Blockchain Project White Paper

Table of Contents

1. Introduction

IT From Bit, everything comes from bits, everything is information. In today's world, informatization and digitization are irreversible trends. As a data democratization revolution to the traditional Internet, blockchain provides a powerful technical guarantee for data right confirmation, free data flow, and unlimited exchange of value.

As the basic means of production for the future digital economy, data work as land, labor and capital in modern society. Therefore, building a democratic, secure, and freely exchanged data market is an important foundation for the future society.

Decentralized storage represents the future direction of large-scale storage development because of its huge advantages in efficiency and economy. Decentralized storage eliminates centralized control and allows users to freely store and share data; decentralized storage eliminates the risk of data loss and service interruption, while increasing data storage security and data privacy protection.

Although many teams around the world are building such decentralized storage systems, most of them are not satisfactory. Based on our experience in PB-level storage systems, we propose to build a decentralized, modular, and scalable decentralized storage network-Fermat Blockchain Network.

2. Blockchain

2.1 Bitcoin and Blockchain

Bitcoin, a peer-to-peer encrypted digital currency, is a digital simulation of the "mint" of human beings, returning the coinage to individuals. Realize fairness and justice, and realize the protection of private property rights. The spirit of Bitcoin guides thousands of believers to form a "coin-protecting" expedition team to start the journey of the Internet with technological innovation + financial innovation.

If you invested 1 USD in Bitcoin in 2010 when the price of Bitcoin was around USD 0.1, you could get 10 Bitcoins, which will now be worth more than USD 100,000. According to the latest report from the Bank of America, this is the best investment opportunity of this century, not one of them.

Although Bitcoin is still a highly speculative investment, it does not hinder its rapid development. In the past ten years, Bitcoin has become the most popular and widely recognized encrypted digital currency. More and more retailers accept Bitcoin as a payment method. Some investment companies and exchanges have begun to use Bitcoin for futures transactions. Since 2018, the United States, Europe, Russia, and China have all accelerated their legislation in the field of encrypted digital currencies to promote the development of the cryptocurrency industry and compete for the commanding heights of the industry.

Since the second half of 2018, the development of the cryptocurrency industry has entered a new era and has become the frontier field of the game among major powers. The United States has conducted countless hearings in the field of cryptocurrency. The Standing Committee of the Politburo of China collectively studied the blockchain and raised it to the height of national strategy. Specifically, Facebook (FB) plans to launch the Libra digital currency plan, the People's Bank of China is preparing to launch the People's Bank of China digital currency (DECP), and Europe is intensively launching the European Central Bank digital currency, etc., which are further verified that Bitcoin and other cryptocurrencies is the future opportunity.

Blockchain, as the underlying technology of Bitcoin, has now become the most cutting-edge technology.

The essence of the blockchain is a decentralized database ledger, which uses technical and economic incentive mechanisms to ensure 100% security of the blockchain network to ensure that the ledger database is credible, safe, transparent, non-tamperable, and traceable. As a result, a broad consensus has been formed on the value of cryptocurrency (token) assets based on the blockchain network in time and space.

With blockchain technology, for the first time in history, mankind has truly realized the inviolability of private property by technical means; with blockchain technology and consensus, mankind is expected to break the isolation between regions and ideologies and realize value interconnection. Reduce the cost of trust, work together to achieve great progress in human society.

In general, the blockchain is a combination of technological innovation and financial innovation, cryptocurrency (token) is the crystallization of its innovation, consensus is the foundation of the existence of cryptocurrency (token), and technology and economic models are the guarantee of consensus. Therefore, all blockchains without consensus are pseudo-blockchains. Without a strong consensus mechanism to escort, blockchain projects cannot be far-reaching.

2.2 Blockchain and private property rights

Owning well-defined and strictly protected property rights is the foundation of all societies. On top of this, buyers and sellers in the market can freely match, and then achieve specialization, thereby achieving social and economic prosperity and innovation.

If we regard the blockchain as a new way of organization, what powers will it release? We all know the rules of Bitcoin's "social contract": anyone can use the Bitcoin network without permission (no censorship), and only those who own Bitcoin can conduct transactions (cannot be confiscated), and no government can issue bitcoins to steal purchasing power from others (without inflation), and finally, anyone can verify that the rules are

followed (cannot be faked) before accepting payment. And all of this can withstand the test. It can exist independently of the state, centralized authority or traditional legal structure.

In the future, the blockchain network and its encrypted digital currency (token) will enable mankind to have the highest form of property rights than at any time in history. It will not only make people have property rights, but even machines will have property rights.

It separates property rights from the legal system and gets rid of the monopoly of violence. For the first time, we can own property that does not depend on local government enforcement and protection. It is easy to hide, defend, split, transfer and verify-all by yourself, which allows you to have the highest personal sovereignty.

Property rights were once firmly dependent on other aspects of the social system, especially the monopoly on violence and legal systems. If the foundation of property rights is slightly unstable, one cannot have strong property rights, and social unrest will follow. But because the blockchain is completely independent, it can bring the highest level of property rights to anyone in the world, regardless of the quality of its underlying institutions, government or legal system.

Today, human society is accelerating its entry into the digital economy era. In the future, similar to land, labor and capital in modern production relations, data will become the basic means of production. How to confirm data rights? How to establish a data trading market for data is the most fundamental issue in the digital economy era. This is not only related to production relations, but also to the distribution mechanism, and to the long-term development, peace and stability of human society.

Blockchain will empower the digital economy era and give data ownership to its producers (owners).

2.3 The development path of blockchain

By 2020, the blockchain has been developed for ten years, and three different eras have gone through in between.

The era of agreement (2008-2013). When the protocol era reached its peak, Bitcoin became the dominant cyberspace economy by virtue of its relatively simple economic entity. In this era, there are great obstacles to introducing new types of economic agents (scripts). In addition, in this era, there are major obstacles to changing economic rules (forks). These shortcomings are the main driving force behind the emergence of the new cyberspace economy, specifically the changes in agreements and the emergence of new economic entities.

The era of smart contracts (2014 - 2019). With Ethereum becoming the dominant cyberspace economy, the era of smart contracts has reached its peak. This era provides solutions to the drawbacks of the agreement era by lowering the barriers to introducing new economic entities and allowing the creation of sub-economy in a larger cyberspace economy. The Ethereum Virtual Machine (EVM) and its programmable smart contracts have spawned the explosive growth of new professional economic agents (smart contracts) and sub-economy (token). More importantly, this era has brought so-called internal interoperability: that is, the interoperability between these sub-economies, but still within the larger cyberspace economy. The limitation of the capacity (cost, throughput) of the smart contract platform is the main driving force for the emergence of the alternative smart contract blockchain, in the change of the agreement and the emergence of new economic entities.

Today, we are in the third era.

The era of interoperability (>2020). Most current blockchains are in a fully self-sufficient state, and each blockchain project is rarely connected with other blockchain projects or actual economic activities. However, there are clear signs of major innovation in the industry, and many projects are making significant progress towards a more open cyberspace economy. On the one hand, it is working day and night to study and develop new technologies such as interoperability, cross-chain communication and atomic exchange; on the other hand, it is connected with the real economy through technologies and mechanisms such as data confirmation, oracle, and probabilistic random verification. Which is what everyone calls "real economy on the chain".

Conclusion

Based on our understanding of the industry and experience in the field of distributed storage. We proposed the Fermat blockchain protocol.

The Fermat protocol is based on the POC consensus algorithm. It will build a decentralized, modular, and scalable decentralized storage network, establish a globally distributed data center, powerful distributed cloud storage service capabilities, and prosperous data transactions the market is committed to becoming the infrastructure of the future digital economy.

3. Fermat Network Framework

The Fermat Blockchain Network system will use technologies such as P2P network communication, data encryption, IPFS network protocol, cross-chain communication and interoperability, and at the same time develop a payment system to meet the millions-level transaction payment needs of the data market.

3.1 Framework Overview

The foundation of Fermat Blockchain Network is as follows:

Data storage: When storing data on the network, the client encrypts the data and cuts it into multiple data fragments. These fragments will be randomly distributed to the nodes of the entire network. At the same time, metadata will be generated, which contains information about where to find the data, etc.

Data retrieval: When retrieving data from the network, the client will first refer to metadata to identify the location of previously stored data fragments. Then the fragments will be retrieved and the original data will be reassembled on the client's local computer.

Data maintenance: When the amount of redundancy drops below a certain threshold, the necessary data on the missing fragments will be regenerated and replaced. Thereby ensuring the integrity and long-term storage of data.

Payment system: Send a certain amount of Fermat tokens in exchange for services, including data storage and retrieval, and data transaction markets.

After further decomposition, the following parts will be included:

1. Storage node
2. P2P communication
3. Redundancy
4. Metadata
5. Data encryption

6. Audit and reputation
7. Data recovery
8. Payment

3.2 Storage Node

The role of storage nodes is to store and provide data. In addition to providing reliable data storage, nodes also need to provide network bandwidth to meet service requirements. The factors affecting the storage capacity of a storage node include: ping time, latency, throughput, bandwidth, hard disk space, geographic location, response time, etc.

As a requirement for providing storage services, the network provides certain rewards for storage nodes, and users pay storage fees for data storage.

Due to many factors in the selection of storage nodes, the selection of nodes is uncertain. Therefore, metadata must be produced every time after storing data to track storage nodes.

3.3 P2P Communication

All network nodes communicate through standard protocols, which are required to meet:
1. It can be accessed even when facing a network firewall. This means the need for corresponding technology.
2. Provide identity authentication similar to Kademlia, allowing nodes to identify each other. Each node provides identity authentication and communication in encrypted form to avoid man-in-the-middle attacks.
3. Absolute privacy and security. The protocol should ensure that the client and node communicate with each other without any eavesdroppers.

In addition, the protocol also needs to provide a way to look up the node's identity address so that the nodes can connect to each other, which is somewhat similar to the DNS domain name system. But there is no centralized registration.

3.4 Redundancy

Assuming that at any point in time, each storage node has the possibility of permanently shutting down. The redundancy strategy must ensure that even if a certain number of nodes are offline, a large amount of access to the stored data can be provided. If a node fails the audit or is unreachable, we initiate a network replication process by transferring an existing copy on the network to a new node. Therefore, the network can be restored to normal after each audit.

In order to achieve a certain level of durability (data is still available even in the face of a certain amount of node failure), most current systems use simple replication and backup, but such a solution links the durability of the network with storage costs, which greatly increases the cost of data storage.

For example: supposed to reach a certain level of data durability and need to replicate 8 backups, which means that 8 times the hard disk space and bandwidth are required, and the result is an 800% cost increase.

As an alternative to the simple copy method, erasure coding provides a better solution to the redundancy problem. Erasure coding is a coding scheme used to solve data durability without linking it to bandwidth usage, and it greatly improves data repair capabilities compared to copy methods. More importantly, there is no increase in cost while providing durability.

Erasure coding is used in many streaming media data, such as audio and satellite communications. Therefore, it must be pointed out that the use of erasure coding is not too difficult in terms of design requirements and is deeply integrated with future technology development trends

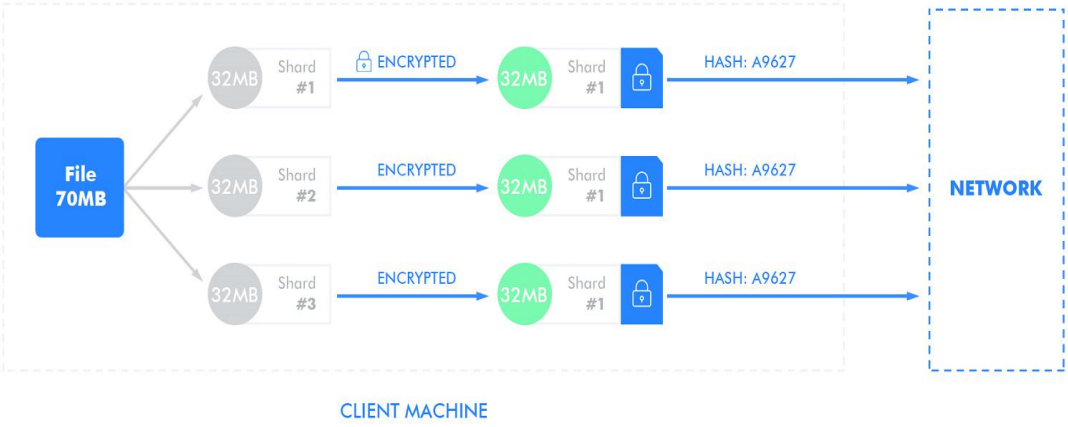
3.5 Metadata

Once we store certain data on specific storage nodes in erasure coding, we need to track the selected nodes. We allow users to select storage nodes based on factors such as geographic location, hard disk space, performance, etc. To this end, we choose to use an explicit node selection scheme, such as directory-based search.

Therefore, we designed a metadata storage system that supports: hierarchical objects (prefixed paths), key/value storage for each object, arbitrarily large files, any number of files, storage and retrieval with any key, and so on.

3.6 Data Encryption

To meet absolute security and privacy protection, all data or metadata will be encrypted. Therefore, data needs to be encrypted before it is uploaded to the network. We provide users with multiple encryption schemes. It also provides encryption of metadata, allowing users to restore or update data with appropriate decryption mechanisms.



The file is cut into standardized fragments, and the nodes are stored randomly in the form of fragments, and no node has a complete fragment, which better guarantees the security of the data. For the same file, each fragment is encrypted with the same method, or a user-defined method, such as an external encryption key.

At the same time, in order to support rich data management functions, multiple security keys are used. It also allows users to share functions such as common access to certain files.

3.7 Audit and Reputation

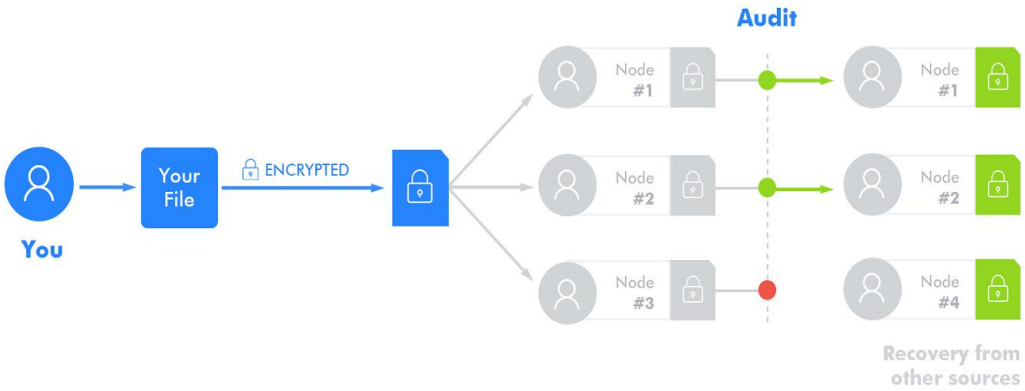
Encouraging storage nodes to accurately store data is of great significance to the entire system. The key is to be able to verify and review that the node accurately stores the user's data, which means that the storage node

is behaving well, can store its declared data, and is not susceptible to hardware failure or other influences. Most storage systems use probabilistic spot check methods to replicate the proof. We adopt a universal probabilistic proof mechanism based on file retrievability, covering all nodes and their stored files, with higher certainty and lower cost.

The audit mechanism is used to determine the stability of the storage node. The result of the failure of the audit is that the storage node is marked as bad, and it is used to determine which files need to be repaired. Storage nodes are marked as bad and will be punished, and will affect the distribution of data among nodes.

3.8 Data Recovery

In any decentralized storage system, data loss is an ever-present risk. Although there are many reasons that can cause file loss. But shutting down or leaving the storage node is the biggest risk. Because the audit mechanism has been verifying whether the node has stored the data correctly, the remaining work is to detect when the storage node stops storing data correctly or operates normally. It then reconstructs the data from the remaining parts through erasure coding, then regenerates the missing parts, and then stores them back on a new storage node in the network.



3.9 Payment

Payment, value measurement, and bidding systems are very important for maintaining the healthy development of the decentralized storage network ecosystem. Of course, the decentralized payment system is still in the early stage of development and cannot meet the million-level payment needs.

In order for our payment network to meet low latency and high throughput, the payment system cannot rely on the blockchain, that is, in order to meet the performance requirements of the storage system, it is impossible to wait for payment confirmation on the blockchain. When the operation is measured in milliseconds, it is impossible to wait for the node group to verify the blockchain ledger.

For this reason, we have designed a payment system to meet payment needs in the form of payment channels (similar to Lightning Network). Customers can design different reward strategies for miners. For example, the contract can be set to pay higher and higher fees to the miner over time, or the contract can set the storage price notified by a trusted oracle.

4. Fermat Blockchain Network

4.1 Fermat Consensus Algorithm

The birth of Bitcoin made it feasible for tens of thousands of computing nodes distributed around the world to jointly maintain a database through the Internet, and based on this, realized the decentralized issuance of currency and the predictability of inflation. However, under Bitcoin's POW consensus algorithm, in order to compete for block rights to obtain block rewards, miners must continue to develop new technologies, expand the scale of mining, and find the cheapest power resources. This has caused major changes in Bitcoin's computing power ecosystem: technology monopoly and energy resource utilization.

Bitcoin has also evolved from the original equal participation of everyone to the monopoly of resources and technology by a consortium, which finally led to a consensus of partial and minority participation.

The mission of the POW consensus algorithm has ended. For the major renewal of the blockchain in the next ten years, new consensus algorithms must be explored. This new algorithm-to promote the further development of the blockchain and realize the vision of blockchain decentralization, it should also ensure security, high performance, scalability, transparency, fairness, everyone can participate, transparency, and energy saving, convenient and available.

The foundation of the POC consensus algorithm is the storage and reading of hard disk data. The generation of data stems from human social and economic activities, so its distribution (decentralization) is roughly similar to population distribution, and the corresponding basic equipment (hard disks) that provide data storage services are also distributed in a decentralized manner. This makes it possible for us to build a next-generation blockchain based on the POC consensus algorithm.

Fermat adopts the POC consensus algorithm. When a node submits a block to the network, it must provide a valid proof of capacity. Without corresponding data storage, it is impossible for a node to generate a valid storage capacity certificate. At the same time, any node in the network can easily verify the validity of the submitted certificate. If the stored data and submitted proof are valid, the block will be accepted by all nodes in the network and added to the blockchain network as a new block.

The process of providing proof is as follows: In the initialization phase, a series of hash data is generated according to the protocol and stored in the storage capacity. When a new block is to be generated, the data will be searched in the capacity according to the value of the random number. The data will be used to generate the proof and participate in the competition to generate the next block. The whole process includes five stages: initialization, block construction, block reception, main chain selection and penalty mechanism.

- Initialization: Miners first need to initialize the hard disk and generate two HashMaps, and save them to the hard disk.
- Block construction: After verifying the latest block timestamp, miners obtain challenge parameters from the latest block, find data that meets the conditions in the HashMap, and generate a proof of capacity. If the quality of the capacity proof is greater than the difficulty of the entire network, the right to block production is obtained. The miner signs the block hash and broadcasts the block to other nodes.
- Block reception: After the node receives the latest block, it will perform a series of verifications, such as timestamp, public key, signature, capacity proof, proof quality, transaction legality, etc.
- Main chain selection strategy: When multiple blocks that meet the above rules are received in the network, the main chain block needs to be selected according to certain rules: in turn, choose the largest cumulative difficulty, the smallest Timestamp, and the best proof quality.
- Punishment mechanism: In the Fermat capacity proof consensus protocol, the multi-mining penalty mechanism is used to resist multi-mining attacks. If the node receives two different headers with the same proof, it proves that the person in the block is in double mining. The node can construct a penalty transaction, so that the Pk of multiple miners is added to the blacklist, and blocks can never be generated.

The two characteristics of Fermat's POC consensus algorithm are that it is more decentralized. The distribution of hard disks is far more popular and fairer than the distribution of chips (POW) and capital (POS). The second is energy saving. Hard disk mining has low energy consumption and hard disk resources can be reused. These two characteristics make the threshold of POC mining low and everyone can participate.

Fermat's POC consensus algorithm provides the most complete foundation for the development of next-generation blockchain systems. On the basis that

everyone can mine, a more open and decentralized network can be built, and the development of the Internet of Things, artificial intelligence, cloud computing, big data and other industries can be promoted.

4.2 Fermat's POC algorithm technology basis

The core concept behind Fermat's POC (Proof-of-Capacity) consensus algorithm is that in terms of storage resources, "Prover is inefficient and verifier is efficient", so that the verifier can spend very little Storage resources, in less computing time, verifying that the Prover has a certain storage space.

We will briefly introduce system design based on mathematical models.

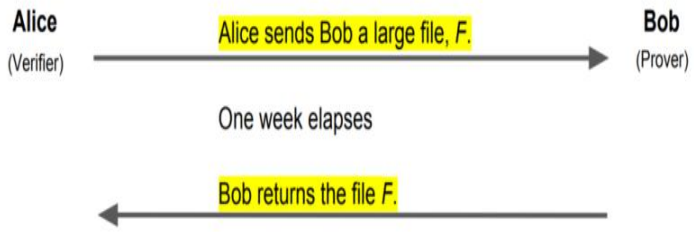
The most critical issue in Fermat's POC consensus algorithm is how the prover (referred to by Bob) can prove to the verifier (referred to by Alice) that he has a file F of a certain file size that always exists in Bob's disk.

In the simplest and most intuitive way, we might think of Alice sending F to Bob in advance, and then Bob returning the same file F when he needs proof.

As shown in the figure below, after Alice receives the file, she checks whether it is consistent with the file sent to Bob before. But doing so obviously violates the characteristics of "verify efficient storage resources".

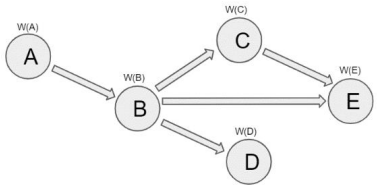
At the same time, in the P2P network, it is obviously unrealistic to use the limited bandwidth to send large-capacity files required by the POC consensus.

Therefore, we need to design an efficient algorithm for both storage resources and network resources to achieve the purpose of "verification efficiency".



In the category of Fermat's POC, the purpose of file F is just to prove that Prover does use a certain amount of storage space tools, that is, we can make any form of requirements on the content of file F (you can think of the CPU calculation process itself in POW , Not related to any specific non-blockchain applications).

In the POC algorithm proposed by Fermat, the content of the file is a Directed Acyclic Graph (DAG) structure, with V representing all nodes in the graph, defining W (V), and requiring it to satisfy a characteristic W (V)=Hash(V, W(V')), where V is the direct predecessor node of V in the graph.



W(A)=Hash(A)
W(B)=Hash(B, W(A))
W(C)=Hash(C, W(B))
W(D)=Hash(D, W(B))
W(E)=Hash(E, W(B), W(C))

As shown in the figure above, the figure simply explains the structure of the directed acyclic graph, where the W value of each node is a long binary string after a hash calculation.
Prover needs to store the W value of each node for Verifier to randomly select and test during the verification phase. The interaction process between Prover and Verifier is as follows:

The Initial Phase:

Verifier negotiates a complex directed acyclic graph G with Prover, and Prover calculates all W (V) and stores the calculation results (the calculation time required for this step is proportional to the storage space and the number of nodes in the graph).
Prover composes all the values of W (V) into a Merkle Tree, and at the same time sends the value of the root node of the tree to Verifier.

Verification Phase:

Verifier randomly selects node V and asks Prover to give the value of W (V) and reveal its path in the Merkle Tree.

Prover extracts the specific W(V) in its storage and reveals its path in the Merkle Tree

Verifier verifies the legitimacy of its W(V) and verifies whether it exists in the Merkle tree rooted at Φ.

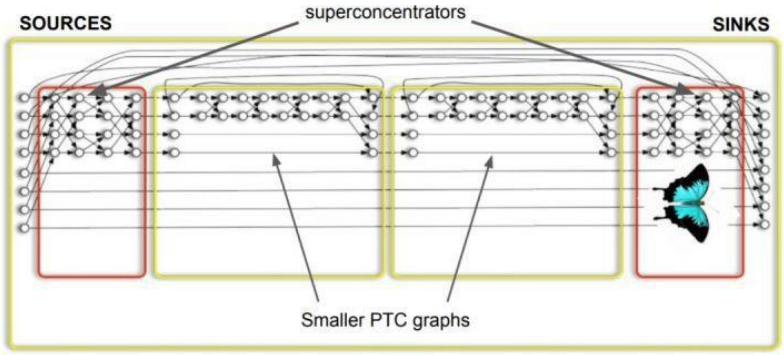
In the initial stage, similar to the POW algorithm, hash is used to prove the usage of CPU. In the initial stage, POC requires honest Prover to store the hash value of each node calculated according to the graph structure.

In practical applications, the number of graph nodes is far more than the above figure, and the connection relationship of the graph is more complicated than the above figure. Considering the most likely case of Prover cheating, Prover does not use a lot of storage in the initial stage Store the result of the Hash operation on the disk, but reuse CPU resources for the Hash operation during the verification phase.

Such cheating with "time for space" is obviously not feasible, because in the limited verification time, investing huge computing resources to recalculate the hash value of each node is not only uneconomical, but also unrealistic.

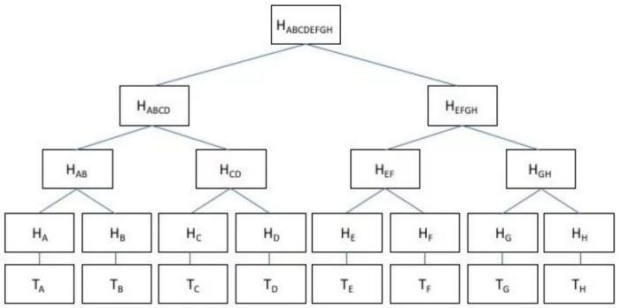
Two specific types of DAGs, Random Bipartite Graphs and Superconcentrator Graphs, are selected in Fermat. The mathematical characteristics of the two types of graphs ensure the high complexity of the connection relationship between nodes.

Through the established Pebble Game model, it is proved that if a dishonest Prover does not store the same number of hash values as the graph nodes, it will not be able to correctly pass the verification of the verifier within a constant finite time.



The above two-stage interaction is the core of Fermat's PoC algorithm.

Attentive readers may notice that the calculation and verification of Merkle Tree are involved in the two steps b and c of the initial stage and verification stage. The core idea here is to use the nature of Merkle Tree to simplify the verification of the verifier complexity, so as to achieve the purpose of "verification efficient" for the verifier.



As shown in the figure above, Prover uses the W value of each node as the leaf node of the Merkle tree, calculates the root of the Merkle tree, and sends it to Verifier at the initial node as one of the parameters.

In the verification phase, Verifier only needs to verify whether the W value of a certain node exists in the Merkle tree sent in the initial phase of the first step.

The algorithm process is exactly the same as the common light wallet verification transaction in the blockchain system, which greatly reduces the complexity of the verification work.

4.3 Technical Details of Fermat's POC Algorithm

4.3.1 Fermat Hard Disk Utilization and Plot File

Plot file is a file that each node or miner participating in block production needs to store in the hard disk, and its content is composed of a large number of hash values with a specific structure. The Plot file contains the following basic concepts:

Shabal256: Shabal256 is the Hash algorithm used by Fermat. Compared with Hash algorithms such as SHA256, Shabal requires more CPU calculation time and amount of calculation. Combining the content of the previous chapter, we can understand that Fermat chose Shabal because on the one hand, miners do not need to perform a large number of Hash calculations during the block generation stage, and on the other hand, it can also calculate the cost to prevent possible malicious miners at each output. The block phase temporarily calculates the required hash value instead of the hash value in the storage.

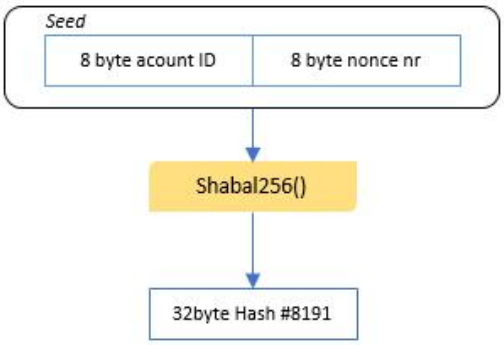
Nonce: Nonce is a basic unit with a fixed number in the Plot file, composed of 256KB of data, and is the basic logical unit used by miners to participate in the POC process.

Scoop: Each Nonce file is composed of 4096 Scoop files, which also have a

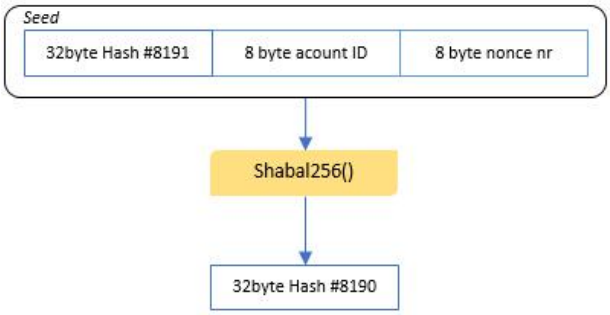
number in the range of 0-4095. Each Scoop file contains 2 Hash values, that is, a Nonce file contains 8192 Hash values.

The generation process of Nonce is as follows:

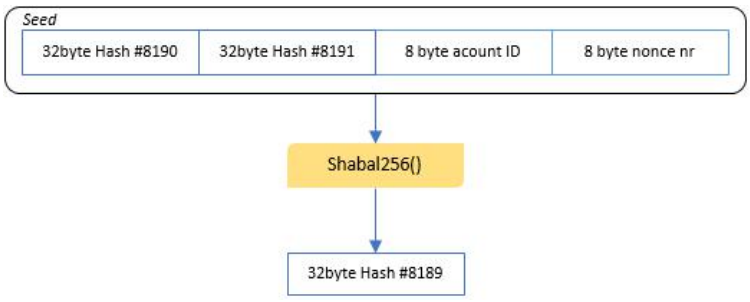
1. The seed of the Nonce file is composed of Account Id (i.e. the user address or user Id in the Fermat network) and Nonce Id (i.e. the nonce number). After the first Hash, Hash #8191 is generated, that is, the number in Non is 8191 Hash value.



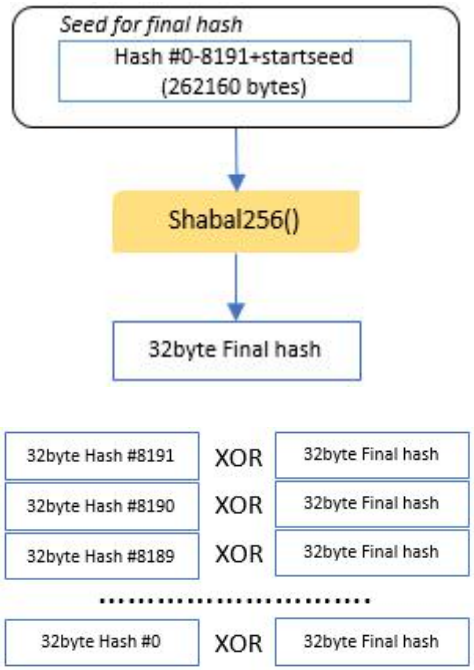
2. #8190Hash value is generated by the previous #8191Hash value and Account Id and Nonce Id.



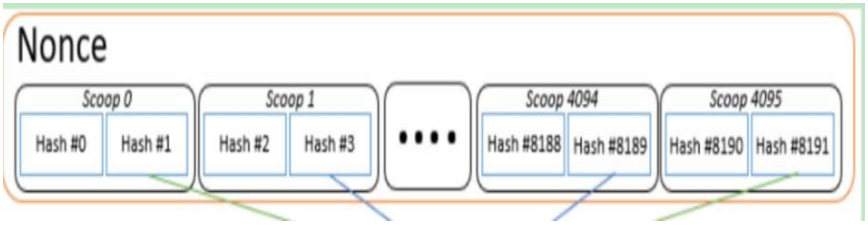
3.。#8189Hash value is generated from the previous two #8191Hash, #8190Hash value and Account Id, NonceId, and so on. For each next Hash value, it has all the previously calculated Hash values and AccountId and Nonce Id. If the process exceeds 4096 bytes, the most recently generated 4096 bytes will be used as the input parameter of the next Hash function.



4. The final Hash is generated by Hash#0-8191, Account Id, Nonce Id, and then 8192 Hash values are XORed separately as the final value of each Hash.



5. After getting 8192 Hash values, the structure of the Scoop file is shown in the figure below:



So far, we have generated a complete Nonce file. A Nonce file contains 8192 hash values and occupies a space of 256KB.

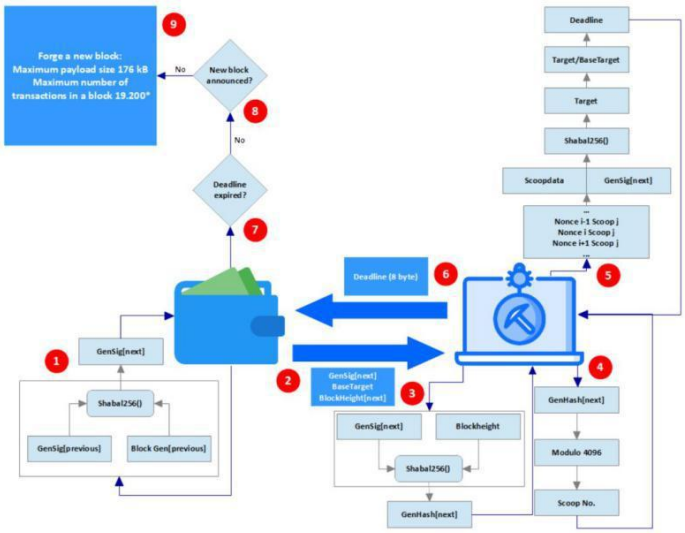
This is also the lowest threshold for miners to participate in mining, that is, as long as there is more than or equal to 1 Nonce file, they can participate in mining.

The general home host takes 500G as an example, which can store 2 million nonce.

Therefore, in the Fermat world, low computing power is basically involved in the mining process in the form of participating in the mining pool.

4.3.2 Fermat Consensus and Block Production

We will Fermat as the blockchain's complete mining process, and discuss the core issues in several consensus.



The figure above is a complete block production process of the Fermat blockchain. Below we will introduce each of its steps in combination with the diagram.

Step 1-2, GenHash generation: GenHash is similar to the concept of BlockHash in BitCoin, and is used to form a successive block chain structure.

In Fermat, because the Hash also participates in the establishment of parameters in the consensus process, it splits the concept into two:

GenSig is obtained by Hashing between GenSig in the previous block and the block producer of the previous block, and GenHash is obtained by Hashing by GenSig and fast high information. Through such two Hash calculations, all blocks before the current block form a chain structure of unmodifiable historical blocks, and at the same time, the important parameter GenHash in the POC consensus is obtained.

Step 3-4, Calculation of Scoop Number: After the wallet generates GenHash, it sends this value to the miner, and the miner calculates the Scoop Number required for this block generation. GenHash Modulo 4096 is the value of Scoop Number. The Scoop Number is used to define that in this block generation, all miners in the entire network should query all the Scoop data in Nonce they own. Combining the content of the previous chapter, we can know that it has two Hash values in a Scoop.

Step 5. Calculate the target and deadline: First, the miner needs to traverse the disk and find the two hashes corresponding to the Scoop Number calculated in the previous step among all the nonce they own, and record them as scoop data, so that the expression target=Hash(scoop data, GenSig) Has the smallest value. Then use the minimum value target to calculate

target/Base Target to get the deadline. The target is similar to the difficulty target parameter in bitcoin, which controls the difficulty of mining in the entire network, and the deadline determines whether the block generated by the miner successfully obtains the casting right of the block in the entire network.

Each of the above parameters:

Deadline: It is an integer type value. A block with a specific deadline needs to wait for the time specified by the deadline in the entire network before it can be regarded as a legal block. For example, if the deadline is 60, it means that this block can be allowed to be added to the main network as a legal block one minute after the block generation time of the previous block. From this we can know that the miner with the smaller deadline is calculated, the more likely it is to win the casting right of the current block. The calculation process of the deadline is calculated by the miner by traversing all the values in all of their randomly generated Nonce, which means that the more Nonce they have, the larger the disk space, and the greater the probability of obtaining a deadline with a lower value. Therefore, the probability of obtaining the ingot weight is also greater.

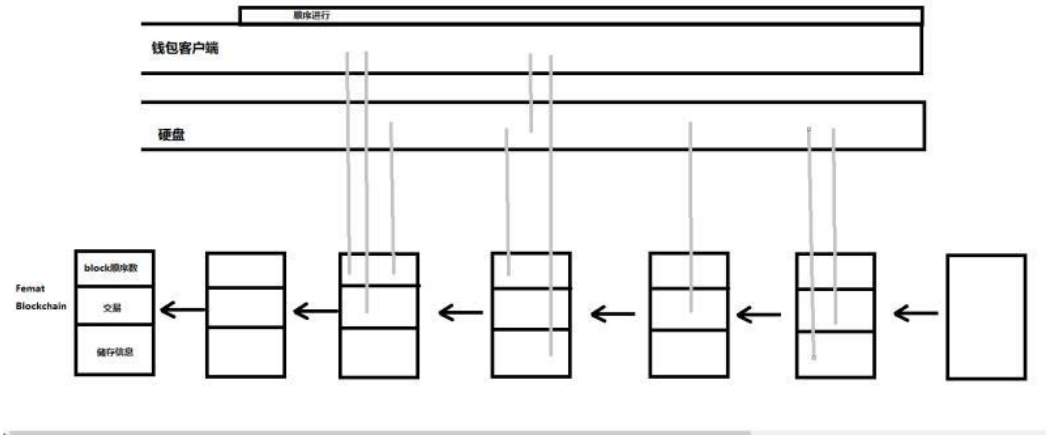
Base Target: The average block generation time of the entire network set by Fermat is 4 minutes. The storage computing power of the entire network fluctuates. How to control the average block generation time of the entire network under the fluctuating computing power? Similar to Bitcoin, Base Target represents the difficulty of mining. The smaller the value, the higher the difficulty of mining on the entire network. In Fermat, the smallest target needs to be divided by Base Target to get the final deadline. Therefore, the dynamic adjustment of Base Target can directly control the interval between blocks of the entire network, that is, the block time.

Steps 6-9, package transactions, mint blocks, broadcast blocks. This process is similar to all blockchain systems. It is worth mentioning that Fermat's block load size is limited to 176KB, which can carry about 19k transactions on average. It is not difficult to conclude that its theoretical tps limit is at about 80, which is similar to POW-type blockchain systems such as Bitcoin and Eth. Ratio, its energy level is also similar.

4.4 Fermat Distributed Storage Protocol

The bottom storage of Fermat distributed storage protocol is implemented by ipfs, and the upper network is built by Fermat's POC consensus protocol.

The user transfers the file to the ipfs network through the Fermat wallet, and the upper Fermat blockchain network permanently saves the file information transferred by the user. The Fermat distributed storage protocol defines a set of file standards, which can safely protect the security and privacy of user files. When storing files, users pay corresponding fees according to the Fermat payment system, and nodes will receive corresponding storage fees other than mining.



The stored files will be encrypted and cut into multiple data fragments, and then transmitted to other nodes through a specific network transmission channel for backup and corresponding metadata production. Even if there is an accident on the node storing the data, the file will be stored by other nodes in the network (Fermat redundancy strategy and data repair mechanism ensure data security and access performance).

The Fermat distributed storage protocol can be combined with the Internet of Things to help complete information on the chain, information backup, information storage and remote information sharing.

5 Fermat Incentive Mechanism

Fermat proposed an innovative incentive mechanism to achieve sustainable and rapid development of the network and ecology. This incentive mechanism makes the rational interests pursued by each participant consistent with the interests of the entire ecosystem, and finally realizes a highly decentralized and stable network system.

Fermat serves as a means of economic reward and punishment for ecological participants to prevent malicious nodes from doing evil and the infinite loop of logic bombs that may appear in smart contracts, the payment and settlement currency in the Fermat ecology, and the chain of Fermat ecology and other large public chain ecology. The lock-in and payment settlement method of economic activities on the Internet.

Fermat Financial Model	
Total number of tokens	1,002,144,000
Supply reduce cycle	Half Year
Reduction ratio	25%
Mortgage ticket	It is divided into several mortgage cycles according to the block height, and a certain amount of Fermat tokens can be locked in a cycle to generate a ticket. If you mine with a ticket, you will get the full reward, and the output ratio of mining without a ticket will adjust itself based on community feedback.
Staking	After the project runs for a certain period, the community will start the staking pool to strengthen the stability of the entire network.

6 Fermat Application Ecology

6.1 Fermat and IPFS Ecological Data Storage

6.1.1 IPFS Ecological Overview

The full name of IPFS is "Inter Planetary File System", and the Chinese name is "Star File System". IPFS is a low-level network transmission protocol equivalent to the HTTP (hypertext) protocol in the current Internet world. HTTP is a relatively simple request-response protocol used for interaction between users and servers.

The function of IPFS is similar to HTTP, but the architectural features of p2p network are added to it. Compared with the HTTP protocol, the IPFS protocol is more efficient. HTTP is single-threaded communication, and only one task can be performed on a server at a time, while IPFS uses p2p for multi-threaded downloads, which can save more than 50% of bandwidth costs. At the same time, because of the centralized nature of current Internet servers, the information in the network can be completely controlled and difficult to save. However, if decentralized protocols such as IPFS are used, as long as the information is owned by any user in the network, the entire network can get this information.

In recent years, with the development of IPFS technology, excellent talents from all over the world have been attracted to this magical open source world. Combining the advantages of IPFS, we continue to innovate and apply in various fields, creating unlimited imagination for the new era of the Internet. The following are examples of applications in the IPFS ecosystem

DAPP example

(1) IPFS e-commerce: OpenBazaar, benchmarking Taobao and Amazon, a decentralized global free trading market. Open Bazaar is a decentralized commodity trading market that combines the characteristics of eBay and BittTorrent. This platform does not have a central server. When every user wants to use the Open Bazaar platform to shop, they need to download a piece of software. It also serves as a server node for the entire network.

It has formed a decentralized global free trading market. I believe that many people who have used Taobao and Tmall absolutely believe in the third-party arbitration guarantee of Alibaba Group, but the difference is that OpenBazaar uses encryption as guarantee. Trust comes from code and mathematics, not people, which means no need to pay Fees, and without your files, your transactions will not be reviewed.

At present, this software is already in use in more than 30 countries, and you can buy music, games, food, beverages, clothes, art, jewelry, etc. from various countries on it. OpenBazaar uses the power of IPFS to create a completely free e-commerce! Here, BTC, ETC, LTC, ZEC, Dash can all be used as payment currencies. OB is a bit like a small shop, the shop becomes gray after it goes offline, very cute. Currently there is only the desktop version, if you download, you need to adapt the environment.

(2) PeerPad is a collaborative real-time editor. It does not use a third party. All participating nodes talk directly without a central server. At the same time, Peerpad is open source, showing how developers can use IPFS to build their own serverless, real-time, offline-first multi-person collaborative distributed applications, established by the protocol laboratory and the IPFS community. Four functions can be realized: 1. Meeting notes, 2. Collaborate or share code snippets, 3. Write and share articles, 4. Collaborate with multiple users at the same time.

(3) IPFS music player: such as Spotify, the slogan is: Music for everyone, dedicated to sharing millions of songs. Using Spotify, we can easily find suitable music on mobile phones, computers, tablets and other devices at any time, and we can also browse the music collections of friends, artists and celebrities, or create a radio station. Spotify will store it on the IPFS network. Which greatly reduces the storage cost of audio data. Others: 1) Ujomusic: A blockchain market for musicians on the IPFS that benchmarks Xiami and Migu Music; 2) DIFFUSE, an online music player.

(4) IPFS video player: D.Tube is the first encrypted distributed video platform, built on the STEEM blockchain and IPFS peer-to-peer network, and will support the FIlecoin network in the future. It aims to become a substitute for YouTube, allowing Users watch or upload videos based on IPFS/FIlecoin, and share or comment on the immutable STEEM blockchain.

(5) IPFS social network: Orbit, the replacement of QQ on IPFS. Orbit is a fully distributed, peer-to-peer, real-time chat application based on IPFS, which can be regarded as a decentralized Slack or IRC. Orbit uses IPFS and CRDTs to store and process real-time communications: it can work without any central point, completely peer-to-peer. Orbit uses Ethereum and uport to register identities, track users and identity information. This is a demonstration of the powerful combination of IPFS distributed applications and the Ethereum processing system.

Other IPFS social networking tools such as: Akasha, Facebook, WeChat and other social tools; textile, dedicated to replacing Instagram; implementation of magicleap, VR and AR on IPFS; Neocities, an open source social network for creating personal web pages for free.

6.1.2 Fermat: Incentive Layer Network of IPFS Ecology

At present, the application of the IPFS incentive layer is actively explored in many projects around the world. Fermat is one of the most concerned projects. The emergence of Fermat aims to promote the rapid application and development of the IPFS protocol in some specific fields. The popularity and promotion speed of these fields will be at the forefront of the industry. These areas that Fermat is committed to developing include: medical and health, identity authentication data storage, high-definition video, VR/AR, cloud gaming, industrial Internet, driverless, etc.

Fermat itself has also formed an application ecosystem, including storage networks, economic systems, and technical frameworks.

6.2 Fermat Serves HD Video Data Storage

Present the information using video and pursue high definition of video has become a major trend in the development of the global information industry. The essence of high-definition video services is the combination of high-quality content and high-speed channels, serving the broad consumer market and industry application markets. Ultra-high-definition video transmission the demand for large network traffic, high speed, and low latency is highly consistent with the characteristics of 5G networks, and it is expected to become the basic business of the new media industry in the future and the main 5G related industries.

After 5G empowers mobile terminals to connect to the cloud in real time to gain powerful performance, the user experience is greatly improved. The application scenarios no longer have harsh requirements for the hardware configuration of mobile terminals, and mobile terminals will deeply penetrate all walks of life. For example, the 5G bandwidth is as high as 1Gbps, which can support a smooth playback of 5K panoramic video with a duration of 8 minutes, a size of 1.3GB, and a code rate of about 20.8Mbps. 5G can improve the image quality of VR cloud games and reduce the network latency in cloud gaming technology.

Use the powerful CPU and GPU in the cloud to perform 3D graphics operations, and send it back to the local VR/AR device in the form of a video stream, so that the VR/AR device with a built-in mobile chip can also display the top image quality. The powerful communication capabilities of 5G can support UAVs to implement cloud AI computing and process sensor data and video data generated by UAVs in real time. The application of 5G connected drones can be fully extended to scenarios such as logistics transportation, entertainment live broadcast, infrastructure inspection, agriculture,

forestry and plant protection, geographic surveying and mapping, urban planning, emergency rescue and other scenarios that require real-time big data transmission.

High-definition video under 5G will require super-strong data storage service capabilities. Fermat's distributed cloud storage ecosystem can not only guarantee super-strong, high-experience data storage requirements, but also ensure data security, privacy protection, and data confirmation.

Based on the computing power (mining) ecology, Fermat can quickly establish a large number of cloud storage centers and data centers around the world. Fermat can store and share data nearby based on the distribution of ultra-definition video viewing needs, which guarantees experience and performance, and can reduce costs.

6.3 Fermat Serves Cloud Game Data Storage

Based on 5G cloud processing technology, all mobile phones can operate cloud games, greatly reducing the price of gaming terminal equipment. The essential difference between 5G and 4G is that its speed is 10 times faster than the latter. For ordinary users and ordinary game application scenarios, there is no difference between 4G and 5G conditions for videos with a picture quality lower than 4K; but for complex application scenarios, diverse game elements, faster speed, greater bandwidth and ultra-low latency And it supports real-time, multiplayer, and immersive gaming experience, and 5G provides the possibility of popularization.

In the era of 5G cloud gaming, all resource consumption caused by screen rendering is done in the cloud. With the advantages of 5G's large bandwidth and low latency in milliseconds, more mobile phones only require video display functions.

Games are human nature. With the development of social productivity, humans will only spend more and more leisure time in the future, and the demand for games will only increase. Fermat solves the data storage needs of cloud games. Under Fermat’s POC consensus algorithm, everyone can participate in mining. Anyone can establish a small cloud storage service center. It is common in distributed storage technology, IPFS and 5G technology. Under the effect, the speed of data retrieval and transmission will be greatly improved, and the delay can be reduced by 10ms, which makes it possible for Fermat to serve cloud games.

6.4 Fermat Serves Medical and Health Data Storage

As a large country with a population of 1.4 billion, China has always suffered from insufficient supply of medical resources and uneven distribution. The development of 5G provides technical support for telemedicine, which can promote the online flow of medical resources, realize interconnection between hospitals at different levels in different regions, break the space constraints of doctors and patients, greatly improve medical efficiency, and help remote areas obtain high-quality medical resources so as to improve the current situation of insufficient supply and uneven distribution of medical resources.

The large-scale Internet of Things involves the Internet of Medical Things (IOMT) ecosystem, which will include millions or even billions of low-energies, low-bit-rate medical health monitoring devices, clinical wearable devices and remote sensors. Doctors will rely on these instruments to implement remote monitoring and collect patient medical data, such as vital signs, physical activity, etc., to achieve multi-party interactive sharing, which will help doctors effectively manage or adjust treatment plans.

The combination of big data and medical services has become a hot spot in recent years. High-quality data can effectively increase the efficiency of new drug development and improve clinical treatment methods. After a period of operation of telemedicine, the accumulated and deposited data gradually form economic value.

。Fermat serves medical and health data storage, such as the rapid storage and sharing of somatic cancer data and related clinical information, extracts key data from medical data on a global scale, and enables researchers, clinicians and scientists to be in real time, open and Access data in a trusted environment. Further improving the circulation of medical data is conducive to medical research. At the same time, the rights to medical data are confirmed, so that data owners can also get corresponding benefits, such as the income of data sales and more reasonable insurance prices.

6.5 Fermat Serves Industrial Internet Data Storage

Industrial Internet is an advanced production model applied in the digital age. It relies on 5G networks and cloud service platforms to face industrial customers. It integrates cloud computing, big data, and artificial intelligence, through deep perception of industrial data, real-time transmission, rapid calculation and advanced modeling Analyze, realize

the transformation of production and operation organization, and help the transformation of traditional industrial enterprises. 5G has the characteristics of enhanced mobile broadband, ultra-reliable, low-latency, and wide coverage and large connections. It solves the problem of massive data communication and transmission in the industrial Internet, and has become an important technical support for industrial enterprises to reduce costs and improve benefits. Based on the 5G Pioneer Industry Identifier, it can be judged that 5G can be the first to be applied in power production and smart manufacturing.

The rapid development of the Industrial Internet is inseparable from the continuous development of the supply chain.

Fermat can realize supply chain management innovation based on the central link of each industry. Fermat data confirmation, privacy protection, data market and other technologies can make every supply chain link willing to share data, protect data privacy, and obtain data benefits, thereby promoting the continuous optimization of the entire supply chain. In turn, it promotes the innovation of industrial production models, realizes in-depth data perception, real-time transmission, fast calculation and advanced modeling analysis, realizes the transformation of production and operation organization, and helps traditional industrial enterprises to transform and upgrade.

6.6 Fermat Serves Data Storage in the Blockchain Industry

In the future, the mainstream of blockchain development is a multi-chain ecology, and the interconnection of ten thousand chains is inevitable. Therefore, cross-chain communication, interoperability, and atomic transactions are the general development trends of blockchain technology in the next decade. Like the current ecological structure of the Internet industry, the future blockchain ecology will be ecologically structured, and different public chain ecology will provide different basic services throughout the industry.

Data confirmation, data transaction, and data storage are the basic facilities of the blockchain industry.

As a decentralized storage system based on IPFS, Fermat can provide basic data storage layer services for all public chain systems and DAPP based on public chains.

7.Fermat Development Plan

1.Project Launched 2019.Q3
2.Fermat Testnet Released 2020.Q3
3.Miner Ecological Construction 2020.Q3
4.Fermat Mainnet Launched 2020.Q4
5.Fermat Global Node Establishment 2020.Q4
6. The first phase of the Fermat Ecological Fund was established to support the ecological development based on IPFS and Fermat 2021.Q1
7. Fermat two-layer network development, improve network performance, support application construction 2021.Q2
8. The second phase of the Fermat Ecological Fund was established to promote the ecological promotion of Fermat in the commercial field 2021.Q3

8. Fermat Ecological Governance

The corporate governance structure is derived from the company system and is the general outline for restraining corporate strategy, risk management, operating principles, human resources, and legal compliance.

Although blockchain technology is based on decentralization as a starting point to establish an efficient and collaborative community platform, the experience of corporate governance structure can certainly be used for reference to improve the collaborative efficiency of the blockchain community and regulate the operation activities of the community; we want to structure It is a "non-traditional" community. In addition to individual participants, there are also large and small business users and enterprise users. A reasonable corporate governance structure can resonate among corporate participants.

Of course, it cannot be completely mechanically applied. It is necessary to seek a dynamic balance between community culture and traditional corporate management culture. The governance method we propose here is just a combination based on our experience in traditional enterprises combined with the experience accumulation in the blockchain industry in the past few years. It does not mean perfect, and it needs to be continuously developed in the future.

8.1 Fermat Foundation

The Fermat Foundation is a non-profit entity, initiated by the founding team of Fermat, and supported by technical geeks and community enthusiasts. The foundation will act as the advocacy entity of the Fermat blockchain, dedicated to the development and construction of Fermat and the advocacy and promotion of governance transparency, and promote the safe and harmonious development of the open source ecological community.

The Fermat team highly agrees with the essence of the “decentralized” construction of the blockchain, and at the same time absorbs the essence of the traditional corporate governance structure, improves the efficient formulation and implementation of the Fermat development and promotion strategy, and avoids possible serious blocks. The divergence and irreconcilability of the chain design concept reappeared. The general blockchain community aims at a high degree of autonomy or decentralization, allowing community participants to make diversified discussions and suggestions, and usually use "voting" to make important decisions. However, such deliberation behaviors become inefficient or unresolved due to the

diversified opinions of participants, which is not conducive to the continuous iteration and evolution of blockchain technology. What's more, due to the serious divergence of opinions, the blockchain forks. The repeated hard fork solutions have made people question the concept of decentralization of Ethereum and even the blockchain. This kind of governance is not so much "democracy" as "anarchy".

The Fermat team highly agrees with the essence of the "decentralized" construction of the blockchain, and at the same time absorbs the essence of the traditional corporate governance structure, improves the efficient formulation and implementation of the Fermat development and promotion strategy, and avoids the divergence and irreconcilability of the chain design concept reappeared.

The Fermat team will entrust a credible third-party organization to assist the team in promoting the foundation entity, and to maintain the daily operation and reporting affairs of the entity's structure. After the foundation is established, appropriate community members will be selected to join the foundation's functional committee to jointly participate in actual management and decision-making.

8.2 Fermat Foundation Governance Principles

The design goals of the Fermat Foundation's governance structure mainly consider the sustainability of the Fermat blockchain open platform, the effectiveness of strategy formulation, the effectiveness of management, risk control, and the efficient operation of the platform economy.

Although there have been arguments advocating that the blockchain is an autonomous community system with "decentralization" or "distribution" as the core, we believe that complete decentralization may bring absolute "fairness" or more "Inefficient". Therefore, the foundation will still absorb certain core ideas of centralized governance in the management structure, including the highest decision-making authority of the strategic decision-making committee and the centralized discussion power of major issues, so as to improve the efficiency of the operation of the entire community.

If any technology is separated from commercial applications, its development is often difficult. If it is impossible to prove that the technology lacks practical applicability and significance, it will even stagnate and die. The Fermat team has always adhered to the principle of close integration with business since the creation of the concept.

Therefore, there are the earliest cases of commercial application landing. The establishment of the Fermat Foundation also follows this principle. Even if the foundation exists in the form of a non-profit organization, the foundation hopes to gain recognition from the business world as much as possible, to win the benefits of commercial applications, and to feed back to the foundation and the community to further promote the development and upgrade of Fermat.

At the same time, the foundation will also disclose the information of the operation of the foundation and the development progress of Fermat to all parties involved in the community through regular reports and irregular news releases. At the same time, the contact information of the main management personnel of the foundation will also be completely open, accepting the supervision from all of the participants.

8.3 Organizational Structure of the Fermat Foundation

The organizational structure of the Fermat Foundation proposes a combination of professional committees and functional departments to deal with daily work and special issues. The establishment of the foundation refers to the operation of traditional entities, and various functional committees will be established, including the strategic decision-making committee, the technical review committee, the remuneration and nomination committee, and the public relations committee.

9. Disclaimer

This document is a conceptual document [white paper] elaborated by the Fermat blockchain project, and is not intended to sell or solicit shares, securities or other regulated products of companies related to the bidding.

According to this document, it cannot be used as a prospectus or any other form of standardized contract document, nor does it constitute advice or investment advice for securities or any other regulated products in any jurisdiction.

This document cannot be any sale, subscription or invitation to other people to purchase and subscribe to any securities, as well as a form of contact, contract or commitment based on this.

Any information or analysis presented in this document does not constitute any recommendation to participate in token investment decisions, and will not make any specific recommendations with a tendency.

Fermat Foundation does not bear any direct or indirect asset losses caused by participating in this project.

This document may be revised or replaced at any time, but we have no obligation to update this version of the white paper or provide channels for readers to provide additional information.