Abstract

Metaverse™ is the first public blockchain in China, developed by ViewFIn™, a market leader in visionary finance technology. Designed to facilitate low-cost, convenient transfer of digitized personal data and assets with unprecedented security and privacy, Metaverse aims to revolutionize the way financial services and transactions are processed, and to improve outdated and inefficient identity verification services with a network of **Digital Assets**, **Digital Identities**, and **Oracle** intermediaries.

1. Introduction to Metaverse

1.1 A Brief History of Blockchain

In the latter half of the 20th century, the adoption of digital computing and digital record keeping brought about sweeping socio-economic changes. The proliferation of communications technology transformed entire industries, yet some services have been slow adopters of digital record keeping, especially where data is particularly sensitive and/or valuable.

As early as 1998, computer scientists proposed using cryptography to create new ways to store and transfer value--cryptocurrency. For example, Wei Dai helped spark interest with his publication of “b-money, an anonymous, distributed electronic cash system.”[1] Nick Szabo designed a mechanism, never implemented, for a decentralized digital currency he called “bit gold,” as well as for securing contractual relationships over unsecured public networks.[2] After the global financial crisis of 2008, the pseudonymous person or group of persons known as Satoshi Nakamoto published the seminal paper “Bitcoin: A Peer-to-Peer Electronic Cash System” which “would allow online payments to be sent directly from one party to another without the burdens of going through a financial institution.”[3]

The emergence of Bitcoin and its underlying blockchain technology enables the secure transfer of sensitive and valuable information such as personal data and assets while remaining highly accessible and openly verifiable. Blockchains achieve security through decentralized consensus with high Byzantine fault tolerance. While bitcoin is the first digital currency to solve the double-spending problem without the need for a trusted authority, the potential applications of blockchain extend to various records management activities, including identity management, transaction processing, proof of existence, and proof of ownership.

[1] Wei Dai (1998). "B-Money". http://www.weidai.com/bmoney.txt

[2] Nick Szabo (2005). “Bit gold”. https://unenumerated.blogspot.com/2005/12/bit-gold.html; “Formalizing and Securing Relationships on Public Networks” (1997), http://journals.uic.edu/ojs/index.php/fm/article/view/548

[3] http://article.gmane.org/gmane.comp.encryption.general/12588/; https://bitcoin.org/bitcoin.pdf

1.2 Blockchain Evolution

Blockchains are distributed digital ledgers that record data **transparently**, **securely**, and **immutably** by consensus of the entire network. These characteristics give the technology advantages over the centralized databases traditionally used to record information. The centralized approach uses trusted authorities (i.e., banks) to prevent double-spending in online financial transfers. Even the most trusted of these authorities are imperfect: they make mistakes, their databases can be hacked, they have control of personal identity and financial information, and they charge high fees for their services. As the financial crisis of 2008 shows, traditional financial institutions do not always behave responsibly. Their monopoly on global finance is being challenged by the emergence of fintech.

With blockchain, the ledger is maintained and authenticated not by central authority but by distributed consensus among all the computers on a network powered by collective self-interest. The built-in reward system makes transfers inexpensive, while consensus ensures that transfers are immutable and irreversible. Fraudulent transactions are prohibitively expensive--the larger the network, the more resources required to attack it, and the cost of doing so is much greater than the reward--thus ensuring network security. Data are transparently recorded to the ledger so that everyone on the network can verify and audit transactions at low cost. At the same time, data are encrypted so that a high level of privacy is maintained.

Beyond Bitcoin: Altcoins

After the success of Bitcoin, a number of alternative coins or “altcoins” began to emerge. While many are simply forks of Bitcoin with minor changes, a few add innovative features that are worth mentioning here. Namecoin, the first of these new coins, was designed as a “decentralized DNS” to register and transfer domain names.[4] Namecoin introduced merged mining, allowing the simultaneous mining of Namecoins and Bitcoins to guarantee network security; extended bitcoin functionality to store data within its own blockchain; and added new transaction types, making it a predecessor of current blockchain-based approaches to digital identity.

Bitcoin’s Proof-of-Work (PoW) consensus algorithm secures the network by rewarding participants for solving cryptographic puzzles. This method has at least two major drawbacks: poor scalability, and wasted energy consumption. Anticipating these issues, Peercoin was the first cryptocurrency to introduce Proof-of-Stake (PoS), a mechanism in which users secure the network using the coins they already hold.[5] While not without issues of its own, PoS “minting” encourages saving and is an energy efficient solution when compared with PoW.

[4] https://github.com/vinced/namecoin

[5] https://talk.peercoin.net/t/what-is-peercoin-intro-important-links/2889

Bitshares

Bitshares improved PoS by implementing the Delegated Proof-of-Stake consensus protocol.[6] In addition, Bitshares introduced digital asset tokens, multiple types of transactions, and user-friendly issuance of digital assets and identities as well as their own decentralized asset exchange. Their numerous innovative features and open platform design offer a range of flexibility, but sacrifice stability of some systems. Metaverse aims to incorporate many of Bitshares' best design elements without sacrificing security and stability, while curating a more efficient set of applications for improved user experience.

Ethereum

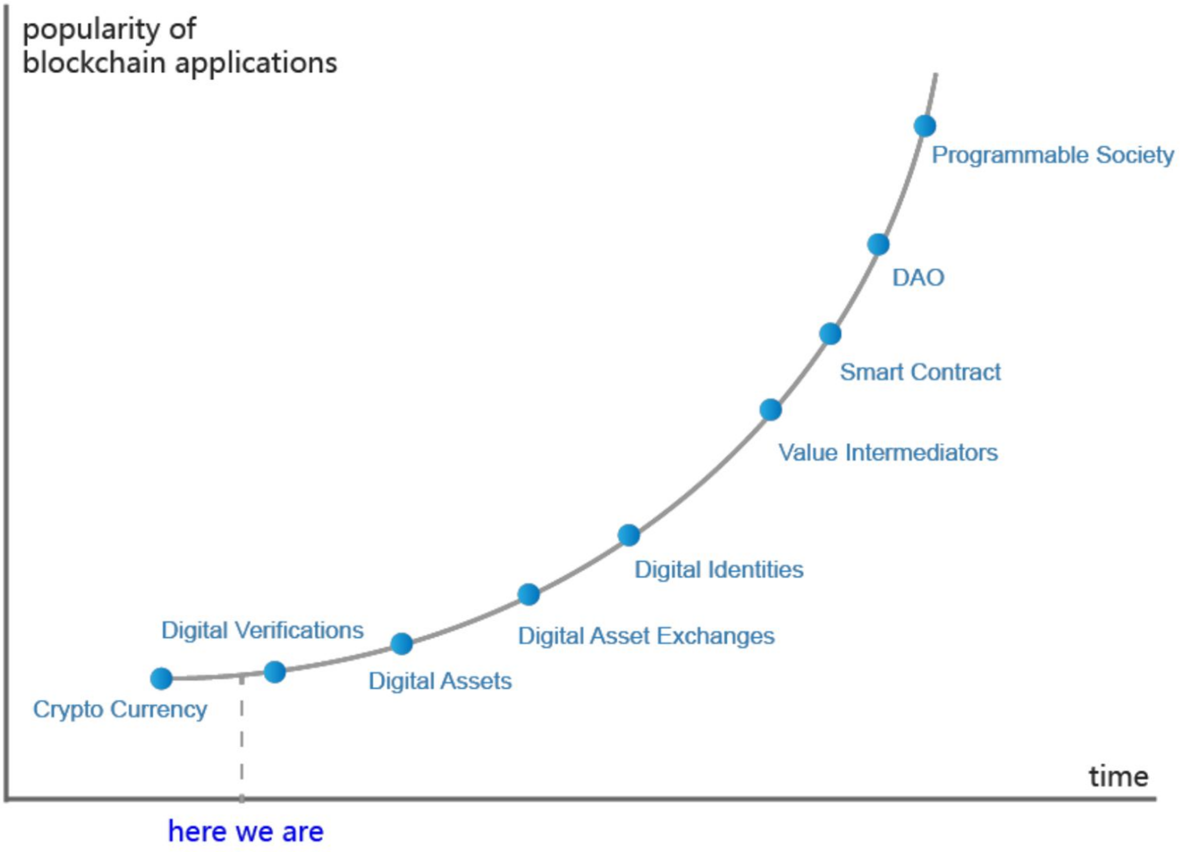
The value stored in blockchain networks is simply information about who owns what--it can be similar to digital cash, like bitcoins, but it can also be extended to other applications by using digital tokens to represent assets, such as securities, commodities, other currencies, and properties. Similarly, smart contracts are code that is uploaded to and executed on the blockchain, allowing the extension of blockchain functionality to software. These decentralized applications, or dApps, are stored immutably and executed automatically when their programmed conditions are met.

The most prominent platform for smart contracts is Ethereum.[7] Coded from scratch and launched in 2016, Ethereum is well-known for its innovative development roadmap, which includes a planned transition from PoW to PoS consensus in 2018. It is also controversial, with issues such as the $50 million hack of The DAO hack and subsequent hard fork. Smart contracts are nevertheless an important contribution to blockchain development.

1.3 Metaverse Roadmap

[6] https://bitshares.org/technology/delegated-proof-of-stake-consensus/

[7] http://ethereum.com



Metaverse is designed to build on the aforementioned contributions and continue evolving with the development of blockchain. The technology is in a nascent stage, and though numerous cryptocurrencies exist only a handful are serious financial tools with potential to change the future. Metaverse is actively developing the next generation of dApps that will revolutionize entire industries and be a powerful force for change.

The term ‘Metaverse’ refers to the future of the internet: “a virtual-reality space in which users can interact with a computer-generated environment and other users.”[8] In this case, however, “virtual” is not a useful distinction, because Metaverse is the network that will connect virtual reality and physical reality: Metaverse is the new reality.

2. Metaverse Economic Model

2.1 The Metaverse Token - Entropy

[8] https://en.wikipedia.org/wiki/Metaverse

Entropy

The token of Metaverse is called Entropy (ETP). A total of 100 million ETP will be eventually be issued, with a minimum unit in 10^{-8} =0.00000001. Security is guaranteed by ECDSA(elliptic curve digital signature algorithm). Entropy will be used to measure value of smart properties in Metaverse or used as collateral in financial transactions. Meanwhile, the ETP will be used whenever system fees are applied on Metaverse, i.e. to create a new Smart Property, register a new Avatar, apply to become an Oracle, or to invite institutions on Metaverse to verify the assets mentioned above and identity.

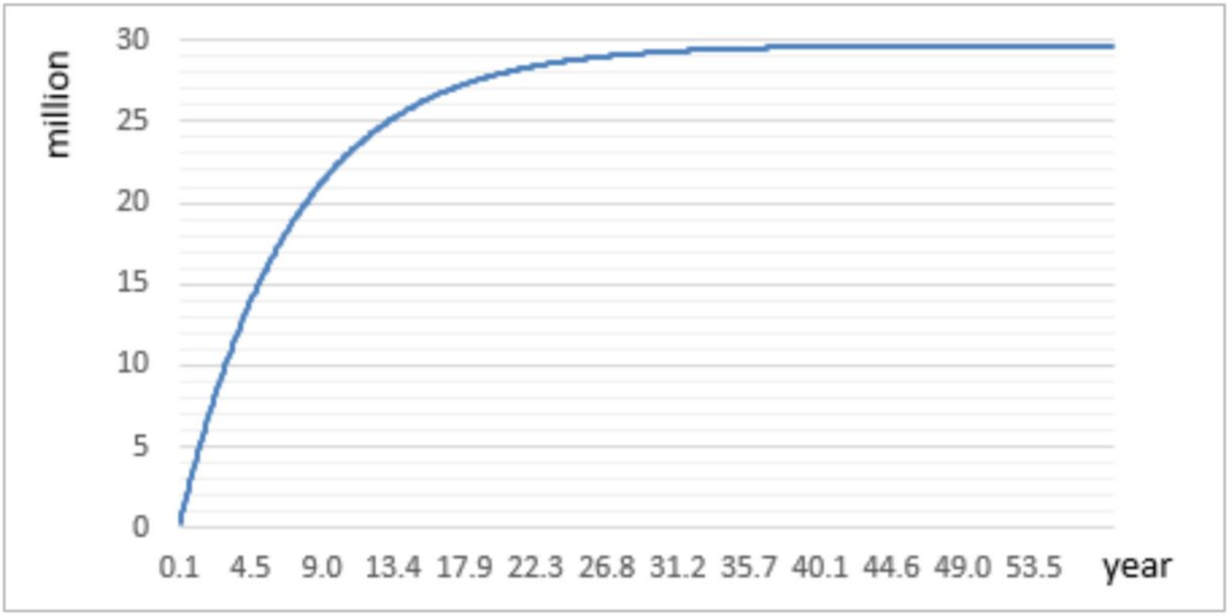
Issuing ETP

(1) ICO and community construction

Initial Coin Offerings (ICOs) are a new form of crowdfunding that also distribute blockchain tokens. Metaverse will distribute half of the total 100-million tokens in two successive ICOs: about 25% in August 2016, and another ~25% after the Metaverse mainnet comes online in late 2017. The other half of ETP will be distributed through mining.

(2) Proof-of-Work mining

The block difficulty of Metaverse will increase as the computing power of the whole network grows, with target block speed of 23 seconds and mining reward of 3 ETP. A total of 30 million ETP are allocated for PoW mining:



(3) Proof-of-Stake minting

Metaverse is currently developing a new Delegated Proof-of-Stake algorithm incorporating token height to solve the design issues resulting from PoW mining (discussed later in Section 5).

For a further step, we will push the vitality of ETP in centralized and decentralized exchange market. The ETP transactions from those markets would be a significant data foundation to the interest rate of ETP, the adjustment parameter of ETP's economic model will be influenced by methods like voting or directly acquiring data from decentralized market. There is chance for the vitality of transactions, numbers of accounts, special transactions to get involved in the parameter.

ETP micro-inflation

Tokens loss may occur for a number of reasons, including accidents, carelessness, or death. In the Ethereum white paper, Vitalik Buterin predicted an annual loss rate of 1%. To provide sufficient liquidity and to accommodate an increasing number of smart properties on Metaverse, we have designed a micro-inflationary linear issuance scheme. After the end of the PoW phase, 4 million ETP will be added to the circulation at the initial rate 4% per year and will gradually trend down towards the 1% annual loss rate.

2.2 Smart Properties

The term "smart contracts," coined by Nick Szabo in 1994, is "a computerized transaction protocol that executes the terms of a contract."[9] The most prominent implementation is Ethereum, although Namecoin and other platforms also implement smart contract technology. Digital assets generally require smart contracts to come into existence. In Metaverse, however, contracts require properties--**Smart Properties**--not the other way around. Thus, transactions involving Smart Properties in Metaverse will require minimal coding, and smart contracts will be implemented only when complex transactions are involved.

Registration of SmartAssets

The registration of SmartAssets takes several questions into considerations:

(1) Why do we register SmartAssets?

[9] Tapscott, Don; Tapscott, Alex (May 2016). The Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World. pp. 72.

One of the value of blockchain is that it offers a data storage that could be public shared: but append-only with timestamps, and not allowed to operate modification and cancelation to the past records (notice that it says “not allowed” rather than “not possible”, but in the real calculation, the possibility of getting canceled and modified is low for the essence of the technology of blockchain).

This property fulfills the design requirement of registration, which is public, unique and trustworthy. In this case it is not only that the registration of SmartAssets need to get on the top of the blockchain, but other valuable data seeking some kind of storage scheme have good reason to get on the top of the blockchain.

(2) How to design the function for registration of SmartAssets?

The first step to registration of SmartAssets is to find a set of data that could describe an asset with two key characteristics:

A. this set of assets should be reusable
B. command sets should be designed with potential future applications in mind.

SmartAsset registration form template:

Category	**SmartAssets**	**Explanation**
General attributes	Identification	Unique identification of s series of character string to that asset
	Totality	The validate basic attributes to verify the asset during transactions
	Minimum units	
Special attributes	Description	The locations to deposit special attributes

Registration will incur a small fee weighted by the value of ETP in Metaverse. A fixed rate of transaction fees will be recycled back into the Metaverse development community, while the rest will be distributed as mining fees.

(3) What can you do after registration of SmartAssets?

The registration of SmartAssets confers proof-of-existence on the Metaverse blockchain. Once verified by an Oracle, discussed below, the asset gains value and auditability. Value depends on market price, while auditability adds constraint conditions to property transactions in real life (based on Smart Contract and scripting language of business).

2.3 Avatars - Digital Identity

Smart Properties require owners--**Avatars**--or digital identities, which may be individuals, organizations, or computer programs among others. Most real world activities require some level of personal identification information. In Metaverse, personal data are encrypted onto the blockchain and verifiable through zero-knowledge proof on a need-to-know basis, that is, at its owner's discretion.

Each user may have multiple Avatars serving different functions. One Avatar may own multiple smart properties, while ownership of one property may be shared amongst many Avatars. ***Then, let the party of trading, lending, renting, leasing and mortgaging start.***

Data Sovereignty

Avatars return control and sovereignty of personal identity information to the user. Currently, digital identity relies on users giving up control of their personal information to service providers, many of whom then sell the accumulated personal data to advertisers, PR and marketing firms, or anyone else who wants to acquire this information--for a price. This means that essentially all "free-to-use" services are not truly "free": users are paying for the service by giving up their privacy and their sovereignty over personal data.

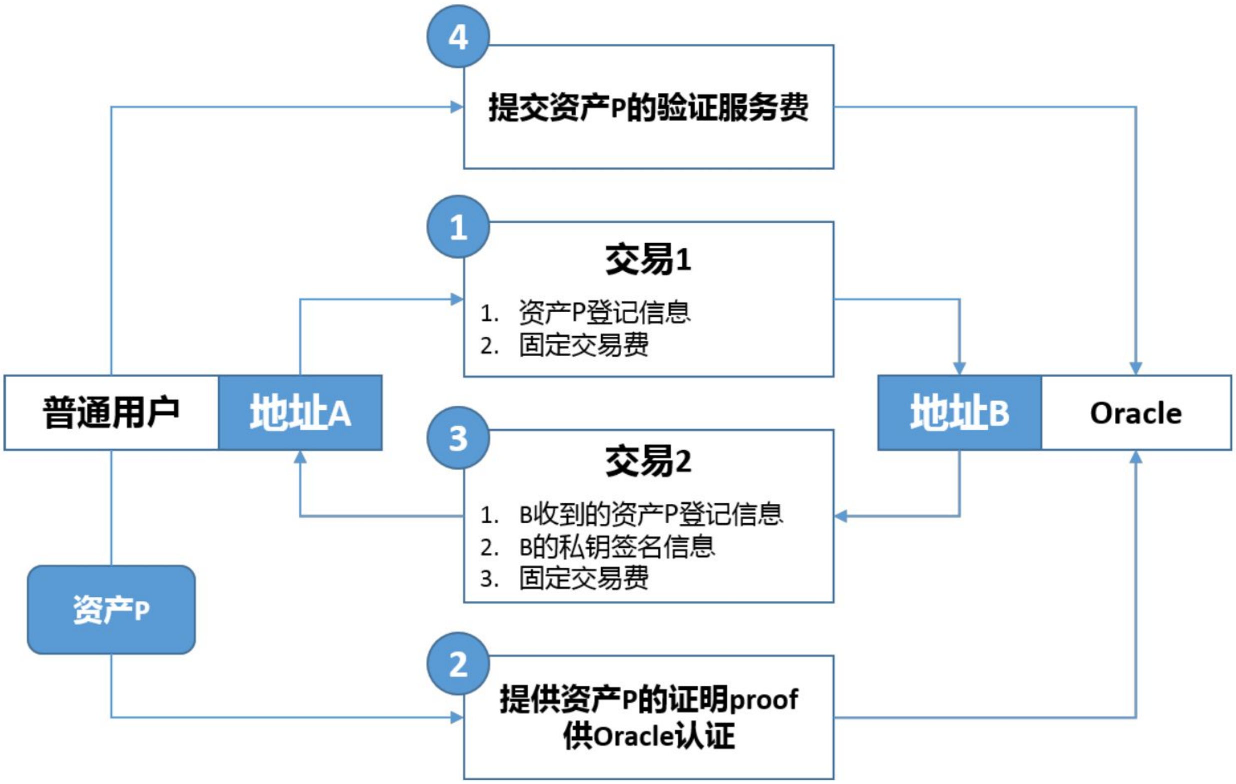
In Metaverse, digital identity is treated as a form of intellectual property. By putting sovereignty back into the user's hands, the user decides who can interact with what personal information and for what price. Furthermore, Avatars mean that once personal identification information is verified by an Oracle, that information is stored immutably on the blockchain and the verification status is publicly accessible without releasing private data. In other words, sensitive personal information (such as bank account numbers, government ID, credit cards, etc.) need be verified only once. Services will be able to trust the third-party Oracle that a given Avatar's information is accurate and truthful, in other words, that this person is who he says he is, without needing to verify independently every time new services requiring personal information are used. This promises to reduce costs by streamlining the entire Know-Your-Customer (KYC) supply chain for entire industries.

2.4 Oracles - Value Intermediary

In Metaverse, **intermediary institutions (Oracles) are invited on-chain to ensure that all information shared, stored, and provided by members of the community is trustworthy and reliable**. For instance, Manager Oracles will handle physical assets and upload digital assets to the blockchain. Identity Oracles can verify and upload personal information to online

Avatars. Supervisor Oracles (i.e., for special transactions and government agencies) will verify the authenticity and compliance of transactions. In addition, there are many other possible functions and services that Oracles can bring to the Metaverse ecosystem, such as enriching the types of possible transactions and enhancing the value of the blockchain.

Blockchain technology makes claims it will disintermediate, or “cut out the middleman” entirely. At the moment, this seems like a fantasy. We believe that intermediaries will continue play an important role for some time to come. As critical thinking is not yet programmable, we still depend on intermediaries to apply sound judgement, determine value, and verify our actions.



3. Metaverse Design Principles

3.1 Minimalist Design

In high-level design, we focus on keeping the underlying core functions as simple as possible, expanding only when necessary in order to minimize complexity.

3.2 Stable Evolution

As MVS evolves only two cases require MIP:

- Enhancing core functions; and
- Repairing security issues

In any case, MIP should have a minimal impact on the underlying architecture.

3.3 Compatibility

MVS version must be backward compatible and fully support platform operation.

3.4 Modular Design

Hierarchical sub-modules to reduce the level of coupling between modules, primarily implemented with Libbitcoin.

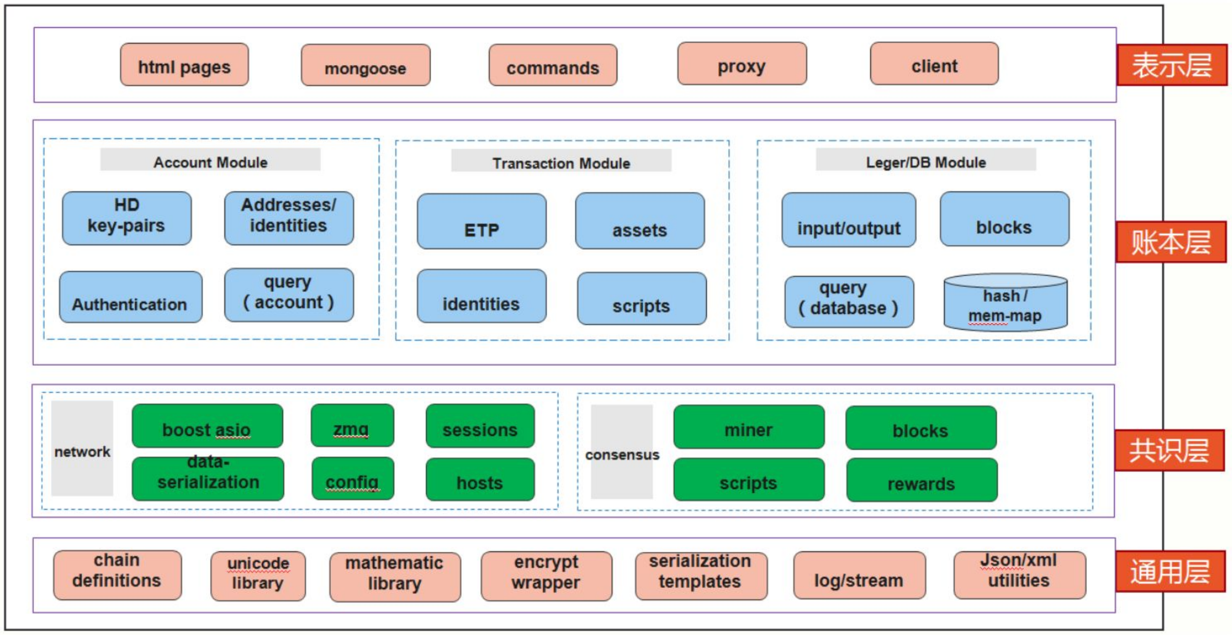
4. Metaverse Design Architecture

Metaverse development is divided into the following two phases:

First Phase: the Metaverse consensus algorithm will be based on Proof-of-Work. It will mainly provide the following: digital identity, digital asset registration and transactions, simple built-in scripts, datafeed, and credit evaluation among other functions. Metaverse can be used to support all affiliated blockchains, forming an open platform ecosystem.

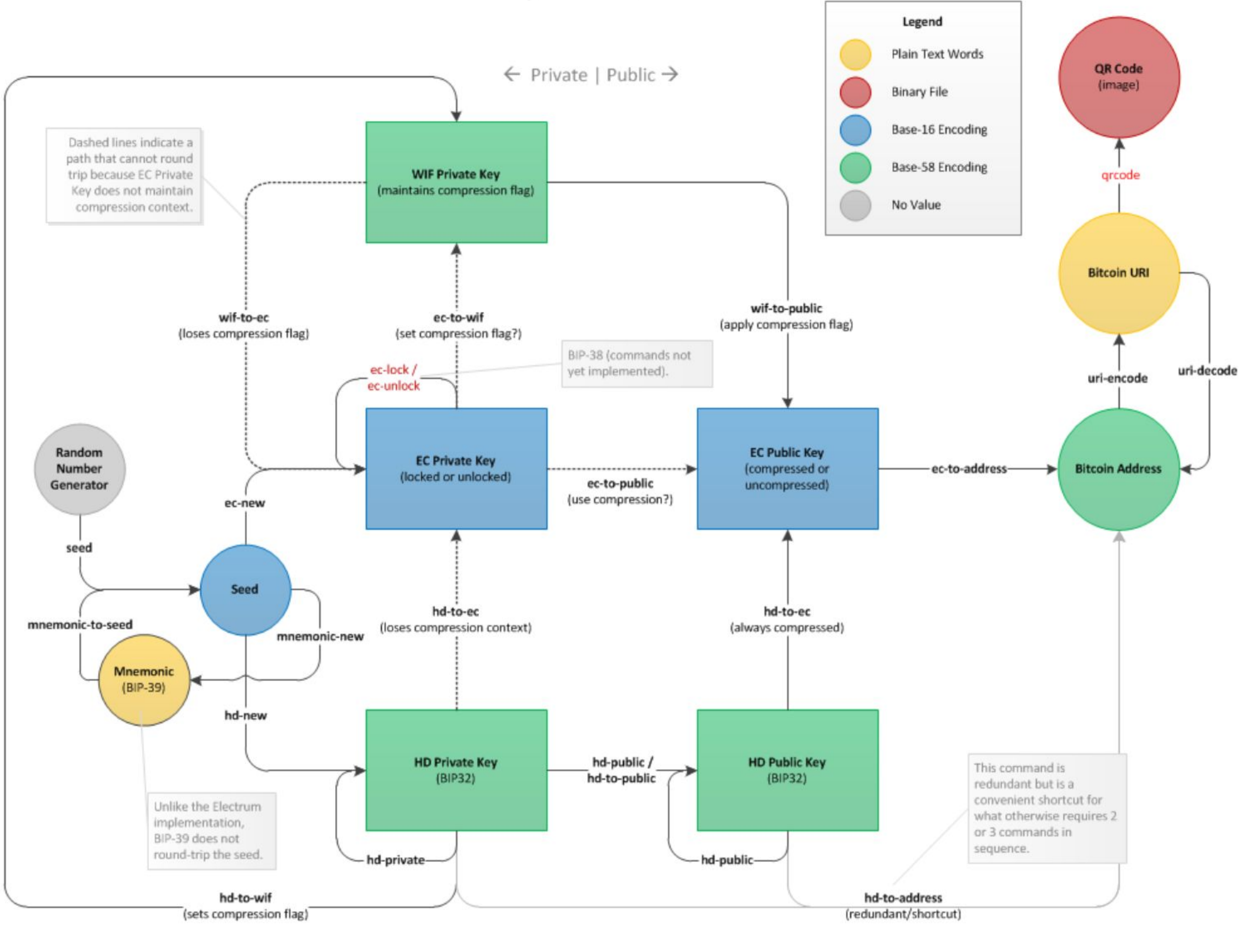
Second Phase: Metaverse will shift to a DPoS-based consensus algorithm. Building upon the ecosystem consolidated in the first phase, it will expand smart contract functions to provide complete Oracle services.

v0.2版架构图如下图所示：



html pages: 元界的前端页面，主要为浏览器端提供；

Explorer - Wallet Commands

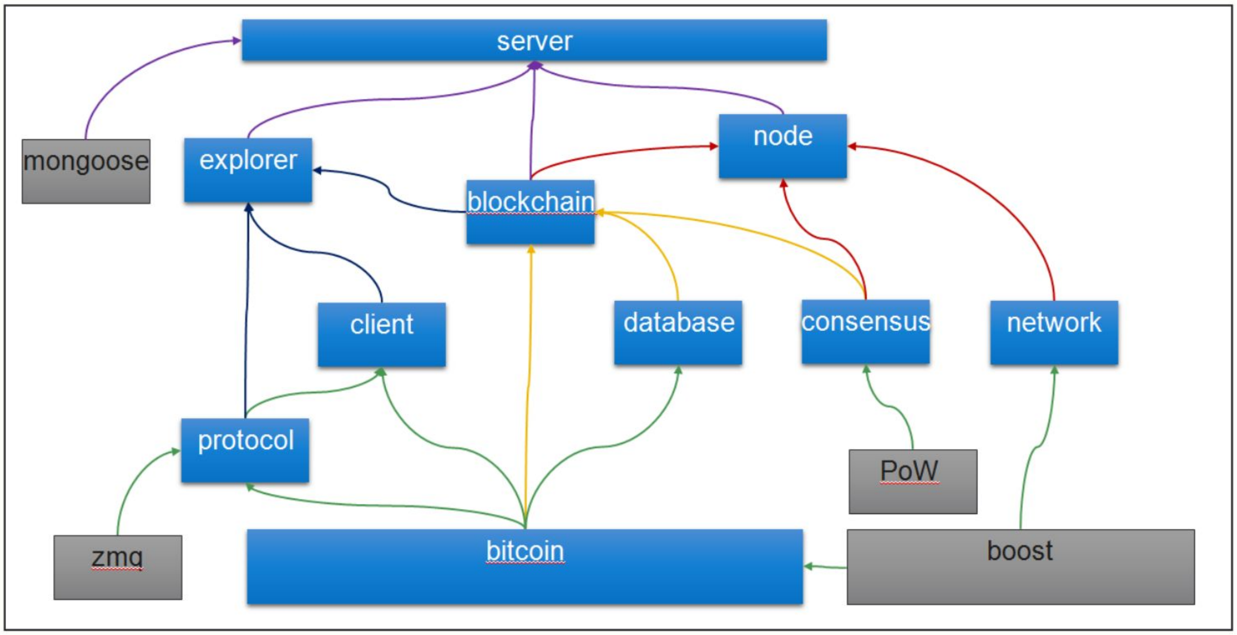

Legend
Plain Text Words
Binary File
Base-16 Encoding
Base-58 Encoding
No Value
← Private | Public →
QR Code (image)
qrcode
Bitcoin URI
uri-encode
uri-decode
Bitcoin Address
WIF Private Key (maintains compression flag)
wif-to-ec (loses compression flag)
ec-to-wif (set compression flag?)
wif-to-public (apply compression flag)
ec-lock / ec-unlock
EC Private Key (locked or unlocked)
ec-to-public (use compression?)
EC Public Key (compressed or uncompressed)
ec-to-address
Random Number Generator
seed
ec-new
Seed
mnemonic-to-seed
mnemonic-new
Mnemonic (BIP-39)
hd-new
hd-to-ec (loses compression context)
hd-to-ec (always compressed)
HD Private Key (BIP32)
hd-public / hd-to-public
HD Public Key (BIP32)
hd-private
hd-public
hd-to-wif (sets compression flag)
hd-to-address (redundant/shortcut)

Dashed lines indicate a path that cannot round trip because EC Private Key does not maintain compression context.

BIP-38 (commands not yet implemented).

Unlike the Electrum implementation, BIP-39 does not round-trip the seed.

This command is redundant but is a convenient shortcut for what otherwise requires 2 or 3 commands in sequence.



5 MVS Consensus Algorithm and Token Model

5.1 Consensus

The consensus process refers to how all transaction data on the network are recorded, securely and immutably, on the blockchain. Currently, there are several prominent consensus algorithms for public blockchains, including Proof of Work (PoW) first used by Bitcoin, Proof-of-Stake (PoS) first used by Peercoin, Delegated Proof-of-Stake (DPoS) first used by Bitshares, and various other forms of Byzantine Fault Tolerance (BFT).

These algorithms secure the blockchain by creating an economic incentive structure that rewards honest actors and discourages malicious actors. They ensure that cheating is unprofitable, as the cost of cheating is much greater than the reward of honest mining, thus ensuring stability and security.

Although the original PoW algorithm developed in Satoshi Nakamoto's Bitcoin whitepaper made an important contribution to computer science by solving the Byzantine Generals Problem, most cryptocurrencies today bypass the BFT algorithm as it doesn't solve the issue of token distribution. Metaverse distributes Entropy (ETP) tokens to miners as incentive for securing the network.

For the early stage of any blockchain project, network is small enough that it is vulnerable to a 51% attack. Therefore, in the first phase of Metaverse development ETP will be issued to miners as reward for PoW. As Metaverse grows and the number of full node miners increases, Metaverse will transition to a modified DPoS consensus algorithm that takes into account transaction volume.

PoW Mining

The first phase of Entropy distribution will employ GPU mining for several years to ensure network security and implement a decentralised timestamp server system. As the Metaverse blockchain grows, the PoW algorithm will encounter a number of issues, including:

- cost of electricity (wasted resources);
- mining centralisation;
- speed and scalability bottlenecks, etc.

HBTH-DPoS

To overcome the limitations of PoW mining, Metaverse will transition to a Delegated Proof-of-Stake (DPoS) model as it matures. DPoS was first adopted by Bitshares as a more robust and decentralised consensus algorithm than PoW and PoS. More importantly, DPoS distributes voting rights more equitably to its participants than alternative models.

Two major issues arise with DPoS consensus. First, financial interference: by acquiring a majority of tokens, delegates can interfere by voting for harmful protocol changes or manipulating the token price for short-term profit. For example, it would take *N $* to acquire majority stake in *X blockchain* and change the underlying design for profit or render it useless.[10]

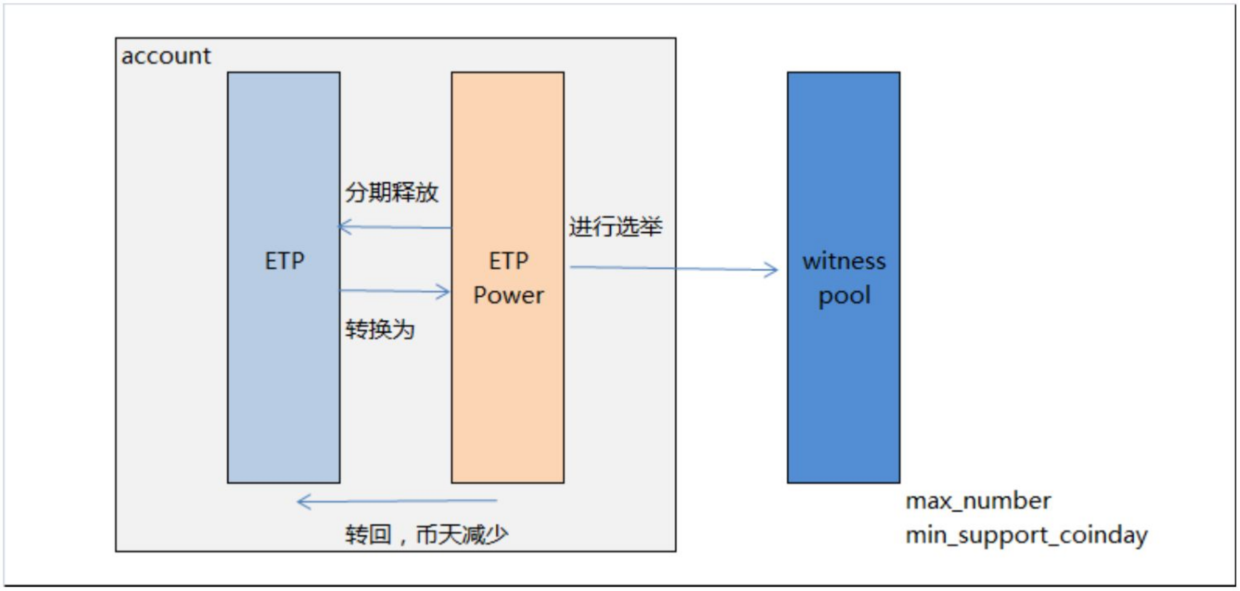
Second, voter apathy: as voters (users) are not usually personally invested in how the underlying system functions, most transfer their votes to delegates and are unlikely to monitor potentially malicious delegate behavior. Nowadays, only 1% of voters changed their delegates in the past three months.[11]

Metaverse solves these problems with DPoS consensus by adding Token-Height and HeartBeat. Token-Height is similar to the Bitcoin Days Destroyed concept, which measures the transaction volume of Bitcoin. The number of Bitcoin Days Destroyed is the number of Bitcoins in a transaction multiplied by the number of days since those coins were last spent. Similarly, in Metaverse the Token-Height is calculated as the number of ETPs multiplied by the number of blocks since last spent. By weighting the voting power in DPoS in such a way, Metaverse will prevent financial interference by significantly reducing the voting power of attackers who acquire large amount of ETPs from the market. In order to accumulate enough voting power to make an impact, would-be attackers would either have to acquire much more ETP than 51% attack or hold the ETP for a long period of time to increase its voting power, ensuring that the opportunity cost of such an attack would be prohibitively high.

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

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

[10] Citation needed
[11] Citation needed



To address voter apathy, Metaverse will require stakeholders to send a HeartBeat to prove they are alive and active before claiming new ETPs distributed by the algorithm. HeartBeat is a digital signature from their private key, and stakeholders will choose whether to reelect current delegate or select a new delegate. The benefits of this method are twofold: first, it provides incentive for delegate review; second, it prevents distribution of ETP to ‘dead’ (inactive) tokens, thus mitigating the lost token inflation issue.

5.2 Types of Transactions

Besides transactions on the Coinbase exchange, there is only one other type of bitcoin transaction: transfer of coins between sender and receiver.

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

In Metaverse, we seek a balance between efficiency and user experience. Neither the one-contract-fits-all (Ethereum) nor the half-dozen contract type (Bitshares) model are best for the types of transactions our platform emphasizes from the outset: smart property issuance and digital identity registration. An Ethereum-style transaction type will be added for those transactions that do not fit directly with our smart property, digital identity, ETP-transfer model.

5.3 Accounts

Metaverse combines the Bitcoin UTXO model for ETP transactions with a balance-based model for user-defined digital asset transactions.

5.4 Digital Identity and Data-feed

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

Data-feed is another important function in Metaverse. Unlike Ethereum, in Metaverse the Oracles will be charged with data-feed responsibilities. Their credibility will be based on two factors: (1) their valid credentials; and (2) their records on Metaverse.

The market will provide feedback on their credibility in several ways. First, data-feed users will “vote” through their transaction records. Appropriate votes will accumulate, providing rewards similar to evaluation rebates according to a mechanism that will evolve over subsequent versions. Second, inappropriate votes will be translated into costs according to the voting mechanism.

The reason for this feedback mechanism is that business-level rules should not be hardcoded into Metaverse. All blockchains are bounded by their basic function: consensus. For data-feed, malicious behavior will affect the business itself but not the Metaverse consensus mechanism. Indeed, malicious behavior at the Oracle or BAPP level will still pay fees for consensus, thereby preserving the ecosystem as a whole even if one part fails. On the other hand, a healthy data-feed will be beneficial for all.

6. Challenges

Potential Risks and Concerns

Blockchain technology is still in early stages and remains inherently risky.

Scalability is currently an issue with the Bitcoin blockchain. As the Bitcoin blockchain grows ~1MB every 10 minutes (1GB weekly) the cost of running a full node grows, thus we have seen a decline in the total number of full nodes since about 10,000 in 2013 to roughly 5,500 in mid-2016. While this issue can be mitigated in the near-term with miners, Metaverse will need creative solutions to deal with scalability as the cost of maintaining a full node grows.

Mining centralization poses another risk. While miners secure the network by verifying all transactions securely, the network is vulnerable to 51% attacks. Until the transition to HBTH-DPoS consensus, Metaverse will be , although it can be mitigated through optimisation of the mining algorithm .

As Metaverse grows and becomes successful it may become profitable to sabotage the platform while shorting assets in the exchanges. This depends crucially on a number of factors including the total volume of ETP traded. Thus, the total value of digital assets on Metaverse becomes a function of the cost of defending/attacking the system. Ideally, the total value of digital assets should not exceed 5 times the mining cost under the current PoW scheme.

7. References

1. Bitcoin Whitepaper ——Satoshi Nakamoto http://bitcoin.org/bitcoin.pdf
2. Namecoin: https://namecoin.org/
3. Bitshares whitepaper——Daniel Larimar http://docs.bitshares.org/bitshares/papers/index.html
4. Ethereum WhitePaper——Vitalik Buterin: https://github.com/ethereum/wiki/wiki/White-Paper
5. Smart Contract ——Nick Szabo http://szabo.best.vwh.net/idea.html
6. Smart Property —— https://en.bitcoin.it/wiki/Smart_Property
7. Blockchain— from Digital Currency to Credit Society ——ChangJia, HanFeng and etc. ISBN:9787508663449
8. Snow Crash——Neal Stephenson 1992
9. Metaverse——https://en.wikipedia.org/wiki/Metaverse
10. Tim Swanson ——http://www.coindesk.com/smart-property-colored-coins-mastercoin/
11. Coin Days Destroyed ——https://en.bitcoin.it/wiki/Bitcoin_Days_Destroyed
12. http://blockchaindev.org/article/consensus_introduction.html
13 ZeroCash——http://zerocash-project.org/paper