based on the six points above, Metaverse MST proposes the six functions below.

- **MST Secondary Issue;**
- **MST Lock;**
- **MST Conditional Unlock;**
- **MST Swap;**
- **MST Burn;**
- **MST Exchange;**

These functions, along with **issue** and **transfer**, form the eight core functions of MST, and they will iteratively upgrade through MIP.

### Investment Threshold

MST not only can support targeted asset requirements but can also be connected to the Metaverse digital identity Avatar. This means that an Avatar's Reputation can be reflected on MST. For example, if an Avatar called "ERIC" wants to participate in an ICO called "NEW-NASDAQ", the ICO's project initiators can design a Reputation barrier to participate for this Avatar. If ERIC's Reputation does not meet the threshold, then this transaction cannot be accomplished on the blockchain.

### Mining Token Rewards

PoW produces two types of transactions. The first one is ordinary Coinbase; the second is the reward generated by the token deposit lock. For the first type of transaction, Coinbase, we can upgrade this with MST. From a technical viewpoint, this entails extending UTXO to new types.

The discernible effects of this upgrade are:
A miner can configure a MST mining site, i.e. when the target token is SONY.GAME, as a miner mines ETP, the miner can obtain SONY.GAME as a reward. This bonus can be configured when SONY.GAME is released. Considering the block contents, there should be not a lot of MST mining sites. A suggestion is 1~2, as we need miners to proactively choose to target MST.

### MST Offering Curve

The setting of the mining sweet spots will allow miners to obtain ETP related tokens through the token release process. This will help build the economic ecosystem of MST. We discovered, however, that sometimes people do not need to mine to produce the "candy reward". More commonly we set a token release curve directly rather than see a "candy reward" location mine.

Therefore MST must support the following three token release curves:

- Initial Offering
- Additional Offering
- Transferring Tokens

### MST Compatibility Under Mainnet Protocol Upgrade

The smart contract Token also faces the problem of upgrade incompatibility. For example, when ERC20 was upgraded to ERC223, smart contracts had to be rearranged, which means users must convert one smart contract to another under the new standard (e.g. 1:1 conversion losses when exchanging from ERC20 to ERC223).

Thus, in designing our upgrade model, we consider Bitcoin's soft and hard fork upgrades, and how these did not cause trouble to users such as asking mine pools and users to upgrade their wallet programs.

For Metaverse, using Bitcoin's upgrade model is more user-friendly. This allows business to continue, as opposed to stopping business activities due to a technology upgrade.

Therefore, the MIP (Metaverse Improvement Proposal) can make MST's iterations backward compatible. MIP does not require users to redeploy contracts and to redeem new tokens.

# Digital Identity - Avatar

Unlike assets such as gold, we are unable to take physical possession of digital assets. Instead, the ownership of digital assets is controlled by individuals through digital identities and secured through mathematical proofs that ensure these identities cannot be forged. As a symbol of a user's online identity, an Avatar can be used to represent oneself and hold digital assets on the blockchain.

Creating an Avatar is far more than giving your public key an alias, just as ID cards and mobile numbers are not an alias for your name. Various pieces of valuable information will be attached to 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 using smart contracts), users will not have access to encrypted or unencrypted information. Hence, 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 a user 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.

We call the digital identity on the Metaverse Blockchain the **Metaverse Avatar**.

## Four Primary Issues

The current model of digital identity – focused on service access (eg: OAuth2.0 standard), does not provide true identities.

In fact, the Internet does not have an adequate identity layer. Consequently, companies and public institutions have implemented an ad-hoc system of workaround internal databases – incompatible data silos in which they manage the identities of people and things in their data ecosystem.

Currently, blockchain also does not provide an identity layer. If we want to build a blockchain-based identity, we need to analyze the current issues of the existing identity model.

### Issue 1: Identity Data Ownership Issues

Personal information we give out when joining a club or shopping online has more or less directly been submitted to operators. In other words, our identity has always been recorded by others, not by ourselves. Our identity information and data are used by different service providers, so suffice to say the right to use the data as well as the management and protection of the ownership of this data does not belong to anyone.

From the perspective of property, digital identities are a kind of special personal asset. It is in fact a violation of personal property if a user's digital identity information is read without authorization. For example, if I share a photo of a landscape on social media platforms, the photo is stored in the database of social media service providers. Then, service providers launch travel ads of nearby places to users through various cookie tracking technologies, analyzing and categorizing the photo's information. Thus, the providers take advantage of initial data of the photograph and gain indirectly from it. This is where the boundaries of data ownership and usage rights are blurred.

Here, we can find that today's identity systems, whether based on IT technology or other media, have the problem of blurred identity data ownership and user rights.

### Issue 2： Maintaining the Security of Identity Data (Leak and Loss)

Even if we clearly define the boundaries of data ownership and user rights, we still face a second problem, namely the risk of information leak. As long as users' identity data are hosted at a centralized service provider, they will inevitably face:

1) Moral hazard of the internal staff: Your identity information cannot be protected from prying eyes of internal employees, for the evil side of human nature can never be avoided through the management system, and we can only assume that employees do not have malicious intentions. This situation is even worse in Mainland China. Internal employees can make high profits on the black market by selling users' personal information, including mobile numbers.

2) Data leak caused by hacker attacks: Every computer software system has a bug; as long as defects exist, the system faces the risk of malicious attacks. As social media platforms continue to gain popularity, the possibility of attack is increasingly relevant. The data leak of Facebook accounts and trading accounts of cryptocurrency trading platforms provides a recent example of how this issue persists.

### Issue 3： Duplicate and Incompatible Identity Data

After opening a new website, we repeat the process of registration and verification which generates a large amount of identity data. We fill the age, birthplace, and education status repeatedly. All of these suggest there are no effective identity systems with unified specifications and standards. We need to build an identity system that is independent from service providers.

Digital identity projects such as CardSpace and OpenID tried to build such systems, but the results were not what we expected. Going forward, we expect a digital identity project that could help us manage users' reputations and personal assets, instead of simply managing application data.

### Issue 4： Fraud

We believe an atmosphere of ineffective digital identity standards is the fundamental reason why e-commerce service platforms such as Taobao gained so much popularity in China. Since the Internet lacks effective identity standards, Internet companies cannot uniquely identify bad actors who may receive the commodity but never pay for it. Users may purchase fakes or never receive the goods they bought.

The most common case is the Sybil attack, where the user can launch an attack on the counterparty, resulting in false identities being able to access normal services.

The statistic data below are quoted from the Sovrin whitepaper:

- 30-40% of contact center call volume is related to password and account recovery
- 18% of shoppers abandon their shopping cart due to username and password issues
- 82% of businesses struggle with fake users and on average 10% of a web-facing organization's user base will be fake
- The average retailer cost for each stolen record containing sensitive and confidential information is $165.
- 25 people in the U.S. fall victim to identity theft every minute—leading to $15 billion in losses from 13.1 million consumers in 2015.

## Digital Identity Standards References

Blockchain-based digital identity will face these same problems, and as agreements become auto-enforceable and entries in the database become immutable, these problems may get even worse. Thus, we need to research existing digital identity standards and projects. There are some decentralized identity standards we can refer to:

- FIDO U2F/UAF, FIDO Alliance
- Web Authentication, W3C
- DIDs, W3C
- DKMS, W3C
- Verifiable Claims, W3C
- OAuth1.0 and OAuth2.0, IETF
- OpenID Connect, OpenID Foundation
- UMA and OTTO, Kantara Initiative
- Sovrin, Sovrin Foundation
- Facebook Connect, Facebook

We found that OpenID Connect and Sorvin are close to the Metaverse Avatar, so we focus on analyzing these two identity standards. Four types of identiy classifications are mentioned in the Sovrin white paper. We believe that this classification method is in line with reality. They are:

- Centralized Identity
- Federated Identity
- User-centric Identity
- Self-sovereign Identity

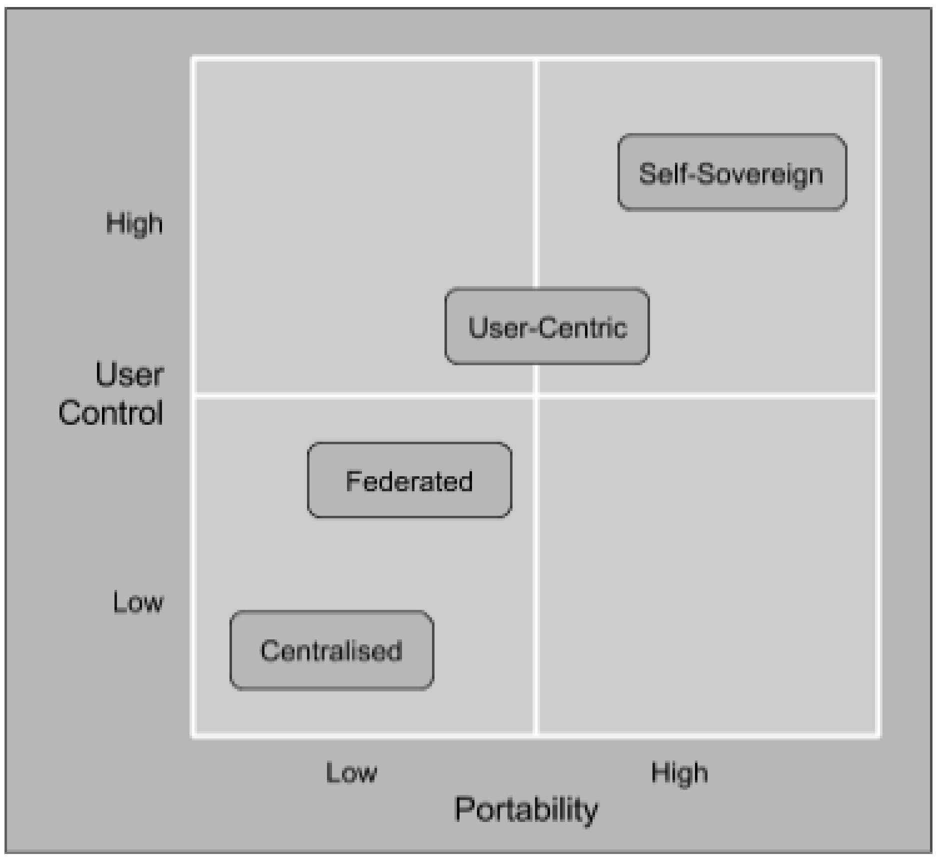


*Fig 2: The four stages of online identity (from Christopher Allen #1) against at the axes of portability and control*

We expect identity standards will not be centralized and federated. User-centric reflects the situation of current Internet identity standards.The representatives of the User-centric model is Facebook Connect which is like the OpenID standard. However, due to commercialization, the User-centric model only recognizes User-centric data, and in reality, users cannot control their identity.

Self-Sovereign Identity can be regarded as the ultimate ideal of digital identity, which is essentially changing from an identity island model to a standard hierarchy model. In order to have a true self-sovereign identity, we need identity data usage and operational rights to return to the user.

As an exploration of blockchain-based decentralized identity, selective compatibility with already existing identity standards is necessary. After all, the complete construction of digital identity standards belonging to the blockchain is a huge undertaking and involves much repetitive design work. In order to better understand this process, we need to clarify the concept of Identity Ledger and Identity Terminal.

## Identity Ledger and Identity Terminal

There are many blockchain related projects, such as UPort, Shocard, Netki, and Ping Identity. People are apt to be confused about concepts such as Identity Ledger and Identity Terminal when discussing digital identities.

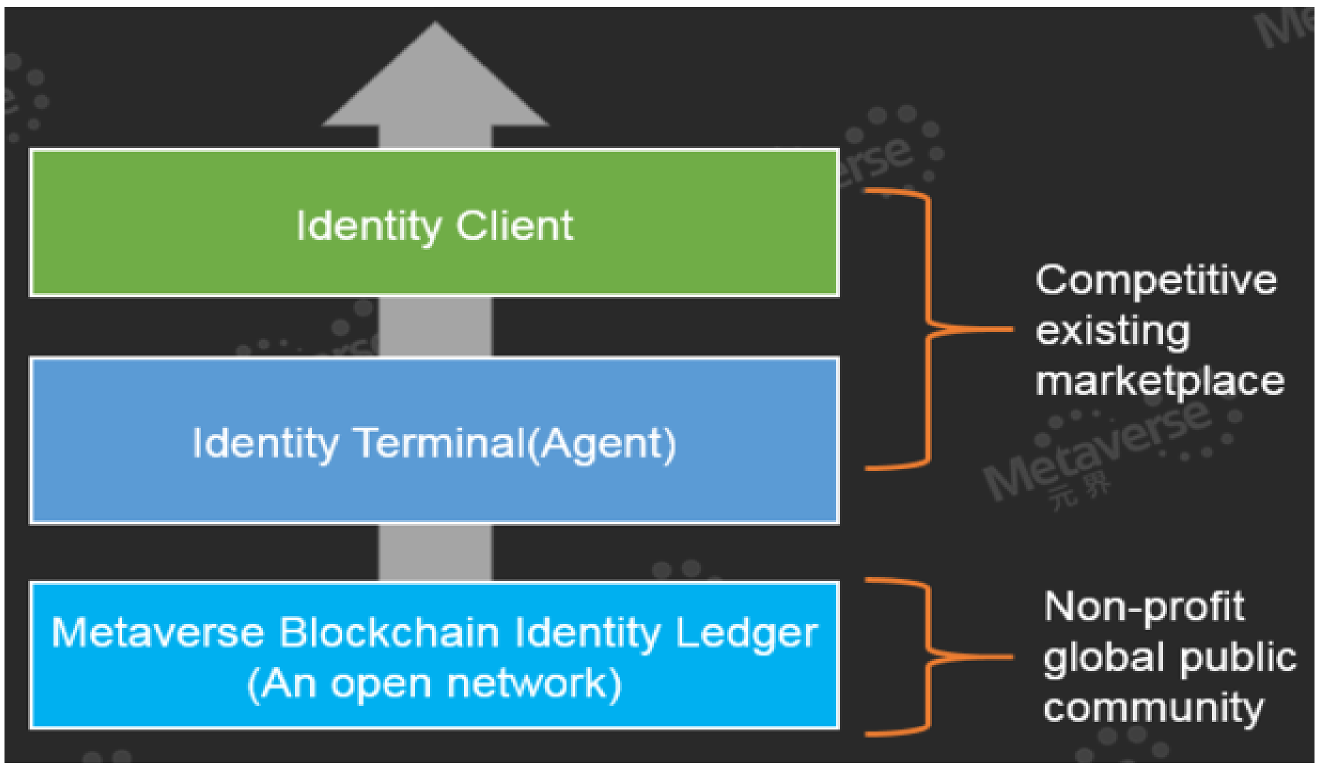
First of all, we need to define Identity: Identity refers to the collective name we give to all of the objective events that occur for any individuals or institutions in the natural sequence of time. The event set has two features that can be verified and authorized.

Then we define Identity Ledger: Identity Ledger consists of pieces of records, which reflect the objective events that occurred in an identity. The Identity Ledger must satisfy two conditions. First, it should record the objective event as faithfully as possible. Second, the recorded event should be the segment we focus on but not all of the event. For example, Bob was born in Shanghai in 1991, and this event was recorded in the internal database of the Shanghai Public Security Bureau. All of the records about Bob in this database constitute Bob's Identity Ledger.

Finally, we define the Identity Terminal, which is the proxy terminal that users access to enter into the Identity Ledger. The terminal supports the functions of identity authentication and identity information access authorization. For example, your passport contains a search index. When you show your passport, the inspector reads the ID and then connects it to the Identity Ledger to find out and verify the validity and legality of your information. Thus, the passport itself is only an index and has the function of containing credentials. However, it does not represent your true identity. Instead, the records in the system form your identity.

The identity terminal is the closest part to users. Terminal technology developed rapidly and has improved from the previous magnetic stripe card to the recent IC chip, and then to the current face recognition and fingerprint verification.

However, we do not intend to innovate the Identity Terminal. Blockchain is essentially a ledger and Metaverse can provide people-centered and blockchain-based digital identity standard protocols. Based on this idea, Metaverse is able to cooperate with various Identity Terminal providers to construct a set of standard Identity Terminal interface specifications suitable for blockchains to enhance the compatibility and practicality of the entire digital identity system. Next, we can take advantage of the biometric terminal to allow the hardware to support the digital identity protocol of Metaverse. For example, fingerprinting, facial recognition, voiceprint recognition, iris recognition, and other technologies can be used to access the Metaverse Identity Ledger.


Identity Client
Identity Terminal(Agent)
Metaverse Blockchain Identity Ledger
(An open network)
Competitive existing marketplace
Non-profit global public community

If we reach a consensus on the concept of Identity Terminals and Identity Ledgers, we will design Metaverse Avatars based on the following principles:

(1) The Principle of Identity Protection
The basic principle is to protect users' identity information from infringement. First, users are obliged to actively claim the ownership of digital identities on the Metaverse blockchain by "creating an Identity", "updating an Identity", and "certification". Therefore the Metaverse blockchain is obligated to provide users with secure and diverse interfaces, and to help users exchange services with authorized access.

(2) The Standardization of the Identity Terminal Interface
The data format of the Identity Ledger can be customized according to users' requirements. However, the format must meet the unified standard and can be extended on the interface, otherwise there will be trouble in accessing the Identity Terminal.

## Identity Profile and Its Claim

It is very difficult to build a blockchain Identity Ledger that standardizes all identity data. However, after comprehensive analysis, we need to ensure that digital identity on the Metaverse blockchain satisfies the following characteristics and establishes an open specification to provide incentives that allow users to get what they need through the Identity Ledger.

### Privacy Boundary

Records generated by any identity have different sensitivities for disclosure. This sensitivity is defined as the privacy boundary.

The privacy boundary is composed of two parts: human instinctive security and cultural constraints. For example, even if there are no moral constraints, most people cannot accept nudity in public places. People lose their sense of security because there is no refuge or escape. Finding a sense of security is the main appeal of privacy. Secondly, cultural constraints vary depending on geographic location. For example, people in European countries are highly sensitive about PII(Personally Identifiable Information). In East Asian countries, people are more tolerant of privacy boundaries due to the prevalence of collectivism. For instance, parents can intervene in the marriage and employment of their adult children.

The diversity of privacy boundaries also determines the neutrality of digital identities. The design must provide enough freedom so that people can control their own privacy boundaries. Thus, digital identities of Metaverse can take the following two methods to guarantee the privacy boundary:

1. Provide anonymous transactions.
2. PII should not be stored on the blockchain, even if this data is encrypted.

### Reputation and Profile

Assuming users now have the Identity Ledger of Metaverse, what is the most important factor for them to operate in this ecosystem? It is Reputation.

The probability that the general public will accept a new or infrequently used digital identity is low. The higher the frequency of use, the more identity records will be involved, which makes the identity more credible. In other words, if an identity has a more comprehensive record, and has been verified many times, the identity's credibility is higher. Thus, for Metaverse, measuring the confidence of the digital identity is significant.

Confidence is reflected in two aspects:
1) Original on-chain records: These refer to users' records originally generated on the Metaverse blockchain, such as transfer records based on digital identities and assets held under digital identities.
2) Records imported off-chain: These refer to the data filed off the blockchain, namely the data-feed that users could import onto the Metaverse blockchain.

Here we can infer the basic structure of the Metaverse digital identity. First we define a profile as the basic unit of the Identity Ledger that describes an identity. The Profile includes the two records above and allows users to calculate their own recognized Reputation based on these records.

A couple of things to note:
1) The profile type is guaranteed by the transaction history of the blockchain. Metaverse provides an accurate and convenient query interface.
2) The profile type has multiple design patterns. ERC725, a self-sovereign identity system, provides an easy-to-use design solution called Claims-based Identity.

From a large sample of business cases, we find that KYC certification systems for trading platforms are also claim-based. When the platform grants the user a claim, it indicates that the user has passed the KYC certification for the platform.

The main function of the data-feed is to fill in information for claims-based Identities. Theoretically, one digital identity could have an unlimited number of claims with the following features:

1. Timeliness: any Claim must have a certain validity period. For example, KYC certification has a validity period and is not permanently valid.
2. Multi-faceted: any person or institution is multi-faceted. For example, an engineer in a company could also be a parent of a child in school.
3. Privacy control: Based on a Profile, any user can extrapolate this Profile's information to define Reputation. For example, we could make the rule that only the qualified profiles could participate in an ICO.

## Digital Identity Designation (DID) Connects Digital Assets

An Avatar may represent a real person, a virtual figure that is supported by artificial intelligence (AI), a machine in the Internet of Things (IOT), or even a company. While one type of digital asset may be owned by multiple Avatars, each Avatar should be able to own multiple types of digital assets. There should be a multi-point relationship between Avatars and digital assets. This relationship seems complicated but reflects the real ownership relationship in real life.

Even if we have a Profile, this Profile is isolated unless it is linked to digital assets. Thus, we need a unique index of the entire network, and this index is also the certificate of the identity, connecting the digital assets and digital identities.

Here we define this kind of index as Digital Identity Designation (DID) whic is globally unique on the Metaverse blockchain as well:
DID can be uniquely indexed to a certain profile and can be bound to any items on the Metaverse blockchain, which brings benefits of anonymity. Users can still use address-based digital assets, or they can choose to use DID to disclose their relationships with digital assets.

With DID, users can issue, transfer, collateralize, and secure digital assets without having to rely on wallet addresses. For example, my DID is “Chenhao”. When Eric pays me ETP or issues his Metaverse Smart Token (MST), he could use “Chenhao” to substitute the wallet address.

DID looks like an isolated "Domain Name System", for DID is not enough to express its own relationship with MST and Avatar. In regard to MST and Avatar, we can refer to OOP (Object Oriented Programming). At least three kinds of relationships will be shown between MST and Avatars and also between Avatars, namely Has-a, Is-a, and Like-a.

In order to realize the above three relationships, DID, Profile, and Claim may need to integrate with existing Internet identities. For example, the Claim of the End User in the OIDC can be mapped to the Claim under the Profile that is under the DID.

## Authentication and Authorization

Profiles and DID's solve data problems and do not describe how users operate digital identities. There are only two core operations about digital identities: authentication and authorization. Thus, we have studied existing standard protocols for authentication and authorization: X.509 standard, OAuth2.0, and OIDC (OpenID Connect).

### x.509

Applications based on the x.509 standard are very broad, such as the Transport Layer Security (TLS)/Secure Sockets Layer (SSL) protocol. The TLS/SSL protocol has been applied to many Internet applications. Therefore, x.509 is a basic infrastructure standard.

x.509 standard is essentially (Certification Authorities) CA-based, which describes the behavior and format of certificates. Nevertheless, x.509 does not meet the concept of Identity Ledger and Identity Terminal. It only provides a certificate model and has the following defects:

- Root CA cannot be revoked;
- The centralization issue of using Certificate Revocation Lists (CRLs) and Online Certificate Status Protocol (OCSP) reduces the security threshold;
- Structure is complex and is not user-friendly;
- Privacy and maintenance issues exist due to over-aggregation of different types of Claims;
- EV (Extended Validation), DV (Domain Validation), and OV (Organization Validation) are susceptible to repeated man-in-the-middle attacks

Therefore, building Avatars directly based on x.509 is not a good choice. Although this standard can immediately support a large number of applications, a lot of extra work remains in order to make this option viable.

### OAuth2.0

OAuth2.0 is an open standard protocol for authorization that enables an application to access certain user information or resources from another web service, without giving the user's credentials for the web service to the web application.

OAuth2.0 has already become the widely used standard protocol for Internet application authorization. Through analysis, we can find that the popularity of OAuth2.0 is based on the authorization agreement of the User-Centric model, which also reveals that OAuth2.0 can only complete parts of functions for digital identities, rather than all functions.

OAuth 2.0 is an excellent tool, but it is still oriented towards centralized services. Since there is no concept of defining digital identities, the centralization issue will not be solved until the establishment of the next standard - OIDC (OpenID Connect).

### OpenID Connect

OpenID Connect 1.0 is a simple identity layer on top of the OAuth 2.0 protocol. OpenID Connect allows Clients to verify the identity of the End-User based on the authentication performed by an Authorization Server. This also allows Clients to obtain basic profile information about the End-User in an interoperable and REST-like manner.

Currently Google Identity Platform and Google+ applications play the biggest roles for the promotion of this project.

Google, as a super portal to the Internet 2.0 era, stores a large amount of personal identity data. Third-party applications are allowed to access and use Google account-related information through the authorization by OIDC.

Although Facebook, Google, Tencent, Alibaba, and Microsoft all use OIDC, the personal data in each platform is independently stored and cannot be mutually authorized and verified. In other words, identity data is compatible within the platforms (Issue 3), but this data is not compatible between platforms. Since personal data is hosted on the platform, Issue 1 has not been resolved.

It can be argued that OIDC has improved the situation of Issue 1, Issue 2, and Issue 3, but these issues have not really been resolved, i.e. the recent data leakage incident of 87 million users on Facebook.

### Metaverse Avatar

MAV (Metaverse Avatar) is an open identity standard protocol based on blockchain and can be compatible with OIDC.  From a technical perspective, Avatar is OIDC's protocol extension on the blockchain. To be clear, MAV is not a mapping of the existing identity system and is unable to fully achieve the ideal of autonomous identity. The reason is as follows:
Due to the limitation of blockchain storage capacity, people cannot store massive amounts of identity information on the blockchain. Increasing blockchain performance only exacerbates block growth. When the size of the blockchain is overused by an application, resulting in a 1GB per day size increase, the blockchain loses its significance as a public resource.

So we need to divide MAV into two levels to solve this problem: the first level is OIDC, and the second level is MAV MetaData.

We recommend using OIDC to solve the problem of mass storage. OIDC can implement IPFS as a storage protocol or use cloud storage. Both solutions can be solved in MBaaS.

MetaData provides blockchain-level records, and this is where MetaData refers to the key information of the identity. In the KYC case of the trading platform, MetaData refers to the verification result of KYC. MetaData can be stored in the profile under the DID. In other words, the MAV profile provides MetaData with an on-chain data container.

MAV needs to consider the following two aspects:

**1. Relationship Management:**  The relationship between MAV's manifested by MetaData as well as the relationship between MAV and MST;
**2. Permission Control of Avatar:** MAV's permission control over MetaData, MAV's permission control over OIDC;

MetaData is a sign to distinguish whether the identity data is on the chain. For self-aware subjects (usually humans, the future may be artificial intelligence), we suggest that PII information resides in OIDC instead of MetaData. For all kinds of physical and virtual assets, such as private cars and pets, we can generate MetaData via Identifiable Information, then register the MetaData on the chain.

Firstly, the verification and authorization of MAV is based on OIDC. Secondly, the authorization process based on zero-knowledge proofs or the authorization process based on homomorphic encryption is also provided on the chain.

## Oracles —— Value Intermediaries

Some blockchain projects claim they do not need trusted intermediaries ("cutting out the middleman"). At the moment, we believe this is a bit out of reach.

The credibility of the off-chain data-feed cannot be guaranteed by the blockchain since the blockchain cannot judge whether the data-feed is reliable. For example, a MST contract could only be unlocked if the rainfall reaches 50 milliliters in Shanghai three days later. During the process, an Oracle will inevitably be involved since blockchain is unable to forecast the weather conditions. The MST contract imports the off-chain data-feed from the Yahoo Weather database. Thus, one Oracle is needed to guarantee the unlock, and another Oracle is needed for arbitration in case of disagreement. Three Oracle intermediaries are needed in this contract regarding a weather forecast in Shanghai: one for imputing data, the second for group arbitration, and the third to act as a guarantor.

Instead of "destroying the middleman", Metaverse will reserve a position for one on the blockchain, which we call Oracle. Host Oracles can store physical assets and then issue smart assets on the blockchain. Authentication Oracles can provide proof of personal information and correlation with Avatars. Supervision Oracles (for example, government departments that regulate special transactions) can provide proofs, such as transaction authenticity or proof of compliance. There are many other Oracles that can provide such services on Metaverse.

An Oracle is a special type of Avatar and is based on an Avatar's authentication and authorization system. These are many built-in functions of the Metaverse blockchain, and anyone can claim to be an Oracle unconditionally. However, how can we prove that the service provided by an Oracle is faithful? It depends on whether the Oracle's Avatar record is rich enough and whether the Reputation is high enough to support the credibility of the services he claimed. This will greatly expand the types of transactions on Metaverse. Each transaction type can be connected to the digital asset MST, so we can expect that the added value of total transaction fees and the transaction volume will increase.

We used to discuss how to reduce transaction fees (usage fees) for Bitcoin or Bitcoin-like payment systems. The expansion of the volume and the speed of block production on the one hand meets the needs of the business, and on the other hand allows the continuous injection of value into the system, which allows miners and billing nodes to have enough incentives to join our system. If we re-examine the problem, charging transaction fees not just for transactions, but for blockchain services such as the purchase of 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 can 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 fees. 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 since all services will be priced in blockchain tokens based on their market value, scarcity, importance, and other characteristics.

## Two Phases

The development of Avatars will go through the following two phases. We call them the introduction proof phase and the self-proving phase.

**Introduction proof phase:** When the on-chain data is insufficient to support the credibility of a digital identity, it is necessary to directly introduce off-chain data to prove the credibility. For example, to prove that your birth date is true, you may use your passport as proof.

**Self-proving phase:** When the on-chain data is enough to support the credibility of the Avatar, there is no need to import the off-chain data. For example, if your date of birth has been verified by other Oracles, the authenticator could use this data directly.

The introduction of proof is the initial stage of digital identity development. The increase of users causes the number of proven Oracle verifications to be sufficient. Then new applications can be directly established in the system without the need to reintroduce proofs. An Oracle plays an essential role during this process.

# Blockchain as a Service（BaaS）

From the perspective of Oracles, the existence of value intermediaries is inevitable, which makes Metaverse different from other blockchain platforms that only provide decentralized applications.

The blockchain itself is decentralized, but that does not mean the applications must also be decentralized. A decentralization of applications is like breaking the civilized structures of mankind that have lasted for thousands of years.

Information providers and information consumers will always exist in information circulatory systems.This phenomenon is determined by the structure of human society, as it is very difficult to eliminate the gap between the two roles. Assuming that information asymmetry is eliminated (in fact, it can only be reduced and cannot be eliminated), cognitive asymmetry still exists between people. Since human energy is limited, individuals cannot absolutely learn all the knowledge that humans have obtained. For example, when taking a doctor's advice, the premise is a patient trusts the doctor.

If there is a new model that can build applications without relying on trust, this implies that human social structure will change dramatically. For example, if we do not need to trust any doctors and could get valuable advice from any hospitals, will this system break down when doctors disagree on their diagnosis?

No matter what type of application, the provider of the application must act as both the server and the party that takes advantage of the information. The users play the role of consumers. As long as these two roles exist, the application cannot be decentralized. Further, centralization could gather high quality services and resources only if all the services of human society could be replaced with artificial intelligence and code, which is highly unlikely to happen.

For example, what if an intelligent decentralized trading platform that uses TLS/ SSL to encrypt network communications leads to the similar Heartbleed loophole in 2014? Who will be responsible for the loss of thousands of users’ assets?

Based on the above discussion, Metaverse believes that the best link between the blockchain and reality is for the Metaverse blockchain to become one of the underlying infrastructures of the Internet. Metaverse does not destabilize centralized Internet applications. Instead, we complement the Internet by introducing cryptocurrencies and digital assets, thus quickly penetrating the Internet. This allows all of our applications to enjoy the convenience of digital finance at virtually no cost.

In this process, an Oracle can be a centralized human-controlled application, or it can be the code of a certain DApp. Oracles provide services for people and are also supervised by the people. All of these actions occur on Metaverse, instead of on different IT systems.

# Smart Contracts and BISC (Built-in Smart Contract)

The development of blockchain technology can be compared to the development of computer technology. For example, Bitcoin is an assembly language and achieves basic payment functionality. Then we consider dozens of smart contract platforms such as Ethereum that can provide advanced programming languages.

Most technical personnel may not agree that the development direction of computer technology is the same as the development of programming languages. Technology is all-encompassing, and programming language is just one tool set underneath technology. Besides, the popularity of a programming language is determined by the ecological diversity of applications that support the language's framework. We could say that some common libraries and frameworks of these programming languages are development directions, such as Vue.js for Javascript, Boost library for C++, Tensorflow for deep learning framework, and Apache Hadoop for big data processing.

What is Vue.js in the field of blockchain? The answer is a series of generic smart contract standards (templates) that can help real-world modeling, like ERC20 and ERC725. The reason why ERC20 gained popularity rapidly is because of its ability to tokenize. Due to the prevalence of ERC20, not many people understand what the ERC55 standard is.

Then what is Tensorflow in the field of blockchain? It is the basic framework incorporated by the digital assets and digital identities that are built on the system, rather than a single functional infrastructure consisting of individual templates.

As we further analyze, we can find that Bitcoin is trying to avoid using Turing complete language for smart contracts. For Bitcoin, the first priority is to complete stable, efficient, and secure payment. Bitcoin scripting is actually a light smart contract template, for example P2SH scripts can support multi-signature payments, which then could meet Bitcoin's payment demand. Radical programmable smart contracts often bring potential security issues, and we do not think Bitcoin's core developers want these issues. Adding Turing complete and programmable languages are not required for the security of Bitcoin's payment system.

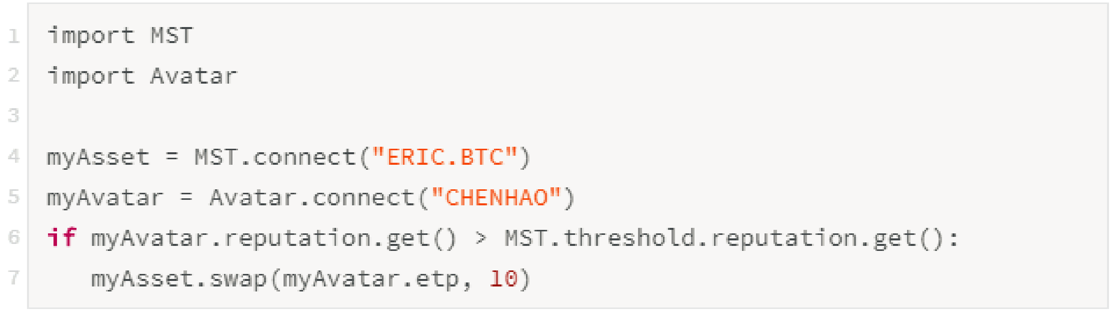
Following the idea of Bitcoin, Metaverse should provide users with stable and secure smart contract templates for digital assets (Metaverse Smart Token) and provide smart contract templates for digital identities (Metaverse Avatar) on the Metaverse blockchain. We uniformly name these standard templates Built-in Smart Contract (BISC).

BISC can be implemented through Bitcoin Script, Ethereum Virtual Machine (EVM), or WebAssembly (WASM).

In programming, we have two common patterns. The first is OOP (Object-Oriented Programming) and OOD (Object-Oriented Design), and the second is FP (Functional Programming). Considering the account-state model now, smart contracts based on account models are more suitable for OOP, while UTXO models are more suitable for FP. Due to the security of the constructed BISC, ETP and digital assets by themselves may be more suitable for the UTXO+FP model. Building on this UTXO+FP model to construct more complex codes of conduct requires the experience of OOD.

Based on the above ideas, BISC first needs generalization standard templates for digital assets (MST) and digital identities (Avatar). These may be based on UTXO+FT rather than redefining their own applications with OOD (realization, dependency, association, aggregation, composition and inheritance).

We are considering to provide BISC block-areas on the Metaverse blockchain. Developers can use BISC directly or run an instance of BISC. The effect may look like this:



```
import MST
import Avatar

myAsset = MST.connect("ERIC.BTC")
myAvatar = Avatar.connect("CHENHAO")
if myAvatar.reputation.get() > MST.threshold.reputation.get():
   myAsset.swap(myAvatar.etp, 10)
```

The code shows the procedure of buying ERIC.BTC using 10 ETPs. The MST and Avatar here are the BISCs of the Metaverse blockchain. This code also determines whether the Avatar named CHENHAO has achieved the reputation threshold. Depending on the scenario, this code can be deployed on the blockchain, or it can be an ordinary Python script. We recommend people to use BISCs with sidechains or traditional applications. This is the concept of BaaS that we will discuss next.

## Blockchain as a Service

If we want to define BaaS, first we need to find the connection between BaaS and PaaS.

PaaS provides useful basic business components, such as Amazon Translation Service and Aliyun SMS Service. These services are not simply technical frameworks, but services that can achieve specific functions.

Consider that Bitcoin provides global payment processing, will this function be integrated into cloud computing platforms? Definitely yes. For many applications with payment needs, the process of building Bitcoin nodes and data structure in the blockchain database is extremely time-consuming and painful. After all, the API provided by Bitcoin's full nodes is limited, and users' query requirements may be meticulously accurate to the transaction output and script signatures.

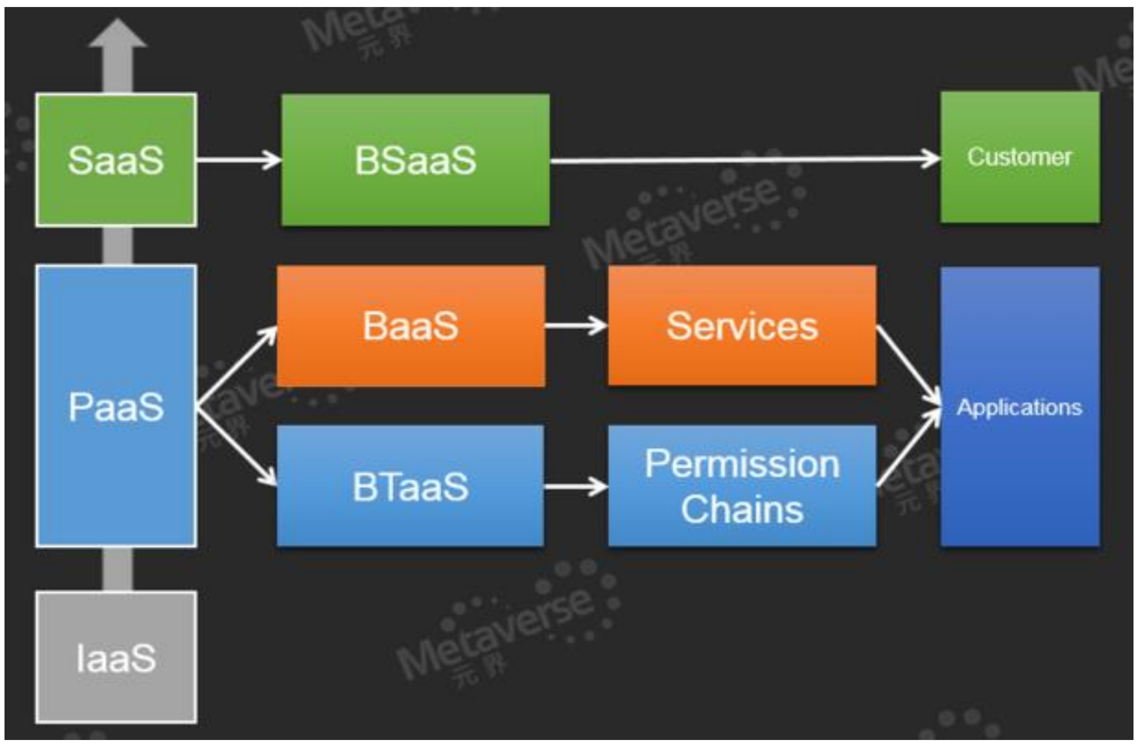
Based on the analysis above, we can find that many cryptocurrencies can be made available to users based on PaaS services. Thus, we can give a definition of blockchain as a service (BaaS).

Blockchain-as-a-Service represents public blockchain services that can be integrated into traditional IT architectures or Internet architectures by providing multiple ways of querying, transaction broadcasting, and transaction verification. These services were previously fragmented, including tokenization, Avatar services, and Oracle services. Now BaaS gives these services standards and specifications.

Currently, most block explorers and cryptocurrency trading platforms are built on public cloud services. Then, these platforms must build their own digital asset management and verification services in the cloud. Cloud service vendors can provide a common basic framework, just like Amazon Translate services. We can provide a derivative version of PaaS based on blockchain technology: BaaS.

Next we consider Software as a Service (SaaS). The best example of SaaS is Google Docs. Service fees for using vendor's applications are charged based on length of use and users' actual needs. This is the distinguishing feature of SaaS. Bitcoin is also a kind of SaaS, but Bitcoin does not have a specific cloud service provider. If we regard the Bitcoin network as an open cloud that can provide notary announcement services and transaction fees charged by block size, then we could say Bitcoin is SaaS, like the example of blockchain.info.

The diagram below can explain these concepts:



- BaaS (Blockchain as a Service) – the variant of PaaS
- BTaaS(Blockchain Technology as a Service) – the variant of PaaS
- BSaaS(Blockchain Software as a Service) – the variant of SaaS

BSaaS allows users to quickly build services directly with blockchain technology and to visualize the construction process. At present, BSaaS is not mature. There are no mature applications available currently. CryptoKitties, however, provides one example of  BSaaS.

IBM and Microsoft have proposed the concept of BaaS that benchmarks PaaS. Here, we split the BaaS concept into BTaaS and BaaS.

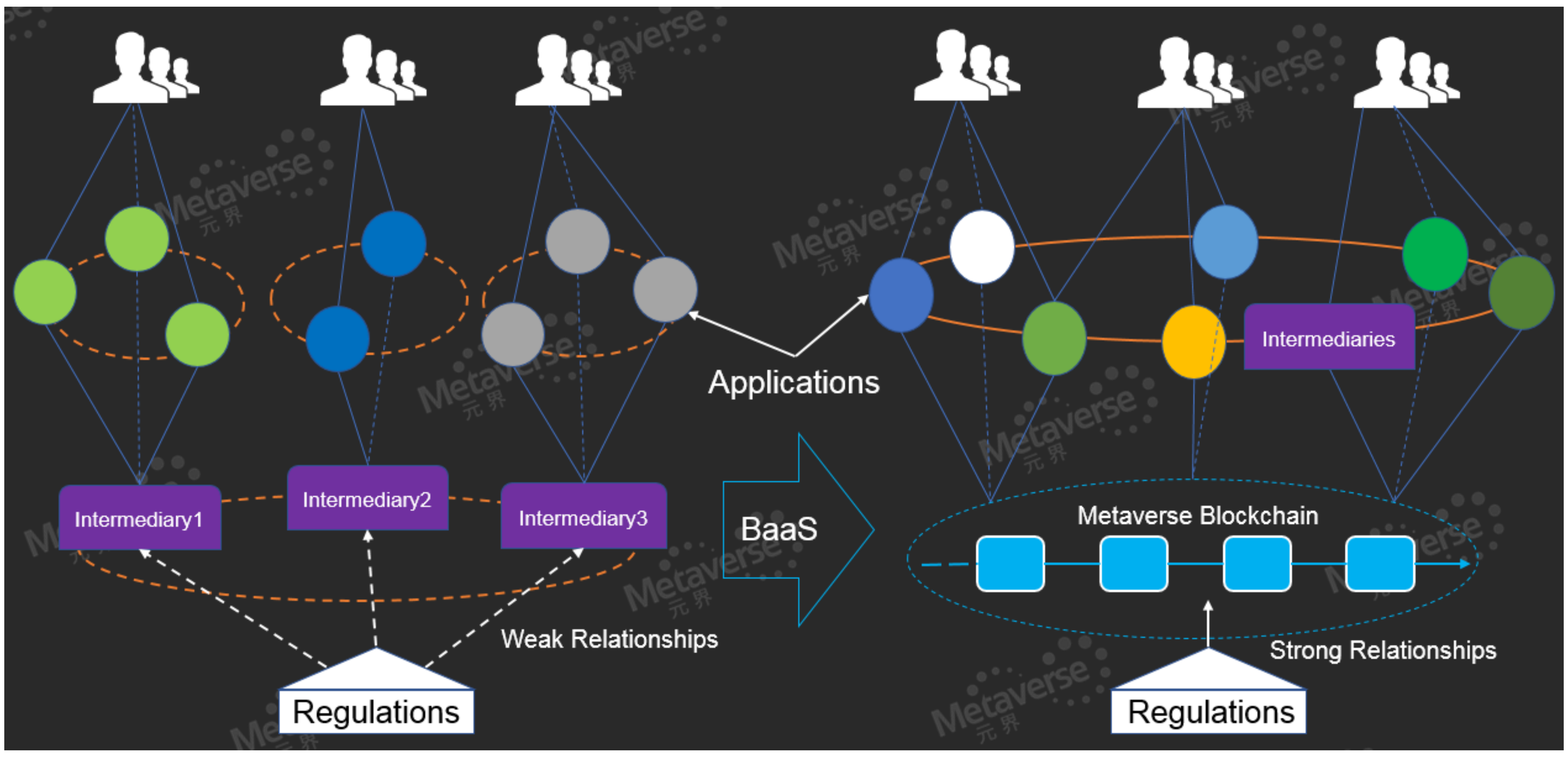
The difference here is whether to use the blockchain technology framework to build its own permissioned chain or to use the services on the public blockchain. IBM and Microsoft have proposed the former concept of BaaS. Here we change this concept into BTaaS, which can be solved through traditional IT solutions, such as using service-oriented architecture (SOA) based software to replace blockchains to build complex in-house enterprise applications.

The permissioned chain represents the activity between a few nodes and often degenerates into a game of microeconomics. Therefore, using a permissioned chain to build a collaborative system between a small number of nodes does not pose a technical challenge and evolves into how to construct a stable microeconomic model that enables collaborators to achieve Pareto improvement. In this case, the technology is secondary.

The services provided by the public blockchain are often richer than the services provided by the permissioned blockchain. If the public chain has anonymity and rights management mechanisms, the public chain can completely replace the permissioned chain.

BaaS, not BSaaS and BTaaS, concerns Metaverse the most.

BaaS means that the service provided by public blockchains will be conveniently integrated into existing internet applications and services, such as the payment function provided by Bitcoin. Metaverse will provide Avatar and MST services. For example, e-commerce providers can provide MST registration services for stores. Then the stores can issue their own bonus-point system based on the Metaverse blockchain. These bonus points share the advantages of blockchain that enable immutable P2P transactions to circulate freely on the chain. The process is described below:

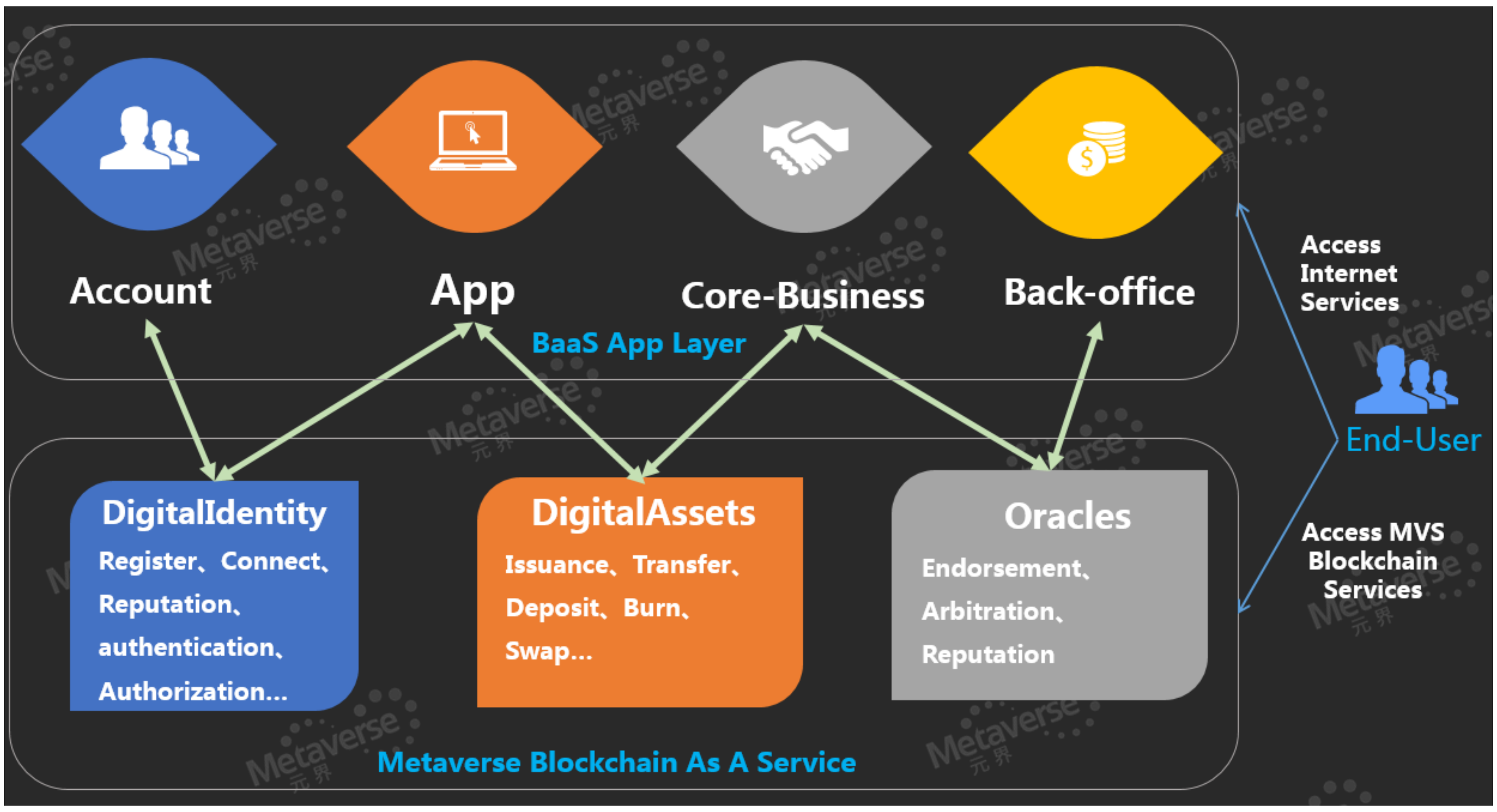


Finally, Oracles and project developers can utilize BISC, and BISC can be processed through the BaaS model. Furthermore, project stakeholders can use BISC to develop a variety of centralized applications, and Oracles can use BISC to endorse their digital identities. Users can supervise the project stakeholders via BISC. These three parties can form an on-chain closed loop.

## Metaverse Blockchain as a Service (MBaaS)

The basic function of a cryptocurrency is payment, so the integration of cryptocurrency payment services is quite simple. If Bitcoin is considered to be defined as a payment gateway, its position on the architecture will be clear and can be incorporated into the fund management module.

Regarding MST and Avatar services provided by Metaverse, Metaverse blockchain is able to play the following roles in common IT systems:



We assume that all systems have their own account module, login module, core-business module, and back office. Digital identities can be used to support the account module in existing internet applications and services; digital assets MST allows you to create your own digital assets without having to build your own blockchain infrastructure. Oracles can increase risk resistance capacity for a business.

The above services are collectively referred to as MBaaS. MBaaS can provide infrastructure services for any existing internet applications, services, and even Internet of Things (IoT) devices. These services use digital identities as the main entry point to provide people with convenient and simple asset digitization capabilities.

Considering the complexity of blockchain application development, Metaverse endeavors to reduce the difficulty of technology integration and focus more on innovation rather than the underlying technology of the blockchain. The BaaS model essentially provides an integration idea. Below are two BaaS problems that need to be solved urgently.

1. **Integration issues: There exists a need to establish a stable technical framework for the integration of BaaS solutions and existing internet applications and services**
2. **Digital asset management issues: digital asset management tools for companies that provide secure access to private key management mechanisms**

MBaaS also faces the above issues, and our solutions for these issues are below:

1. The full-node wallet and the light wallet are crude partitions, and they cannot meet the diverse demands of the architecture. As a result, the decoupling of the wallet function is needed to provide independent module programs that run separately.
2. Solved by HD (Hierarchical Deterministic) private key management mechanism that provides multi-signature. HD and multi-signatures are relatively mature technologies. Thus, aggregation will be of prime concern for MBaaS.

## MBaaS in Architecture Patterns

There are many architecture patterns. We will only discuss monolith applications, layered architecture pattern, event-driven architecture pattern, and micro-service architecture pattern. Then we will discuss where MBaaS should fit in these architecture patterns.

### MBaaS and Wallets

Firstly, MBaaS is a collection of services that is manifested in the system as daemon processes. A running wallet program usually provides MBaaS.
Hence, there are two modes for wallet programs:

1. **Decoupling mode:** Separation of functions from the wallet program, each function runs as a detached multi-process that provides a MBaaS service.
2. **Combined mode:** The wallet program provides MBaaS, but the wallet can form a dominant relationship and create an internal distribution network instead of connecting to the public network. The combined mode puts higher requirements on the optimization and stability of wallets.

### Decoupling Mode

Metaverse provides the following basic module separation:

- P2P network service;
- Transaction verification and parsing;
- Private key management;
- Structured persistent storage of blocks, MySQL/mongoDB.

Light-wallet is the first decoupling mode program derived from the full-node wallet.

### Combined Mode

The wallet program provides a high speed synchronization mode in an internal network. Those nodes can be architectured as a wallet cluster, which has strong stability, even when the chain has forked. Regarding block storage, wallets should support RDS(MySQL/mongoDB) connections.

Decoupling mode or combined mode are not used alone; they may be combined into a hybrid in real use cases. Next, we will discuss MBaaS in the popular architecture patterns with these two modes.

### Monolith Applications

Monolith applications can be classified into client-side monolith applications and server-side monolith applications. An example of a Monolith application is WordPress. If we want WordPress to support MST, the fastest way is to deploy a Metaverse wallet on the WordPress backend server, then call MST APIs to send through the blockchain transaction. The front-end displays the MST token. This situation is suitable for combined mode and easy deployment.

Monolith applications are more commonly used in the Micro-kernel Architecture Pattern. For example, the Metaverse Avatar can be embedded in the Eclipse IDE, which requires the Metaverse light wallet to be plugged into Eclipse as a plugin. This situation is suitable for decoupling mode, such as the light wallet.

### Layered Architecture

Layered architecture is suitable for both decoupling mode and combined mode, depending on the scale of architecture. The decoupling mode is suitable for large scale layered architectures. For example, the combined mode is not satisfactory in SOA.

Considering the decoupling mode, MBaaS is suitable for the business layer in the layered architecture. To become a common component, MBaaS only requires the wallet's API to be as compatible as possible with other modules of the business layer. If there is a persistence layer, structured block storage may be required, otherwise the wallet itself may be used instead of the block storage.

Considering the combined mode, MBaaS is suitable for small scale applications. The MBaaS can be built with reference to the server-side monolith applications.

### Event-driven Architecture

Event-driven architecture is suitable for the decoupling mode since it focuses on the forward processing of events. The process of blockchain is based on transactions, and the transactions themselves are events, so in the event-driven architecture, the decoupling mode is the most appropriate.

In the Mediator model, transactions need to be parsed and forwarded. In the Account-base model, the system also needs the ability to read the account-state directly.
In the Broker model, each Processor has the ability to parse and validate transactions, and the broker will stay at the same state.

The above analysis considers incoming transactions as an event. Regarding outgoing transactions, we can think of a wallet as a processor, as the wallet only processes target events from the blockchain. Here we may have a problem, as the wallet evolves into a central processor. Since the ultimate purpose of any core business is payment, the wallet will face a performance bottleneck. Therefore, we may need wallet clusters to solve this issue.

Horizontal scalability is important for the decoupling mode in Event-driven Architecture pattern.

### Micro-services Architecture

Micro-services architecture is suitable for combined mode and can also be applied to decoupling mode.

In the combined mode, for the wallet to be a microservice component only requires the wallet function to be cohesive enough. For example, the wallet can play the role of payment in component A and play the role of transaction verification in component B. This requires that the wallet's behavior fits as closely as possible to the micro-services in the micro-services architecture, and provides ample query and verification APIs.

The decoupling mode seems to fit well with micro-services architecture. Therefore, providing standardized Metaverse micro-service components is not too difficult and can be the primary solution we consider.

# MST Exchange

To be able to trade on the blockchain is an advanced requirement of MST, mainly for scalability under these options:

**Option 1: Graphene**
Graphene is the more mature technology presently. To support transactions on the blockchain, Metaverse considers integrating Graphene, which faces the following technical challenges:

1. MST backward compatibility
2. Avatar and DPoS algorithm compatibility
3. Compatibility of UTXO Model and Graphene Account Model
4. Transaction compatibility
5. Encryption module compatibility
6. Coupling module controllability

**Option 2: On-chain settlement, off-chain matching (0x protocol-like)**
Bitcoin's SegWit and the Lightning Network provide good scalability. After upgrading to SegWit, Metaverse can set up an on-chain settlement agreement similar to the 0x Project, using incentives to exchange order and market data for many trading platforms.

# Potential Risks and Concerns

Blockchain technology is still in a stage of rapid development, and continuous research will explore how best to mature this technology. Metaverse comes from the Bitcoin system, so it will inherit the advantages of the Bitcoin system, as well as some flaws.

## The Ever Increasing Blockchain Size

The Bitcoin Blockchain grows approximately 1 MB every 10 minutes, that is 1 GB weekly, which makes the cost of running a full bitcoin node increasingly expensive. The number of full nodes has been in decline since the peak of more than 10,000 nodes globally in  2013 to roughly 5,500 in July 2016. The Ethereum Blockchain grows by roughly 2GB monthly at an ever increasing rate.

Metaverse Blockchain will suffer the same problem. If we disregard the decentralization principle, the UTXO model can support block cut off. The cut off position can start from the block where the oldest UTXO is located. Starting from this position is defined as the "Milestone" block, since its meaning is close to the Genesis block.

## Mining Centralization

Mining is a double-edged sword. On the one hand, mining can arithmetically protect the system from attacks. On the other hand, mining has created new problems, such as the problem of mining centralization and the threat of 51% attacks.

Mining centralization is much detested in the Bitcoin industry, and Ethereum is also gradually losing its initiative in the face of mining centralization.

Metaverse will optimize its mining algorithm, and although this probably will not be sufficient enough to eliminate this problem, we can slow the centralization process until the consensus algorithm switches from POW to HBTH-DPOS.

## Failure on Success

Should Metaverse become very successful in the future, a new risk will arise. When the total value of digital assets on Metaverse rises to a certain level, it will become profitable to sabotage Metaverse while shorting the assets in the exchanges as a means of attack. Thus, the total value of digital assets on Metaverse is a function of the cost of defending/attacking the system (mining cost in the POW stage). Ideally, the total value of digital assets should not exceed five times the cost of mining.

## Conclusion

Like Bitshares and Ethereum, Metaverse was derived from Bitcoin, utilizing blockchain technology to solve problems other than simply being a digital cash system. From Bitshares came decentralized exchanges, and from Ethereum came smart contracts and decentralized application platforms. By clearly defining digital assets and digital ID, and emphasizing the importance of the on-chain Oracles, Metaverse assures the rightful ownership of assets digitally, building the foundation for future digital finance.

In Metaverse, Avatars are able to securely transact digital assets with the help of value intermediaries Oracles. Thanks to blockchain technology, Metaverse inherently has its own immutable ledger and solves the problem of double spending, penetrating beyond the realm of digital cash to all potential digital assets.

# References

- Bitcoin Whitepaper ——Satoshi Nakamoto http://bitcoin.org/bitcoin.pdf
- Namecoin: https://namecoin.org/
- Bitshares whitepaper: http://docs.bitshares.org/bitshares/papers/index.html
- Ethereum WhitePaper: https://github.com/ethereum/wiki/wiki/White-Paper
- Smart Contract ——Nick Szabo http://szabo.best.vwh.net/idea.html
- Smart Property —— https://en.bitcoin.it/wiki/Smart_Property
- Blockchain—from Digital Currency to Credit Society ——ChangJia, HanFeng and etc. ISBN：9787508663449
- Snow Crash——Neal Stephenson 1992
- Tim Swanson——http://www.coindesk.com/smart-property-colored-coins-mastercoin
- https://en.bitcoin.it/wiki/Script
- https://steemit.com/dpos/@dantheman/dpos-consensus-algorithm-this-missing-white-paper
- https://en.wikipedia.org/wiki/Claims-based_identity
- https://en.wikipedia.org/wiki/Digital_identity
- https://en.wikipedia.org/wiki/X.509
- https://en.wikipedia.org/wiki/Personally_identifiable_information
- Shocard whitepaper - https://shocard.com/wp-content/uploads/2016/11/travel-identity-of-the-future.pdf
- https://tokensale.civic.com/CivicTokenSaleWhitePaper.pdf
- ERC725 - https://github.com/ethereum/EIPs/issues/725
- The Construction of Reputation in a Negotiation - Carl-Erik Torgersen
- Digital Identity Interoperability and eInnovation - Berkman Publication Series
- Software Architecture Patterns —— Mark Richards 2015
- https://github.com/bitcoin/bips/blob/master/bip-0032.mediawiki
- https://blockchainhub.net/blog/blog/decentralized-identity-blockchain/
- https://sovrin.org/wp-content/uploads/2017/07/The-Inevitable-Rise-of-Self-Sovereign-Identity.pdf
- https://github.com/mvs-org/mips/blob/master/mips/mip-2.md
- http://openid.net/connect/