Metaverse

Digital Identity White Paper

Revision Timeline

Version		Author	Date	Email
V1.0	First draft	Ofelia Hao Ahmed	201706	zhenlin.huang@viewfin.com hao.chen@viewfin.com ahmed@viewfin.com

CONTENTS

ABSTRACT **1**

1 INTRODUCTION **2**

1.1 Identity Issues: Blockchain's Missing Link 2

2 DIGITAL IDENTITIES (AVATAR) **4**

2.1 Metaverse Introduction 4
2.2 The Nature of Digital Identity 4
2.3 Use Cases 5

3 TECHNICAL OVERVIEW **6**

3.1 Definition of Digital Identity 6
3.2 Operational Flow of Digital Identities 7
3.2.1 Creation *7*
3.2.2 Verification *7*
3.2.3 Authorization *7*
3.2.4 Query *8*
3.3 Asset Association Relationship 9
3.3.1 Relationships between digital identities *9*
3.3.2 Relationships between digital identities and assets *9*
3.4 Off-chain Data Management: Data-feed 10
3.5 Application Management 11
3.6 Credit Data Collection 13
3.6.1 Transaction record statistics *13*
3.6.2 Asset information statistics *14*
3.6.3 Risk Assessment *15*
3.7 Digital Identities and BaaS (Blockchain as a Service) 15
3.8 Digital Identities and Trading Intermediaries 17
3.9 Application Scenarios for Digital Identities 18
3.9.1 Credit Reports *18*
3.9.2 Borrowing *19*
3.9.3 Insurance *20*
3.9.4 Audit *20*
3.9.5 Government *20*

4 CONCLUSION **21**

5 REFERENCES **22**

Abstract

Metaverse Project (MVS)

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

Digital identities will be built on the Metaverse ecosystem. Its applications will be developed around BaaS and the Metaverse Wallet according to the underlying functions provided by the Metaverse blockchain, and will offer verifiable and authorizable infrastructure services for all walks of life.

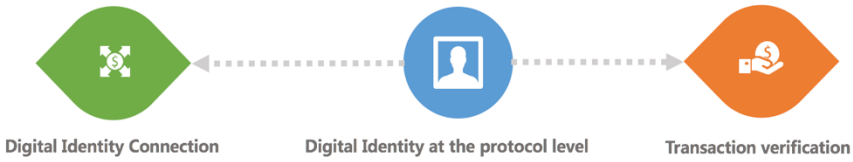
1 Introduction

In reality, questions about identity often begin with: “Who are you?”. The spread of the Internet has made digital identity applications increasingly common across industries, and businesses as well as individuals have become aware of the importance of digital identities. Following significant growth in the interactions between the public and service providers, usernames and passwords have become a common method of identity verification. However, this method is flawed – for example, a database environment must be created to establish relationships with centralized institutions, but identity providers with poor cybersecurity systems are vulnerable to attack. Additionally, the lack of interoperability between current identification systems cause repetitive registration. One is repeatedly asked to verify their identity, wasting time and resources.

Many current business models, processes and solutions did not exist before the rise of emerging technologies. Amongst them, blockchain technology has been the most groundbreaking; like the Internet, it has the potential to revolutionize many industries. First used by Bitcoin, blockchain is now looking for solutions for the financial, supply chain management and anti-counterfeit industries. Most importantly, digital identity applications on the blockchain are now being extensively researched by identity and blockchain technology experts – currently, over 40 projects are ongoing. Regardless of whether these applications are built on public blockchains or integrate public key infrastructure (PKI) and blockchains, digital identities still have a long way to go.

1.1 Identity Issues: Blockchain’s Missing Link

There are many different blockchain protocols and implementations in the current blockchain ecosystem, but all questions about identity follow a process: proving who owns what, and who has done what with whom. While pseudonymous protocols such as Bitcoin have certain advantages, any more applications still require identifying information. We need to know who we are dealing with in real life, and here a string of numbers falls short. Hence, the ‘missing link’ in decentralized applications is identity. Overlooked in many public blockchain protocols, a decentralized, self-sovereign identity system would allow an ecosystem of digital assets to flourish. Digital identity is vital for blockchain-based financial applications to demonstrate their full potential in online banking systems and other financial services.



By embedding digital identity at the protocol level, Metaverse Digital Identity facilitates development of verification functions for applications based on public blockchains.

Additionally, we have noticed the value of inviting middlemen to the blockchain because they play a key role in corroborating and verifying a user's claims using digital identities.

2 Digital Identities (Avatar)

2.1 Metaverse Introduction

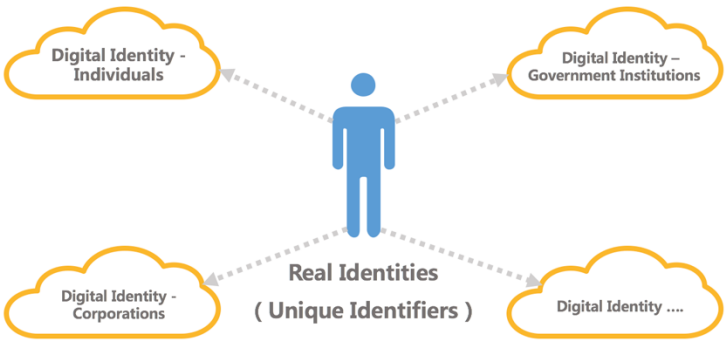
Metaverse aims to provide safe and convenient infrastructure services based on blockchain technology for a wide range of users, including individuals, corporations and government institutions. Composed of three pillars – Digital Assets, Digital Identities and Value Intermediaries (Oracles), Metaverse intends to build a network with smart properties. These core elements will provide protocol-level support for all decentralized applications built on Metaverse.

As our lives become increasingly digitalized, Metaverse and its three pillars will leverage the advantages of the Internet to establish a virtual world for its users. Businesses and communities will depend on users' digital identities to manage assets: we call this the internet of value.

2.2 The Nature of Digital Identity

Digital Identities in Metaverse are unique. The identification module will be built into the protocol, and supplementary applications will be developed. Users will have autonomy over their identity—a self-sovereign identity—meaning that they are in full control of their personal identification information and hence need not rely on any central entity or third party for identity verification. With a truly self-sovereign identity, users can create, sign and verify claims, while parties who interact with a user will be able to prove their identity. Additionally, users will be able to selectively disclose their information.

Digital identities are an integral part of the virtual world and can take many forms, such as that of an individual or value intermediary (institutions and entities). Therefore, a user can have different digital identities under different scenarios (such as a workplace identity and personal identity), but they are ultimately all based on the user's real-world identity.



Users can establish a reputation on Metaverse through digital identities, improving the way we exchange value. Value is exchanged through digital signatures, requests for verification and transactions; these transactions then allow a user to gradually build a reputation which can be inspected and verified by other digital identities and value intermediaries. If a centralized entity's servers crash, the identities and reputations established by their users over the years could be permanently lost. With Metaverse, a user's digital identity and reputation will be protected by blockchains.

2.3 Use Cases

There are many use cases for identity systems embedded within a blockchain protocol.

If a person owns multiple digital identities and wants to open an account at Bank B, then he can indicate that he has already opened an account at Bank A. Because of this, Bank B will authorize him to open an account at their bank. This use case can be replicated at multiple banks within the same legal jurisdiction.

In addition, digital identity is also applicable in areas such as digital copyright, where end users will be able to claim copyrights and other assets using their digital identities. In addition to authorizing their authentication information, users will also be able to authorize others to view private data such as reputation and credit data.

3 Technical Overview

There are three types of ledgers in Metaverse: digital asset ledgers, digital identity ledgers and data-feed ledgers. Digital identity ledgers are realized based on ETP transactions, similar to digital asset ledgers on Metaverse and elsewhere. After analyzing a large number of cases, we found that digital identities have just two core functions: identity verification and operation authorization.

Hence, we have set the following design goals:

- **Interrelationship with assets** – Digital identities can reflect their relationship with digital assets;
- **Data-feed –** Off-chain data can be imported into digital identities, and through this relationship display the Oracle's credit endorsement characteristic;
- **Application management –** identity information for multiple Internet applications can be managed through a digital identity;
- **Credit data collection –** digital identities can provide immutable credit datasets.

3.1 Definition of Digital Identity

Digital identity is the general name given to an account's Profile information, corresponding to the master private key that belongs to a user. Each Profile has a unique identifier that we call DID (Digital Identity, similar to an alias in BitShares) in Metaverse. Digital identities include the roles of Oracle and ordinary users – any digital identity can apply to be an Oracle or ordinary user, and participate in applications using their digital identities.

A Profile contains the following information:

- Personal transaction records
  - Kept on the statistical level, contain record details, no additional storage required.
- Asset information
  - Kept on the statistical level, contains UTXO details, no additional storage required.
- Customized description field
  - The customized field has a lifecycle, and users should specify the height interval at which the field is valid. This field can be modified to correspond to different blocks height intervals.
  - This field is expressed in the form of key:value and has no upper limit, but the transaction fee collected increases exponentially with the word count.
  - Additional storage required.

More details about statistical level data can be found in the "credit data collection"

section below.

3.2 Operational Flow of Digital Identities

3.2.1 Creation

Any user can create a digital identity and bind it to his/her master private key.

If a user creates a digital identity but does not bind it to any master private key, this DID will be regarded as an unauthenticated account and will not be able to utilize any digital identity functions or applications.

Master private key holders who have already registered assets on the Metaverse blockchain may choose not to bind a digital identity to their key. Users must take the initiative to bind digital identities to their keys; Metaverse will not automatically create digital identities for any user. The right to bind a DID lies with the master private key's holder.

3.2.2 Verification

Profiles can provide effective chains of proof that contain objective facts about a digital identity. Users must first prove that a digital identity belongs to them by binding a transaction to the DID (since the transaction domain contains DID information).

3.2.3 Authorization

First, we should clarify the situations that would require authorization. Assume A requests B's digital identity information (asset information) to review his assets before providing any services. In this scenario, there are two possibilities:

1. B has large amounts of on-chain assets exceeding 1 million ETP. If so, B can simply disclose his asset information to A.
2. B has few on-chain assets, but many off-chain assets. Usually, B would have to convert his assets to ETP and proceed with authorization. The approach Metaverse currently recommends is to issue one's own assets on the blockchain and have them verified by an Oracle, after which they will be registered as valid assets belonging to one's digital identity.

<u>Authorization process</u>

A sends B an asset verification request. This request triggers a script that verifies the target account's asset information and returns the result. This result has been encrypted by A such that B does not know which result corresponds to the information that has undergone verification. Furthermore, the request is also encrypted such that B knows what information was requested, but not the specifics

of A's request. Personal transaction and asset records can be accessed after permission is given on-chain, with the basic principle remaining unchanged.

The authorization process for personal customized fields is similar to the asset verification process facilitated by Oracles described above. (Information that has not been authenticated by an Oracle can still be authorized, but this is not recommended).

If the personal customized field contains nonpublic information such as email addresses or phone numbers, no Oracle authentication will be required. However, if the information is certified (such as schooling records), then Oracle authentication will be required.

Authentication process

Authentication of personal customized information:

An Oracle's data-feed is used for endorsement. An Oracle is introduced as a third party and publishes all Profiles on the blockchain for public inquiry and supervision. Oracles are usually organizations; these organizations should also publish their profile and DID information on their official website.

First, B fills in the customized field with information that needs to be authenticated. The Oracle must then use its master private key to sign the information and employ a larger sum of ***coindays*** to endorse it.

A can make a request for the information contained in this field (including the Oracle endorsement) on-chain. If A is convinced that B's information is valid, he can continue providing services to B.

3.2.4 Query

Digital identities introduced the concept of DID identifiers; as such, they can be used as the main entity for over-the-counter (OTC) trading since they can create transactions in trading markets.

We can query a DID's current transaction requests and past transactions in the open market by entering the DID into the address query bar in trading markets. Conversely, a DID's behavior and records in the market can be used as data to build digital identities.

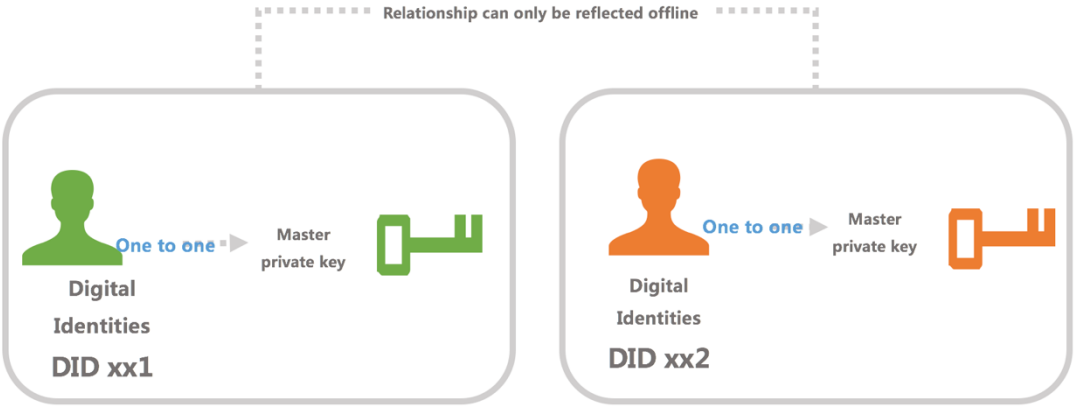
3.3 Asset Association Relationship

Digital identities have a one-to-one relationship with master private keys: one digital identity can correspond to one master private key. There is also a one-to-one relationship between digital identities and assets – an issued asset must belong to an address, and that address must belong to a digital identity. Digital identities cannot be transferred or destroyed, but a user's actual relationship with it may change.

3.3.1 Relationships between digital identities

Relationships between digital identities are only manifested off-chain. Let digital identities A and B both own one digital asset, A and B company respectively. If company A acquires company B, digital identities A and B can announce this subsidiary relationship off-chain. However, there is no way to express this subsidiary relationship on-chain, and hence no way to express that digital identity B belongs to digital identity A.

In addition, assets belonging to a digital identity can be transferred to another digital identity. However, this transfer can only serve as credit rating data and is unable to express any relationship that may exist between the two digital identities.



3.3.2 Relationships between digital identities and assets

The relationship between digital identities and assets is expressed through the transfer of an identity's assets. Extending the example above where company A acquires company B, company B's tokens will be transferred to addresses held by company A after they reach an agreement offline, completing the asset registration process. At this time, digital identity B no longer holds Company B's assets, while the composition of digital identity A includes both company A and B.

3.4 Off-chain Data Management: Data-feed

- **Off-chain data and asset registration**

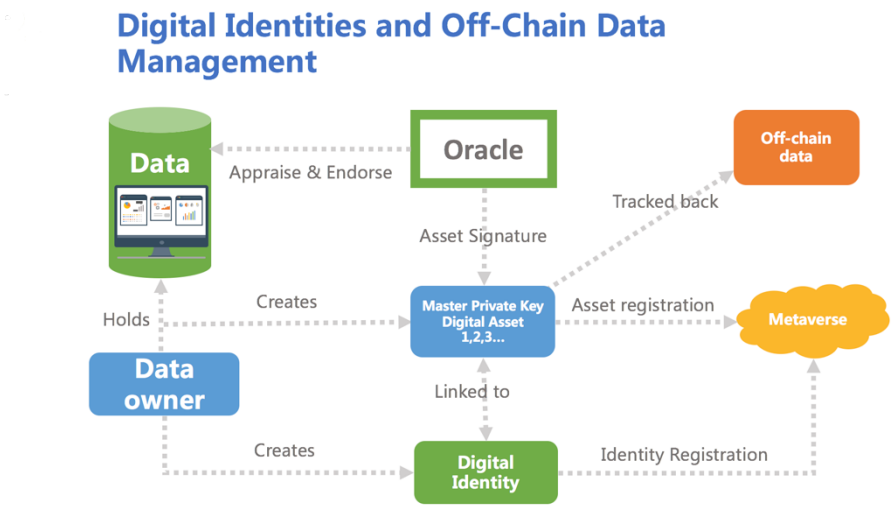
Off-chain data refers to data that is not recorded on the blockchain, which is often massive and complex. We aim to link off-chain data to their corresponding digital identities.

This process is similar to patent registration in the real world. After specialized agencies examine and appraise some piece of intellectual property created by an entity, those that meet the criteria can be patented. Users who wish to obtain the right to use this work in the future must pay a fee to its owner. Additionally, the owner can also sell his ownership of the rights through certain procedures and receive profit.

Likewise, each piece of data in the Metaverse ecosystem should have a corresponding owner. We can regard each piece of data as an asset or a token, where each token contains the details of the data and its owner. Hence, to ensure the authenticity and validity of this data source, Oracles must be introduced to endorse it. Different types of data will require different Oracles to provide different appraisal criteria or fields for review. Finally, to indicate a data asset's validity, an Oracle will use its private key to sign the data. After the procedures outlined above are complete, a digital identity will be linked to the piece of data; these pieces of data with specific ownership can be called **valid off-chain data**.

Registering valid off-chain data linked to a digital identity requires the following four steps:

1. Users with data must establish a digital identity on Metaverse, provide data in a user-defined format, and submit this data to an Oracle who is responsible for data appraisal and endorsement.
2. Oracles (a digital identity) qualified to appraise data will assess the validity and authenticity of the submitted data;
3. After the data is signed by its owner and the Oracle, it will be bound to the owner's digital identity through master private keys.
4. With the data owner's authorization, other users may view the detailed information represented by the data asset.
5. Other users can view the details of the data after the data's owner gives his authorization.



We know that certain types of equity can generate profits for their holders. In Metaverse, because digital assets are linked to off-chain data, digital assets can bring similar profits to its owners. The digitization of off-chain data will increase its liquidity and allow it to be portioned out and simultaneously held by multiple digital identities. Each digital identity can sell its portion to other digital identities.

- **Off-chain data and market forecasts**

Prediction markets in the blockchain industry are essentially aggregations of off-chain data. During predictions, the data can be expressed in the form of options. As a financial application tool, prediction markets are another way to manage off-chain data. Thus, we encourage third parties to build prediction market applications based on the Metaverse blockchain.

3.5 Application Management

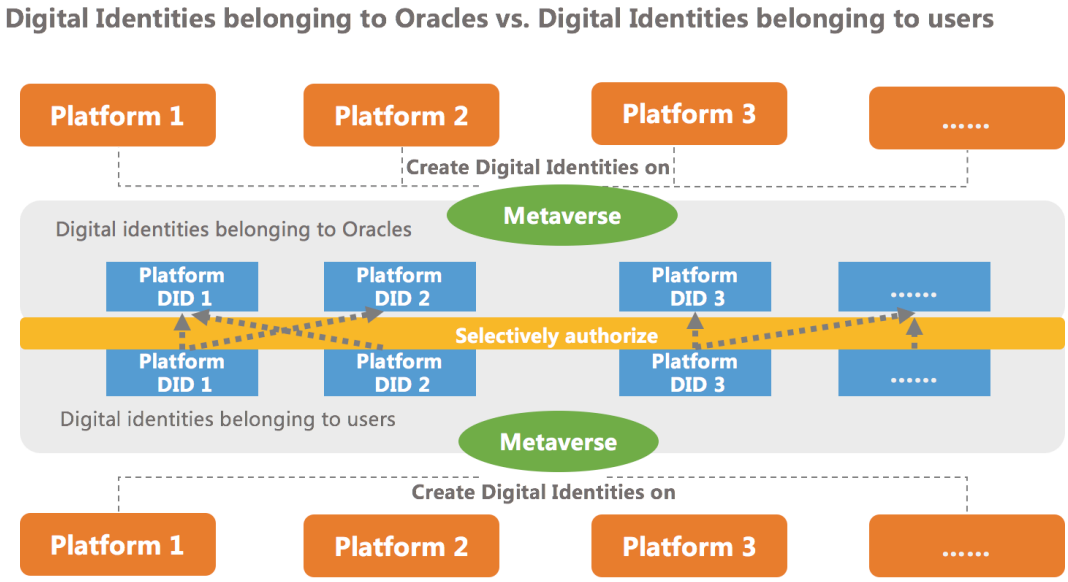
The databases of traditional Internet applications are centrally managed, causing account and asset information to be unable to flow between different platforms. For example, Alipay accounts cannot be used to log in to WeChat applications, and one's WeChat wallet balance cannot be used in Alipay.

The birth of digital identities will be able to solve these pain points. Through just one Metaverse account, users will be able to log into and access different application platforms. Furthermore, these applications can all access the assets stored in one's Metaverse Wallet.

Application Management Process

First, application platforms must register a digital identity on Metaverse and define their own identifier, then link their digital identity to their corresponding master private key and configure Metaverse Wallet services into their application.

Next, users of this application platform must also register a digital identity on Metaverse which can then be used to log in to different application platforms. When users log in to application platforms via their digital identities, they can selectively grant the application access to their identity information, hence removing the hassle of registering and authenticating their identity information repeatedly.



This also simplifies the process of registration when users wish to use cross-regional applications, since users will not need to have their identity information authenticated in different formats by different applications for AML/KYC purposes. A single digital identity allows users to access various application platforms. For application platforms, they simply need to use their own inbuilt rules to determine which functions a user may access, based on the identity information they have provided.

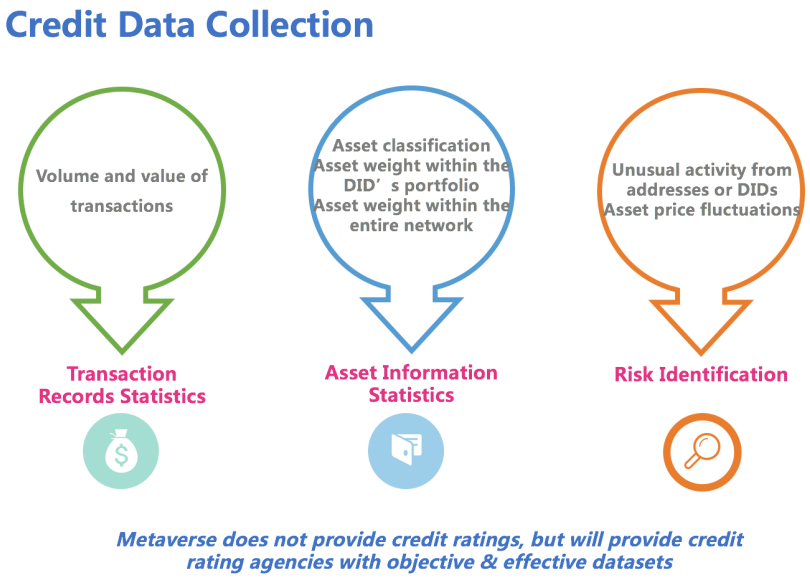
Moreover, a user's digital identity is not owned by any centralized application platform. As such, digital identity holders need not worry about their digital identity, assets and information being deleted, leaked or tampered with, because they can selectively grant applications the right to view the information bound to their digital identities. Thus, the right to use and ownership of a digital identity truly lies in the hands of users, and only users can choose if their digital assets increase or decrease. This not only protects a user's identity security and privacy, but also the security of his/her assets.

3.6 Credit Data Collection

(The Metaverse blockchain does not provide credit rating services, but will provide objective and effective datasets for credit rating agencies.)

A digital identity's credit data is determined by certain statistical information, including transaction record statistics, asset information statistics and risk assessments. After data collection is completed, a comprehensive analysis will be performed on the data that can be digitized and indexed. The compiled information linked to a digital identity will then be compared to the information available across the network and scored.

Digital identity holders may authorize third-party trading platforms to provide the price data of their assets on these third-party platforms as a statistical basis. Currently, we have defined three types of statistical data.



3.6.1 Transaction record statistics

Asset transfers on Metaverse leave a transaction record searchable on the block explorer. A digital identity owner confirms whether or not to use his master private keys to build a digital identity. The Wallet can analyze any transaction in any address by accessing data in the blockchain explorer, and confirm the transaction information of multiple addresses belonging to one digital identity, following the dimensions outlined below:

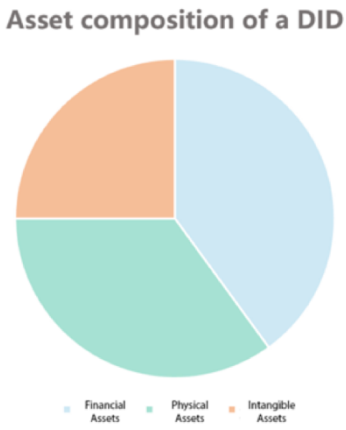
- The transaction volume of each address within a certain time period: confirmed based on the proportion of total assets represented
- The transaction value of each address within a certain time period: if the assets have entered the trading market, the transaction value of

each address in a certain period of time is confirmed by its market price (eg. in accordance with the asset's MA20); if the asset has not entered the trading market, then the transaction value will be confirmed using the market price of the tokens (such as ETP) exchanged for the asset. ETP's price will also be confirmed using the above method.

3.6.2 Asset information statistics

Asset information statistics are compiled according to the master private keys corresponding to a digital identity. We primarily compile three types of information:

- Classification of a digital identity's assets:
  - Financial assets (digital currency such as ETP / BTC / ETH, accounts receivable and interest rates, derivatives, etc.)
  - Physical assets (corresponding to real-world assets, including houses and buildings, transportation, machinery, etc.)
  - Intangible assets (corresponding to assets without physical representation, including patents, copyrights, land use rights, etc.)
- Each asset's weight within the DID's portfolio: the proportion of financial assets, physical assets and intangible assets within a DID's portfolio.
- Each asset's weight within its asset class within the entire network: calculate the percentage of its asset class (financial, physical or intangible) each asset represents within the entire network, then calculate the weightage of each asset using the last three transaction prices recorded. Assets without transaction records on the blockchain will not be factored into the weightage in order to encourage asset circulation, by incentivizing owners to create transaction records on the chain. The compilation process makes the following assessment:
  - Whether an asset has transaction records.
  - If transaction records exist, extract the average price of the last three transactions from the records.



Proportion of the entire network					
Financial assets		Physical assets		Intangible assets	
BTC	x%	Houses and buildings	x%	Patent right	x%
ETP	x%	Equipment / machinery	x%	Copyright	x%
...	...	...	...	...	...

3.6.3 Risk Assessment

Risk data collection and identification is carried out by address. Currently, risk data can be divided into several categories:

- Unusual address identification

Abnormal behavior is tagged by collecting reports made by digital identities about addresses. Abnormal behavior includes the address showing signs of being used for extortion or fraud. It will cost a certain amount of ETP to make a report and each DID can only report an address once, so as to discourage prevent parties from making malicious address reports. Furthermore, because the reporting party is a DID and digital identities are gradually built by leaving traces, digital identity holders will be more inclined to provide real and accurate information considering the seriousness of building credit records. When the abnormal tags exceed a certain value, the system will give a prompt that the address is unusual.

- Unusual DID identification

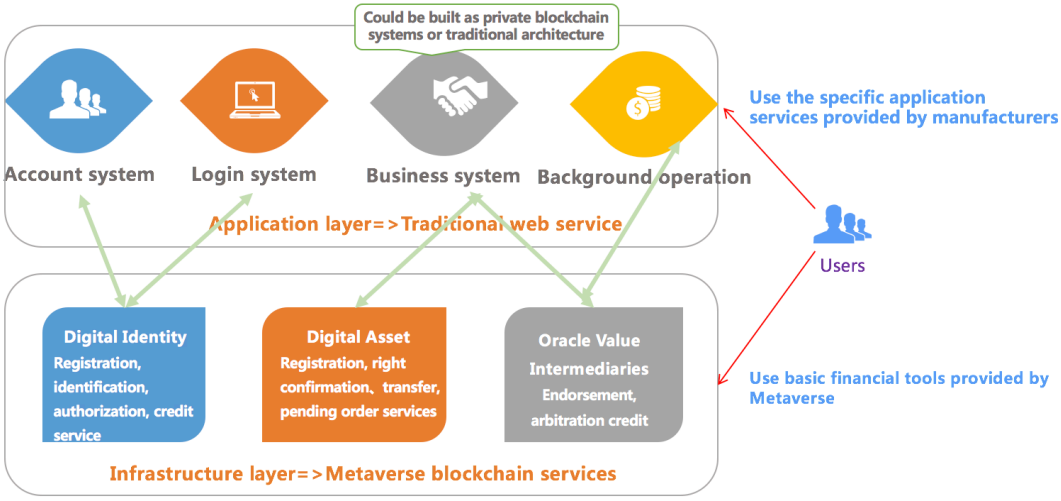
As addresses are linked to a digital identity, similarly, once the number of unusual addresses belonging to a master private key exceeds a certain value, the information of the digital identity who owns these addresses may also be tagged as abnormal. Additionally, once Oracles receive updated off-chain data with information indicating that the data holder is engaged in a series of illegal activities including but not limited to being wanted and detained, the digital identity itself will also be marked as abnormal.

- Asset value fluctuations

The fluctuation of an asset's value is decided by its daily weighted amplitude in the trading market, and together with the weightage of each asset within a digital identity's entire portfolio, it is used to calculate a user's total asset value fluctuation. Users can set a warning percentage, prompting a risk notification when the fluctuation reaches a certain value.

3.7 Digital Identities and BaaS (Blockchain as a Service)

The concept of BaaS (Blockchain as a Service) was first proposed by Metaverse, that is to say enterprises or individuals can request for customized blockchain services from blockchain solutions providers according to their needs.



- **User base**

Metaverse's BaaS framework primarily caters to business users, such as individuals or enterprises with transaction or asset management needs. As Metaverse continues to perfect its infrastructure, its target user base may expand. Furthermore, business users can no longer be grouped as they traditionally were – any entity and hence any digital identity could potentially be a business user.

- **Asset Registration**

Digital asset registration is the most important segment of the entire digital identity system. As a user, any entity has the right to issue assets on Metaverse. This segment is necessary if business users are to accept BaaS services.

- **Building Digital Identities**

Digital identities and BaaS services are interdependent – digital identity data from individuals and businesses helps Metaverse provide BaaS services to enterprises, while subsequent data and information flows generated by the service can be fed back into digital identities, creating sustainable development and closing the ecosystem loop.

- **BaaS services**

1. *Object management based on digital identities*
   Business users will access BaaS services through their digital identities. Business users who engage in related-party transactions and register their assets on the Metaverse blockchain can enhance the credibility and validity of their and their trading partners' digital identities.

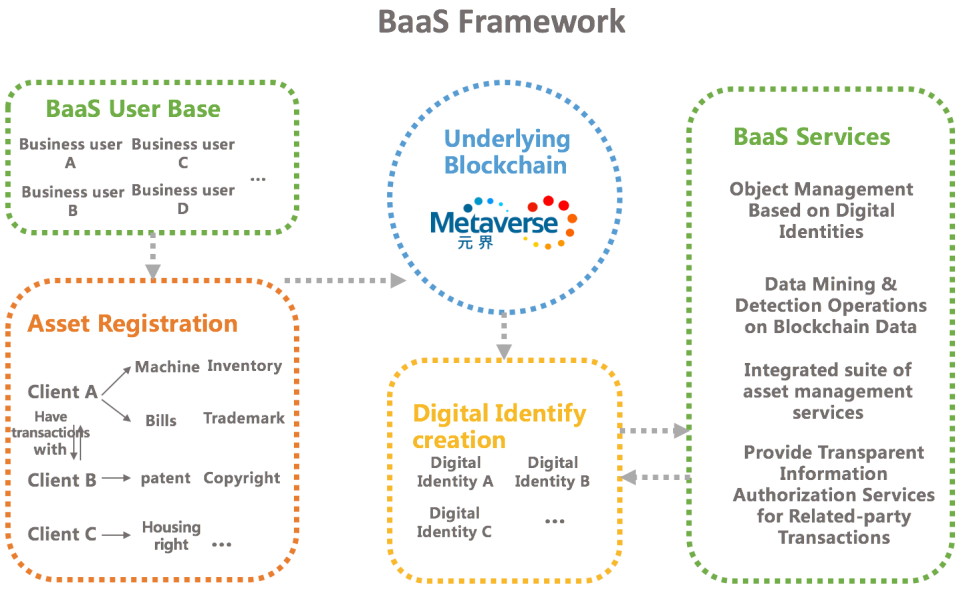
2. *In-depth data mining and examination*
   Business users and third parties can make use of Metaverse's digital identity data

by mining and examining the relevant content and transaction history.

3. *Provide integrated underlying asset management services:*
   - In essence, BaaS makes use of assets registered by business users on the Metaverse blockchain. To some extent, this is a class of asset management services built into Metaverse's infrastructure. Metaverse will provide the basic application module framework in its client.
   - In addition to the basic BaaS services provided by Metaverse, more third-parties may get involved in Metaverse blockchain services in the future. Like auxiliary tools or plugins, they will further enhance asset handling and management for BaaS service users.
   - BaaS services integrate a series of traditional upstream, downstream and supporting business services, emphasizing the integration of data supply and management.

4. *Provide transparent information authorization for entities involved in related-party transactions*

   A BaaS service user is not an independent entity that exists in isolation. Once a BaaS user generates a relationship with other users, the authentication, authorization and query functions within their digital identity will be activated. This gives rise to tracking channels between BaaS users, thus providing transactions and cooperation methods backed by credit endorsements.



3.8 Digital Identities and Trading Intermediaries

Any third-party trading intermediary can access the Metaverse blockchain. Its users access its services by registering a digital identity on Metaverse. After digital identity

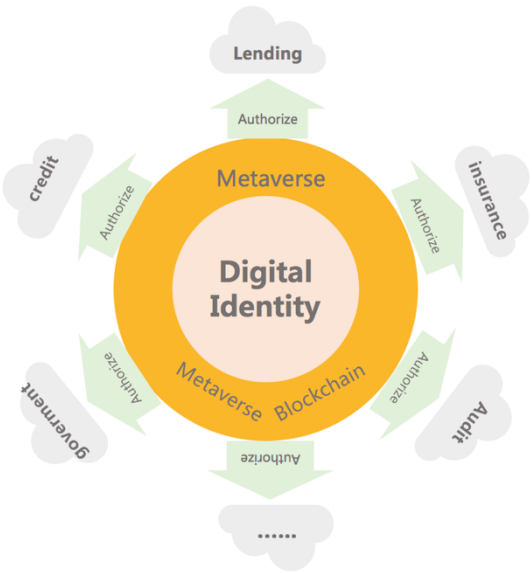
holders authorize the trading intermediary, they can purchase and transfer assets on its platform. Unlike Metaverse's asset transfer service, trading intermediaries focus more on the digital asset's liquidity. In addition, digital identities can implement high-frequency trading and other operations on the intermediary platform. The trading intermediary itself belongs to a class of digital identities that can be called Oracles. In principle, any digital identity can apply to be a trading intermediary, but reputable trading intermediaries (digital identities) will be able to attract more users, lowering their risk exposure.

After users authorize their digital identity, only fund transfer data will be registered on-chain. Transaction data held within the trading intermediary belongs to off-chain data.

To ensure the safe operation of trading platforms and the privacy of their users, Metaverse will introduce separate third-party Oracles in the explorer to endorse trading intermediaries. They will act as notaries between users and trading platforms.

3.9 Application Scenarios for Digital Identities

In practical application scenarios, we need digital identities to authorize companies that may come from various fields. As Metaverse continues to improve upon and expand digital identity functions, its scope of application will also be extended.



3.9.1 Credit Reports

Presently, the credit industry has established a variety of channels to collect credit data. Digital identities provide a portrayal of the user and can return the favor to

the credit industry. As digital identities continue to improve (the number of assets registered, transactions and archival information increase), a person's digital identity is more likely to serve as a main data source, subverting the credit industry's existing ecological model. It connects data networks, opens up other application interfaces and covers more individuals and businesses to improve data sharing and exchange between data owners. It also optimizes resource allocation and significantly enhances the level of risk control. Just as credit itself is part of the infrastructure of many industries, using digital identities as credit is a part of the blockchain industry's infrastructure.

3.9.2 Borrowing

- **Regarding funds**

Digital identities can help their owners evaluate his/her own digital assets and assess their investments based on statistical data. Asset management agencies can access valid digital identities and provide professional financial services for users by customizing a personalized asset management program. Digital identities intrinsically contain data collection and analysis functions, and can track or query the flow of funds through an identity. Additionally, financial management tools can be introduced to help digital identity holders manage their finances and daily cash flows, allowing them to gain a better understanding of their assets through statistical data.

- **Regarding assets**

1. The decision to issue loans can be based on one's digital identity information (activity records and credit status). The focus is on establishing an accurate portrayal of the user and authorizing one's digital identity to the relevant agencies. Thus, lending institutions can obtain all the required information at once and make decisions quickly.

2. Behind a digital identity may be an individual or a business. Hence, digital identities could be used in supply chain management and play a role in the following two areas:

I. Authentication: The verification and authorization functions built into digital identities can help business partners better understand each other's transaction records and asset status, facilitating more accurate business evaluations and credit analysis.

II. Role management: Enterprises can also manage their own digital identities by compiling statistics and performing risk assessment on their own assets and transaction records, helping them better understand their operational status.

In this process, we can perform a comprehensive analysis on digital identities that

belong to core businesses, supply chains and distributors and simplify the supply chain financing process.

3.9.3 Insurance

The most intuitive application of digital identities is in the insurance industry, because its services are directly linked to personal information. As traditional insurance corporations become more reliant on the Internet and more insurance verticals emerge, insurance companies have an incentive to track policyholders' digital identities. The effect of this is reflected in the following:

- Underwriting and approval: risk assessments can be performed on the digital identities of the insured, and information registered on-chain such as medical records, employment status and asset value can be retrieved quickly. The insurance company can eventually classify its customers by risk level and decide on detailed terms and conditions through digital identities.
- Claims settlement: policies can be treated as an asset and registered immutably on-chain under the ownership of a digital identity. If accidents occur, the insurance company can then pay off the insurance compensation to the relevant persons according to the policy's details.

3.9.4 Audit

An enterprise registers its own digital identity; all its employees (including management and general staff) can also register their digital identities and authorize it to the enterprise or its shareholders. This will benefit shareholders by helping them understand the trustworthiness of their partners and employees.

In an audit of an company by external agencies, auditors can similar leverage verification and authentication functions to view the company's asset status on the blockchain (e.g. receivables and payables). This can be combined with BaaS services. Relevant auditors can also monitor the company's accounts through real-time tracking of blocks and use the information to issue asset descriptions as well as related audit reports. Compared to traditional audit strategies, assets registered on-chain are already endorsed by Oracle authorities, simplifying the tedious audit process. It also reduces auditing firms' reliance on auditors and their employee costs while increasing their degree of automation.

3.9.5 Government

Governments can record their citizen's personal identification information on the Metaverse blockchain, including but not limited to: identification numbers (such as IDs, passports and driver's licenses), biometric information (such as fingerprints and facial features) and personal archive information (such as academic

qualifications, relatives, criminal records and other information). In this process, governments and other authorities can be regarded as Oracles. This dataset forms the data-feed portion of a digital identity.

In many situations, such as security checks at the airport or candidate admission during exams, the inspectors present can personally verify the information present on one's digital identity. If one passes the biometric checks and gives his authorization, the inspector can retrieve all relevant information including other records associated with one's biometric records. Digital identities can help us:

- Reduce the time required for identity verification: information can be verified through biometric scans when passing through security
- Reduce the cost of identity verification: for example, the police might have to collect biological information for lab verification when pursuing criminals. However, if they require more information, they must make a request for it from other institutions. The use of digital identities would reduce the complexity of this process.

Apart from regulation and law enforcement, governments can also employ digital identities in common governmental activities such as tax registration, voting and IPOs.

4 Conclusion

As Metaverse continues to improve its digital identity system, we will expand applicable infrastructure services in order to engage more third-party developers to build applications based on the Metaverse blockchain, increasing the ease of use of registration and management services for digital assets and identities for ordinary users.

5 References

1. Metaverse Whitepaper: http://newmetaverse.org/white-paper/Metaverse-white-paper-v2.1-EN.pdf

2. Bitcoin Whitepaper: https://bitcoin.org/bitcoin.pdf

3. Metaverse: https://en.wikipedia.org/wiki/Metaverse

4. Delphy Whitepaper: https://delphy.org/papers/Delphy_Whitepaper_EN.pdf

5. Bitshare Whitepaper: http://docs.bitshares.org/bitshares/papers/index.html

6. Augur Project: https://augur.net

7. IPFS Whitepaper: https://ipfs.io

8. Waves Project: http://www.wavesplatform.com/downloads.html

9. Bitcoin Days Destroyed: https://en.bitcoin.it/wiki/Bitcoin_Days_Destroyed