METAVERSE

From Smart Properties, Avatars and Oracles to A New Virtual Society

Viewfin

1st Edition

Abstract

Metaverse is a decentralised platform of smart properties and digital identities, based on public blockchain technology. It is initially developed and supported by development team from Viewfin, it is a project under MIT licenses agreement. Once reaching maturity, the codes of Metaverse will be published on github (https://github.com/ViewFin/Metaverse).

Introduction to Blockchain

The Blockchain technology originated from Bitcoin, the decentralised, immutable ledger-keeping technology kept Bitcoin from the problems like counterfeiting or double spending; many believed Bitcoin was the first application of Blockchain Technology.

Bitcoin was an ingenious invention, Satoshi Nakamoto, the mysterious creator of Bitcoin, call bitcoin a peer to peer digital cash system. For the past 7 years since its inception, Bitcoin ecosystem has grown in the midst of doubts and misconceptions, its market value has nonetheless surpass 10billion USD.

It became clear than ever, what the invention of Bitcoin brought us is NOT only a new digital cash system, but also Blockchain, the technology Bitcoin uses to keep its decentralised ledger. Even more importantly Bitcoin assured us that physical assets can be and will be digitised. Blockchain, the decentralised technology cryptographically ensured the immutability of the ledger and enables counter-parties to interact/trade in a trust free environment, will be a revolution in banking, insurance, medical, logistic and many other industries.

Brief history of Blockchain

To be defined

Name coin and Peercoin

To be defined

Bitshares

To be defined

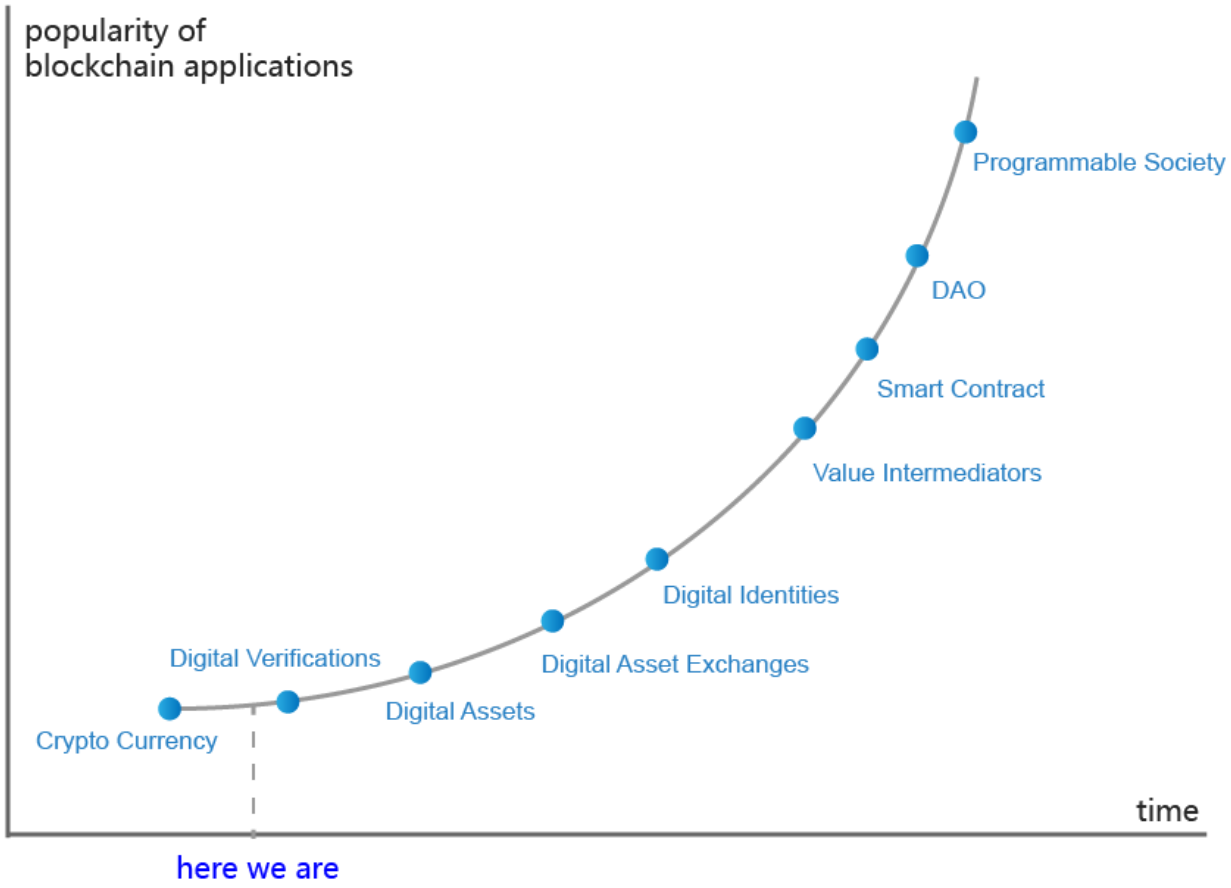
Ethereum

To be defined

Public Blockchain, Permissioned Blockchain

To be defined

The roadmap of Blockchain


popularity of
blockchain applications
Programmable Society
DAO
Smart Contract
Value Intermediators
Digital Identities
Digital Asset Exchanges
Digital Assets
Digital Verifications
Crypto Currency
time
here we are

Metaverse

The New Reality

The word Metaverse first coined in Neal Stephenson 1992 science fiction “Snow Crash”, where humans, as avatars, interact with each others and software agents, in a 3D space that uses metaphors of the real world.

Nowadays, just like Stephenson described in 1992, our work and life are heavily relied on the Internet, people spend more and more time online than offline, interact with each other more often online than offline, and soon, people will transact more often online than offline as smart properties, avatars (digital IDs) and intermediary Oracles become main stream.

The project was named after Neal Stephenson’s Metaverse.

Entropy the token of Metaverse

The Entropy

Borrowing the measurement of particle disorderedness from thermodynamics, the base token of Metaverse is called the Entropy. There are 100,000,000 ETPs in total. It is divisible into 10^8 =0.00000001, just like Bitcoin, and it is transferable on Metaverse blockchain and secured by ECDSA(elliptic curve digital signature algorithm).

The Entropy is NOT claim to be a form of digital currency, rather it is the equity of Metaverse. As a result, the price of ETP won’t pegged to any fiat or crypto currencies, including Bitcoin.

The Entropy could be used to measure value of smart properties in Metaverse, or used as a collateral in financial transactions. And the ETP will be used whenever system fees are applied, i.e. creating a new Smart Property, register a new Avatar, or apply to become an Oracle.

Distribution of the Entropy

ICO(initial coin offering) has become a popular method of token distribution in Blockchain realm. Starting from January 2014 Bitshare’s 200 days ICO, follow by the July 2014 Ethereum staggering 25000 Bitcoins ICO, then DigixDAO, Lisk in 2016, not to mention the controversial THE DAO. Antshares in China also successfully crowdsaled 2100 Bitcoins in October 2015.

The Entropy of Metaverse will distribute 50~60% of the total 100-million tokens in two ICOs in succession. 20~30% of the tokens will be distributed through first ICO in August, 2016, and another 20~30% will be distributed through second ICO approximately November 2016, after the Metaverse client (wallet) and the main blockchain are completed.

The rest 40~50% ETP will be distributed through POW mechanism, AKA mining.

Micro-Inflation

The Entropy is the equity of a DAO(Democratic Autonomous Organisation), namely The Metaverse. It is NOT a currency, it shouldn't have inflation at all, but, tokens are always lost for various of reasons, accidents, carelessness, or death. 1% of annual lost rate was predicated by Vitalik Buterin in Ethereum white paper. To provide sufficient liquidity and to accommodate more smart properties on Metaverse, a micro-inflationary linear issuance scheme is designed. 4 Million ETPs will be added to the circulation each year after the end of POW phase, the initial inflation rate will be 4% annually and trend down gradually towards 1% lost rate Vitalik predicted.

Smart Properties

Bitcoin wiki mistakenly pointing Nick Szabo as the one who coined the phrase "smart property" in his 1997 work of "The Idea of Smart Contracts", instead, Szabo only described a type of properties which has smart contracts embedded within, to execute its contractual terms.

In Ethereum project, the concept of smart contract was over emphasised, where digital assets require smart contract to take existence. This is a rather counterintuitive design.

In Metaverse, the importance of smart property is recognised, contracts require properties, not the opposite. Take object oriented programming as an analogy, if Smart Properties is a object CLASS, then contracts are METHODs in the class.

Different from Ethereum, Smart properties in Metaverse follows Bitcoin's UTXO methodology(Unspent Transaction Output), with a denomination and address/Digital ID, Any transaction will contain inputs from existing UTXOs with the signatures made by private keys of current owner, and send to the new owners' address, and then form new UTXOs.

As a result, Smart properties in Metaverse are able to be easily sent and received just like Bitcoin, requiring smart contracts only when complex transactions are involved.

Avatars - the Digital Identities

Smart Properties require owners, how would a person in physical world owning a piece of smart property online? Avatar, a digital representation of identity online, though which the ownership of smart property can be claimed.

Creating an avatar is much more than giving an alias to your public key. Other informations are also collected and protected cryptographically. These information are verifiable through zero-knowledge-proof technique on need-to-know basis and under owners discretion . Because unlike owning bitcoins anonymously through private and public key system, Most real world activities require some level of personal information, for instance, to join a young female entrepreneur club, you need to disclose your age and gender.

Behind an avatar, it could a real human being, an AI, a machine that is part of the IOT, or a organisation.

One avatar could own multiple smart properties, and the ownership of one smart property could belong to multiple avatars, it is a many to many relationship. Though It look seemingly complex, the certainty of the property ownership has been securely established on the Metaverse blockchain cryptographically.

Then, let the party of trading, lending, renting, leasing and mortgaging start.

Oracles - Value Intermediators

How many Oracles are required in a simple NYC weather prediction contract between Alice and Bob? the answer is at least 3, a weather data input oracle, a group of arbitrators and an escrow.

The blockchain technology promised disintermediation, or “cut the middleman”, it is a myth as least for now. Value Intermediators are still important now, and will be important for a very long time. They acting like the warm holes that linking between parallel universes, linking the physic world to the virtual digital world.

Instead of “cut the middleman”, Metaverse invites them on chain, become Oracles. Custodian Oracles keep the physic assets as collateral and issue smart properties on chain; Identity Oracles prove the linkage between physical Identities and avatars; Regulatory Oracles for regulatory bodies including governments to supervise transactions, and many more other Oracles to grease gear for the Metaverse.

Technical Aspects

Consensus Algorithm

Metaverse is a public blockchain. There are several prominent consensus algorithm for public chains, including POW(Proof of Work) first used by Bitcoin, POS(Proof of Stake) first used by Peercoin, DPOS(Delegate Proof of Stake) first used by Bitshares, and various of forms of BFT(Byzantine Fault Tolerance).

Most cryptocurrencies bypass BFT algorithm, as it doesn’t solve the token distribution quest. Though not a crypto currency, Metaverse choose to distribute Entropy, the token of Metaverse, to those who helped defending the security of the network.

In the early stage of any blockchain projects, the number of total full nodes are limited, make it harder to secure the entire network. By introducing proof of work mining, giving out Entropy as mining rewards, Metaverse will gain large number of miners as full nodes, providing much needed security in the beginning of the project.

As the project grows mature through the time, as Entropy mine is depleting, Metaverse will switch to a modified DPOS consensus algorithm. This algorithm will take Coin Day Destroyed into consideration.

POW - Mining

Metaverse will employ GPU mining scheme in the first several years to ensure network security, and implement a decentralised timestamp server system. The algorithm of Metavere mining is still being researched, but it would not be Bitcoin's SHA256 nor Litecoin's Scrypt, for the obvious reason of avoiding 51% attack from Bitcoin/Litecoin mining pools.

HBTH-DPOS

POW mining will help Metaverse establish secure network in the first several years, Mining has its own vice, namely waste of energy, mining centralisation and etc.

Delegated Proof of Stake, first appeared in Bitshares was much more robust and more decentralised than POW and POS, more importantly, every participant in the system is a eligible voter.

However, there are two major downfalls in the DPOS consensus, firstly, Financial Interference, by acquiring large amount of system tokens and voting for or against major system proposals, to manipulate the token price highly, and then quickly sell the token for profit. In current Bitshares system, it takes only $3 million USD for attackers to acquire enough votes change Bitshares underlying design.

Secondly, Voter Apathy, voters usually don't care much about how system function, most of them delegate their votes to a delegator and never change their votes ever if the delegator commit evil. Nowadays, only 1% of voters changed their delegators in the past three month.

Metaverse improves the DPOS consensus by adding Token-Height and HeartBeat concepts.

Token-Height(TH) was originated in Bitcoin as Coin Day Destroyed.

Bitcoin CoinDays=number of Bitcoins * days since last spent

TH= Number of ETPs * Number of blocks since last spent * MV Constance

Metaverse takes TH to weight the voting in DPOS, to avoid Financial Interference problem, if attacker acquires large amount of ETPs from markets, the "days since last spent" value will be very small, thus, the voting power is weak too. The attacker could

either acquire more ETPs or hold the ETP position for a long period of time to increasing its voting power, either way, vastly increased costs of attacking.

In the DPOS stage, Metaverse, like other POS consensus, will distribute new ETPs to Stakeholders based on there holdings. However, instead of receiving new tokens passively, Stake holders are required to send a HeartBeat to proof alive, then claim the new ETPs. the HeartBeat is a digital signature of from the private key, the stake holders will be asked to re-elect delegate or keep the current delegate. The benefits of the HeartBeat are two folders, first, it incentivise people to review the delegate, though not completely solving, improve the voter apathy problem. Second, system will not distribute new ETPs to lost tokens, and eventually dilute the lost tokens.

Types of Transactions

Other than coinbase transaction, there are only one type of transaction in bitcoin, transfer coins from senders to receivers.

Ethereum added another type called contract, contracts are used to for almost all other type of transactions other than ether transfer, including issuance of assets and etc. The users of Ethereum are required to know a little coding, although Ethereum project team tried their best to make the coding as simple as possible, in some case, only a few lines of codes are needed, the concept of coding still alienated large amount of business users.

Bitshares has multiple type of transactions, asset issuance, order placement, order cancellation and etc. The architect design is inefficient to say the least, but very intuitive for the users.

There are multiple type of transaction in Metaverse, a balance between efficiency and usability is sought in Metaverse, it won't neither be one contract fits all like Ethereum, nor has half dozen type of transactions like Bitshares.

Smart property issuance and Digital ID registration are two paramount types of transactions other than the ETP transfers, and then an Ethereum contract like transaction type will be added as well.

Cross Chain VMs

Ethereum codes are executed through EVM (Ethereum Virtual Machine), research efforts will be put in to seek solutions for CCVM(Cross Chain Virtual Machine) to enable cross chain transactions.

Potential Risks and Concerns

Blockchain technology is still in its early stage, yet to reach its maturity. It derived from Bitcoin, and inherited its virtual as well its vice.

The Ever Increasing Blockchain Size

Bitcoin Blockchain grow approximately 1M bytes every 10 minutes, that is 1G bytes weekly, the cost of running a full bitcoin node increases rapidly. The number of total full nodes has been in the decline since the peak of more than 10, 000 nodes globally later 2013 to roughly 5,500 July 2016, at time of this writing. Ethereum Blockchain grows roughly 2G bytes monthly in an ever increasing rate. Metaverse blockchain will suffer the same problem and probably worse because of implementing UTXO methodology. As elaborated in Ethereum whitepaper, this problem will be mitigated by miners, as they are required to maintain a full node.

Mining Centralisation

Mining is a double edged sword, It help to secured the network fend off attacker while creating new problem of centralisation and potential dreaded 51%.

Mining centralisation was much detested in Bitcoin realm, Ethereum is also fighting a losing battle against its own mining centralisation.

Metaverse will optimised its mining algorithm, probably not sufficient to eliminate but to slow down the problem, till it switch from POW to HBTH-DPOS consensus algorithm.

Failure on Success

Should Metaverse become very successful in the future, a new risk will arise. when the total value of digital assets on Metaverse rise to a level, that make it profitable to sabotage Metaverse while shorting the assets in the exchanges.

Thus, the total value of digital assets on metaverse is a function of the cost of defending/attacking(mining cost in POW stage) the system. Ideally the total value of digital assets shouldn't exceed 5 times of the mining cost.

Conclusion

Like Bitshares and Ethereum, Metaverse was derived from Bitcoin, utilising the blockchain technology to solve problems other than digital cash system; decentralised exchange in Bitshares case and smart contract, decentralised application platform in Ethereum's case. By clearly defining digital assets, digital ID, and emphasising the importance of the on chain Oracles, Metaverse assures the rightful asset ownership digitally, building the foundation of future digital finance.

In Metaverse, mediated through Oracles, Smart Properties are able to securely transact amongst Avatars. Thanks to the blockchain technology, Metaverse inherently has its own immutable ledger and double spending free, sailing beyond the realm of digital cash to all the assets that can be digitised on earth.

Bibliographies

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