NUM

Metaverse
Blockchain
CA–NFT

Content

A.

Project overview

A.1 Background
A.2 Characteristics
A.3 Project brand

B.

Metaverse NUM Plan

B.1 NUM Public Chain
B.2 Virtual reality platform
B.3 NUM_DID
B.4 NFT value system

C.

NUM idle mobile phone computing power mining

C.1 Equipment
C.2 Rules
C.3 CA–NFT
C.4 Characteristics

D.

NUM layered architecture

D.1 Design principles
D.2 Five–layer–architecture

E.

Other technical solutions at the bottom layer

E.1 Encrypted P2P network
E.2 Metaverse NFTs scheme
E.3 New fragmentation commands
E.4 Scalability
E.5 Changing data layer to LevelDB
E.6 StateTrie tree
E.7 Data processing

F.

Economic model

F.1 Issuance, distribution and destruction
F.2 Value

G.

Disclaimer

Project overview–1

A.1 Background–1

2021 is the first year of Metaverse. From now on, the human being has owned one more promised land. Metaverse provides a new path for the digital transformation of human society and intersects with post–human society in all directions. It shows a new era with the same historical significance as the era of great navigation, the era of industrial revolution and the era of aerospace.

At present, the global technology giants have successively arranged the related industries of Metaverse. Facebook has changed its name to meta and turned to the Metaverse in an all–round way. Facebook continues to invest in VR/AR terminals, content and others, which has been regarded as the most comprehensive Metaverse planner. The exploration of Roblox in the field of PUGC assets has realized the economic closed loop of game producers and consumers. Satya Nadella, the CEO of Microsoft, stated that the company is committed into building the "Corporate Metaverse". NVIDIA, a graphics chip manufacturer, has launched the first basic simulation platform for Metaverse in order to accelerate the launch of Metaverse business. Through acquiring NextVR which is a VR start–up last year, Apple Company entered into the key hardware industry of Metaverse. It is expected to launch glasses products in the second half of 2022. The investment of Tencent on Epic Games has continued to focus on content and social networking in order to lay out the Complete Reali-ty of Internet (CRI).

NUM team believes that the internet giants and the investment insti-tutions are actively to lay out the Metaverse. That is because the Metaverse is the "aggregation" of multiple key core tracks. Metaverse is an iterative upgrade of the third generation Internet Web3.0 rather than a simple new internet track. It is a new digital space with higher dimensions on PC Internet and mobile Internet. From the perspective of specific investment direction, the investment direction and compa-ny layout of the present Internet giants are mainly focused on infra-structure and ecological construction. Their investment field is not only limited to the field of games and entertainment, but also more and more inclined to the whole track layout.

NUM
CA–NFT
Metaverse

A⁻¹

Project overview–2

A.1 Background–2

In such market context, NUM team announces to launch the Metaverse NUM Plan and lay out the public chain infrastructure of Metaverse. The Metaverse NUM Plan includes the CA–NFT idle mobile phone computing power mining, the bottom layer of commercial–grade DISTRIBUTED cloud storage, the decentralized communication or transmission bottom layer, virtual reality platform, the decentralized identity system based on repu– tation (NUM_DID) and the NFT value system. The mature NUM Metaverse will be the sum of a series of "connecting points into lines" technological innovations. Vast amounts of digital assets will be created, traded and consumed, which contain the potential beyond imagination.

A.2 Characteristics

1) Metaverse is committed to create the "real world" existing in parallel with the real world. Although the Metaverse NUM Plan can not replace real life, it can become the second space for human survival and provide people with a new life in another dimension. It can give birth to new social dimensions with second identity, two–track social relations, ideal– ized lifestyle and so on.

2) Metaverse will not replace the real economy with the virtual economy. On the contrary, it takes the real economy as the material basis and endows new vitality into the real economy from the virtual dimension. In the NUM Metaverse, the distinction between virtual and reality will be meaningless. Everything in the real world can be reflected in NUM ecolo– gy, and the virtual things in NUM ecology can also have real effects. NUM will deeply integrate into the structure and operation of the existing society in the fusion way of the virtual and the real.

3) Metaverse includes the digital technology which is composed of the blockchain technology achievements, the NFT integration and other digital financial achievements.
Metaverse is an online virtual world that reflects the real world, which is an increasingly real digital virtual world. The Metaverse NUM Plan hopes to show the possibility of building a holographic digital world parallel to the traditional physical world to the human beings through blockchain, digital finance and other technologies.

NUM
CA–NFT
Metaverse

A^{-2}

Project overview–3

A.3 Project brand

The reincarnation number 142857, which contains the infinite mathematical laws, is the project brand of the Metaverse NUM Plan. It was found in the Egyptian pyramids and has been known as the most magical number in the world.

The reincarnation numeral 142857 can prove that there are seven days in a week. After self–accumulation, these six numbers need to be on duty in turn. When it comes to the seventh day, they will have a holiday. At this time, 999999 will take over. When the numbers get bigger and bigger, they take turns every more than a week. Thus, every number needs to be separated once. You don't have to use a computer to know how it is separated and the accumulation results of numbers.

142857 makes it possible for humans to go into Metaverse and make superior understanding of Metaverse. Therefore, it is also known as the code for human beings to open the universe. The mysteries of the universe have not yet been fully solved. The real magic of this number series (142857) still needs to be excavated slowly. It likes the fledgling NUM which is exploring and practicing a series of cutting–edge technologies. It hopes will be the first batch of key "passwords" leading to the Metaverse world.

Summary:
Initially, the Internet needs the pioneers and enterprise development tools to make it become an accessible infrastructure. These precursors have been duly rewarded. Now, the transformation from Web2.0 to blockchain Web3.0 and Metaverse is a long–term process. This requires countless attempts, changes in user behavior and technological innovation. Metaverse will fundamentally change our interaction method with the virtual world. When we approach to the world which has been increasingly controlled by science and technology, it is important that we provide a high–performance bottom layer, redesign the system, and adjust the incentive mechanism to benefit the public. The decisions and work made by NUM today will accumulate and affect the subsequent era. It is just like the financial revolution led by DeFi, as the blockchain Web3.0 and the Metaverse process can not be stopped.

NUM
CA–NFT
Metaverse

A⁻³

NUM
CA–NFT
Metaverse

B⁻¹

Metaverse NUM Plan–1

Metaverse NUM Plan is supported by common chain technology and spatial computing. It builds a secure and high–speed bottom layer of commercial–grade DISTRIBUTED cloud storage and decentral–ized communication or transmission. It also designs four major technical solutions (functional platforms) which includes CA–NFT idle mobile phone computing power mining, virtual reality platform, the decentralized identity system based on reputation (NUM_DID) and the NFT value system. The four major technical solutions aims to become the infrastructure of the future Metaverse of Web3.0 with the elements of immersion, low delay, diversity, anywhere, real–time, connectivity and so on.

B.1 NUM Public Chain

Metaverse is based on many technologies. and closely related to the real society. It has a digital giant system of independent economic system. Generally speaking, Metaverse is mainly composed of 6 sup–porting technologies, namely blockchain technology, interaction tech–nology, video game technology, AI technology, network & computing technology and Internet of things (IoT) technology.
NUM public chain chooses the block chain technology as the focus to help build the economic system of Metaverse. Depending on the decentralized, tamper proof, open and transparent characteristics, NUM public chain provides a feasible path for the Metaverse to trans–fer value and rights.

It lays the foundation for future digital economic transformation and digital asset circulation:

1) At the network computing level, the bottom layer of commer–cial–grade DISTRIBUTED cloud storage and the decentralized com–munication or transmission can provide Metaverse with high–speed, low delay, and large–scale access transmission channel and powerful computing power, which show the possibility of building a holographic digital world parallel to the real physical world to the people.

2) In terms of developer tools, its core idea is ease of use and devel–oper friendliness. It provides the cloud BaaS platform with the modular development function to B–end users of Metaverse.

3) At the level of smart contract, it gives the priority to meeting the rigid demand scenario of blockchain + Metaverse landing in order to make superior use of main chain to provide a basic smart contract

Metaverse NUM Plan–2

B.1–1 Consensus

The focus of the dispute over the public chain largely focuses on the consensus mechanism. Although the workload proof mechanism of Bitcoin realizes the complete fairness, it greatly sacrifices the efficiency. Lately, other consensus mechanisms significantly make improvement of efficiency, while sacrificing the fairness to the varying degrees.

No matter what kind of consensus mechanism we come up with alone, there are reasons to challenge and question. Now, all the choices of each public chain are to achieve the ideal balance point. The people who can conform to the process of development and get closer to this bal–ance point will be more likely to win in this public chain dispute.

We believe that the public chain consensus as the bottom layer of blockchain Web3.0 and Metaverse technology is definitely not a simple theory, or covered by a single technical solution. It will become more and more complex. After all, a single functional main chain can not fully meet the good combination of Metaverse on computing level, ledger level, smart contract level, unstructured data storage level and user interface.

Therefore, on the VDF consensus main chain, we increase the block time to 15S each block by superimposing the consensus principle of PoSt. At the same time, we support the traditional HTTP interface and IPFS file transfer protocol. The layering realizes the ledger consensus and the storage proof consensus. It builds a fast and stable bottom layer of the blockchain and realizes the CA–NFT (license) idle mobile phone comput–ing power mining function. It breaks the over dependence on the com–puting performance of the server CPU or even GPU of the node, result–ing in extremely low block efficiency and waste of computing data. Thus, it is to achieve the truly low energy consumption, low threshold and green mining.

NUM

CA—NFT

Metaverse

B⁻³

Metaverse NUM Plan–3

B.1–1–1 VDF consensus main chain

Since Ethereum included the Verifiable Random Function (VDF) in its research plan and used it in Ethereum 2.0, VDF has received the extensive attentions.

B.1–1–2 Introduction

VDF is a kind of mathematical function, which can make the calculation of the function take at least a known time. Even when a small number of CPUs are used for parallel computing at the same time (this is different from the Proof–of–Work of bitcoin, which will be explained in detail later), the parallel computing greatly reduces the computation time for algorithms that are not well designed.

Take the mining algorithm of bitcoin as an example:
In the assumption of $0 \leqslant nonce \leqslant 232 - 10 \leqslant nonce \leqslant 232 - 1$,

● If there is only one arithmetic unit, it may cost the time which can be used to make 232 times SHA–256 calculations at least.

● If there are two arithmetic units, it can split the task in half and let them calculate the hash value in parallel. It only takes 231 times SHA–256 calculations at most.

At the same time, the following properties shall be met:

1) The test of VDF results should be very efficient.
2) Uniqueness: For the input of any VDF, there should be a unique output result that can pass the inspection. In other words, there are no two different outputs from the same inputs. If the output result includes "result" and "proof" about the result, the proof part may not be unique. In this situation, it is necessary to make sure that the probability of "the verifier passing because of the proof, while the output is not the correct result" is small enough to be negligible.

Metaverse NUM Plan–4

B.1–1–2 Introduction–2

3) Sequentiality: Even if the attacker can calculate for a long time in advance rather than any long time and own many parallel processors rather than any number of processors, as well as make full use of calculating methods which are deterministic calculation or continuous montage guess, the probability of calculating the VDF results within less than t time is small enough to be ignored.

Some readers may feel that VDF and PoW are one kind of things. In fact, although they are not easy to calculate, there are many key differences between them.

4) PoW does not resist parallel computing acceleration, while VDF does. In fact, the non–resistance to parallel computing acceleration of PoW is in line with Satoshi Nakamoto's assumption of "one CPU, one vote". However, the VDF's nature of anti–parallel acceleration only works against this purpose. VDF will make the multi–CPU computers with little advantages in comparison with the single CPU computers.

5) As for the fixed difficulty setting of d, PoW POW can have many legal solutions, this is also the premise to ensure that PoW consensus network has stable throughput and stimulate miners to make competition. However, VDF has the unique output for the given input of x. This is also why it is called a function.

NUM
CA–NFT
Metaverse

B⁻⁴

Metaverse NUM Plan–5

B.1–1–3 Purpose

1) Strengthening the security of public verifiable random numbers
The random numbers on the blockchain have always been a hot topic. No matter in the design of some equity proof consensus protocols (such as Proof–of–Stake, POS and so on), or in some very popular game applications on smart contract platforms (such as Ethereum, EOS and so on), the random numbers occupy the core position. At the same time, the actually designed random number acquisition scheme is still very immature in many of these applications, so that there is often news happened that applications are attacked by hackers because of unsafe random numbers.

VDF is very useful for some methods of obtaining random numbers from public sources, such as the stock market or the pow blockchain. These random number sources have enough randomness. More strictly, it's the minimum entropy. However, the high–frequency traders can affect stock prices. meanwhile, the miners in PoW blockchain can also reduce the probability of unwanted random number results by not broadcasting their excavated blocks. Nevertheless, the premise of such an attack is that the attacker has time to predict the results of random numbers before other honest participants. VDF can just stop such kind of situation. If the time parameter TT of VDF is set long enough (such as the interval of 10 blocks), the latest block header is thrown into VDF as an input and the output will become the random number result. Then, the attacker can only know the result of the random number after 10 blocks. At that time, it is difficult to change the result again, as it needs to fork the 10 blocks.

In addition, VDF can also enhance some multi–party random number schemes. Taking the scheme of Commit–and–Reveal as example, the attackers can wait until the end of the reveal phase before deciding whether to reveal their commitments. Assuming the scenario, we remove the commit phase. We put the integration of owners' input at the end of the protocol into the VDF rather than directly take it as the random number result. In addition, we set the time parameter TT of VDF to be long enough which is later than the deadline for submission. In this scenario, even the last–minute submitter cannot know the result of random numbers. Then, manipulating the results become impossible. In contrast, other multi–party participation schemes usually tolerate less than half of the malicious nodes at most, and their interaction overhead is greater than the above schemes.

Metaverse NUM Plan–6

B.1–1–3 Purpose–2

2) Solving Nothing–at–stake Attack
As described in the previous section, VDF can be used to enhance the security of random number generation schemes. Thus, VDF can also be used in some consensus protocols that used random numbers to select Leader. In order to prevent the Nothing–at–stake attack, some energy–saving consensus protocols, such as POS (Proof–of–Space), Proof–of–Storage and others, need to use the random election to elect a Leader at regular intervals. Most of the random number protocols used by these protocols remain safe only when the majority are honest. Using VDF, it can reduce such restrictions to the presence of at least one honest participant.

What is the Nothing–at–stake Attack? When the PoS blockchain bifurcates, the consensus participants will choose to mortgage the collateral assets on the different fork chains for their own interests participate in block creation. In this way, the bifurcated chain may exist all the time and bifurcate more and more, which seriously endangers the consistency of the system. Such an attack is called Nothing–at–stake-attack. Such an attack on the pow chain requires decentralized computing power. Thus, such an attack is only applicable to the consensus protocol of "energy saving".

In addition to random elections, there is a scheme called Proofs of Space and Time to prevent such attacks. In fact, the scheme simulates the mining process of PoW. In the process, the time to dig out the blocks is uncertain. In addition, every miner is competing to be the first to dig out the blocks.

There is one different point between the Proof–of–Time and the Proof–of–Space. As for Proof–of–Time, simulating the mining process does not need to consume a lot of parallel computing resources. As for Proof–of–Space, there is only a certain threshold when entering mining. Specifically, the whole mining process is divided into different intervals based on the chronological order. Each interval has a common random challenge C. For example, it can be the hash value of the block dug out in the previous interval. Assuming that the space unit owned by a miner is N, he needs to generate a proof π to prove that he owns the space of N units, which is specially used for mining of the blockchain. It is guaranteed by Proof–of–Space. The goal of miners is to find the smallest $\tau = H(c, \pi, i), 1 \leq i \leq N$, it needs to take C as input to calculate a VDF (actually the incremental VDF). The time parameter of the VDF is positively correlated with τ. In this design, the miners with more space are more likely to find smaller τ. At the same time, VDF ensures the passage of time, which cause the large amount of bifurcation and cost a lot of time.

Metaverse NUM Plan–7

B.1–1–3 Purpose–3

3) Proof of Replication
The problem to be solved by the Proof of Replication is how the server proves to the client that it has stored the specified data on a dedicated storage medium, even if such data is easily gained from another storage source.

Note: Proof of Replication is to prove that the server has a copy of data rather than it has such data.

For example, the cloud storage service provider claims to make two extra redundant backups of the customer data to guarantee the availability of the user data. Therefore, the customers need to pay more money for such redundant backups. However, how to prove that the cloud service provider has a total of three copies instead of two or only one? It needs to use the Proof of Replication.

One idea is to use an asymmetric coding scheme in time, that is, the coding is very slow, while the decoding is very fast. VDF can do this. In fact, it is a decodable VDF. The server with the identity of id firstly divides the file into the blocks of B_i, $1 \leq i \leq n$, whose size is similar with b–bit, calculates the $B_i \oplus H(id\|i)$ secondly and put the result into VDF as input to calculate y_i, $1 \leq i \leq n$. Among them, H is the anti–collision hash function with the output length of b–bit. The server stores all y_i and the client constantly randomly selects i_i, polls and asks the server to come back y_i. The server needs to respond to the corresponding results to the client within the required time. At the same time, the client can complete the verification by decoding y_i to get b_i in a very short time. If the server does not store y_i, then calculating y_i becomes what the server must do to respond to clients correctly. However, such calculation cannot be completed within the required time duration. The server can also store only a portion y_i, whose portion is ρ. Since the client is randomly polled, the probability that the server successfully deceives the client every time is ρ. As long as the client repeats such polling K times, the probability of server successfully deceives the client can be reduced to ρk.

It should be added that the server can not store B_i. The y_i decoding is very fast. Even if only y_i is stored, it will not affect performance too much.

Metaverse NUM Plan–8

B.1–1–4 Operation process

Since VDF is a function, it must have such a form: f:X→Y. In order to realize the functions mentioned above, namely "resisting the delay of parallel computing" and "verifiable results", In VDF, there must be an algorithm for calculating the results and an algorithm for verifying the results. At the same time, such cryptographic tools usually include a configuration phase. It is used to determine the parameters to be used later. Therefore, VDF is described as a triple of three algorithms (Setup(Setup, evaleval, Verify)Verify).
Each algorithm is defined as follows:

● Setup(λ,t)→pp=(ek,vk)
It accepts the safety parameters λ and the time parameter t and generates the public parameter pp which can be seen by all the people. The public parameter pp contains a parameter ek for calcu–lation and a parameter vk for verification.

● Eval(ek, x)→(y, π)
It accepts the calculation parameter ek and the input x∈X, and calculates the output y∈Y, as well as proving π.

● Verify(vk, x, y, π)→{accept, reject}
It accepts the VK, x, y and π. If the output is the "accept", it means the verification passed. If the output is the "reject", it means the verification passed.
As shown in Figure 1, we can see the normal operation process of VDF.

NUM
CA–NFT
Metaverse

B^{-8}

Metaverse NUM Plan–9

B.1–1–4 Operation process–2

The above algorithms need to be supplemented:

● About SetupSetup

1) The running time of SetupSetup cannot be too long. It is limited by the security parameters λ.

2) In this stage of setup, the random numbers are usually required as parameters to the ensure security. If the random number is privately selected, that is, it is not publicly available, then a trusted party will be required to select the random number at this stage, which is called trusted setup. On the contrary, if the random number can be a public random number, such a trusted setup is not required at this stage. Obviously, we want to avoid trusted setup as much as possible.

● About Eval

1) It's not necessary to prove π, if it can be verified by y only.

2) In the calculation of y, the random numbers are not allowed to be introduced in order to ensure the uniqueness. However, they can be introduced in the generation process of π.

3) In order to ensure the serialization, Eval must have a running time of t when it has no more than poly log parallel processors about t.

4) Why should Eval allow parallel computation up to time t to a certain degree. There may be no structure that can perfectly make parallel and serial computing times exactly the same. Thus, we need to tolerate a certain amount of parallel acceleration which is no obvious.

● About Verify

1) In the Verify, the random numbers are not introduced, that is, it is a deterministic algorithm.
2) The running time of Verify is much smaller than t. Specifically, they have an exponential gap in the running time.

NUM
CA–NFT
Metaverse

B^{-9}

Metaverse NUM Plan–10

B.1–1–5 VDF construction and calculation of NUM

AboutAs mentioned above, the use of continuous hash operations is a means to prevent parallel computing acceleration. However, such means are very inefficient and do not meet the definition of VDF. We hope to find the anti–parallelism construction method with faster verification. Please consider the example:

The first step is to select the number λ=161.

The second step is to perform the following operations t times for any input x:

Calculate k=X2

Take the remainder of k divided by λ to get 1

Make k as l and return to the first step. If it is the last operation, the output result is y.

Assuming our input is x=11, t=8, then the result is 95. As a matter of fact, if we let t take different values and record all the results, we can get the following table:

t	1	2	3	4	5	6	7	8
y	121	151	100	18	2	4	16	95

More generally, if a≡b mod, m means that if the remainder of a and b divided by m is the same, then the above operation is actually the calculation:

$$y \equiv x^{2^t} \mod \lambda$$

If we know the factorization of λ, e.g. 161 = 7 × 23, then we can quickly calculate the value of y through two exponential operations. The first step is to calculate the function ø(161)=(7—1)×(23—1)=132. The second step is to calculate remainder of 2t divided by ø(161).

$$2^8 \equiv 124 \mod 132$$

Then, calculate the remainder of x124 divided by λ.

$$11^{124} \equiv 11^{2^6+2^5+2^4 \; 2^3+2^2} \equiv 4 \times 2 \times 18 \times 100 \times 151 \equiv 95 \mod 161$$

NUM
CA–NFT
Metaverse

B–10

Metaverse NUM Plan–11

B.1–1–5 VDF construction and calculation of NUM–2

The above process does not seem to reduce much workload compared with squaring eight times in a row. However, in fact, when t and are very large (t≈230), it is much faster than the continuous square. The generally function is in the following:

$$\phi(n) = \prod_{i=1}^{r} p_i^{k_i-1}(p_i - 1)$$

If

$$n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$$

This function is called Euler's Totient Function. The above example can be generalized as:

$$e \equiv 2^t \mod \phi(\lambda), \quad y \equiv x^e \mod \lambda$$

Thus, if no one knows the factorization of λλ, the (λ) can not be calculated quickly. Thus, it can only be used by repeating the square operation t times.

$$x \to x^2 \to x^{2^2} \to \cdots \to x^{2^t} \mod \lambda$$

Then, y can be calculated.

Metaverse NUM Plan–12

B.1–1–5 VDF construction and calculation of NUM–3

In fact, this construction can be explained more essentially by using group theory.

Based on our findings, the value of modular operation y is less than λ. All the numbers which are smaller than λ and of coprime with λ form a group. This group is called the integer modular λ multiplication group, which is written as (Z/λZ)*. The order of this group, that is, the number of elements, is equal to the value of Euler function　(λ). Therefore, key question falls on how to generate such a group of order with the high level awareness.

At present, there are mainly two methods: using RSA group and using the class group of an imaginary quagratic number field. We chose the former method.

The generation of RSA group is similar to RSA encryption algorithm. The prime number of p and q are selected.
Among them,
p = 2m + 1
q = 2n + 1
m and n are prime numbers.
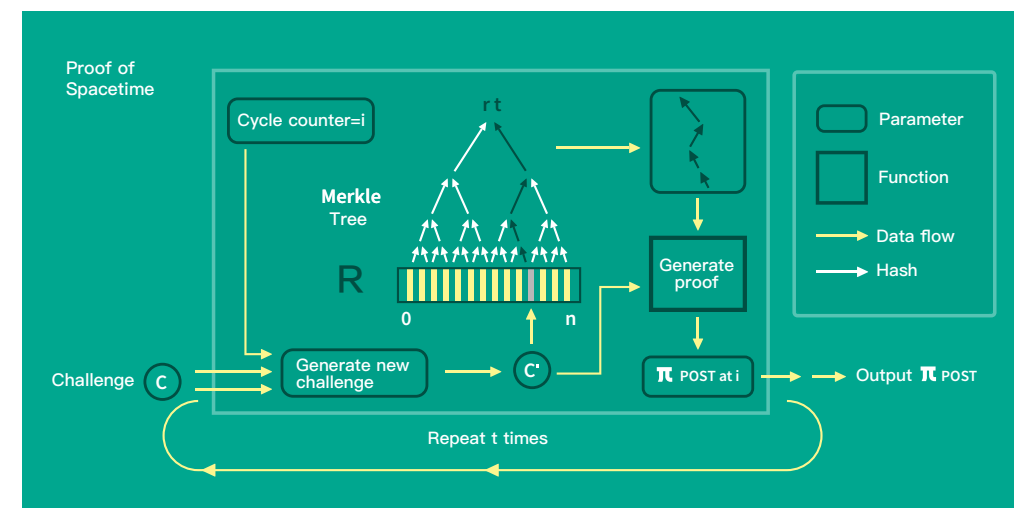Make N=pq, then (Z/NZ)* becomes the required group.

NUM
CA–NFT
Metaverse

B^{-12}

Metaverse NUM Plan–13

B.1–1–6 Superimposed PoSt consensus

PoSt (Proof of Spacetime) consensus mechanism is a consensus mechanism superimposed by NUM on the main chain of VDF consen–sus.

PoSt is an innovative computing power mechanism. In essence, it is a kind of storage proof — it is to use the data stored by the user itself as the proof of the computational power. It's used to show how much data a miner owned over the period of time and then use that amount of data to prove the amount of computing power.

The main difference between PoSt and PoW is that the storage capacity of PoSt in NUM is based on real and useful storage services. It is different from using a lot of energy to do meaningless hashing in order to gain computational power. Mining based on the PoW consen–sus mechanism causes the huge waste of energy, which has no sub–stantial value to the real economy. The difference between PoSt and PoS mainly lies in that PoS is to reach consensus through the mining method with coin age. It has been improved by NUM. Its superimposed PoSt consensus takes the proportion of the effective storage in the whole network as the basis for obtaining the block right, which does little damage to the liquidity of NUM (token).

It is worth noting that the NUM main chain superposition post consen–sus selects some mature technical schemes to support the VDF con–sensus main chain rather than completely adopt all of its algorithms. Its goal is to build a more complete, easy–to–use and mining compatible large storage ecosystem.

We know that there are many problems to be solved in the decentral–ized distributed storage project. However, we need to avoid too long

Metaverse NUM Plan–14

B.1–1–6 Superimposed PoSt consensus–2

It is worth noting that the NUM main chain superposition post con-
sensus selects some mature technical schemes to support the VDF
consensus main chain rather than completely adopt all of its algo-
rithms. Its goal is to build a more complete, easy-to-use and mining
compatible large storage ecosystem.

We know that there are many problems to be solved in the decentral-
ized distributed storage project. However, we need to avoid too long
project cycle and to set too large goals. In the field of software, there
is a famous book called the myth of man and moon, which tells the
failure process of a famous software project. In fact, any software
whose design goal is too ambitious can not escape the fate of failure,
while the correct development method is to complete through agility
and iteration.

FileCoin is a project with a long history. The technical scheme adopt-
ed in its white paper has been changed many times. The PoST v1
which is core consensus algorithm of FileCoin has completely over-
turned the design of V1 in 2017 from the earliest POW like consensus.
It changes to use similar algorithm of Algorand to join the achieve-
ment of Poreps' VDE. There is no perfect design scheme for prob-
lems, such as retrieval market and micro payment, and so on. File-
Coin has been involved in too many technical and academic problems,
making the development cycle very uncontrollable.

The idea of NUM is to realize some advantages of PoSt by the
superposition method on the main chain of VDF consensus. There-
fore, the development difficulty of num project is reduced, which
provides a new idea and research direction for the underlying field of
Metaverse distributed storage underlying fields.

NUM
CA–NFT
Metaverse

B–14

Metaverse NUM Plan–15

B.1–2 NUM Cloud

The distributed cloud of NUM gives priority to individual sovereignty to benefit the public and Metaverse ecology rather than the rich elites and rent seekers in the world. Anyone can rent out the storage space on an idle mobile phone. Similarly, anyone can buy storage on the NUM network. It can be regarded as Amazon Web services or Google cloud. They can support the DAPP at the enterprise level and the decentralized data storage / retrieval services of complex Metaverse APP. However, we allow anyone to participate in the process rather than the company to control the data flow.

Bitcoin is designed as a virtual currency. What it stores in the bitcoin blockchain is its ledger, which is the bookkeeping required to deter– mine the ownership of bitcoin. Later, many people tried to use bitcoin blockchain to store data to achieve the various application purposes. Nevertheless, the bitcoin itself basically does not encourage this practice, and its own design makes this application very difficult and expensive.

Generally speaking, the Blockchain technology should be regarded as a distributed database system. This means that a large part of the data in the world may be stored in such systems. NUM explores this aspect of blockchain technology. It proves that blockchain may become a very competitive choice for decentralized storage cloud (distributed database) in the future.

NUM
CA–NFT
Metaverse

B–15

NUM
CA—NFT
Metaverse

Metaverse NUM Plan—16

B.1–2 NUM Cloud–2

The distributed cloud storage of NUM is the infrastructure of com—mercial blockchain and Metaverse. It is a perfect response to appli—cation scenarios such as high concurrency, relational, key value pairs, large capacity, efficient indexing, data security and so on. The block—chain database feature is object—oriented. With this feature, it can support more complex Metaverse application scenarios with high requirements for Storage Cloud (database), such as finance, games, social communication, NFT deposit certificate,

NUM Cloud	Traditional Cloud
Highly Decentralization	Centralized control
Public Database of Digital Privacy Based on Cryptography	Private database
Distributed Cooperation Based on Rules	Centralized administration
Tamper Proof	/
Security	/
Open	/
Lower Cost	Expensive

B−16

NUM
CA–NFT
Metaverse

B–17

Metaverse NUM Plan–17

B.1–3 NUM Network

By combining blockchain and encrypted P2P network (see Chapter 5 for details), NUM has developed a global peer–to–peer secure communication network which can provide support for real users participating in the Metaverse. The bottom layer of our decentralized transmission can cover the world. It can realize free communication and protect users' privacy, as well as let users really have their own data.

B.1–3–1 Core elements

NUM Network will change the use of blockchain technology, so that it can be used not only for financial transactions, but also to establish a safe and efficient communication connection for Metaverse applications.

Data ownership: the unbreakable network will effectively protect the security and the content privacy of users' data.

Decentralized server: due to the shortage of central server, NUM Network can not only hardly be attacked, but also cause data leakage.
Security & Encryption: metadata is stored on a decentralized network using a dedicated encryption key.

Anonymity: by using anonymous authentication, the users can set their own username and communicate freely.

Global interconnection: it can establish an effective and safe connection with anyone at anywhere in the world.

NUM
CA–NFT
Metaverse

B–18

Metaverse NUM Plan–18

B.1–3–2 Smart contract platform

The new generation of NUM smart contract:

● Contract engine optimization to support the new version of Solidi–ty contract

● Criteria integration of NRC721 and NRC1155 to achieve more powerful NFT description

● Support to the new versions such as require and so on
With above efforts, it can give priority to meeting the rigid needs of blockchain + Metaverse landing scenario and make superior use of the main chain to support Metaverse applications on the service layer.

In order to achieve better compatibility, NUM introduces a smart contract virtual machine supported by multi languages. For example, an Ethernet virtual machine (EVM) is set up in the NUM distributed system, which can support the existing Ethereum contract. At the same time, in order to adapt to most of the current contracts, we adopt the contract specification of Solidity and build an execution stack interpretation engine based on assembly operation. It gener–ates the bytecode by the solc compiler, packages and confirms by the node and solidifies into the instructions of the main chain.

The smart contract function of NUM does not support duplicate names. It takes NUM (test currency) to release the contract in the test environment. For formal release in production, a certain amount of NUM (primary currency) needs to be spent on the operation node.

The smart contracts are divided into contracts with constructors and contracts without constructors. The bottom layer is to call the com–pilation method of solc module. It compiles and generates the bin and abi codes. The bin code is an executable binary code, while the abi code is a collection of all methods and method parameters in the contract.

Metaverse NUM Plan–19

B.1–3–2 Smart contract platform–2

The contract publishing is to publish the bytecode to the main chain and generate the contract address. At the same time, the contract can decide when to open the contract by publishing the contract source code and verifying it. The related information about the contract can be checked on the main chain through the contract address. The release process is actually a transaction to the main chain.

To run a contract is to call the method of the contract. The methods in the contract are divided into parameters and no parameters. To call the methods in the contract, it needs to compile the methods into bin code. As for the methods with parameters, it needs to compile the parameters into the bin code here. Then, the data will be published to the main chain in the form of transaction. After the main chain is blocked, the users can run the bin code through EVM to perform the operations in the method. The methods in the contract are divided into those with return value and those without return value. The return value of method with return value needs to pass the transaction hash and can only be obtained after re querying on the main chain.

NUM
CA–NFT
Metaverse

B–19

Metaverse NUM Plan–20

B.1–4 Cloud BaaS platform

In terms of developer tools, the core idea is ease of use and developer friendliness. It provides the Cloud baas platform with modular development function for B–end users of Metaverse: Support and improve the Buffle test framework and SDK development frameworks such as num.js and so on, which provides better cases and convenience for third–party access.

Support chrome plug–in wallet, Bip44 protocol, and the interface of pc–web offline transaction and signature.

At the same time, NUM provides different frameworks and library modules for the B–side. As long as the interface API can be connected, it can also be universal. From the perspective of the application developers, the overall development efficiency has been greatly improved and the stability has been guaranteed. For example, developers can focus on how the blockchain is applied to their own the Metaverse business logic, and select the most suitable network model from the modular function.

B.1–4–1 Toolkit

The BaaS platform plans of NUM provides the toolkit needed to build on the blockchain for Metaverse applications. The template preparation of blockchain allows users to choose from different protocol parameters and pluggable components, such as consensus model and so on. Once the templates and options are determined, the toolkit provided by NUM may even deploy an entirely new blockchain for an application before the specific business logic required by the application is fully developed. In this way, NUM can greatly reduce the developer threshold. In addition to the fast–processing speed of the main chain and low service charge, NUM will attract more ordinary developers. This is conducive to the emergence of a large number of Metaverse applications in NUM ecology and the rapid formation of scale effect.

NUM
CA–NFT
Metaverse

B–20

NUM
CA–NFT
Metaverse

B^{–21}

Metaverse NUM Plan–21

B.2 Virtual reality platform

After the demand for the Metaverse applications, increases expo–nentially, the iterative role of Metaverse in the digital ecology will be gradually reflected.

Therefore, NUM virtual reality platform aims to provide a new scene including experience layer and discovery layer, and then gradually promote the explosion of more applications and demands, so as to promote the Metaverse to gradually change its entertainment mode, social mode, business format and business model.

Among them, the experience layer dematerializes the real space, making previously unpopular experience forms within reach, including games, social networking, shopping, music and other scenes. The discovery layer focuses on how to attract people to the Metaverse, which is the way for people to understand the experience layer. It is divided into the active discovery mechanism through spontaneous search by users and the passive input mech–anism promoted to users when users have no exact needs, includ–ing various application stores and so on.

B.2–1 Function

NUM virtual reality platform can provide equipment, products and services in the virtual world with clear value. It is not only the entrance for b–end users to access virtual reality products, but also the entrance for C–end users to experience virtual reality products.

Its core functions focus on:
1) Make the real world users interact with virtual world, virtual equipment, virtual users and virtual assets in the same space. The users can get better situational experience on num virtual reality platform.
2) Completely save and reproduce all user interactions in the NUM ecology, including the value circulation and other processes.
3) The Metaverse entrance which is highly interconnected, perma–nent preserved, panoramic reproducing and highly immersive.

Metaverse NUM Plan–22

B.2–2 AR development kit

The AR development kit of num virtual reality platform can assist b–end users to develop the "real world Metaverse".
For example, the toolkit uses the computer vision technology to identify the objects, such as the ground, the sky, the water, the buildings and so on. It also digitizes the terrain of the room and calculates the surface and depth of the environment in real time for use during the game. It also includes the semantic segmenta–tion API, which can place a virtual object behind a real object. The idea behind computer vision object recognition and mesh mapping is to better integrate virtual objects and environment to provide real occlusion. It makes the virtual ball roll behind the sofa and disappear from the view, which just likes seeing the trajectory of the real ball.

The toolkit is planned to be open to all developers in Q4 in 2022, and most software toolkits are free.

B.3 NUM_DID

NUM_DID is not only a decentralized identity system based on the reputation, but also the digital twin of users in the virtual world.

Metaverse has a premise that each Internet user has a unique internet identifier which is similar to e–mail address. It can be locally linked to any software, while being stored on a blockchain network. As part of "decentralized identity", part of a person's online activities will be on the chain. This also means that it is public and can be easily searched through personal encrypted wallet.

NUM_DID allows each individual participating in the Metaverse to hold (unique) accessible history. For example, a person's encrypted wallet will play a role similar to the personal profile on Facebook or LinkedIn. Nevertheless, it is different from the web2 personal pro–files. NUM_DID is supported by conclusive evidence: the achieve–ment, the contributions, the interests and the activities, as well as the permanent, time–stamped record.

NUM
CA–NFT
Metaverse

B–22

NUM
CA–NFT
Metaverse

B–23

Metaverse NUM Plan–23

B.3–1 Function

NUM_DID is an important achievement in the development process of the Metaverse NUM plan. It supports the users to put the users' names, passwords, private keys, fingerprints, faces and all personal privacy data in the decentralized storage space for storage, man–agement, display and identity authentication. Therefore, it is not limited on logging in to the NUM network. If the NUM_DID is widely used, the people will be able to carry and show their complete self when shuttling through different cyberspace. This will bring us closer to the way we operate in the physical world – property and reputation are related with ourselves instead of the platforms. We can take the property and reputation with us and use it at will.

B.3–2 Reputation system

In order to make the NUM_DID as the mainstream, we firstly establish a system to map people's relevant off chain experiences and social relations on the chain. Then, we establish a mechanism to standardize and process the data flow to be added to the chain, as well as prioritize them in order. In this process, we need to solve the unique challenges of decentralized identity, which includes the lack of background information about records on the chain and problems related to access to decentralized networks.

In addition, the management of reputation information also requires publicly accessible data standards which is the agreed data formats. For instance, "what is the proof of a contribution or how to represent a record on a necklace".

We make structured process for the input information to ensure the interoperability:

1) it enables the people to meaningfully combine "identity" infor–mation from different services,

2) Meanwhile, it also minimizes the possible conflicts when the platform interacts with different aspects of reputation information on the personal chain.
On this basis, in view of NUM_DID's open and searchable charac–teristics, it will be able to bring the reputation on the chain into real–world activities in the future. Thus, we can explore more use cases triggered by Metaverse.

NUM
CA—NFT
Metaverse

B-24

Metaverse NUM Plan–24

B.4 NFT value system

The integration of data into production factors has gradually formed a consensus around the world. In the contemporary society, there are some popular trends with the deepening development of the digital technology and the consumers' demand for digital design and that the different digital spaces need to be aggregated. Under the influence of these trends, Metaverse is the ecosystem of data generation, circula–tion, utilization and reorganization. The one of the indispensable tools for Metaverse is NFT.

NFT, that is a non homogenous certificate, is a new data container. The emergence of NFT has realized the capitalization of virtual goods. We can map virtual goods up the chain and make the data content become an asset entity, so as to realize value circulation.

In other words, through NFT, digital assets, works of art, music, game equipment and land property rights have their "entities" in the Metaverse. Moreover, they can realize the right confirmation, the pric–ing, the free trade and the transfer. They can also break the threshold restrictions on property rights, copyright and regulation under the traditional economic paradigm, and give full play to the potential of data, knowledge and other elements. On the one hand, the NFT boosts the development of virtual economy that meets the human imagination and release the vitality and the energy of digital economy. On the other hand, the NFT not only promotes the combination of the virtual and the real, but also realizes the digitalization of physical assets and the digital original Asset Mapping Token (AMT).

Metaverse NUM Plan–25

B.4–1 Metaverse NFTs

NFT value system of NUM can provide an easy–to–use channel for the release, deployment and sales of Metaverse NFTs to the B–end users and meet the users' demands to obtain, trade and manage Metaverse NFTs.

1) Releasing and deploying
Support the entry and release of standardized NFTs in batches. We hope to provide a platform for publishing the Metaverse NFTs, which is as simple as uploading a file to Google cloud disk. Initially, the scheme of integrating Cross Chain Wallet will be adopted to ensure the smooth Multi Chain user experience in NUM NFT value system and realize the operation of viewing Multi Chain Metaverse NFTs at the same time. The NFT value system of NUM will support Ethereum layer2, Heco and BSC protocol standards and be connected to the most mainstream blockchain Oracle Chainlink and Polkadot parallel chain slots in the market.

2) Transaction and management
We have built the online trading market of Metaverse NFTs, which is simple and lightweight and costs low level handling fee. It supports the seamless trusteeship between buyers and sellers and regular encrypted payment mode to provide protection for buyers and sellers at the same time.

Sales or resales with direct pricing: The project party displays the Metaverse NFTs in the trading market and gives a price for sale. The users pay according to the price. After payment, the assets are trans–ferred. The multiple resales of NFTs between users is also supported. Setting the customer service and the transaction time can ensure the smooth the transaction progress and protect the rights and interests of both parties.

Through the bottom layer of the blockchain and NFT technology that facilitates the recording of ownership assets, we will provide a comfort–able and smooth use experience, the rapid recharge and withdrawal, and the secure storage, as well as the complete decentralization. The Metaverse NFTs owned by the users can be stored in NUM, viewed and traded at any time, transferred to their own digital wallets and other operations.

NUM

CA–NFT

Metaverse

C⁻¹

NUM idle mobile phone computing power mining–1

IPFS and FileCoin have adopted the PoSt storage capacity consensus algorithm, which has realized the storage main chain. However, as for the nodes, the POC capacity proof algorithm based on zero knowledge proof leads to excessive dependence on the server CPU of the node and even the computing performance of the server CPU, resulting in extremely low block efficiency and waste of computing data. However, the "80–20 rule" ("Pareto Principle") is obvious that the BTC ore pool is becoming more and more concentrated.

In contrast, NUM adopts the mining algorithm of VDF consensus main chain + superimposed PoSt. It has provided the computing power market for the ordinary users, which has low power consumption and runs locally. As there is no need to communicate between partial collection nodes in the market, its calculation speed is very fast. Even the ordinary mobile phones can become the main participants in NUM mining.

C.1 Equipment

1) Access device: Android, IOS

2) Mobile mining license NFT: CA–NFT
CA–NFT uses the encryption algorithm to encrypt and decrypt data. It encapsulates the main chain consensus, the smart contract and the mining license.

Any party holding CA–NFT can use the "token" to decrypt data to participate in mining. Thus, CA–NFT must be protected from unauthorized agents (users).

The specific implementation is in the following: purchase by using NUM token and win the lottery through the growth of block height in order to activate the mining function above a certain block.

3) Value certificate and circulation medium: NUM token

NUM idle mobile phone computing power mining–2

C.2 Rules

Any mobile phone with internet access can participate in mining. NUM has set up the mining nodes all over the world, which can keep the network running smoothly and mining stably. The greater the contribution of miners to the network is, the higher the probability of mining income will become. Specifically:

1) Starting with the 0–714285 block height, the mining can be carried out directly without CA–NFT and P disk pledging num tokens, after connecting the equipment.

2) Starting with the block height of 714286, the equipment needs to be bonded and activated by CA–NFT and pledged the specified number of NUM tokens on P disk. After that, the mining can be started.

3) There is no limitation on the total amount of CA–NFT. A lottery will be drawn for every 75 pieces growth in block height and draw 1 CA–NFT each time. The larger the number of NUM tokens is held and the higher the number of exploding blocks is, the higher the probability of winning the lottery will become.

4) Number of NUM tokens pledged on P disk = the 24h estimated income of 1GB computing power * 20(maximum 10NUM).
The greater the number of the NUM token pledges, the greater the estimated income of 24h will be.
Similar with Bitcoin, the miners of NUM compete to dig blocks for huge rewards. However, NUM mining directly provides the useful services for customers. Different from the Bitcoin mining, the miners of NUM are only to maintain the consensus of the blockchain.
In the NUM computing power market, the low hardware threshold and random mining can be accepted.

Mining capacity and revenue depend on two factors:
●The first factor is the size of mobile phone hard disk capacity and the number of used mobile phones.
●The second factor is the number of NUM token pledged and the number of CA–NFT assets held. The larger the number of the two factors are, the higher the mining capacity will become. In this situation, there will be more benefits to be obtained.

NUM
CA–NFT
Metaverse

C^{-2}

NUM

CA–NFT

Metaverse

C⁻³

NUM idle mobile phone computing power mining–3

C.3 CA–NFT

The full name of NFT is non–fungible token, and the Chinese name is non homogenous pass.

The biggest feature of NFT non homogenous token is that it is indivisible and unique. Just as There are no two identical leaves in the world, so is the performance of NFT attributes. Moreover, such feature of NFT is guaranteed by its token contract in the chain, which can not be tampered with and erased.

It brings a great feature: scarcity.

From the rules, we can see the important role of CA–NFT mobile mining license in NUM mining system.

Each CA–NFT is original, scarce and unique. Its DNA is the digital symbol of mining permission.
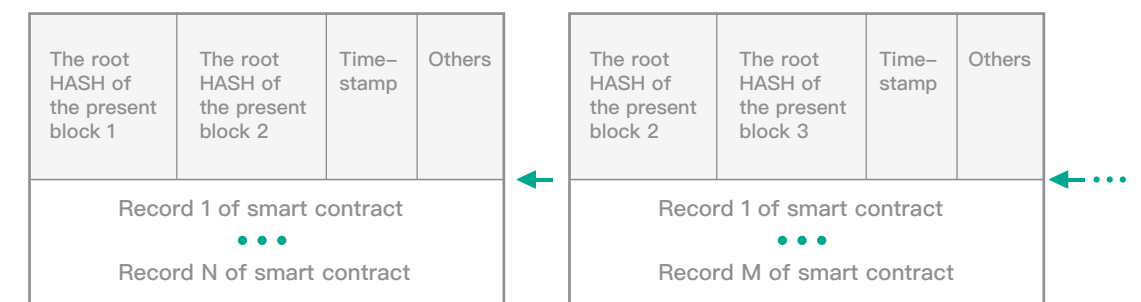
NUM idle mobile phone computing power mining–4

C.3–1 Generation

CA–NFT is a piece of code stored on the blockchain and triggered by the smart contract. The generation specifications are as follows:

● It has a unique token_id within the setting range of num smart contract.

● The token_id can only be owned by one owner (i.e. num address).

● An owner can have multiple CA–NFTs. There is another storage list record corresponding relationship between the token_id and the owner_addr.

● CA–NFT has the functions of approve, transfer, takeOwnership and other interface methods which are suitable for circulation. These methods are defined by integrating ERC721 standard.

● Defining a multiaddr type of composite address to index the metadata, including the name, certificate content or other information, which is corresponding to the CA–NFT. By using the tokenMetadata method, it can obtain the multiaddr, which is the string shaped like a URL to obtain the token metadata.

● Final transaction process

The verification node will package all contracts into a contract set and calculate the hash value of the contract set. Finally, the hash value of the contract set is assembled into a block structure and spread to the whole network. After receiving the block structure, other verification nodes will take out the hash value of the contract set which contained therein and compare it with the contract set saved by themselves.

The root HASH of the present block 1	The root HASH of the present block 2	Time–stamp	Others
Record 1 of smart contract ••• Record N of smart contract			

The root HASH of the present block 2	The root HASH of the present block 3	Time–stamp	Others
Record 1 of smart contract ••• Record M of smart contract			

Through the above mathematical programming methods, CA–NFTs has built a set of contract mode, which brings great convenience and accuracy to the identification of mobile mining license. It is far beyond the signature, seal and stamp in the real world, which is difficult to tamper with.

NUM
CA–NFT
Metaverse

C–4

NUM idle mobile phone computing power mining–5

C.4 Characteristics

● More intelligent

Due to the huge power consumption, the PoW mining represented by BTC has been listed as a backward production capacity industry in many countries. Bitcoin mining machines can only be placed in remote valleys at present. the NUM mining makes full use of the idle mobile phones, which avoids a lot of resource waste. Without con–suming a lot of power, the NUM mining users can easily mine in their own home. Moreover, the life cycle of the hard disk is much longer than the ASIC chip used by the BTC. It has no need to upgrade the equipment hardware frequently.

● More anti–centralization

BTC mining has developed from CPU to GPU, and then to FPGA to the current ASIC. The specialization of mining machinery and the concentration of computing power are becoming higher and higher. A computing power of a professional miner is tens of thousands of times that of an ordinary personal computer, while NUM mining enables everyone to participate, which can not be centralized natu–rally.

● Lower barriers to entry

NUM supports the mobile computing mining. The whole mining ecology has just started, and the dividend effect of early bird miners is obvious. If the customers want to dig BTC or FIL, they often need to invest tens of thousands or even millions. Whether in the early stage or later stage of investment, the mining cost of NUM is far lower than that of mainstream mining projects in the current market.

NUM
CA–NFT
Metaverse

C−5

NUM
CA–NFT
Metaverse

D⁻¹

NUM layered architecture–1

Based on the goal and value pursuit of the Metaverse NUM plan, NUM blockchain system can be defined as an information system used by a group on the Internet, which can act as the trust subject of the group. However, it can not be completely controlled by any individual or interest group. The different understandings and orien–tations of this definition have led to significantly different consen–sus on public chain technology.

We believe if the infrastructure of the Metaverse application sce–narios is not pragmatic, too tangled with the so–called best con–sensus absolute decentralization and unclear positioning of the NUM blockchain system's role, it will fall into the quagmire of non–commercialization.

D.1 Design principles

1) Adopt the concept and technology of service–oriented architecture: follow a series of principles, such as service–oriented principle, stan–dardization and so on, and extract typical business components, so that the system can easily and flexibly adapt to future changes in business and technology.

2) Business process principle: the processing is treated as the method to describe the business processing and differentiate the business, so that each process does not interfere with each other. Through the configurable process design, the business is flexible and easy to adjust.

3) Module reusability principle: For the design of business processing system, the users should break the tight coupling and vertical shaft way, and modularize the business processing with appropriate granu–larity, which is convenient for reuse and conductive to restructure to meet new requirements conveniently and quickly. At the same time, it is conductive to reduce the cost of development and maintenance.

4) Loosely–coupled principle of subsystems: the loosely–coupled principle should be followed among the subsystems. On the premise of not affecting business and performance, the loosely–coupled design is adopted to enhance the independence of each subsystem and make the subsystem division and responsibilities much clearer. The change of the subsystem itself will minimize the impact on other subsystems, so as to ensure the flexibility of the whole business.

NUM layered architecture–2

D.1 Design principles–2

5) Cohesive principle of subsystem: the cohesive principle should be followed among the subsystems, which combines similar functions into corresponding subsystems. The unique data of the subsystem should also be placed inside the subsystem. It makes the subsystem become an organic and complete whole part in order to make the architecture clear and easy to maintain.

6) Layered design principle:
The goal of layering is to decouple the overall complexity of the architecture; maintain the flexibility, the stability and the scalability of the architecture; improve the flexibility, reusability and scalability of the technical architecture; reduce the redundancy at the architecture level and adapt to the continuous change and development of the business.

D.2 Five–layer–architecture

In terms of technical architecture, NUM adopts a five–layer–architecture which includes the data layer, the transport layer, the consensus layer, the protocol layer and the mining layer. Focusing on the possible performance bottlenecks in the operation of large–scale Metaverse applications and the possible problems of distributed data transmission and storage, NUM has taken highly targeted solutions.
As shown below, from the perspective of architecture design, Num has great potential to become a super underlying network that can support a large number of commercial Metaverse application.
●Data layer: this layer contains the basic data unit and data structure of NUM, NUM Chain, NUM Ne, fragmentation, layering, LevelDB, StateTrie tree.
●Transport layer: it can be used for connection, data transmission and load balancing; Encrypted P2P network protocol
●Consensus layer: the hybrid consensus algorithm of VDF+PoSt embedded in NUM, Consensus management, Smart contract
●Protocol layer: the superimposed (partial) post protocol embedded in NUM, the smart contract virtual machine supported by the multi languages, the Solidity contract in new version, the criteria of NRC721 and NRC1155, the digital identity, the transaction processing, and the asynchronous communication
●Mining layer: Provide SDK and API for computing power mining of Android and IOS systems, Blockchain iot gateway, Distributed storage cloud, Buffle test framework, Blockchain browser, Destroy of standard interfaces, Database management / operation / query component

NUM
CA–NFT
Metaverse

D^{-2}

NUM
CA–NFT
Metaverse

D^{-3}

NUM layered architecture–3

D.3 Overview of Architecture

1) Data layer

This layer is the bottom layer of NUM carrying Metaverse applica-
tions and supports data technology facilities when different storage,
transmission and mining requirements are met. This includes ecologi-
cal value facilities and computing facilities. It needs to be considered
from three aspects of the overall technical performance, the scale
capacity and the facility integrity. This is the basic link of project
feasibility.
For example, Num network integrates the underlying blockchain
network with the main chain. It has maximized the advantages of
slicing and layering technology. With high scalability, NUM Network
improves the node processing capacity, which greatly improves the
blockchain trading capacity. It has basically achieved the experience
of quick speed. As another important infrastructure, NUM Network
provides resource support for NUM Chain.

In addition to the rigid index of TPS, no matter how strong the pro-
cessing power of a blockchain is, it is only equivalent to a super
server which is limited by the server processing capacity and IO
access capacity: NUM StateTrie tree is upgraded to a 64–fork–tree
to achieve fast and effective state verification, provide faster parallel
transactions, optimize the complexity of numerical storage and query,
and improve the transaction execution performance. LevelDB also
supports data compression and other operations, which is directly
helpful to reduce storage space and increase IO efficiency. The com-
bination of NUM StateTrie tree and LevelDB can fully meet the con-
currency and load balancing requirements of large–scale applications.

While retaining the distributed advantages of blockchain, this solution
utilizes piecewise infinite expansion of parallel computing, which can
effectively solve the concurrency problem. This is a very pragmatic
and effective approach.

NUM

CA–NFT

Metaverse

D^{-4}

D.3 Overview of Architecture–2

2) Transport layer

The encrypted P2P network of NUM undertakes the efficient opera-
tion of the whole storage ecology from three aspects: connection,
data transmission and load balance.

The P2P network of NUM is a fully encrypted network, which pro-
vides two connection modes of UDP and TCP. In the NUM Network,
there are two ways of initial node discovery. The first one is called
the DNS–seed, which is also known as DNS seed node. DNS is a
query service of the centralized domain name. The second one is to
hard code some addresses in the code. These addresses are called
the seed–node. When all the seed–nodes fail, the whole node will try
to connect these seed nodes.

NUM uses the UPnP protocol as a LAN penetration tool. As long as
the routing device in the LAN supports NAT gateway function and
UPnP protocol, the blockchain node can be automatically mapped to
the public network.

In terms of synchronous blockchain, Num adopts the HeaderFirst
scheme. It provides block header first synchronization. After synchro-
nization, Num obtains the block body from other nodes, which can
provide a better interaction process and reduce the network burden.

3) Consensus layer

Due to the special full backup storage mode of blockchain, the cost
of big data access is unbearable for ordinary users. The expensive
ram price of EOS fully reflects this. IPFS and FileCoin have realized
the storage main chain. However, they rely too much on the server
performance of the node, which lead the very low blocking efficiency.
It does not really solve the problem of the storage data integrity.
Therefore, Num adopts the integrated consensus algorithm of VD-
F+PoSt. The VDF implemented at the block height can delay the
verification capability, making the main chain more stable. By using
the main chain mining, it builds a mobile computing mining market
with ultra–low energy consumption to meet the storage and process-
ing needs of all kinds of long data.

NUM layered architecture–5

D.3 Overview of Architecture–3

4) Protocol layer

In order to facilitate the development of the technical community and promote the establishment of the NUM blockchain model, NUM is equipped with a smart contract virtual machine supported by the multi–language on the basic technology layer. Everything is handled flexibly according to the needs of users.

The protocol layer has established all contract applications supported after the main network mapping, as well as a batch of application protocols and basic templates, such as the digital identity, the trans–action processing, the asynchronous communication, the data input & output protocols and so on. The protocol layer has also enriched the classification application interface. Relying on these protocol specifi–cations and interfaces, the users can easily access the ecosystem through corresponding applications. This is an important technical support for NUM to establish the Metaverse business model.

5) Mining layer

NUM has established a random idle mobile phone mining market that can accommodate the low hardware threshold.
The mining capacity and revenue depend on two factors:
The first factor is the size of mobile phone hard disk capacity and the number of used mobile phones.
The second factor is the number of NUM token pledged and the number of CA–NFT assets held. The larger the number of the two factors are, the higher the mining capacity will become. In this situa–tion, there will be more benefits to be obtained.
The entire mining process is also the process to discover the value of NUM token.

Summary:
NUM is not only a viable public chain project, but also combines basic applications: CA–NFT idle mobile phone computing power mining, the bottom layer of commercial–grade DISTRIBUTED cloud storage, the decentralized communication or transmission bottom layer, NUM_DID — the decentralized identity system based on the reputation, Decentralized identity system based on the reputation, NFT value system, and so on have established a more feasible busi–ness model of Metaverse on the public chain.

Other technical solutions at the bottom layer–1

In addition to the consensus algorithm, NUM also adopts the seven high availability solutions, which include the encrypted P2P network, the Metaverse NFTs scheme, the fragmentation, the layering, the data layer optimization, the upgrade of StateTrie tree, and the data processing. They have solved the problem of the low efficiency of general VDF main chain network communication (transmission) and provides an intelligent NFT integrated solution.

E.1 Encrypted P2P network

If we simply look at P2P technology, its application fields have been very extensive, which are from streaming media to point–to–point communication, and from file sharing to collaborative processing. It has appeared in many fields. Similarly, there are many P2P network protocols. BitTorrent, ED2K, Gnutella, Tor and others are the common P2P network protocols. They are what we often call BT tools and electric donkeys. Bitcoin, Ethereum and many other digital currencies have implemented their own P2P network protocols. However, this model is different from the P2P network protocols discussed above, which refers to the encrypted P2P network protocols and algorithms. The encrypted P2P network of NUM is responsible for the efficient operation of the Metaverse NUM plan in terms of the connection, the data transmission, and the load balancing.

NUM
CA–NFT
Metaverse

E^{-1}

NUM
CA-NFT
Metaverse

Other technical solutions at the bottom layer–2

E.2 Network connection and topology

E.2-1 Network connection

Excepting for a few blockchain projects that support the UDP proto-col, the network protocol at the bottom layer used by most blockchain projects is still the TCP/IP protocol. Therefore, from the perspective of the network protocol, the blockchain is actually on the basis of TCP/IP network protocol, which is at the same layer as HTTP protocol and SMTP protocol, that is, the application layer.

The interaction mode with the server represented by HTTP protocol has been completely broken on the blockchain. It changes to a full point-to-point topology. This is the origin of Web3.0 proposed by the Ethereum and the technical model adopted by NUM. In the following, we discuss the P2P network discovery and routing of NUM in the full-node scenario:

The P2P network of Bitcoin is built based on TCP. The default com-munication port of the main network is 8333.

The P2P network of NUM is different from bitcoin. As the fully encrypted network, P2P network of NUM provides two connected modes which are UDP and TCP connection modes. The default TCP communication port of the main network is 30303 and the recom-mended UDP discovery port is 30301.

E.2-2 Topologies

There are many kinds of P2P network topologies. Some are central-ized topologies; some are semi centralized topologies; and some are fully distributed topologies.

The network composed of all NUM nodes is a fully distributed topolo-gy. The transmission process between nodes is closer to the "flooding algorithm", that is, the transaction is generated from a node, then broadcasted to the adjacent nodes. Then, the adjacent nodes spread from one node to another one, until they spread to the entire network. The full node and SPV simplify the interaction mode between the payment verification clients, which is closer to the semi-centralized topology, that is, the SPV node can randomly select a full node to connect. This full node will become the agent of the SPV node and help the SPV node to broadcast transactions.

E^{-2}

NUM
CA–NFT
Metaverse

Other technical solutions at the bottom layer–3

E.3 Node discovery

Node discovery is the first step for any blockchain node to access the blockchain P2P network. It's the same as traveling to a strange place alone. If there is no map and navigation, you can only ask people nearby for directions. Such kind of action can be understood as node discovery.

Node discovery can be divided into initial node discovery and post startup node discovery. Initial node discovery means that your whole node has just been downloaded. In the first operation, there is no node data. After startup, it is found that the running wallet can follow the network to dynamically maintain available nodes.

E.3–1 Initial node discovery

In the NUM network, there are two ways of initial node discovery. The first method is called DNS–seed, also known as DNS seed node. DNS is a centralized domain name query service. The community defenders of NUM will maintain some domain names. If we try to connect to port 8333 of a host under the domain name through the NC command, we will find that the connection is successful.

So far, we have done the initial node discovery manually, and these operations are done by the code of NUM.

The second method is to hard code some addresses in the code. These addresses are called the seed–node. When all the seed–nodes fail, the whole node will try to connect these seed nodes. When applied in the NUM, the idea is roughly the same, which is to also hard–coded some seed nodes in the code to do similar work.

E–3

Other technical solutions at the bottom layer–4

E.3–2 Node discovery after startup

In the NUM network, a NodeTable is maintained. However, this Node–Table is is different from the simple maintenance of Bitcoin. t uses a mature algorithm in the P2P network protocol, which is called the Kademlia network, or KAD network for short. It uses DHT (Distributed Hash Table) to locate resources. the Chinese name of DHT is distrib–uted hash table. The KAD network maintains a routing table to quickly locate the target node. Since the KAD network is based on the UDP communication protocol, the node discovery of the NUM node is based on UDP. If the node is found, the data interaction will switch to the TCP protocol.

E.3–3 Blacklist and long connection

The network environment faced by public blockchains is very open. Anyone who has downloaded the wallet and opened it will enter the P2P network, which will also bring the possibility of being attacked. Therefore, there will be a control logic in the code of NUM. You can manually remove the nodes you think are suspicious and add them to the prohibited list, and configure trusted nodes at the same time. Of course, the above is not part of the client's standard protocol. Anyone can implement their own P2P network layer. In addition, we can also process the blacklist through the firewall of the operating system.

NUM
CA–NFT
Metaverse

E⁻⁴

Other technical solutions at the bottom layer–5

E.3–4 LAN penetration

In above, we mentioned that the P2P network structure of the block–chain is a fully distributed topology. However, our present network environment is composed of local area networks and the Internet. In other words, when you run a blockchain node on the local area net–work, it cannot be found on the public network. The nodes on the public network can only passively accept connections. They cannot initiate connections actively.

If you can control the LAN, you only need to configure routing in the VPC network and map the public IP and port to your IP and port in the LAN.

This condition is very harsh. Thus, is there a scheme that can create a mapping on its own? The answer is: Yes, it is NAT technology and UPnP protocol.

NAT technology is very common. NUM uses UPnP, which is the abbre–viation of Universal Plug and Play. It is mainly used for the intelligent interconnection of devices. By using it, all devices on the network will immediately know that there are new devices added. These devices can communicate with each other and directly use or control it. Every–thing does not need to be manually set.

NUM uses the UPnP protocol as a local area network penetration tool. As long as the routing equipment in the local area network supports the NAT gateway function and the UPnP protocol, the blockchain nodes can be automatically mapped to the public network.

NUM
CA–NFT
Metaverse

E⁻5

NUM
CA—NFT
Metaverse

E⁻⁶

Other technical solutions at the bottom layer–6

E.3–5 Node Interaction Protocol

Once the node is connected, the interaction between the nodes is to follow some specific commands. These commands are written in the head of the message, while the message body is the content of the message.

There are two types of commands. The one is request command and the other is data interaction command. The first thing to do when the nodes are connected is called a handshake operation. It is to greet each other and provide some brief information, such as, exchange the version number firstly, to see if it is compatible and so on. In addition, NUM provides the symmetric encryption for the handshake process.

After the handshake is completed, no matter what information is exchanged, a long connection is required. In the design of NUM, the PING/PONG protocol is moved to the process of node discovery. The request commands are generally divided into initiator requests and inv command. From the perspective of initiator requests, the getPeers command in NUM is the example which is to obtain a list of available nodes of the other party. However, the inv command provides the data transmission. The message body will contain the data vector.

We say that the most important function of the blockchain is to syn–chronize the blockchain. The synchronization block happens to be the most able to test the capabilities of P2P networks. There are two block synchronization methods. The first one is called the HeaderFirst which provides block header first synchronization. After synchroniza–tion, Num obtains the block body from other nodes. The second method is called the BlockFirst. This block synchronization method is relatively simple and rough, that is, the blocks obtained from other nodes must be complete.
NUM adopts the first scheme, which can provide the superior interac–tion process and reduce the network burden.

Other technical solutions at the bottom layer–7

E.3–6 P2P messages

The bottom layer of the point–to–point transmission adopts the Kademlia protocol, hereinafter referred to as Kad. It is a research result "Kademlia: A peerto –peer information system based on the XOR metric" published by petarp. Maymounkovand David Mazieres of New York University in 2002. Simply put, Kad is a distributed hash table (DHT) technology. However, compared with other DHT imple– mentation technologies, such as Chord, CAN, Pastry, and so on, Kad has established a new DHT topology based on a unique exclusive–or algorithm (XOR) as the basis for distance measurement. Compared with other algorithms, it greatly improves the query speed of routing.

E.4 Metaverse NFTs scheme

E.4–1 Deployment contract

The smart contract scheme adopted by NUM is deployed by sending a transaction. This contract contains functions related to the creation of Metaverse nfts scheme, transactions and others.

E.4–2 NFT content

Taking the game props as the example, the local content nfts of Metaverse application developers can be a pet.png, a weapon.png, a piece of land.png, and so on. They are uploaded and fixed to the NUM network, which generate the link to the content data: Content URI (Games://+CID).
Note: CID is a unique identifier for the description of a piece of con– tent (the hash value of the content).

NUM
CA–NFT
Metaverse

E−7

NUM
CA–NFT
Metaverse

E⁻⁸

Other technical solutions at the bottom layer–8

E.4–3 Tokenization

The NFT content is added with its name and some descriptions to form the metadata to complete the tokenization of the creative content, which form a digital asset. By uploading the metadata to the NUM network, the metadata URI (Games://+CID) will be gained.

E.4–4 Assets on the chain

The developer sends a transaction containing the NFT metadata URI to the smart contract in 1) from his external account to call the casting method in the contract, and then returns the unique identifier of the NFT in the current contract–Token ID. The return of the Token ID indicates that the NFT was created successfully. After the transaction miner is packaged into the block and confirmed, the contract will trigger a transfer event and send the Token ID to the developer. The occurrence of this incident marked the confirmation of NFT ownership and usage rights.

NUM
CA—NFT
Metaverse

E —9

Other technical solutions at the bottom layer–9

E.4–5 Tokenization

In terms of the cross–chain of Metaverse nfts, what users are most concerned about is the security of assets.

What NUM uses is to design a multi–chain interconnection bridge net–work at the bottom of the blockchain. Every time a blockchain is con–nected, a set of interface protocol components needs to be implement–ed, which will be used for data interaction between two chains. Through the consensus node, the multi–signature addresses (smart contracts) are created and managed. The node is responsible for the transfer–in verification and transfer–out execution operations of assets to ensure the safe operation of the network.

1) The oracle

By using the Chainlink, NUM can securely connect NFT to iot data, web API and various data providers. It can also use Chainlink VRF to obtain the verifiable random numbers, interact with off–chain back–end sys–tems, and even trigger cyber–physical systems. All of the above func–tions can be used to create nfts, carry out P2P transactions and check the status.
In addition, the decentralized price feed supported by Chainlink can provide highly accurate, usable and tamper–proof price data for the smart contracts of NUM. It can connect to all on–chain and off–chain high–quality data sources. Each price feed is decentralized at the oracle network and data source level, which enables NUM to provide the highly available and manipulative oracle data and services.

2) Polkadot slot

Whether it is a homogeneous blockchain based on Substrate, or het–erogeneous blockchains like Bitcoin, Ethereum, EOS, and others, they are all independent blockchains and the isolated islands. When NUM is connected to the Polkadot slot, it can interact with the Polkadot relay chain and other parallel chains connected to the Polkadot directly or through a transfer bridge, so as to generate more overlay services. It can improve its scalability, and enjoy the security provided by relay chain.

NUM
CA-NFT
Metaverse

E⁻¹⁰

Other technical solutions at the bottom layer–10

E.5 New fragmentation commands

The fragmentation is not a new thing. It is a general term of a kind of technology, which is not invented in the blockchain. In fact, in the first centralized world, Google and Facebook have been using the fragmentation for many years. At present, there are different types of fragmentation in the market, such as the status fragmentation, the transaction fragmentation, the network fragmentation and so on.

Ethereum is the platform at bottom layer in all blockchains that keeps pace with the concept of fragmentation. To understand why the Ethereum developer community wants to implement fragmenta–tion, the focus is to understand what fragmentation is and why this solution is so attractive.

According to the statistics of ETH Gas Station, adding a transaction to the Ethereum blockchain takes about 1.78 minutes. A new block is generated every 32 seconds, and an average of 15–20 transactions are processed per second. This ecosystem creates an environment which is conducive to miners rather than users. If the users want to give priority to their transactions, they must increase their gas price.

Low throughput, high latency and high price limit the performance of Ethereum network. Therefore, due to the lack of fragmentation, Ethereum is not suitable for deploying services and applications requiring strong scalability such as metauniverse and so on.

As a commercial–level Metaverse application infrastructure, NUM adds the fragmentation instructions to the underlying architecture. The main chain provides the internal transaction execution of frag–mentation and improve the efficiency of single–chip execution and cross– fragmentation execution. By the state fragmentation, the different fragmentation schemes can be realized according to the user needs.

NUM
CA–NFT
Metaverse

E –11

Other technical solutions at the bottom layer–11

E.6 Scalability

The Internet is a symbol of speed and efficiency. We are even accus–tomed to the invigoration of the speed in second. For any product that requires a waiting time of more than 7 seconds, we are increasingly losing patience. This is precisely the real inferiority complex of block–chain.

In order to achieve both security and high throughput, Num designs an elastic fragmentation layer (state fragmentation) on the underlying architecture. In short, this is a partition method, which can disperse the computing tasks and storage workload in the encrypted P2P net–work. After this processing method, each node does not have to deal with the transaction load of the whole network. It just needs to main–tain the information related to its partition (or fragmentation).

In order to further explain the fragmentation of NUM network, we make an association:

As you can imagine, you now only have one highway. Then, what the other public chains want to do is to make cars drive faster. In this case, more cars will pass per unit of time. Nevertheless, the problem is that the car cannot speed up without limit. For example, if it is raised from 50 to 100, it will become not safe with the raised speed. Thus, it can't be speeded up, what should I do? The flexible fragmentation of NUM means that I can run many highways at the same time. If one is not enough, run two, if two are not enough, run four. If four is not enough, run eight. We can repair the new highway without any restric–tions. Even if the car is not driven fast enough, there are more cars passing at the same time.

NUM
CA–NFT
Metaverse

E^{-12}

E.7 Changing data layer to LevelDB

LevelDB is an open source project initiated by Google's heavyweight engineers Jeff Dean and Sanjay Ghemawat.

In short, LevelDB is a C++ library that can handle the persistent storage of key–value data with a scale of one billion.

The replacement of NUM data layer to LevelDB has the following characteristics:

LevelDB is a persistent storage KV system, which is not like a memory–based KV system such as Redis and others. LevelDB will store most of the data on disk rather than eat as much memory as Redis does. When storing data, the LevelDB is stored in an orderly manner according to the recorded key values, that is, the adjacent key values are stored in order in the storage file, and the application can customize the key size comparison function. LevelDB will store these records in order according to the user–defined comparison functions.

Like most KV systems, the operating interface of LevelDB is very simple. Its basic operations include writing records, reading records, and deleting records. Atomic batch operations for multiple operations are also supported.

LevelDB supports the data snapshot function, so that the read operation is not affected by the write operation. In this situation, the users can always see consistent data during read operations.

LevelDB also supports the operations, such as data compression and so on, which directly helps reduce the storage space and increase the IO efficiency.

The performance of LevelDB changed by the NUM data layer optimization is very outstanding: Its random write performance reaches 400,000 records per second, while its random read performance reaches 60,000 records per second. It is more stable, enabling data compression to reduce node space. The automatic snapshot function reduces the memory usage.

NUM
CA-NFT
Metaverse

E-13

Other technical solutions at the bottom layer–13

E.8 StateTrie tree

We call the process of communication between blockchains as the asset bridging which requires an effective mechanism to verify the status of different chains. One way to achieve this goal is to verify the Merkle proof of the state of other blockchains through smart contracts. In this case, it is an asset transfer request. The verification of these proofs needs to be lightweight and efficient to achieve the consumption efficiency of smart contracts.

Ethereum uses a modified Merkle Patricia tree to verify state data. However, the Patricia tree of Ethereum is hexadecimal. Each node contains 16 sub–nodes. This is less efficient than binary trees and more difficult to handle. Realizing the speed and performance required for the commercial application of Metaverse requires state authentication to be as efficient as possible. It promotes the NUM technical team to improve the sparse Merkle tree accordingly in order to help us to increase throughput.

The StateTrie tree is an improved sparse Merkle tree. It stores the value in the highest subtree that contains only one key. The advantage achieved by this is: on average, in a tree containing N random keys, only log(N) hash operations are required to update the keys in the tree.

The NUM StateTrie tree is upgraded to a 64–ary tree. It realizes fast and effective state verification, provides faster parallel transactions, optimizes numerical storage and query complexity, and improves transaction execution performance. At the same time, it also contains the following features: efficient Merkle proof verification; efficient database reading and storage through node batch processing; reduction of data storage and hash calculation; and use of goroutine to update multiple keys at the same time.

NUM
CA—NFT
Metaverse

E—14

E.9 Data processing

E.9—1 Fault tolerance mechanism

In the process of block breaking, 2/3 of the BFT parameters are used for fault tolerance. In the transactions, P = 60% – 80% is used for fault tolerance. If the node block cannot keep up or the data is lost, the block with the most ideal height will be selected from the network for transaction rollback and automatic repair.

E.9—2 Cache processing of pending block transactions

NUM has a transaction data caching mechanism. After the current invoke application submits the transaction data to the node server through the SDK interface, the node server will save the received transaction data in the transaction buffer queue of the pending block, and return the receipt of invoke application data. The queue of pend—ing block transactions includes a two—stage cache architecture of a memory queue and a permanently stored database. Transaction data will be stored in the database first, and then in the memory queue. Once the memory queue reaches the preset maximum value of pre—served cache space, the cached transaction data only stays in the database until the space occupied by the memory queue is lower than the present value. The set value will be automatically reloaded into the memory queue again.

E⁻¹⁵

Other technical solutions at the bottom layer–15

E.9–3 Data deduplication

The transaction data legality verification mechanism of NUM confirms whether the received transaction data has been encrypted by the legal SM4 authorized by the system. Otherwise, it will directly refuse to receive it, as the risk of being intercepted and tampered by the network is too high. After that, the transaction data will be verified to verify whether the transaction data is signed and authenticated by legal users, so as to further avoid the probability of tampering with the transaction data.

In the transaction data consistency verification mechanism of the system, each node server will verify the data consistency when receiving the broadcast synchronized transaction data. At the same time, each node server will compare with the existing transaction data in the trans–action data queue to be blocked. Once it is determined that the system has received the same transaction data, it will no longer be recorded, thereby avoiding the repeated recording of the transaction data.

E.9–4 Data storage expansion and frag– mentation

Achieving application–transparent data storage expansion can easily implement a variety of data storage methods. Through storage fragmen– tation, the data storage performance can be greatly improved without changing the way the application is used.

E.9–5 Unstructured file storage consensus

The data is stored on each node, which is not shared with each other. The data storage's loss of a small number of nodes will not affect the normal operation of the main chain.

Economic model–1

The Metaverse NUM plan itself covers:

1) NUM public chain, distributed cloud storage and decentralized com‑
munication/transmission bottom layer
2) CA–NFT idle mobile phone computing power mining
3) Metaverse application support products including virtual reality
platform, the decentralized identity system based on reputation
(NUM_DID) and the NFT value system.

Its business logic is to enable all pass holders to reach a consensus on
a global scale and devote themselves to the construction of the whole
Metaverse NUM plan. Therefore, NUM provides a new way of com‑
puting power value – NUM token. It can be used as a value voucher in
all links and production of the Metaverse NUM plan. The specific char‑
acteristics of the token are: universality, ease of use, commercializa‑
tion, and the realization of lower development cost and higher devel‑
opment efficiency of Metaverse.

NUM tokens are completely mined and produced by the mobile phones
of users without the pre–excavation and the private placement. Its
price is based on the relationship between market supply and demand.
It is a real application token, which can fully penetrate the application
layer and the incentive layer of the Metaverse NUM plan.

F.1 Issuance, distribution and destruction

There is no limit to the total amount of NUM tokens issued.
The foundation has a long–term destruction plan for NUM tokens. The
transaction gas fee is completely destroyed, and the destruction
address is publicized, which can ensure the stable increase of the
value of NUM tokens and maintain the steady development of the
NUM's ecology.

The distribution method is as follows:
1) All mining output.
2) At block 0–714285, each block will be rewarded with 0.1 coins.
There is no need for mortgage and CA–NFT certification. The users
all over the world only need to hold a mobile terminal, and there is no
threshold to enter NUM.
3) Starting at block 714286, 1 coin per block. Each mobile phone
needs to be bound to NUM's CA–NFT, and the estimated amount of
currency produced per mobile phone share (maximum 10NUM). in the
next 20 days can be connected to the network.

NUM
CA–NFT
Metaverse

F⁻¹

Economic model–2

F.2 Value

As the cornerstone of the Metaverse NUM plan, NUM token was given appreciation logic as early as the beginning of its design to ensure the income of miners and the stable operation of the main chain.

Value performance also lies in the following factors:

●The ability to implement smart contracts
●The ability to attract and carry Metaverse applications and products. Specifically, it manifested in the scale of the developer community.
●The more users there are, the greater the consumption of resources and the more coins the relative project party needs.
●The mobile computing power mining market constructed by NUM creates a rich profit model for NUM tokens;
●In the future, with the development of NUM's main chain, its tokens will be empowered with more usage scenarios.

NUM
CA–NFT
Metaverse

F^{-2}

NUM
CA–NFT
Metaverse

G

Disclaimer

This document is only used for the purpose of conveying information rather than constitute opinions related to the sale of shares or securi–ties. Any similar proposal or levy will be carried out under a trustworthy clause and permitted by applicable securities laws and other relevant laws. The above information or analysis does not constitute investment decisions or specific recommendations. This document does not con–stitute any investment advice, investment intention or abetting invest–ment in the form of securities. This document does not constitute or be understood as offering any trading behavior, or any behavior of inviting to buy and sell any form of securities, nor is it a contract or commitment in any form. NUM clearly stated that the relevant intended users clearly understand the risks of the NUM project. Once the par–ticipant participates, it means that he understands and accepts the risks of the project and is willing to personally bear all the correspond–ing results or consequences.

Many digital asset exchanges have stopped operating because of security problems. We attach great importance to safety. However, there is no absolute 100% safety in the world, such as various losses caused by force majeures and so on. We promise to do everything possible to ensure the security of your transaction. Before participat–ing in this project, you must carefully read the project white paper. Unless you fully understand all the contents of the project white paper, the project vision and the risk of possible failure. Otherwise, you should not participate in this project.