Merkle RO

——white paper

With the advent of the Internet + blockchain era, a disruption is taking place in our network environment: centralized servers are being replaced by decentralized open servers, trusted participation is replaced by verifiable computing, and vulnerable locations Addressing is replaced by flexible content addressing, inefficient monolithic services are replaced by the point-to-point algorithm market, and blockchain technology has proven the feasibility of decentralized ledgers. Client-side encrypted peer-to-peer cloud storage networks will allow users to transfer and share data without relying on third-party storage providers. Eliminating central control will alleviate most traditional data failures and outages while significantly improving security, privacy, and data control. Merkle RO is a decentralized blockchain distributed cloud computing service platform that transforms cloud storage into an algorithmic marketplace. This market runs on a blockchain chain with local protocol tokens. Miners on the blockchain can participate in sharing and exchanging data resources such as their remaining space, bandwidth, and files to earn Merkle RO rewards. Merkle RO's cloud storage network provides security for the entire process because content is encrypted end-to-end, while storage providers and other users cannot access the decryption key. It is very useful for decentralizing data, building and running distributed applications, and implementing smart contracts.

1 .project background

1.1 blockchain background

In 2008, a man named Nakamoto published a paper entitled "Bitcoin: A Peer-to-Peer Electronic Cash System" in a cryptography forum. In the text, the concept of blockchain was first proposed as a basic technology for constructing Bitcoin networks and encrypted transmission of transaction information, which can support the mining and trading of Bitcoin. Nakamoto believes that if the transaction data is processed by means of centralization (intermediary), it will not only overcome the mistrust between the merchant and the customer, but also the transaction cost is high and the transaction size will be limited. In order to solve such problems, Satoshi Nakamoto created a blockchain and invented Bitcoin on the basis of it, which quickly attracted the attention of countries around the world. Some countries have recognized and realized the blockchain technology in various fields.

With the advent of the digital currency era, more and more people are beginning to deploy digital assets. Most of the current major methods are stored in exchanges, mobile wallets or computer wallets. However, since these storage media are often networked, hacker theft incidents occur frequently, causing significant property damage to users. In addition, due to the loss of the mobile phone wallet, the risk of losing the digital assets caused by the damage of the hard disk of the computer wallet cannot be ignored. The theft of digital assets is shocking and affects the hearts of every currency holder. Searched for "bitcoin stolen" and the result was 2,380,000.

1.2 Development of blockchain technology

Since the birth of Bitcoin in 2009, blockchain technology has begun to take shape on the historical stage. The core advantage of blockchain technology is that it does not need a traditional centralization mechanism. It only implements peer-to-peer transactions that do not depend on a credit center in a distributed system through encryption, consensus mechanisms, timestamps, and other technical means. Coordination and collaboration to circumvent issues such as data security, synergy efficiency and risk control that are common in centralized organizations. In recent years, people have mainly focused on decentralization, consensus algorithms, and security anonymity of blockchains, such as:
graphene, lightning network to improve transaction performance; Proof of Stake (POS), entrusted rights Proof (DPOS), Practical Byzantine Fault Tolerance (PBFT) enrich and improve the consensus
algorithm; Zero-knowledge Proof (ZKP), and the promotion of transaction security.

1.3 Problem definition

In today's world, the biggest threat to information freedom is the Internet operator itself. Server hosts, governments, and Internet service providers control the network and can restrict content access by shutting down the server, blacklisting, and taking over DNS (Domain Name System). The prior art is not mature enough to stop these authorities and their attacks on the Internet. Various technologies are poised for use and will be used to create new distributed Internet and reduce the threat posed by censorship.

The meaning of Merkle RO

Merkle RO is a blockchain-based decentralized distributed sharing system for forming and executing storage contracts between end-to-end, negotiating contracts, transmitting data, verifying the integrity of remote data on Merkle RO. Availability, retrieved data, and content addresses are available. By optimizing the block interval, block size, and consensus algorithm, Merkle RO can theoretically achieve 1000 TPS usable performance. As the core part of the platform, Merkle RO links all terminals, so that all network terminal nodes can act not only as the role of Browser or Client, but also as the operator of this network. Everyone can be a server.

2.1 Rational use of resources

By decentralizing and sharing files, the problem of idle resources of personal computer hard disk, CPU and other resources is solved, and the user's idle hard disk and CPU resources are collected and distributed, and the resources distributed everywhere can be rationally utilized to form a set of Merkle. Application in the ecosystem of the RO chain.

2.2 Storage Advantage

The distributed storage technology solves the waste of storage space, can automatically redistribute data, improve the utilization of storage space, and connect all computing devices with the same file system. The principle replaces the domain-based address with a content-based address, that is, the content that the user is looking for is not an address but is stored somewhere. There is no need to verify the identity of the sender, but only the hash of the content. This will make the page faster and more secure.

2.3 Improve efficiency and solve network congestion

With distributed storage with high fault tolerance, high throughput, proximity and portability, data collection is more convenient and geographically restricted, and the probability of error is greatly reduced. Between points and points is an autonomous agent that can perform these operations without major human interaction.

2.4 Decentralized network

The decentralized network DSN is used to aggregate global users as storage providers, and to provide storage data and retrieve data services to customers in a self-coordinated manner. This coordination is decentralized and requires no trust: the system can obtain security operations through protocol coordination and individual participants can perform verification operations. DSNs can use different coordination strategies, including the Byzantine protocol, the gossip protocol, or CRDT, depending on the needs of the system.

3. data security

The data files are encrypted by default in the client and then stored in the storage node. This means that the data store can't actually view the contents of the file. For sensitive data, the data owner can choose to use the hardware encryption method to generate the encrypted file data and then publish it to the Merkle RO node.

The file should be encrypted on the client before fragmentation. The reference implementation uses AES256-CTR, but can implement convergence encryption or any other tunable system. This will protect the content of the data from the storage provider's stored data. The data owner retains full control over the encryption key to control access to the data. The data owner can keep the file fragmentation and the location information on the network confidential. As the collection of fragments in the network grows, it will become more difficult to find any given set of shards without knowing where they are. This means that the security of the file is proportional to the square of the network size.

The fragment size is a negotiable contract parameter. To protect privacy, it is recommended to normalize the fragment size to a multiple of one byte, such as 8 or 32 MB. The standardized size prevents the side channel from attempting to determine the content of a given fragment and can mask the fragmentation flow through the network. Fragmentation of large files (such as video content) and cross-node distribution of shards reduces the impact of content delivery on any given node. Bandwidth requirements are more evenly distributed across the network, and end users can take advantage of parallel transmissions. Data failure is irrelevant because peer nodes typically rely on separate hardware and infrastructure. This means creating a redundant mirror of the fragment, or applying a parity scheme across the fragment set is an extremely efficient way to ensure availability. Availability is proportional to the number of nodes that store data.

4 presentation layer

Like many layered applications, end users interact with top or presentation layers. In Merkle RO, the presentation layer consists of a distributed tracking system that works in conjunction with the storage and service layers.

4.1 Distributed Tracking System - Content Relationship System

A content management system is a web application that publishes documents and website content without technical knowledge. The end user is able to submit plain text and the software will present a consistent layout. Sites with dynamic content and frequent updates leave CMS and it's hard to run. To overcome some of the limitations, such as the inability to run some common server-side language-writing software and the lack of support for many database systems, custom CMS was created.

The custom CMS, called Hydra, is a new technology that runs as a CMS built on the web. Hydra works with the file manager and is currently able to handle most common tasks such as adding, modifying, and deleting content. The basic function settings will satisfy most user service needs, and the open source library enables developers to customize and tailor the software to their individual needs. Hydra writes are extendable to end customers and their code base is modular. For example, a web page and a blog have the same drawing engine, but may have different architectures. Create a new module programmatically using Node.js by specifying some configuration items. The result files can be served only through IPFS, and all the reposts occur on the client.

The front end and back end components are separated separately. This allows developers to use their preferred framework, such as Vue, React, or Angular. Data files and module structures are written to JSON files for use with external systems such as APIs.

4.2 Merkle RO – File Manager

Merkle RO equips the UI with a smart file management interface that enables end users to view and modify system managed content. End users track their content by using an account. The content submission request is paired with this account and the user can access it from any system. This allows the network to present file and file changes after the file is published.

Users can manage storage content in the same way as a typical modern operating system. Every user action will be propagated to the cluster. The interface provides a high-level code editor with full syntax highlighting for all common file types. Create a unique hash for each data file that prevents hosting or uploading the same content. This feature simplifies the upload process because duplicate files can be identified before submission. In addition, this feature enables the system to operate efficiently and reduce the broadband usage of end users and operators.

Merkle RO includes a DNS wizard to control the addressing of hosted domain names by using a managed storage cluster. This feature eliminates the single point of failure that requires content submitters to host their systems. Populate the health node list with Jenga, which will provide content for the requested domain.

4.3 Content Search

The data stored in the system is done at the content level rather than at the location level. This new method has many advantages. The main advantage is that the data locations are no longer relevant, allowing many nodes to present the same information, and when the data changes, a new hash is generated. Combine these advantages to create a merkle hash (root) and a relative path to a subfolder or file, and the file system will become smarter

The website address is addressed by a URL and the content is obtained by hashing. The domain name resolution system uses a variable hash. The end user can update the mutable hash using a private key in conjunction with an immutable hash. This feature does not require domain name record updates to enable content updates.

4.4 Consensus and block

Consensus is made up of trading packages. This algorithm is based on the DPOS consensus mechanism, and a transaction package contains the transaction records of Merkle RO. Blocks containing different transaction packages are generated by the full node and posted to the block network.

Information chain

Not all data and information needs to be published to the chain. The object stored on the chain is the tag of the content address as the resource address. In addition to the basic block information, stored in the chain are: accounting transactions, object data, storage transactions, certification transactions.

5 project realization

5.1 Decentralized network storage

In the application of decentralized computing, there is an epoch-making concept that is an incentive decentralized online file storage system. Currently, if you want your files or data to be safely backed up in the cloud, you have three options: 1. Upload them to your own server; 2. Use a centralized application such as Google drive or Dropbox, or; Use existing decentralized applications like Freenet. These methods have their own drawbacks: the first method has expensive setup and maintenance costs; the second method relies on a single trustworthy entity and often involves significant price increases; the third method is slow, for each Users have a high limit on space capacity because it relies on users voluntarily contributing storage space. The motivated file storage protocol has the potential to become the fourth method to provide high-capacity storage and high-quality services by decentralizing incentive executors (customers who store user data) to participate as nodes.

Simply put, you have a 10 GB file and you want to spread it across the network. First, you encrypt the file and then you split the file into 125 blocks. You arrange these blocks to form a 3D 5X5X5 cube, point out the polynomial for each axis, and extend each axis, and at the end you get a 7X7X7 cube. You can look for 343 nodes that are willing to store these blocks, and only tell each node which entity information it belongs to on that axis. In order to download the entire file, you will make a request for all blocks and then see which piece of the block has the highest bandwidth. As long as the minimum number of blocks is reached, you can use mathematical operations to decrypt the file and restore the file locally.

Decentralized storage is technically different from distributed storage. Decentralized storage is the need to meet a more secure, more trusted, and more controllable storage environment in a more distributed, less trusted network environment. There are three main goals for decentralized storage:

The first is security. Traditional central storage is vulnerable to hackers. For example, Japan’ s bitcoin exchanges have been attacked by hackers. The banking systems of various countries have been hacked, and even the situation of self-stealing has occurred. Data is cut and distributed across the entire network, and hackers cannot attack all the anonymous nodes on the entire network.

Secondly, the speed is fast and the efficiency is high. The centralized server is not close to all users, and Merkle RO's decentralized storage preferentially selects the node closest to each user.

Finally, the price is high. The decentralized storage network forms a trading market, using idle resources, the cost is much lower than the centralized fixed cost, and the sharer is free to bid to reach a minimum price, and the user can customize the security for each file. Level and cost are different.

5.2 proof of storage

The introduction of Merker Tree and Zh-Snark constitutes POR (Proof-of-Replica) and POST (Proof-of-Storage&Time) as the quantitative credentials issued by the storage. Trust-class storage nodes allow POR to provide proof in a shorter period of time, and lower credit ratings require POST to provide storage market certification.

5.3 Storage Market Certificate

Although POR can guarantee that the data store will save the data at least once, but can't avoid the spoofing of the perpetrator, consider the following scenario:

After the first backup of the data as required, the store calculates its Merkle checksum for all data cuts and split sequences, and deletes the data fragment file to save only the Merkle checksum.

After receiving the certification instruction, the storage requesting other nodes that have saved the data backup to obtain the data, and calculating the corresponding → (Merkle check tree) of C.

In the above scenario, the perpetrator can obtain storage rewards using extremely low computational and storage costs. Therefore, POST is introduced to ensure that the Merkle checksum tree cannot be correctly calculated as long as the data store does not store the data fragment file, and thus cannot get paid:

After the data is cut into fragments, an entropy sequence S is generated, and then the hash value R is generated using S and data fragments.

At regular intervals, the data owner sends Sx (time-based entropy value, globally unique) to the Merkle RO network. The store needs to calculate Rx based on Sx and the corresponding data fragment, and generate a corresponding Merkle check tree based on Rx. With the pre-entropy value sequence, data checking by the observer agent can also be implemented. The data owner can provide a partial entropy sequence to the observer, and the observer completes the proof of POST verification. In order to be safer to execute, the future will rely on smart contracts to implement agent inspection logic.

5.4 Credit certificate

In the Merkle RO agreement, the credit certificate is tied to the account. The specific scoring system varies according to different clients:

- Storage node: total storage, storage duration, online duration, and amount of penalty;
- Full node: maximum transaction processing capacity, outbound speed, fork convergence speed, online duration;
- Observing nodes: indexing service performance, online duration;
- Data owner: storage data volume, transaction volume;
- Proof: the amount of proof;

6. safety ecology

The Safety Ecology will operate as a Merkle RO Global Foundation, comprised of Merkle RO and its partners, including global exchanges, mines, individual investors and companies involved in the blockchain. Merkle RO partners can share Merkle RO's security technology and will benefit from the entire ecosystem.

Participating in the safety ecosystem of Merkle RO can achieve the following benefits:

1. Special price to get Merkle RO products and services, and other security technologies.
2. Share the benefits of the Merkle RO security ecosystem

The process of trading in the blockchain generally requires a certain amount of handling fee, which is a compensation for the miners to process the resources used in the transaction block in the blockchain. The account that initiated the transaction needs to specify the fee that he is willing to pay for the transaction; the miner can specify the lowest transaction fee he is willing to handle, and only the transaction with the handling fee above this minimum will be processed by the miner. . The miners prioritize the transaction of high transaction fees. If the transaction fee for a transaction is too low, the transaction may take a long time to be confirmed. As a partner of Merkle RO, the transaction can obtain the preferential packaging rights of the cooperative miners and increase the transfer speed. This is a huge advantage in the blockchain network, especially the increasingly congested Ethernet network.

7.Merkle RO features

7.1 three characteristics

reliability

Merkle RO has a wide geographical distribution. In order to serve users in different regions, the same service will be deployed in the block points of each region, making high reliability an intrinsic property of Merkle RO. Once a service in a certain area is abnormal, the user requests You can quickly move to other nearby areas to get related services. In addition, as Merkle RO reduces the amount of data sent to and from the cloud, security reliability is further increased.

Portability

Merkle RO supports high mobility, mobile phones and other mobile devices can communicate directly with each other, the signal does not have to go to the cloud or even the base station to go around! In addition, Merkle RO also supports real-time interaction, diverse hardware and software devices, and cloud online analytical computing.

Low latency

Merkle RO has a lower position in the network topology and has a smaller network latency (total latency = network latency calculation latency) and is more reactive.

7.2 distributed

The Merkle RO architecture is distributed, closer to the edge of the network, and data storage and processing is not dependent on cloud servers.

8.Merkle RO works

The service Merkle RO provides to users is the utilization of all facilities, including processing, storage, networking and other basic computing resources, allowing users to deploy and run any software, including operating systems and applications. Merkle RO provides server services, CDN acceleration services, file storage services, and data exchange services to individuals or small and medium-sized businesses through distributed cloud storage at low storage prices.

8.1 Calculation

A set of controllers that manage the entire lifecycle of a virtual machine instance for a single user or group, providing virtual services based on user needs. Responsible for virtual machine creation, boot, shutdown, suspend, pause, adjust, migrate, restart, destroy, etc., configure CPU, memory and other information specifications.

Merkle RO is based on content, peer-to-peer hypermedia protocol, high fault tolerance, scalability, and more secure, open source storage. Provides users with persistent image storage and volume backup services for the platform.

Keystone. Provides authentication, service rules, and service tokens for other OpenStack services, managing Domains, Projects, Users, Groups, and Roles.

8.2 Network and Address Management

Provide cloud computing network virtualization technology to provide network connectivity services for other OpenStack services. Provides interfaces for users. You can define Network, Subnet, and Router. Configure DHCP, DNS, load balancing, and L3 services. The network supports GRE and VLAN. The plugin architecture supports many major network vendors and technologies such as OpenvSwitch.

8.3 storage and access methods

Provides a stable block storage service for running instances. Its plug-in-driven architecture facilitates the creation and management of block devices such as creating volumes, deleting volumes, and mounting and unmounting volumes on instances.

Data is transmitted via Merkle RO. The user exposes that the client application may upload or download the fragmented endpoint. The customer's request is authenticated by the token provided by the previous delivery and retrieval message.

The data owner must bear the burden of network access to maintain the availability and integrity of the data on the Merkle RO network. Because nodes cannot be trusted, and hidden information security challenge sets cannot be outsourced to an untrusted peer, the data owner is responsible for pre-processing fragmentation, release and verification audits, providing payment, managing file status, and collecting and managing files through fragmentation. Key, and so on.

Miners receive payments only when the network can audit whether their services are properly provided.

Merkle RO is one of the world's first distributed storage applications supported by blockchain. It is implemented as a distributed application on top of the blockchain. By leveraging Jenga and Hydra, Phantom provides a review rejection platform for web hosting and content delivery.

9. Team introduction

9.1 Initiating members

核心成员

9.2 Advisory Team

Yang Bodong Strategic Consultant

Block chain consulting company TOKEN-FUND strategic consultant, MBA micro-circle blockchain consultant, continuous entrepreneurs in the mutual gold field. Proficient in block-based ecological strategic planning, good at Token economic model construction, ecological organization model building. Provided consulting services in the blockchain field for a number of listed companies of China Mobile and Guangdong Power.

Hu Qihang Product Consultant

Blockchain consulting company TOKEN-FUND co-founder, senior Internet product expert. It has provided blockchain related consulting services for many well-known enterprises and listed companies in various vertical fields such as government

affairs, finance, entertainment, logistics, and supply chain.

Zhou Liyi Technical Expert

China University of Science and Technology Software Engineering, China Mensa, Shenghan members. He has served as the technical leader of Renren.com, Cool Dog Music, Alibaba and other well-known companies, and has more than 20 years of development experience. In 2012, he participated in the development of Bitcoin mining machine and has rich experience in blockchain algorithm optimization.Industry consultant, investment consultant

Xu Meijiao

He is currently the president of Tianxia Network Co., Ltd. and secretary of the party branch. Director of China High-Tech Industrialization Research Association, Informationization Work Committee, Vice President of Beijing Haidian District Cultural and Creative Industry Association, and Beijing SME Entrepreneurship Instructor.

Lin Feng

Founder of TAOGO, a veteran of TMT and mobile internet. Former Beijing Gehua Network Vice President/Director. In 2010, TAOGO has covered 500 million mobile phone users and has completed share reform and C round financing.

Sesogo

The world's first new generation of social networking based on billions of users GMB (Global Mercy Chain) founder, the founder of Southeast Asia's leading mainstream high-end live platform Kitty Live. Former ZTE’s overseas leaders in Southeast Asia, the Middle East, Latin America and other countries have made great contributions to ZTE’s journey to become the world’s number one in CDMA. At the same time, he is also a staunch supporter of blockchain technology. He is determined to use blockchain technology to subvert Facebook, Line, WeChat and other centralized social networks. He has also played the role of “manager” and “arbitrator” in the past. The role and revolution.

Note: before and after the ranking

9.3 Strategic partners

基金会投资

10. Merkle RO Release Plan

10.1Merkle RO Foundation

Merkle RO stores the ecology of the industry and belongs to every institution or individual that joins the ecology. However, the entire ecology needs to regularly adjust the rules of the industry, and an organization is needed to review, supervise and manage the daily affairs within the ecology. The Merkle RO Foundation was therefore established and members of the Foundation were elected from among the various members of the Ecology. And do the following:

Foundation operation

Democratic supervision decentralized distribution platform operation democratic decision-making hardware access assessment arbitration arbitration among members of the ecological disputes

10.2 Merkle RO allocation ratio

The total production and distribution limit for Merkle RO is 1.5 billion.

10.3 Fundraising Fund Allocation Planning

All proceeds are only used for the development and promotion of the Merkle RO Ecology. The following is a preliminary allocation plan, which will be supervised by the Merkle RO Foundation and will be rationally adjusted according to the actual situation on the premise of the ecological development of Merkle RO.

Ecological construction accounts for 50%

Ecological construction refers to the development and operating costs of all technologies, including smart contracts, wallets, SDKs, APIs, Merkle

RO hardware, third-party plug-ins, and any other Merkle RO related updates. It also includes the cost of hiring full-time developers and professional consultants to achieve the goal of accelerating ecological development and ultimately achieving ecological development. Wind control construction accounts for 10% of the total

Financial risk control measures were taken to conduct regular risk control assessments and risk control of the Merkle RO Ecology. These include: technical wind controls, all APIs, smart contracts, professional code auditing and penetration testing of flash plugins and SDKs; financial risk control, monitoring and risking of financial attributes such as Merkle RO's distribution, circulation, price fluctuations, etc. Evaluation.

Basic technical operation and maintenance costs accounted for 5%

Includes technical operation and maintenance costs related to ecological operations such as web servers, firewalls, load balancers, DDOS protection and network extensions.

Market operation, accounting for 30%

Used for ecological promotion, marketing, and daily operations. This includes the continuous promotion of the Merkle RO ecosystem to the global market. Integrate users in the ecological resources and storage areas of multiple target countries around the world.

Legal cost, 5%

Used to obtain appropriate legal advice to ensure that the project complies with local laws and regulations. Conduct legal operations in accordance with the laws and regulations of the jurisdiction in which the project is located. The funds will be used to reserve any problems or challenges that may arise in any future region.

11. Risk warning

a) Policy risk

At present, the state's regulatory policies for blockchain projects and private equity financing are still unclear. There are certain policy factors that may cause participants to lose. If the overall value of the digital asset market is overvalued, the investor risk will increase. Under the existing national policy, Merkle RO does not provide any legal currency trading channels to users within the territory.

b) regulatory risk

The digital asset trading including Merkle RO is extremely uncertain. Due to the lack of strong supervision in the digital asset field, digital tokens are at risk of skyrocketing and falling. Individual participants may be unable to resist the market due to lack of experience. Asset shock and psychological pressure caused by instability.

c) market risk

Because the digital currency sales market environment is inseparable from the overall digital asset market situation. At present, there are many blockchain projects, and the competition in the industry is becoming increasingly fierce. Blockchain-related application platforms are emerging one after another, and Merkle RO will face certain market competition pressures and project operational pressures. There is a certain risk that Merkle RO will gain more support from ecological partners and users in the future and become the mainstream ecological platform.

d) technical risks

With the rapid development of science and technology or the development of blockchain fields, the development of such as quantum computers and high-powered mining machines may have a destructive impact on Merkle RO and even lead to the loss of Merkle RO. The project will prevent technical risks through timely updates and constant repair of vulnerabilities, but there is no guarantee that they will not be affected at all.

e) Unpredictable risk

Cryptographic-based digital assets are a completely new technology. In addition to the risks mentioned above, there are risks that have not been mentioned or anticipated by the founding team. Such risks may occur suddenly or multiple risks may occur in combination.