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

Metaverse Project (In short MVS, Yuanjie in Chinese)

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

Digital identities will be based on the Metaverse ecosystem and its underlying functions. Its applications will be centered around BaaS and the Metaverse Wallet, aiming to offer verifiable and authoritative infrastructure services for all walks of life.

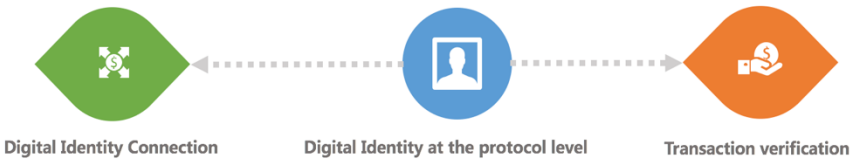
1 Introduction

Questions about identity often begin with “who are you?”. The rise of the Internet has made digital identity applications more prevalent in various industries. At the same time, corporations and individuals are becoming increasingly aware of its importance. As interactions between the public and service providers increase, usernames and passwords have become a common method of digital identity authentication. However, there are some problems with this. For example, a database environment is needed to build relationships with a variety of centralized institutions, but some identity providers with poor cybersecurity systems are vulnerable to attack. In addition, due to the lack of interoperability among current identification systems, repeated register problems also arise. One is repeatedly asked to provide his/her identity to various institutions, which wastes time and resources.

Many current business models, processes and solutions did not exist before the rise of emerging technologies. Among those, the most ground-breaking one is blockchain technology, which like the Internet has the potential to change many industries. First used by Bitcoin, blockchain is now looking for solutions for the financial, supply chain management and anti-counterfeit industries. Most importantly, experts in the field of blockchain technology are now studying its digital identity applications. Currently, more than 40 blockchain projects are being researched. Regardless of whether these applications are built on public blockchains or integrate public key infrastructure (PKI) with blockchain, digital identity still has a long way to go.

1.1 Identity Issues: Blockchain’s Missing Link

There are a number of different blockchain protocols and implementations in the current blockchain ecosystem. All identity issues must follow this process: to prove who owns what, and who does what with whom. While anonymity has some advantages in certain protocols such as Bitcoin, it will not be a powerful trait when blockchain technology and its applications are implemented globally. We need to know what we are dealing with, and we identify people by their names rather than a string of numbers. The ‘missing link’ in blockchains is hence identity, which is often overlooked in many public blockchain protocols: it would allow the concept of digital assets to flourish and financial applications to demonstrate their full potential in online banking and other financial institutions.



Therefore, it is meaningful to embed digital identity at the protocol level, which makes it easier for users to build verification functions for applications on a public blockchain. Additionally, we have noticed the value of inviting intermediaries to the blockchain because they play a key role in corroborating and verifying people's claims by using digital identity.

2 Digital Identities (Avatar)

2.1 Metaverse Introduction

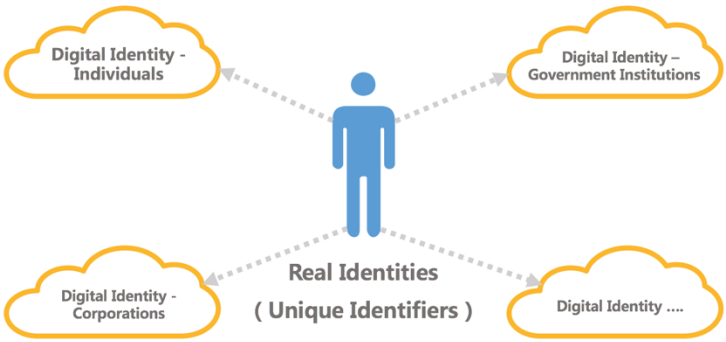
Metaverse aims to provide safe and convenient infrastructure services based on blockchain technology for a wide range of users, including individuals, corporations and government institutions. Composed of three pillars, i.e., Digital Assets, Digital Identities and Value Intermediaries (Oracles), Metaverse intends to build a web of smart properties. Metaverse follows the object-oriented programming paradigm so that users can easily use our smart network. These three pillars will support all decentralized applications at the protocol level on Metaverse.

As our lives become more digital, Metaverse and these three pillars will leverage the advantages of the Internet to pave the way for an inevitable virtual world. Digital identity holders will be able to manage any type of asset easily and allow businesses and communities to support themselves in many ways, ultimately leading us to the internet of value.

2.2 The Essence of Digital Identity

Digital Identities in Metaverse are unique because their modules are embedded in Metaverse's protocols and supporting applications have been developed for them. Users have a defined autonomous identity - they are in full control of their identities, and hence need not rely on any central entity or third party for identity verification. They can create, sign, and verify claims and make transactions, while other people who interact with users can help the user prove their identities. In addition, users with autonomous digital identities can selectively disclose their information.

Digital identities are an integral part of the virtual world and can take many forms, such as that of individuals or value intermediaries (institutions and entities). Therefore, individuals can have different digital identities in different scenarios (workplace or other places), but all in fact will be supported by their true identities.



Digital identities can establish a reputation on Metaverse, and will also improve the way we exchange value. Through digital signatures and authenticating claims and transactions, digital identities gradually build up a reputation which can then be inspected or verified by other digital identities and value intermediaries in the market. Regarding some centralized entities, if their servers crash, the identities and reputations established by their users over the years will disappear permanently. 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 had 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 the field of digital rights. Digital assets that are issued by a digital identity and possess multiple credentials will be more valuable in the market, thereby facilitating the transfer of different types of value other than from encrypted digital currencies. End users will be able to use their digital identity to claim copyrights and other assets. Apart from authorizing certification information, users can also authorize others to access their 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;
Like digital asset ledgers in Metaverse, the design of digital identity ledgers is based on ETP transaction implementation;
After analyzing a large number of cases, we found that the core functions of digital identities only include identity verification and operation authorization.

Design goals:

- Digital identities can reflect their relationship with digital assets – interrelationship between assets;
- Digital identities can correspond to off-chain data, and through this relationship display the Oracle's credit endorsement characteristics - Data-feed;
- Digital identities can manage the identity information uniformly held by a number of Internet applications - application management;
- Digital identities can provide immutable credit datasets – credit data collection;

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 called 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 with no additional storage required.
- ✧ Asset information
  - Kept on the statistical level, contains UTXO details with no additional storage required.
- ✧ Customized description field
  - The customized field has a validity period, and the specific height interval where the field is valid should be pointed out. This field can be changed 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” portion below.)

3.2 The Operating Procedure of Digital Identities

3.2.1 Creation

Any user can create a digital identity and bind it with 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 access to any of its functionalities or applications.

Master private key holders who have registered their asset on the Metaverse blockchain can also choose not to bind any digital identities. Users must take initiative, because Metaverse does not automatically create digital identities for any user. The decision to bind a DID lies with the master private key’s holder.

3.2.2 Verification

Profiles can provide effective chains of proof that demonstrate objective facts of any specified digital identity. For users, they first need to prove that a digital identity belongs to them by binding the 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: authorization is often related to transactions. Assume A requests to inspect B’s digital identity information (asset information) before providing any services. There are two possibilities:

1. B has large amounts of assets on-chain, more than 1 million ETP. B can simply disclose his asset information to A.
2. B has few on-chain assets, but many off-chain assets. The traditional approach is for B to convert assets to ETP for authorization. Currently, Metaverse recommends that users issue their assets and get them verified by an Oracle, after which they will be registered as valid assets belonging to one’s digital identity.

- Authorization process:

A sends a request to B which triggers a script that verifies the asset information of the target account, then sends A’s encrypted result back. B is unable to know which result contains information corresponding to the asset verification. Additionally, the initial request is also encrypted. Thus, B does not know the specific request of A, only what information was requested. Personal transaction and asset records can be accessed after permission is given on-

chain, but the basic principle remains unchanged.

Personal customized fields are similar to assets that undergo Oracle authentication (information that has not been approved by an Oracle can still be authorized, but this is not recommended).

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

- Authentication process:

The 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, and these organizations should publish their own profile and DID information on the official website.

Firstly, B fills in the customizable field with information that needs to be proved. 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 field's information (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

Since the concept of DIDs has been introduced by digital identities at the beginning, DIDs can be used to conduct over-the-counter (OTC) trades with its ability to create transactions in the trading market.

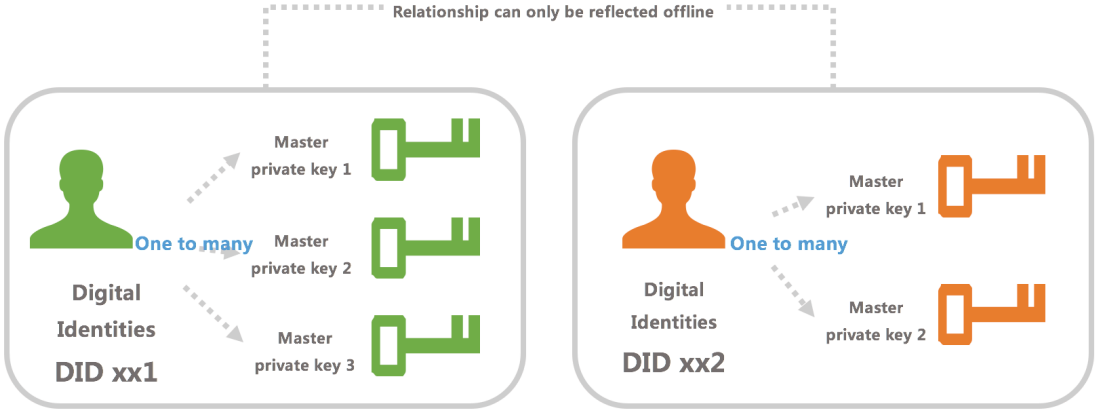
We can query a DID's current transaction requests and past transactions in the open market by entering the DID into the address query bar in the trading market. Conversely, a DID's behavior and records in the market can be used as data to build digital identities.

The Asset explorer contains more detailed content as compared to traditional blockchain explorers, and the latter is a subset of the former.

3.3 Asset Association Relationship

Digital identities have a one-to-many relationship with master private keys: one digital identity can correspond to multiple master private keys. Digital identities and assets must also be in a one-to-many relationship which means 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 demonstrated off-chain. For example, digital identity A and B both own one digital asset – A and B company respectively. If company A acquires company B, company B can be declared as company A's subsidiary off-chain, but there is no way to reflect this subsidiary relationship (digital identity B belonging to digital identity A) on-chain.

Assets belonging to a digital identity can be transferred to another digital identity. However, this transfer serves only as credit rating data and is unable to reflect any relationship that may exist between the two digital identities.

3.3.2 The relationship between the digital identities and assets

The relationship between digital identities and assets is reflected in the transfer of assets between them. In the example above where company A acquires company B, B's tokens will be transferred to company A's online address after they come to an agreement, after which asset registration is completed. At this time, digital identity B no longer holds the assets of Company B, while digital identity A is composed of both company A and B.

3.4 Off-chain Data Management: Data-feed

- Off-chain data and asset registration

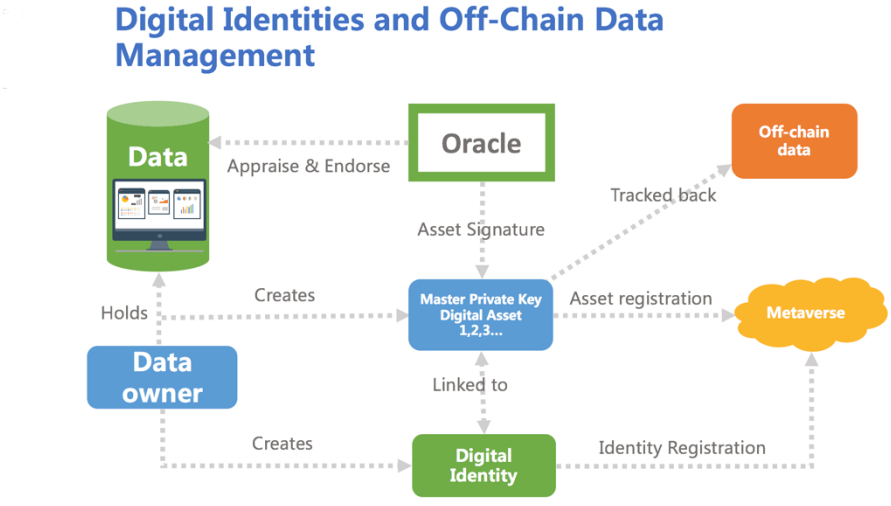
Off-chain data refers to data that is not recorded on the blockchain, by all accounts data that is normally massive and has complex structures. Our aim is to link off-chain data and their corresponding digital identities.

This process is similar to patent registration in the real world. After specialized agencies examine and appraise some piece of work created by a knowledgeable worker, those that meet the criteria can be registered as a privilege. 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 eventually harvest the profit.

Likewise, in the ecology of Metaverse, each piece of data should have a corresponding owner. We can regard each piece of data as an asset or a token that contains the details of the data as well as information about its owner. Hence, to ensure the authenticity and effectiveness of this data source, Oracles must be introduced to endorse it. Different types of data will require different Oracles to provide different identification criteria or fields for review. Finally, to indicate a digital asset's validity, an Oracle will use its private key to sign the data. Digital identities will be associated with certain pieces of data after the procedures outlined above are complete, and these pieces of data with specific ownership can be called valid off-chain data.
Registering valid off-chain data associated with a digital identity requires the following four steps:

1, Users with data must establish his/her digital identity on Metaverse, provide data with the user-defined format, and submit this data to an Oracle who is responsible for data authentication and endorsement.
2, Oracles (a digital identity) qualified to endorse data will verify the validity and authenticity of the submitted data;
3, After the data is signed by its owner and an Oracle, it will be bound with the owner's digital identity through master private keys.
4, Other users can view detailed information about this data after the data's owner gives his authorization.



We know that certain types of equity can generate gains when they are being held. In Metaverse, because digital assets are associated with off-chain data, digital assets can bring similar gains to its owners. Digitizing off-chain data lends it liquidity, and the data can be portioned out or held by multiple digital identities. Shareholders of digital assets can resell their potion to other digital

identities.

- Off-chain data and market forecasts

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

3.5 Application Management

In conventional Internet applications, databases are centrally managed causing account and account asset information to be unable to flow between different platforms. For example, one cannot log in to the WeChat application with an Alipay account, and one's asset balance in WeChat cannot be used in Alipay.

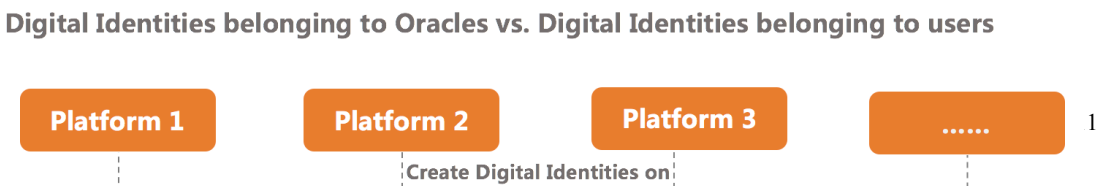
The birth of digital identities will be able to solve these pain points. Users can log in and access different application platforms through just one account at Metaverse. Furthermore, these applications can all access the assets stored in Metaverse Wallet.

In terms of cross-regional (global) applications, users no longer need to be troubled by foreign currency exchange problems, because assets can be directly transferred or used between different platforms.

Application management process:

Firstly, application platforms must register a digital identity on Metaverse and define their own identifier. Then, they should link this identifier with 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 at Metaverse which can then be used to log in to different application platforms. When users log in to other 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 again.



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 AML (Anti-money-laundering) and KYC (know your customer) compliance systems. A single digital identity allows users to access various application platforms. Based on the information it is authorized to access and an inbuilt set of rules, application platforms also determine which functions a user may utilize.

Moreover, a user's digital identity is not owned by any centralized application platform. Therefore, digital identity users do not have to worry about their digital identities being deleted or their asset information being leaked or tampered with, because they can selectively grant applications the right to view the information bound to their digital identities. Thus, the ownership and usage rights 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.)

A DID'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 (upon hundred).

Digital identity holders may authorize their DID to third-party applications, which provide price data of these assets on their trading platforms and these data will serve as further statistical basis.

3.6.1Transaction record statistics

Transferring tokens within a Wallet will leave a transaction record searchable on the blockchain explorer. A digital identity owner confirms whether or not to use one or more of his master private keys to create a digital identity. The Wallet can analyze any transaction in any address by accessing data in the blockchain explorer, as well as the transaction information of multiple addresses that belong to the same digital identity following the dimensions outlined below:

- ✧ The transaction volume of each address within a certain time period: is confirmed based on the proportion of total assets represented

- ✧ The transaction value of each address within a certain time period: if the assets have accessed the trading platform, the transaction value of each address in a certain period of time is confirmed by the latest transaction price (eg. the prices of the trading platform can be confirmed in accordance with the price of the daily MA20); if the asset does has not accessed the trading platform, then this value is decided by the trading prices of tokens (such as ETP) on the trading platform at the time it is transferred. ETP price confirmation mechanism is the same as above.

3.6.2 Asset information statistics

Asset information statistics are compiled according to the master private keys corresponding to a DID. This compilation mainly consists of three types of information:

✧ Asset Classification

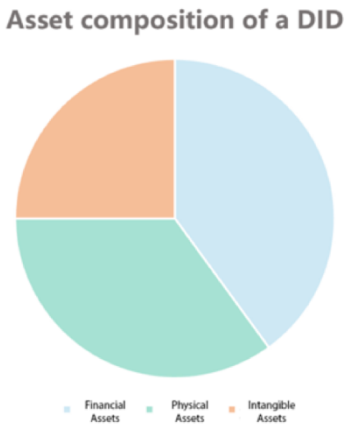
- Financial assets (digital currency, i.e., ETP / BTC / ETH; account receivables and interest rates, derivatives, etc.)
- Physical assets (corresponding to real-world assets, including houses and buildings, transport equipment, machinery, etc.)
- Intangible assets (corresponding to assets without physical representation, including patents, copyrights, land use rights, etc.)

✧ Asset weight within the DID's portfolio: calculate the proportion of financial assets, physical assets and intangible assets within a DID's portfolio.

✧ Asset weight within the entire network: calculate the proportion of financial assets, physical assets and intangible assets in a portfolio, then calculate the weightage of each asset using the last three transaction prices recorded. Assets without transaction records on the blockchain should not be counted into the weightage in order to encourage the flow of assets, since this incentivizes owners to create transaction records on the chain. The following two criteria must be considered:

- 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 Asset identification

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

- Unusual address identification

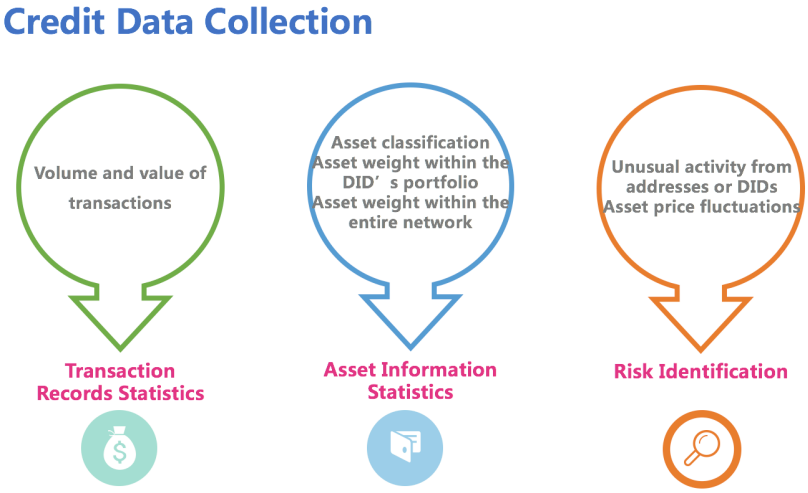
Abnormal behaviors are tagged by collecting reports made by digital identities about addresses. For example, the address may be used for extortion, fraud, etc., it will cost a certain amount of ETP to make a report and each DID can only report an address once. These measures help prevent parties from making malicious address reports. 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 be tagged as abnormal. Additionally, once Oracles update 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, etc., the digital identity itself will also be marked as abnormal.

- Asset value fluctuations

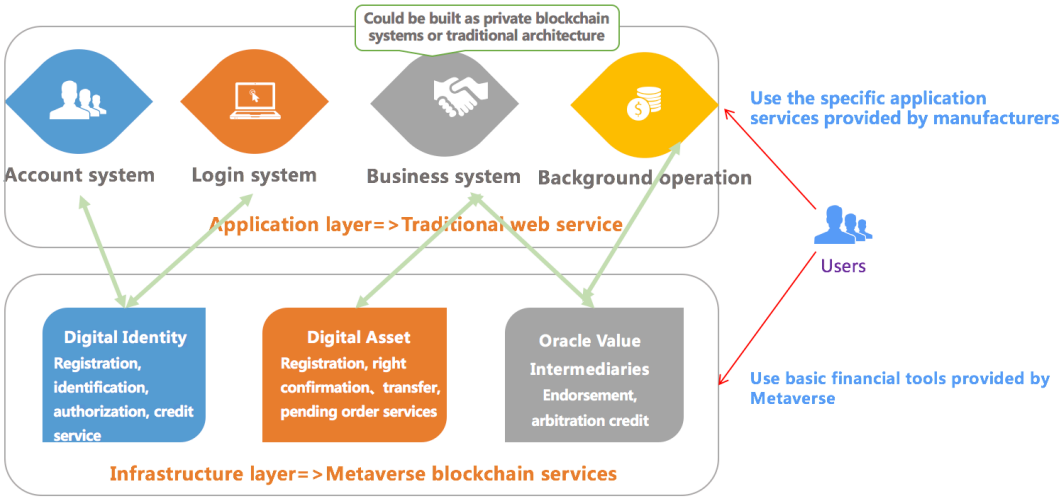
The fluctuation of an asset's value is decided by its daily weighted amplitude in the trading market. Total asset value fluctuation is then calculated based on the weightage of each asset within a digital identity's entire portfolio. Users can set a warning percentage, prompting a risk notification when an asset's amplitude reaches a certain value.



Metaverse does not provide credit ratings, but will provide credit rating agencies with objective & effective datasets

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 customize blockchain services for blockchain solutions providers according to their actual needs.



- User base

Metaverse's BaaS (Blockchain as a service) framework mainly caters to business users, such as individuals or businesses with transaction or asset management needs. As Metaverse's infrastructure continues to improve, its user base will broaden. Business users can no longer be grouped as they traditionally were and BaaS must be able to cater to any user, even digital identities.

- 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

Business users who have transacted with each other can also register assets on the blockchain at Metaverse, which increases the reliability of their digital identities and enhances their validity. Digital identities and BaaS services are interdependent – the digital identities of individuals and businesses help Metaverse with providing BaaS services to enterprises, while the subsequent data and information flows generated can be fed back to digital identities, creating sustainable development and closing the ecological loop.

- BaaS services

1 Object-oriented management based on digital identities

Business users will access BaaS services through their digital identities. Business users who register assets on the blockchain at Metaverse enhance the reliability and validity of the digital identities belonging to themselves and their trading partners.

2 In-depth data mining and examination

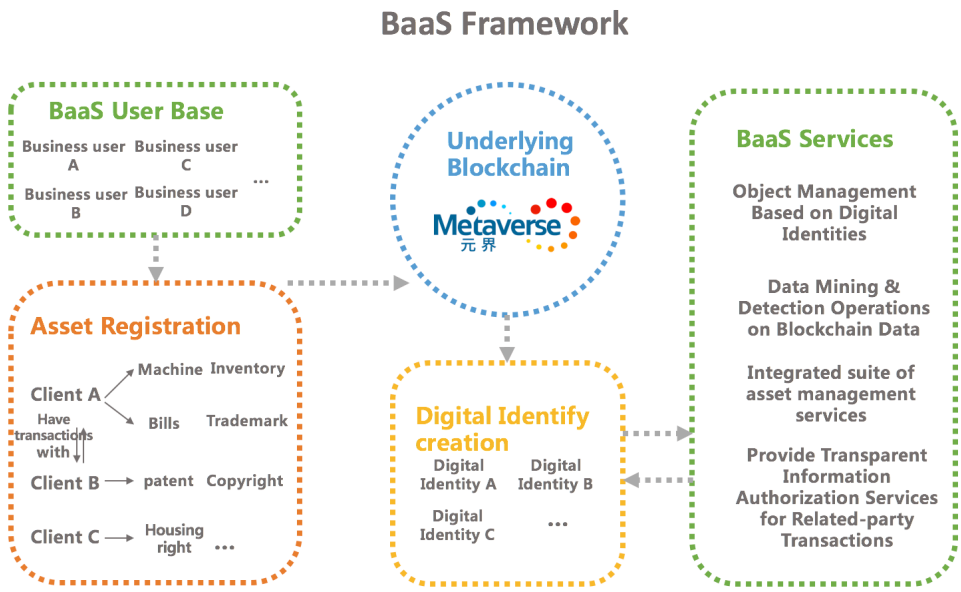
Business users and third parties can make use of Metaverse's digital identity data by mining and examining the contents and transaction history within.

3 Provide integrated and underlying asset management services:

- ✧ BaaS essentially makes use of assets registered by business users on Metaverse blockchain. To some extent, this is a class of asset management services forming part of the underlying infrastructure. Metaverse will provide the basic module framework in its client.
- ✧ In addition to the basic BaaS services provided by Metaverse, there may be more third-parties getting involved in Metaverse blockchain services as a class of auxiliary tools or plugins to help users with optimizing the implementation and management of blockchain services.
- ✧ BaaS services integrate a series of traditional upstream and downstream business services surrounding its ecosystem, emphasizing the integration of data supply and management.

4 Provide transparent information authorization for transacting parties.

The user accepting BaaS services is not an independent individual or an entity that exists in isolation. Once a BaaS user is associated with others, the authentication, authorization and query functions within their digital identity will be activated so that tracking channels exist between BaaS users, thus providing transactions and ways to work together backed by credit endorsements.



3.8 Digital Identity and Trading Intermediaries

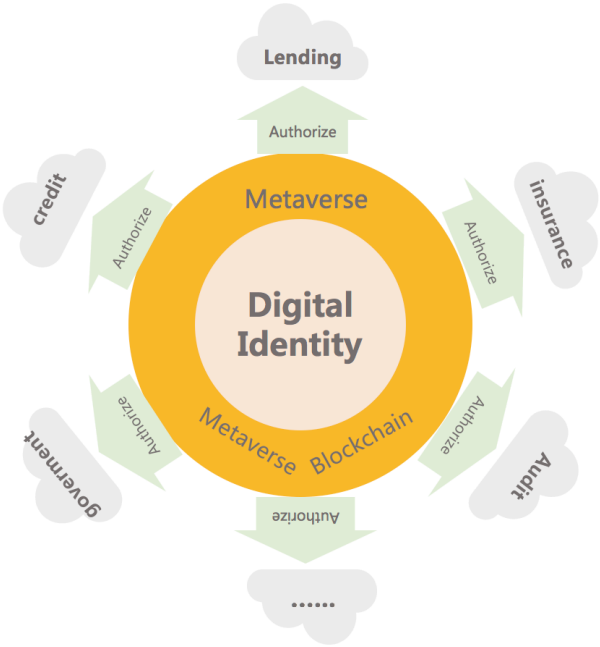
Any third-party trading intermediary can access the Metaverse blockchain, with the participants being digital identities registered on Metaverse. After the digital identity's owner authorizes the trading intermediary, he can purchase and transfer assets on the platform. Unlike Metaverse's asset transfer service, trading intermediaries focus more on the digital asset's liquidity. In addition, digital identities can implement high-frequency trading and other operations. The trading intermediary itself is a digital identity, somewhat like an Oracle. In principle, any digital identity can apply to be a trading intermediary, but a reputable trading intermediary (digital identity) attracts more users in order since it reduces transaction risks.

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

As a means of protecting the operating intermediary's security and user privacy, Metaverse will introduce separate third-party Oracles in the asset explorer to serve as backers for the trading intermediary. They will play the role as notary between users and the trading platform.

3.9 Application Scenarios for Digital Identities

In practical application scenarios, we need to authorize digital identities to companies who request for it. These companies may come from various fields. As Metaverse continually expands and improves upon digital identity functionalities, its scope of application will also be extended.



3.9.1 Credit

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. Furthermore, some financial management tools can also be introduced to help digital identity holders manage their finances and daily cash flows according to compiled statistics.

- Regarding assets:

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.

1) 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 evaluation 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 also thoroughly analyze the digital identities that belong to core businesses, supply chains and distributors and simplify the supply chain financing process.

3.9.3 Insurance

Digital identities are perhaps most intuitively applied in the insurance industry, because its services are directly linked to personal identity information. With traditional insurance corporations becoming more reliant on the Internet, and more insurance verticals emerging, it benefits insurance companies to track consumers who possess a digital identity. Its effectiveness is reflected in the following aspects:

- Underwriting and approval: risk assessments can be performed on the digital identities of the insured to quickly retrieve information including but not limited to: medical records, employment status, asset value, etc. which are registered on-chain. The insurance company can eventually categorize risks and decide on detailed terms and conditions through digital identities.
- Claims settlement: policies can be treated as an asset and registered on-chain, leaving an immutable record belonging to the corresponding 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 can register its own identity, and all the staff within the enterprise from the CEO to the general staff can create their own digital identities and authorize it to the company. This will benefit shareholders by helping them with understanding the trustworthiness of their business partners or employees.

In an audit of an enterprise by an external agency, auditors can similarly be

authorized to view the enterprise's asset status (such as accounts receivable and accounts payable) registered on the blockchain and perform verification. This can be combined with BaaS services. Relevant auditors can monitor the company's accounts through real-time tracking of blocks and issue asset descriptions as well as related audit reports. Compared to traditional audit strategies, assets registered on-chain are already endorsed by Oracles with authority, greatly simplifying the tedious audit process. It also reduces the 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 blockchain, including but not limited to: identification numbers (such as ID, passport and driver's license), 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 could be regarded as Oracles, and this consolidated data constitutes one's digital identity.

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

- Reduce the time required for identity authentication: all information can be verified by a quick scan of one's biological features when passing through the security
- Reduce the cost of identity authentication: for example, when pursuing criminals, the police must collect biological information for lab verification. However, if the police require more information about the criminals, they also need to request for information 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 day-to-day governmental activities such as tax registration, voting and initial listings of enterprises.

4 Conclusion

Metaverse continues to improve its digital identity system and 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 our Wallet and identity management services 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