DIS Chain - A New Type of PoW Blockchain Integrating AI Computing Power and Meme Culture

1. Introduction

In the blockchain field, the concept of decentralization has always been the core driving force for technological development. This concept is particularly evident in the development of the Bitcoin and Ethereum networks, especially at the critical turning point when Ethereum transitioned from Proof of Work (PoW) to Proof of Stake (PoS).

PoW (Proof of Work) , Proof of Work as a consensus mechanism, is one of the most primitive and core elements in blockchain technology. It ensures the security and decentralization of the network by requiring participants to solve complex computational problems to verify transactions and create new blocks. This mechanism of PoW has always occupied a core position in the Ethereum network until Ethereum announced the transition to the PoS mechanism. This shift has sparked widespread discussions about whether the principle of decentralization has been weakened , and the opposition and protests of miners, who believe that the upgrade has sacrificed the support of miners who have always maintained the Ethereum network. This upgrade has caused large-scale economic losses to all Ethereum miners and caused large-scale mining disasters. Miners, whether ASIC or GPU, are very dissatisfied, believing that this change has not respected the opinions of miners, and even has no right to speak and vote , which violates the spirit of decentralization .

POS (Proof of Stake), which stands for Proof of Stake , mechanism is completely different from PoW. Referring to the great design of Bitcoin, people believe that the value of Cryptocurrency is minted by paying a certain cost, which is the true value basis. In the PoS mechanism, holders can become verification nodes by mortgaging a certain amount of tokens, and nodes will receive newly minted tokens, which can be regarded as a form of "coin generation". In recent years, the US Securities and Exchange Commission (SEC) has raised regulatory concerns about Cryptocurrency operating in the Proof of Stake (PoS) mode. The SEC's concerns mainly focus on whether the principle of "coin generation" in the PoS mode constitutes a security publishing. According to the traditional definition of securities, if an asset provides an expected return on investment and this return comes from the efforts of others, then this asset may be regarded as a security. According to the so-called "Howie test", these tokens may be regarded as securities

and therefore subject to relevant regulatory rules. This regulatory prospect has a serious impact on Cryptocurrency

1.1 Ethereum Forks and the Development of Ethereum Fair

Ethereum Fair (ETHF) is a forked chain led by a group of Silicon Valley tech geeks. It insists on maintaining the consensus algorithm of ETH PoW, providing high stability, high security, and a 100% decentralized network environment. It is the direct result of this historical transformation. Its emergence not only represents the adherence to the original Ethereum concept, but also a firm commitment to the principle of decentralization.

After ETH switched to POS on September 15th, 2022 , Ethereum Fair came into being. It not only adheres to the PoW consensus mechanism, but also reaffirms the spirit of decentralization. Forked ETHF not only preserves the original characteristics of the Ethereum network, but more importantly, it maintains the decentralized and community-driven characteristics of the network. This persistence not only shows blockchain loyalty to technology, but also reflects respect for the vast community members and their values.

ETHF's decision reflects a core belief that true decentralization can only be achieved through the PoW mechanism. Based on this, ETHF promises to maintain an open, fair, and non-single entity-controlled network environment, ensuring that every participant has a voice and every transaction is conducted in a fair and transparent environment.

With the continuous development of blockchain technology and the arrival of the AI era, we are facing new challenges and opportunities. In this context, the emergence of DIS Chain not only inherits the spirit of ETHF, but also embarks on a new journey. It is a new PoW public chain that integrates MEME & AI computing power, an advanced path aimed at promoting technological innovation while adhering to the principle of decentralization.

1.2 DIS Token Development History

When telling the story of DIS Chain, we cannot ignore another important component - DIS Token. The history and development trajectory of DIS Token is a key part of understanding the whole picture of DIS Chain, especially its huge support in the community through meme culture and unique role in technological development.

DIS Token originated from a deep passion for blockchain innovation technology and meme culture. It was originally designed as a meme token, initiated by the Chinese miner community (especially the past Ethereum miners) and supporters of the Cryptocurrency community , aimed at rewarding community interaction activity rewards , tipping, public welfare, and dream tokens, with the aim of establishing a fair, open, and democratic blockchain community In the blockchain field, meme tokens usually have entertainment and social value. Over time, DIS Token has surpassed its initial scope Through innovative economic models, it has designed the

deployment of pledged mining, with 50% of the publishing volume as a long-term reward. Like POW mining gameplay, the computing power of the entire network is equal to the total pledged amount. Allowing pledged tokens to divide this reward every second is a reward for holders and long-term benefit development, which has received support and recognition from multiple cross-community communities. Gradually evolved into a digital asset with substantial role and value.

The development of DIS Token is not only an achievement of innovative technology , It also represents a belief that Chinese people have the ability to make healthy and positive contributions to the blockchain ecosystem, from groups to communities to cross-communities, forming a consensus of faith for the innovation and change of blockchain, and supporters have a common vision. It is also a symbol of community strength. The development of this project is very similar to the history of Dogecoin. Its growth process reflects how a grassroots community-driven project can evolve into an important force with practical impact and technological innovation. DIS Token brings new vitality and potential to the decentralized blockchain world by strengthening community participation and Incentive Mechanism.

1.3 DIS Chain - ETHF and DIS Merge Upgrade

Ethereum Fair (ETHF) inherits the spirit of ETH POW, but with the impact of the bear market and various negative factors from 2022 to 2023, the entire Cryptocurrency market, including the computing power market, has been severely hit, and the road to forking is never easy. ETHF forks from PoW to PoS in the Ethereum network. The original ETH holders and holdings also receive the same number of ETHF forked airdrops. It is fair for private key wallet users to add their own ETHF main network for forked asset interaction. However, there is a serious problem that many centralized institutions hold a large amount of ETH at the time of the fork, and do not airdrop or return the forked ETHF to the real users. Some institutions have misappropriated customers' forked assets and privately transferred them to the market with support for ETHF trading to cash out and sell, which has led to the bad performance of ETHF in the price development; the price also represents the capacity of how much miner computing power can be fed. The ETHF solution is to freeze the forked assets that have not been airdropped to

The founder of DIS was originally a miner of Ethereum. Since the Ethereum network transitioned from PoW to PoS, it has continuously supported the ecological development of ETHF and played a role in promoting and managing the Chinese community. Although the publication of DIS started as a joke meme, most of the team and community are miners and decentralized supporters with the same goals and missions. Some Ethereum supporters and miner communities are dissatisfied with the abandonment of the original consensus mechanism. Due to the transformation of ETH, a large number of miners are facing unemployment and computing power transfer problems. DIS has become a bridge connecting traditional Ethereum PoW supporters and uniting multiple miner communities, in Chinese areas It plays a key role in

maintaining the community and promoting the spirit of decentralization, and has also become a driving force for the community and maintaining the concept of decentralization , The DIS community has inspired this part of the population to actively seek solutions through the power of meme tokens, ultimately leading to the merger of DIS and ETHF, and has expressed this vision and dream in its white paper

In order to achieve the goal of the white paper, DIS dreams of upgrading from Token to the main network. This may be the first case in the world. We believe that it is possible to mobilize the power of the community and miners. We hope that DIS can become the vision of the ETH POW main network, uniting more than 51% of the computing power of the entire network, and initiating a merger proposal with ETHF in the name of miners. The ETHF team and technology discussed multiple feasible solutions, and finally democratically accepted the consensus of the community to initiate a hard fork!

ETHF and DIS merge and upgrade in the form of exchange contracts to exchange for the new DIS CHAIN mainnet currency, and promote the best solution. The above mentioned Milan upgrade locks the forked asset freeze of the centralized institution. Based on the reasons for the merger, the new mainnet currency airdrops the original DIS holders and holdings. After evaluation and statistics, about 50% of the frozen circulation will be redistributed. Referring to the pledge mining economic model of DIS Token, these assets will be redistributed to holding users and miners in the same form. This also excludes the original crisis and holds the moral concept of justice and enriches the people.

By combining the persistence of ETHF and the innovation of DIS Token, DIS Chain presents itself as an advanced platform that retains the spirit of traditional blockchain and explores the potential of future technology. Every step of its development is deeply rooted in the concept of decentralization and community culture -driven.
With the birth of DIS Chain, the role of DIS will be further expanded. As a core component of the DIS Chain ecosystem, DIS not only retains its original community-driven and reward mechanism, but also In addition to maintaining and adhering to the concept, the team understands the need for innovation and support from the community. This belief is linked to the fate of miners, believing that only with ecology, users, applications, and support can there be real value.

1.4 DIS Chain

1.4.1 Innovative POW public chain integrating MEME culture

As we all know, the main chains of Bitcoin and Dogecoin do not directly support smart contracts , especially compared to smart contracts on Ethereum. This is mainly due to the UTXO (Unspent Transaction Output) model they use, which is significantly different from the account model (EVM) used by Ethereum.

Dogechain is within the top ten of the global cryptocurrency rankings, with a market value of over 10 billion US dollars. It can be called the world's largest meme consensus and value public chain. However, because Dogechain does not support smart contracts, it cannot publish tokens on the Dogechain public chain.
Currently, meme coins on the market, such as Shiba Inu (SHIB), PEPE, FLOKI, Memecoin, BabyDoge, BONK, ELON, TURBO, AIDOGE, etc., are all ERC20 standard tokens (TOKEN), which are usually deployed on ETH, BSC, and L2 networks. DIS CHAIN has a great advantage in publishing meme projects or tokens on the meme public chain, which may be the world's first public chain that supports EVM with meme attributes and culture. On this basis, it may attract more meme projects and even a gathering place for secondary creation, triggering a new round of MEME craze.

1.4.2 Integration of AI computing power of new POW public chain

The birth of DIS Chain marks the beginning of a new era. It is a perfect combination of the firm decentralization spirit of Ethereum Fair and the community-driven power of DIS Token. It will also play a more critical role in the new AI computing power fusion public chain. In this new era that integrates advanced AI technology, DIS not only represents the economic value of a token, but also a powerful driving force for technological progress and community prosperity. As a new type of PoW public chain that integrates AI technology, DIS Chain not only inherits the original characteristics of the Ethereum network and the vitality of the community, but also opens up a new field of blockchain technology and artificial intelligence integration.

In the world of blockchain, innovation and inheritance go hand in hand. DIS Chain aims to explore and implement a more efficient, secure, and truly decentralized blockchain environment by combining traditional PoW mechanisms with cutting-edge AI technology. This unique positioning not only puts DIS Chain at the forefront of the industry in technology, but also ensures its adherence to community-driven and decentralized principles.

The emergence of DIS Chain is not accidental, but an inevitable result of the development of blockchain technology and the evolution of community needs. In this new ecosystem, DIS Token will play a more core role, not only as a digital asset representing community power, but also as a key to connecting traditional blockchain technology with the future AI world. DIS Chain is committed to providing a platform full of innovation and opportunities for global blockchain enthusiasts and developers, allowing every participant to find their own position in this decentralized new world.

With the continuous development of DIS Chain, we will witness how a powerful community-driven ecosystem embraces the future of technology while maintaining its core values. DIS Chain is not just a blockchain project, it is a story about faith, technology, and community progress together. In this story, each participant is not only a witness, but also a creator, jointly writing a new chapter of decentralization and AI integration.

2. Technological innovation and integration

2.1 Overview

DIS Chain represents the revolution of the Ethereum domain. Its core is based on the ETH POW algorithm, combined with the MEME culture and artificial intelligence (AI) technology, to create a comprehensive Web3 system The development concept is based on three pillars: technological innovation, community consensus, and cultural diversity Continuous pursuit of integration. As the orthodox fork of Ethereum POW , it retains the original TOKEN and NFT, ETHASH's POW algorithm, fully compatible with EVM (Ethereum Virtual Machine), and introduces AI (artificial intelligence) and meme cultural elements In the world of blockchain, decentralization is not only a technical norm, but also a belief , At the same time, actively exploring and integrating emerging technologies, especially AI & MEME , to enhance the efficiency and application scope of its network. This integration reflects respect for the value of traditional blockchain and foresight of future technological trends.

2.2 Original technology and functions

Consensus mechanism:
Proof of Work (PoW), the basic concept and principle is to calculate workload. PoW requires nodes (miners) to solve a computational problem, which requires a large amount of computing resources, thus proving that the node has put in a lot of work. Through Proof of Work, nodes in the network can reach consensus, confirm the validity of transaction records, and prevent the same asset from being reused (double-paid). The mining process solves the hash problem. The miner's task is to find a specific hash value, which must be less than or equal to the target value set by the network. This is usually achieved by constantly trying to modify a random value (nonce) of the block. Block creation: Once a hash value that meets the requirements is found, miners can create a new block and add it to the blockchain. The reward mechanism is that miners who successfully create blocks will receive a certain amount of cryptocurrency as a reward, which is called block reward. Anyone can participate in mining, which helps to decentralize the network.

Smart contracts are compatible with EVM.
Allows developers to deploy and run smart contracts on it. It is composed of solidity language code and can automatically execute contract terms when specific conditions are met. This is the core function of Ethereum, which provides strong flexibility and scalability for building decentralized applications (DApps), and can support complex blockchain operations and business logic, enabling it to support various complex decentralized applications.
Ethereum Virtual Machine (EVM): EVM is the runtime environment for executing smart contracts on Ethereum. It is completely isolated, which means that the code running in EVM cannot access the network, file system, or other processes. This provides security for smart contracts.

Token standard:
Ethereum supports multiple token standards, the most famous of which are ERC-20 (for tokens) and ERC-721 (for non-fungible tokens, or NFTs), ERC1155 (multi-token standard), ERC777 (improving the newer token standard of ERC20), ERC223 (preventing tokens from being accidentally sent to contract addresses that do not support token contracts), ERC721x (a variant of ERC721), etc. These standards ensure that tokens published on the Ethereum platform can be compatible with each other; In the future, we will develop the combination of RC-20 inscriptions and achieve the goal of truly decentralized indexing, establishing a fair coin model.

Decentralized Applications (DApps):
As an Ethereum framework, it can support a variety of DApps, from games, entertainment, and collectibles to decentralized transactions (DEXs) such as Swap, which allow users to exchange tokens directly on the blockchain without going through centralized transactions, to social networks, centralized identity and data management, and oracles. These applications run through smart contracts and do not rely on any centralized server or management entity control, but run on a decentralized blockchain network.

Power builder:
Ethereum power builder has rich power builders in the development process of blockchain applications and smart contracts, such as Truffle automating the deployment process of smart contracts through the Migrations system (supporting JavaScript and Solidity), Hardhat for the development, testing, deployment, and debugging of smart contracts, and Remix, an open-source web and desktop application for the development, testing, debugging, and deployment of Solidity smart contracts (supporting mainnet, testnet, and private network). These tools provide developers with powerful support to make it easier and more efficient to write, build, and deploy smart contracts and DApps.

DeFi and other ecosystems:
Ethereum is the main platform for decentralized finance (DeFi), supporting numerous lending platforms, oracles, exchanges, and other financial instruments. It is also the foundation of many other ecosystems, such as NFT markets and Decentralized Autonomous Organizations (DAOs).

Transaction processing and speed:
The transaction processing mechanism of DIS Chain has been optimized to increase speed and reduce latency. The mining time of each block is about 14 seconds. If the maximum Gas Limit of the block is 30,000,000, it is necessary to calculate how many transactions per second (TPS) it

can support. If we only consider standard transfer transactions, the maximum number of transactions that a block can contain is approximately: 30,000,000 Gas Limit/21,000 Gas per transaction is calculated as 1,428 transactions per second (TPS)/14 seconds is calculated as 102 TPS

This ensures that transactions can be confirmed quickly and reliably, even under heavy network loads.

As for the calculation method of Gas, the fixed amount of Gas required for a standard transfer of Ethereum is 21,000. If the transaction contains data, additional calculation of Gas is required based on the number of bytes of the data. The cost of Gas for non-zero and zero bytes is different. Due to the different computational complexity, smart contract transactions will consume more Gas. Therefore, the gas consumption of each transaction will vary depending on the operation and complexity it performs.
In addition, there are multiple solutions that can be considered or upgraded in the future to improve transaction throughput (TPS), such as Layer 2 solutions and multi-chain strategies.
Layer 2 Scaling Solutions:
Rollups: Rollups are a type of Layer 2 scaling solution that runs on top of the Ethereum main chain. They improve TPS by outsourcing transactions to an independent chain, packaging transaction data into one or more Data Points (or "rollups"), and submitting these Data Points back to the Ethereum main chain. Doing so can significantly reduce the amount of data processed on the main chain, thereby improving efficiency and throughput. Rollups are divided into two main types: Optimistic Rollups and ZK Rollups.
Optimistic Rollups: This method assumes that the transaction is valid unless someone objects. They allow for fast transaction processing, but there is a "challenge period" during which the transaction can be proven invalid.
ZK Rollups: Uses zero-knowledge proofs to ensure the validity of transactions and allows the proof of validity of transactions to be packaged into a small proof and submitted to the main chain. This method has higher security because every transaction is verified as valid.
Sidechains:
Sidechains are independent blockchains that run parallel to the main Ethereum chain. They have their own consensus mechanism, which can process transactions and ultimately anchor the results to the main chain. These chains can have different rules and features, allowing for more flexible transaction processing and different types of applications. However, their security may not be as good as the main chain.
State Channels:
State channels allow participants to conduct transactions outside the blockchain and only send transaction data to the main chain when needed (such as when opening or ending the channel). This method reduces the transaction volume on the main chain, thereby improving throughput, but it requires a certain degree of trust between participants.
Plasma Chains:

Plasma is a framework that allows multiple child chains (or "Plasma chains") to be created from the Ethereum main chain. Each child chain can independently process transactions and regularly submit its state to the main chain. These child chains can have their own rules and structures, but their security depends on the main chain.
These techniques attempt to solve scalability by processing transactions outside the main chain, somehow linking the results back to the main chain. The purpose of these methods is to increase transaction speed and volume while maintaining decentralization and security.

Networks and nodes:
The network architecture design of DIS Chain considers the distribution and connectivity of global nodes, enhancing the anti-attack and fault tolerance of the overall network. The collaborative work between nodes ensures high availability and stability of the network. DAG (Directed Acyclic Graph) is used to implement part of the Ethash proof-of-work algorithm. Every once in a while, the system increases the size of DAG. This growth cycle is fixed and called Epoch. Each Epoch is about 30,000 blocks long, growing approximately every 100 hours. Since the average block production time on Ethereum is about 14 seconds, each Epoch is about 5 days. We maintain the DAG size at 2.8GB. This setting allows more miners to participate in our network, which not only reduces the entry hardware requirements, but also promotes wider decentralization. This careful adjustment of DAG not only takes into account the limitations of Prior Art, but also looks forward to the potential of future hardware development.
* If DAG increases by 1GB, it needs to increase by 1024MB. Divide 1024MB by the growth of 8MB per epoch, resulting in 128 epochs. Each epoch is about 5 days, so 128 epochs is about 640 days. In other words, the size of DAG will increase by 1GB approximately every 640 days. The expected date to reach 4GB DAG is August 2025, and the date to reach 6GB DAG is February 2029.

Application of AI technology:

DIS Chain will provide more intelligent services by integrating artificial intelligence technology, such as AI-driven smart contracts and transaction analysis. AI can create NFTs with Wenshengtu, AI combined with SocialFi, Gamefi, Defi Data Analysis, AI strategy trading, smart contract design or security and vulnerability detection assistance. The application of these technologies not only improves the efficiency of DIS Chain, but also provides users with a more personalized and accurate experience.

Safety:
Security is highly valued and regular security audits and updates are conducted. Since changing confirmed blocks requires recalculating all subsequent blocks, the PoW blockchain is very secure. All transactions are open and transparent, and benefit from the security of blockchain.

2.3 Technological development route

DIS Chain's technology development path closely combines the latest advances in blockchain and AI . The core path includes:

2.3.1.1 Maintain the decentralized principle of PoW

DIS Chain adheres to the POW consensus mechanism of Ethereum, ensuring the decentralization and security of the network, while providing a stable foundation to support future technological integration.

2.3.1.2 Decentralized Autonomous Organization (DAO) Management

Through the DAO model, true community governance has been achieved. Currently, DIS Chain DAO has more than 40 members, with a community audience of about 100,000 users. Community members can participate in the proposal, voting, and decision-making process, achieving true decentralized autonomy. This not only improves transparency, but also enhances the sense of belonging and responsibility of community members to the project.

2.3.1.3 Diversified ecosystem:

DIS Chain has built a diversified ecosystem that covers various blockchain applications such as DeFi, NFT, GameFi, DEX, and others. This ecosystem not only provides developers with a broad development platform, but also provides users with a comprehensive digital economic ecosystem. These applications not only expand the usage scenarios of DIS tokens, but also contribute to the practical application and popularization of blockchain technology.

2.3.1.4 ETHhash mining algorithm upgrade

- New EthashAI Algorithm: DIS Chain plans to implement the newly designed EthashAI algorithm through a soft fork. This important upgrade marks the successful integration of AI technology and traditional POW computing power , paving the way for a new era of AI-POW computing power public chain for DIS Chain.
- Computing Power Fusion Implementation: The introduction of EthashAI algorithm will greatly enhance the processing power of DIS Chain, making it not only suitable for traditional blockchain computing needs, but also effectively supporting complex AI computing tasks. This fusion enables DIS Chain to more effectively utilize and allocate network computing power while maintaining the original mining mode.
- Supporting the development of AI applications: The new algorithm not only brings technical advantages to DIS Chain, but also provides a solid platform for future AI applications. It provides developers with more opportunities to explore and create innovative AI-based blockchain applications.

2.3.1.5 AIEVM compatibility completeness

- Ethereum compatibility : DIS Chain maintains high compatibility with the Ethereum Virtual Machine (EVM), ensuring that existing Ethereum smart contracts can be seamlessly migrated to DIS Chain. This provides developers with a familiar and efficient development environment.
- Support for innovative applications: DIS Chain's EVM compatibility is not limited to current smart contracts and applications, but will also be expanded to support more innovative and diverse applications, including but not limited to decentralized finance (DeFi), Decentralized Autonomous Organization (DAO) and NFT markets.
- The richness of the development environment: DIS Chain will provide a more inclusive and comprehensive development environment, encouraging developers to use the unique features of DIS Chain to create innovative blockchain solutions.

Through these strategies and development paths, DIS Chain has demonstrated its ambition and ability in technological innovation and application integration. It has built a diversified ecosystem covering various blockchain applications such as DeFi, NFT, GameFi, DEX, and others. This ecosystem not only provides developers with a broad development platform, but also provides users with a comprehensive digital economy ecosystem. It also integrates artificial intelligence technology to provide more intelligent services, such as AI-driven smart contracts and transaction analysis. AI can create NFTs with Wenshengtu, and AI can combine with various creative possibilities such as SocialFi, Gamefi, Defi Data Analysis, and develop from Web2 applications to Web3, AI strategy trading, smart contract design, or security and vulnerability detection assistance. It not only consolidates its position in the decentralized field, but also opens up new possibilities for the future development of blockchain technology.

Future development will focus on motivating and supporting high-quality projects, not only for smart contract technology developers, but also for market makers, project promotion, and assistance to listed exchanges. The DIS team is committed to providing comprehensive support for these key roles, ensuring that our ecosystem can continue to attract innovation and vitality.

In this rapidly changing market environment, DIS Chain's roadmap is dynamic and can quickly adapt to changes in industry trends and community needs. We will continue to work closely with our partners and communities to ensure that our strategies and action plans remain cutting-edge and relevant. We will uphold the spirit of open innovation and continuously update the development roadmap to ensure synchronization with the rapid changes in industry trends and community needs. As we enter a new stage of development, DIS Chain looks forward to becoming a more important participant in the emerging blockchain ecosystem, bringing more innovation and value to the global blockchain community.

2.4 Key technological innovations

DIS Chain represents the frontier exploration of the integration of blockchain and artificial intelligence (AI) technology, and is committed to creating a new type of proof-of-work (PoW) public chain that integrates AI computing power . The technical core of this public chain focuses on three major innovation areas: enhanced blockchain security, efficient AI computing power fusion mechanism, and AI-driven network supervision and autonomy.

AI 's computing power and PoW mining computing power are fundamentally different, which is manifested in:

POW mining hashrate :

- Based on solving complex mathematical puzzles such as SHA-256 or Ethhash
- The goal is to maintain the security and decentralization of the blockchain network
- Hashing power is expressed as hash rate, that is, the number of hash operations performed per unit time

AI computing power requirements:

- Focus on complete mathematical capabilities in data processing and pattern recognition
- For training and running Machine Learning models such as deep neural networks
- Computing power is represented by the ability to process large amounts of data and perform complex and complete mathematical operations

The key technical goal of DIS Chain is to achieve the complete integration of POW computing power and AI computing power, upgrade POW mining algorithm through soft fork to support AI computing power, and support AI computing power "dual mining" while ensuring the complete, secure, and decentralized operation of the entire network

1. AI-PoW algorithm:
    - EthashAI Algorithm: A new algorithm is designed through soft fork to achieve the perfect integration of AI and PoW, opening a new era of AI-PoW computing power public chain.
    - Dynamic optimization: The algorithm is continuously optimized to adapt to changes in AI computing power , ensuring the efficient operation and scalability of the network.
2. Dual-purpose mining process:
    - Redesign the mining process, can be used for blockchain maintenance, but also for AI applications to provide computing power
    - Mining nodes participate in the training or computing power output of AI models while performing hash operations
3. EVM Compatibility and Upgrade:
    - EVM Compatibility : Maintain compatibility with Ethereum, support more innovative applications, and provide developers with a rich and flexible development environment.

- Computing Output Interface : A computing output interface designed for AI models, allowing computing power in the blockchain network to support AI applications.
- EVM upgrade: support AI capability on native blockchain application capability.

4. AI Integrated Network Oversight and Autonomy:
   - AI monitoring algorithm: Real-time monitoring of blockchain network, timely detection and response to abnormal behavior, maintenance of cyber security and stability.
   - AI-Driven Governance: Improve decision-making efficiency and responsiveness, enhance community participation and transparency through AI -driven governance mechanisms.
5. Decentralization and Security Enhancement:
   - The decentralized nature of PoW: Continue to maintain the decentralized advantages brought by PoW, ensuring the decentralization and security of the network.
   - Enhanced Security Protocol: Combining AI technology to enhance the security of blockchain and effectively defend against potential security threats.

DIS Chain, as a new type of PoW public chain that integrates AI computing power , not only improves the performance and security of blockchain through these key technological innovations, but also opens up new possibilities for the development of AI applications. These innovations ensure that the network maintains decentralization and high security while integrating AI computing power, while paving the way for future technological progress and community development.

2.5 Key technical solutions

There is an essential difference between the mining computing power of PoW and the computing power demand of AI . One focuses on hashing large integer calculations, and the other is for intensive floating-point operations. It is very challenging to integrate the two. DIS Chain Lab is committed to this challenging task, exploring the implementation **of AI-enhanced PoW algorithm (AI-PoW).**

1. **Infrastructure**

Dual-core processing system: Design a special processing unit with two operation modes, one is the traditional PoW hash calculation mode, and the other is the floating-point number processing mode specifically for AI operations. This processing unit can dynamically switch modes according to network requirements.

2. **Consensus mechanism**

Hybrid consensus algorithm: Design a new type of consensus mechanism that includes not only solving hash puzzles to maintain the security and integrity of the blockchain, but also completing AI -related tasks as part of the network contribution.

3. **AI Task Integration**

Dynamic Task Assignment: The network can dynamically assign AI tasks or PoW tasks to miners based on current computing needs and network status. For example, when the network transaction volume is low, the proportion of AI tasks can be increased.

4. **Mining Incentive Mechanism**

Dual Incentive System: Design an Incentive Mechanism that not only rewards traditional PoW mining, but also rewards contributions to completing AI tasks. This can be achieved by issuing different types of tokens or adjusting mining rewards.

5. **Algorithm optimization**

- AI -Optimized PoW Mining: Utilize AI techniques to predict and optimize the efficiency of PoW mining, such as predicting data patterns that are more likely to generate valid hash values .
- PoW-supported AI operations: Design a mechanism that allows AI-related floating-point operations to be performed with some computing power while performing PoW mining.

6. **Cyber security and efficiency**

- Security protocols and verification mechanisms: Ensure that the execution of AI tasks will not affect the security of the blockchain network. At the same time, implement efficient verification mechanisms to ensure the accurate and reliable execution of AI tasks.

7. **Hardware and software compatibility**

- Compatibility design: Ensure that new algorithms can run on existing hardware, or develop new hardware to optimize this hybrid computing mode.
- Software Development Kit (SDK): Provides power builders and libraries that enable developers to easily write and deploy AI applications for this new type of blockchain network.

8. **Ecosystem construction**

- Open Platform: Create an open platform that allows developers and miners to jointly participate in the construction and operation of the network, promoting the growth of the ecosystem.

The implementation of this AI -enhanced PoW algorithm (AI-PoW) will be a multi-stage, interdisciplinary project that requires close cooperation between blockchain technology experts, AI researchers, and hardware engineers. Although this design is theoretically feasible, it needs to solve many technical challenges, especially in processing power allocation, cyber security, and algorithm optimization. In addition, such a system may require significant initial investment, including investment in research and development and infrastructure building.

3. The economic model of the new era

DIS Chain's economic model is based on Ethereum (ETH), incorporating new elements of AI computing power output to create an innovative token economy system. This system aims to enhance the value and market demand of DIS tokens through the combination of AI computing power and PoW mechanism.

Core elements of the economic model

1. Token supply and publishing:
    - Inheriting the supply limit and publish mechanism of ETH to ensure the stability and predictability of token supply , the new mainnet supply is still 120 million coins after the merger upgrade, and there is no increase in publish, and the upper limit of publish is 210 million coins.
    - Implementing a deflationary strategy, through a mechanism similar to EIP-1559, part of the transaction fee is used for token burning, thereby reducing the circulating supply.
2. Token redistribution and innovative introduction of staking mining model design.
   In addition to the exchange contract, other tokens that have not been exchanged or airdropped to real users and frozen centralized institutions will be redistributed after the completion of the exchange of new mainnet coins. Informal statistics show that about 50% of the supply is unclaimed. These tokens will be distributed for more than 5 years or even 10 years. For example, assuming 50 million tokens divided by 10 years, that is, 5 million tokens per year divided by 365 days or 13,698.63 tokens per day, and then divided by 24 hours divided by 60 minutes and 60 seconds, that is, 0.1585489599188229 tokens are released per second. These unallocated tokens are stored in the contract address using smart contract technology, and then the reward per second is divided by the percentage of the total amount of collateral at that time. For users, there are more asset management methods, such as POW mining, which can be stored in the collateral contract for collateral mining when not intended to be sold, to maximize profits; or you can choose to directly purchase tokens for collateral mining and obtain collateral rewards; and with this collateral economic model Net inflow keeps the price steadily rising, and if the price continues to rise, it will attract more miners to participate. The purpose of this design is to increase the capacity of the entire network computing power, make cyber security more secure, and provide more choices for the ETHASH POW algorithm market. We look forward to more miners restarting the mission of mining machines.
3. AI computing power fusion mechanism:
    - Introducing AI computing power as part of mining increases the difficulty and value of mining DIS tokens.
    - The computing power output reward motivates participants to invest their computing power in AI applications to obtain additional DIS token rewards.

4. Economic incentives and governance:
    - Design an Economic Incentive Mechanism to reward nodes and developers who contribute to the network.
    - Through the Governance Token mechanism, token holders can participate in network decision-making and increase community participation.
5. Token circulation and application scenarios:
    - Promote the circulation of DIS tokens in diverse application scenarios, including DeFi , NFT , payment, etc.
    - Enhance the liquidity of tokens, improve the accessibility and trading convenience of tokens by cooperating with major exchanges.
6. Sustainable development strategy:
    - Continuously monitor market trends and adjust economic models as needed to adapt to market changes.
    - Explore new application scenarios and business cooperation to further expand the ecosystem of DIS Chain.

DIS Chain's economic model combines AI computing power with PoW mining mechanism, which not only increases the practicality and value of DIS tokens, but also brings new market demand and growth potential. The design of this economic model aims to create a sustainable, dynamically adaptable blockchain ecosystem driven by the community. Through these strategies, DIS Chain will become a unique and powerful blockchain network, providing rich value and opportunities for users and developers.

4. DIS Chain's Positioning in the AI Era

4.1 Overview

In the AI era, the main positioning of DIS Chain is to become a bridge, connecting blockchain technology and AI computing power , committed to creating an innovative, efficient and secure platform. This platform not only supports traditional PoW mining, but also provides necessary computing power support for AI applications, thereby promoting the development of AI technology while maintaining blockchain security.

4.2 The strategic focus of computing power integration

DIS Chain creates a dual-effect network by combining PoW mining algorithm with AI computing power . This fusion not only maintains the security and decentralization of the blockchain network, but also provides power for the training and data processing of AI models. This

strategy is in line with the trend of future technological development, aiming to use the security and transparency of blockchain technology to bring innovation to the field of AI.

4.3 Unique value for AI applications

The uniqueness of DIS Chain lies in its ability to provide a decentralized, secure, and tamper-proof data processing environment for AI applications. AI applications, especially those involving Big data and complex computing, can utilize the efficient computing power provided by DIS Chain for Data Analysis and Model Training, while enjoying the security provided by blockchain.

4.4 Market-leading cooperation opportunities

In the era of AI , DIS Chain is committed to collaborating with leading enterprises and research institutions in the field of AI. Through these collaborations, DIS Chain will continuously optimize its AI-POW algorithm while providing a platform to promote the development of AI research and applications. These collaborations will promote technological progress and make DIS Chain a pioneer in the field of AI and blockchain convergence.

4.5 Promoting Ethics and Safety in AI

DIS Chain adopts strict ethical and security standards for the application of AI . By introducing AI applications into the blockchain network, DIS Chain aims to ensure that the development of AI follows ethical and security guiding principles, such as transparency, user privacy protection, and auditability of algorithms.

4.6 Future Prospects: Central Role in the AI Era

With the continuous advancement of AI technology, the goal of DIS Chain is to become a key participant in the AI era, providing a secure, efficient and innovative platform to promote the integration and common development of AI and blockchain technology . DIS Chain will continue to innovate, provide value for enterprises, researchers and users in the AI era, and promote the development of the entire industry.

DIS Chain's positioning in the AI era is not just a blockchain network, but an innovative platform that combines the security and decentralization of blockchain with the demand for AI computing power , providing impetus for the development of AI. Through this unique positioning, DIS Chain can not only bring new opportunities to the AI field, but also promote the application and development of blockchain technology , thus playing a central role in the AI era.

5. Achieve the vision

5.1 Vision overview

DIS Chain is committed to becoming a pioneer in the AI era, creating a decentralized and efficient ecosystem by integrating advanced blockchain technology and AI computing power . Our vision is to promote technological innovation through this unique integration and provide users, developers, and researchers with a secure, reliable, and promising platform.

5.2 Strategy implementation path

To achieve this vision, DIS Chain will follow the following strategies:

- Technological innovation and continuous upgrades: Continuously optimize and update AI-POW algorithms to ensure compatibility with the latest AI technologies while maintaining network efficiency and security.
- Establish a partner network: Establish strategic partnerships with leading companies and research institutions in the AI and blockchain fields to jointly promote technological development.
- Community Development and Engagement: Actively build and maintain an active community that encourages users, developers, and researchers to participate in the development of the DIS Chain.
- Promotion and Education: Popularize knowledge of blockchain and AI technologies through various channels to increase public understanding and interest in this emerging field.

5.3 Achieve technological breakthroughs

DIS Chain will focus on the following key areas for technological breakthroughs:

- AI Algorithm Integration and Optimization: Continuously optimize AI algorithms to improve efficiency and performance, while ensuring seamless integration with blockchain technology .
- Security and privacy protection: We value the security and privacy of user data and ensure that all AI applications adhere to strict security and privacy standards.
- Sustainability and environmental awareness: While developing AI and blockchain technology , focus on environmental protection and sustainable development to ensure that technological progress does not come at the expense of the environment.

5.4 Market expansion and ecological construction

DIS Chain will expand the market and build the ecosystem through the following ways:

- Diversified Application Development: Encourage and support the development of diverse applications on the DIS Chain platform, including DeFi , NFT , smart contracts , etc., to meet the needs of different users.

- Globalization strategy: Through global marketing and promotion strategies, attract more international users and developers to participate in the DIS Chain ecosystem.
- Ecological Incentive Mechanism: Set up a reasonable Incentive Mechanism to encourage the active participation and contribution of community members.

5.5 Continuous innovation and adaptation to change

Facing the rapidly changing technological environment, DIS Chain will remain agile and flexible, constantly adapting to new market and technological changes. We will ensure that DIS Chain remains at the forefront of the industry through continuous innovation and learning.

The road to realizing the vision may be full of challenges, but DIS Chain is ready to meet these challenges. By adhering to technological innovation, deepening cooperation, actively participating in community and market expansion, we believe that DIS Chain will play a key role in the era of AI and contribute to the integration and development of blockchain and AI.

6. Communities and partners

The development of DIS Chain inspires a diverse team from around the world, led by a group of Silicon Valley and Chinese technology enthusiasts with deep technical knowledge and blockchain industry experience. They are passionate about maintaining the Proof of Work (PoW) consensus algorithm of Ethereum.

Ethereum Fair (ETHF) is led by a group of Silicon Valley technology geeks, with about 20 main members, most of whom are blockchain engineers, developers with many years of senior programming operations and multiple public chain project technical experience, ETHF DAO is a group of supporters who support the spirit of decentralization and adhere to POW, TWITTER 60,000 attention and TELEGRAMDIS more than 50,000 people; DIS is a project initiated by the Chinese community in Taiwan, through continuous recruitment of like-minded people, join DIS DAO for common development, before the merger and upgrading, DAO members reached more than 40 people, members are mining circle or currency circle related people, some are mining community or Cryptocurrency community KOL, with many years of blockchain experience Media We or community administrators, including some influential public figures 100,000 and more than 200,000 traffic, long-term active in the blockchain community to share and initiate voice or LIVE activities, including chip mining machine manufacturers, mining pool operators, AI design, automation programming, most of the other members are miners and full-time in the WEB3 field, DIS official Twitter followers 68,000 people and thousands to 10,000 supporters of TELEGRAM or FACEBOOK, 25,000 holders and nearly 200,000 interactions recorded in 6 months in the DIS block explorer; this merger is not only a merger of resources and manpower, but also symbolizes the combination of technology and community.

Our team covers all levels from blockchain experts to influencers (KOLs), distributed in multiple Chinese regions such as Silicon Valley, Taiwan, Hong Kong, Thailand, Vietnam, MY, etc., forming a strong cross-regional and cross-cultural community network. They jointly operate a vast social network. These communities are spread across multiple social platforms such as Twitter, Telegram, Discord, YouTube, Facebook, and Line, actively promoting the growth and spread of DIS Chain.
Our core development team has rich industry experience, including sponsors and developers participating in the Dogecoin community, some participating in the Ethereum fork and Dogecoin fork projects, experts in converting Scrypt algorithm to ETHASH algorithm, and pioneers in the development of DRC20 inscriptions and AI technology. The advisory team consists of a group of senior industry experts, barristers, and financial economists, whose guidance and advice are crucial to the Strategy and Development of DIS Chain. These advisors not only provide industry insights, but also bring valuable resources and networks to DIS Chain, which are key to quickly adapting to market changes, continuous innovation, and development.
As the DIS Chain ecosystem continues to mature and expand, our team and advisors will continue to attract more talents and expertise to ensure that we maintain our leading position in the fiercely competitive blockchain field. Their diverse backgrounds, professional skills, common belief in the blockchain revolution, and firm commitment to the future development of DIS Chain are the powerful driving force for DIS Chain to continue to move forward.

The construction of the DIS Chain ecosystem involves the active collaboration of multiple heavyweight partners. These partners span multiple blockchain fields from infrastructure to application layer, jointly constructing a rich and interconnected digital world.

In terms of wallet services, we cooperate with various multi-chain wallets such as Metamask, BitKeep, TokenPocket, OneKey, OKX, and Coolwallet cold wallets to provide users with secure and convenient asset storage and management solutions. At the same time, we also cooperate with innovative payment service providers such as SWFT and MPC to provide users with convenient cross-chain exchange and encrypted asset payment. In the field of data platforms, we cooperate with Data Analysis service providers such as Ave and OKLink to enable users to obtain real-time market dynamics and in-depth blockchain data insights. These data services not only support market research and decision-making, but also provide powerful data support for developers. In terms of trading platforms, DIS Chain will list leading centralized exchanges (CEX) such as Huobi, Gate, MEXC, Bitget, LBank, CoinW, Poloniex, Bitmart, and DEX will develop Diswap with SWFT and Oriswap. This partnership provides rich trading pairs and liquidity choices.

In order to expand the depth and breadth of the NFT market, we work closely with NFT trading markets such as Musse to support artists and collectors in creating, buying, selling, and exchanging non-fungible tokens (NFTs) on our platform.

In the field of community, DIS Chain recognizes the power of social media and promotes the innovative application of blockchain technology in the field of community through cooperation

with social media platforms such as Linkenetwork and DeNet.

In addition, we cooperate with multiple mining pools, such as TW-pool, coolpool, jingniupool, gteh, ezil, ua mining, crazypool, etc., to provide stable mining services and income for miners. In terms of market statistics services, we cooperate with industry benchmark platforms such as CoinMarketCap, CoinGecko, and AVI to provide real-time market ranking and token price information.

With the further development of the ecosystem, DIS Chain will continue to seek and integrate more partners to enrich our service scope, improve user experience, and meet the needs of efficiency and security. Through the joint efforts of partners, more projects will be attracted to join. We believe that DIS Chain will become a stronger and mutually beneficial ecosystem, jointly promoting the development of blockchain technology to achieve a digital future.

7. Summary

As the chapter of the DIS Chain white paper draws to a close, we review a journey that is both ambitious and innovative. DIS Chain's new POW public chain concept that integrates MEME & AI computing power represents not only a technological breakthrough, but also a profound insight into the future of blockchain.

1. Pioneer of the technological revolution

DIS Chain, on the basis of inheriting the POW core features of the Ethereum fork, bravely integrates AI computing power, thus creating a new era of blockchain model. In addition to the dual mining model of POW mining and pledge mining, this innovation not only improves the efficiency and functionality of the system, but also opens up a new path for the future development of blockchain technology.

2. Evolution of economic models

DIS Chain has proven that technological innovation can bring substantial economic value through its unique economic model. The new POW public chain that integrates AI computing power not only increases the value and demand of DIS tokens, but also creates new opportunities for users and investors.

3. Community and ecological prosperity

DIS Chain always adheres to the principles of community-driven and ecological construction. By encouraging innovation, embracing diversity, and promoting cooperation, With the support of many technical developers in the DIS Chain team, more project parties are attracted to develop in the public chain ecosystem. DIS Chain is building a strong, active, and highly participatory community Community users can freely publish projects to realize their dreams on DIS Chain. We hope that DIS can interact with various blockchain projects and applications, providing users with more choices and possibilities. We hope that DIS can make greater contributions to society,

not only through charity activities or gift-giving and tipping functions, but also through technological innovation and community development.

4. Vision of the future

DIS Chain's vision is to become an important promoter of the new era, and to become a benchmark for the integration of blockchain and MEME & AI through continuous technological innovation and market expansion. We are confident in this goal and look forward to working with the global community to achieve this magnificent blueprint.

Conclusion

The journey of DIS Chain has just begun. We will continue to devote ourselves to technological innovation while actively responding to the needs of the market and community. Let us work together to create a more open, fair, and vibrant blockchain world. The future of DIS Chain is full of infinite possibilities. Let's work together and cheer together to make Ethereum POW and miners great again .

Explanation citing the original technology of Ethereum

Ethereum

The purpose of Ethereum is to integrate and improve the concepts of scripts, altcoins, and on-chain meta-protocols, enabling developers to create arbitrary consensus-based, scalable, standardized, feature-complete, easy-to-develop, and collaborative applications. Ethereum enables anyone to create contracts and decentralized applications and set their freely defined ownership rules, transaction methods, and state transition functions by establishing the ultimate abstraction base layer - blockchain with Turing-complete programming language built-in. The main framework of domain name coins can be implemented with only two lines of code, while other protocols such as currency and reputation systems can be implemented with less than twenty lines of code. Smart contracts - encrypted boxes that contain value and can only be opened if certain conditions are met - can also be created on our platform, and are much more powerful than smart contracts provided by a Bitcoin script due to the added power of Turing completeness, value-awareness, blockchain blockchain-awareness, and multi-state.

Ethereum account

In the Ethereum system, state is composed of objects called "accounts" (each account consists of a 20-byte address) and state transitions that transfer value and information between two accounts. Ethereum accounts consist of four parts.

- Random number, a counter used to determine that each transaction can only be processed once

- The current Ether balance of the account
- The contract code of the account, if any
- Account storage (empty by default)

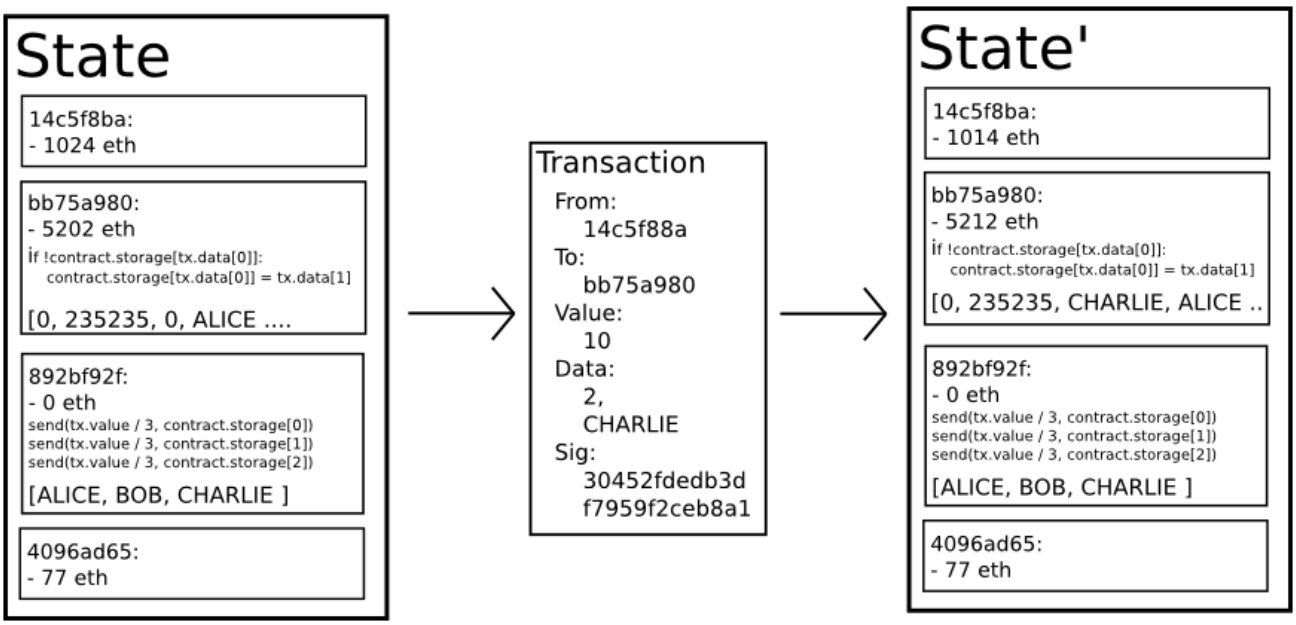
Ether is the main encryption fuel inside Ethereum, used to pay transaction fees. Generally speaking, Ethereum has two types of accounts: externally owned accounts (controlled by private keys) and contract accounts (controlled by contract code). Externally owned accounts have no code, and people can send messages from an external account by creating and signing a transaction. Whenever a contract account receives a message, the code inside the contract is activated, allowing it to read and write to internal storage, send other messages, or create contracts.

Messages and transactions

Ethereum messages are similar to Bitcoin transactions to some extent, but there are three important differences between the two. Firstly, Ethereum messages can be created by external entities or contracts, while Bitcoin transactions can only be created externally. Secondly, Ethereum messages can choose to include data. Thirdly, if the recipient of Ethereum messages is a contract account, they can choose to respond, which means that Ethereum messages also include the concept of functions.
In Ethereum, "transaction" refers to the signed data packet that stores messages sent from external accounts. The transaction includes the recipient of the message, the signature used to confirm the sender, the Ether account balance, the data to be sent, and two numerical values called STARTGAS and GASPRICE. In order to prevent the exponential explosion of code and infinite loop, each transaction needs to impose restrictions on the calculation steps triggered by the executable code, including the initial message and all messages triggered during execution. STARTGAS is the restriction, and GASPRICE is the fee that miners need to pay for each calculation step. If "gas is used up" during the execution of the transaction, all state changes will be restored to the original state, but the transaction fees paid cannot be recovered. If there is still gas left when the execution of the transaction is suspended, the gas will be returned to the sender. There is a separate transaction type and corresponding message type for creating contracts; the address of the contract is calculated based on the account random number and the hash of the transaction data.
One important consequence of the messaging mechanism is the "first-class citizen" property of Ethereum - contracts have the same rights as external accounts, including the right to send messages and create other contracts. This allows contracts to play multiple different roles at the same time. For example, users can make a member of a decentralized organization (one contract) become an intermediary account (another contract), providing intermediary services for a paranoid individual using a customized quantum proof-based Lambert signature (the third contract) and a co-signing entity using an account secured by five private keys (the fourth

contract). The power of the Ethereum platform lies in the fact that decentralized organizations and proxy contracts do not need to care about what type of account each party to the contract is.

Ethereum state transition function



Ethereum's state transition function: `APPLY (S, TX) -> S '` , can be defined as follows:

1. Check if the transaction format is correct (i.e. has the correct value), if the signature is valid, and if the random number matches the random number in the sender's account. If not, return an error.
2. Calculate the transaction fee: `fee = STARTGAS * GASPRICE` , and determine the sender's address from the signature. Subtract the transaction fee from the sender's account and increase the sender's random number. If the account balance is insufficient, an error is returned.
3. Set the initial value `GAS = STARTGAS` , and subtract a certain amount of gas value according to the number of bytes in the transaction.
4. Transfer value from the sender's account to the receiver's account. If the receiving account does not yet exist, create this account. If the receiving account is a contract, run the contract's code until the code runs out or the gas runs out.
5. If the value transfer fails because the sender's account does not have enough money or the code runs out of gas, the original state will be restored, but transaction fees will still need to be paid, and the transaction fees will be added to the miner's account.

6. Otherwise, return all remaining gas to the sender and send the consumed gas as transaction fees to the miner. For example, suppose the code of the contract is as follows:

```
if not self.storage[calldataload(0)]:
    self.storage[calldataload(0)] = calldataload(32)
```

It should be noted that in reality, the contract code is written using the underlying Ethereum Virtual Machine (EVM) code. The above contract is written in our high-level language Serpent language, which can be compiled into EVM code. Assuming the contract memory is empty at the beginning, with a value of 10 ETH, a gas value of 2000 ETH, a gas price of 0.001 ETH, and 64 bytes of data, the first 32-byte block represents number 2 and the second representative word `CHARLIE` . After the transaction is sent, the processing process of the state transition function is as follows:

1. Check if the transaction is valid and the format is correct.
2. Check that the sender of the transaction has at least 2000 * 0.001 = 2 Ether. If so, deduct 2 Ether from the sender's account.
3. The initial setting is gas = 2000. Assuming the transaction length is 170 bytes, the cost per byte is 5, minus 850, so there is still 1150 left.
4. Subtract 10 Ether from the sender's account and add 10 Ether to the contract account.
5. Run the code. In this contract, running the code is simple: it checks if the contract storage index is used at 2, notices that it is not used, and then sets its value to CHARLIE. Assuming this consumes 187 units of gas, the remaining gas is 1150-187 = 963.
6. Add 963 * 0.001 = 0.963 Ether to the sender's account and return to the final state.

If there is no contract to receive the transaction, then all transaction fees are equal to GASPRICE multiplied by the byte length of the transaction, and the data of the transaction is independent of the transaction fees. In addition, it should be noted that the messages initiated by the contract can allocate gas limits to the calculations they generate. If the gas of the sub-calculation is used up, it will only return to the state when the message was sent. Therefore, just like transactions, contracts can also set strict limits on the sub-calculations they generate to protect their computing resources.

Code execution

The code of an Ethereum contract is written in a low-level stack-based bytecode language, called "Ethereum Virtual Machine Code" or "EVM Code". The code consists of a series of bytes, each representing an operation. Generally speaking, code execution is an infinite loop. The program counter is incremented by one (with an initial value of zero) and an operation is performed until the code is executed or an error is encountered. `STOP` or `RETURN` instruction. The operation can access three types of data storage spaces:

- **Stack** , a last-in, first-out data storage, 32-byte values can be pushed onto and off the stack.

- **Memory** , infinitely expandable byte queue.
- **The long-term storage of the contract** , a CDKEY/value storage, where CDKEY and the value are both 32 bytes in size, and the stack and memory that are reset after the calculation are different, the storage content will be kept for a long time.

The code can access values like accessing block header data, data in the sender and received messages, and the code can also return a byte queue of data as output.

The formal execution model of EVM code is surprisingly simple. When the Ethereum virtual machine runs, its complete calculation state can be defined by tuples `(block_state, transaction, message, code, memory, stack, pc, gas)` , where `block_state` is the global state containing all account balances and storage. During each round of execution, the current instruction is found by calling up the `pc` (program counter) byte of the code, and each instruction defines how it affects the tuple. For example, `ADD` takes two elements off the stack and adds their sum to the stack, subtracts `gas` by one and adds `pc` by one, `SSTORE` takes the top two elements off the stack and inserts the second element into the contract storage location defined by the first element, also reduces the gas value by up to 200 and adds `pc` by one. Although there are many ways to optimize Ethereum through instant compile, the basic implementation of Ethereum can be achieved in a few hundred lines of code.

Blockchain and mining

Although there are some differences, Ethereum's blockchain is similar to Bitcoin's blockchain in many ways. The difference in their blockchain architecture is that Ethereum blocks not only contain transaction records and recent states, but also block numbers and difficulty values. The block confirmation algorithm in Ethereum is as follows:

1. Check if the previous block referenced by the block exists and is valid.
2. Check if the timestamp of the block is larger than the previous block referenced and less than 15 minutes.
3. Check if the block number, difficulty value, transaction root, uncle root, and gas limit (many Ethereum-specific underlying concepts) are valid.
4. Check if the proof of work for the block is valid.
5. Assign `S [0]` to the `STATE_ROOT` of the previous block.
6. Assign `TX` to the transaction list of blocks, with a total of `n` transactions. For `i` belonging to `0... n-1` , perform a state transition `S [i + 1] = APPLY (S [i], TX [i])` . If any of the conversions fails, or the gas spent by the program to execute here exceeds `GASLIMIT` , an error is returned.
7. Assign `S [n]` to the `S_FINAL` and pay the miner a block reward.

8. Check if the `S_FINAL` is the same as the `STATE_ROOT` . If they are, the block is valid. Otherwise, the block is invalid.

This confirmation method may seem inefficient at first glance, as it requires storing all the state of each block, but in fact, Ethereum's confirmation efficiency can be compared to Bitcoin. The reason is that the state is stored in a tree structure, and only a small part of the tree structure needs to be changed for each additional block. Therefore, generally speaking, most of the tree structure of two adjacent blocks should be the same, so storing data once can be referenced twice using pointers (i.e. subtree hashes). A tree structure called "Patricia Tree" can achieve this, which includes modifications to the Merkel tree concept, allowing not only changing nodes, but also inserting and deleting nodes. In addition, because all state information is part of the last block, there is no need to store the entire block history - if this method can be applied to the Bitcoin system, it can save 10-20 times the storage space.

Application

Generally speaking, there are three types of applications on top of Ethereum. The first type is financial applications, which provide users with more powerful ways to manage and participate in contracts with their money. This includes sub-currencies, financial derivatives, hedging contracts, savings wallets, wills, and even some types of comprehensive employment contracts. The second type is semi-financial applications, where money exists but there are also heavy non-monetary aspects. A perfect example is self-imposed rewards designed to solve computational problems. Finally, there are completely non-financial applications such as online voting and decentralized governance.

Token system

The on-chain token system has many applications, from sub-currencies representing assets such as US dollars or gold to company stocks, individual tokens representing smart assets, secure and unforgeable coupons, and even token systems used for point rewards that are completely unrelated to traditional values. Implementing a token system in Ethereum is surprisingly easy. The key point is to understand that all currencies or token systems are fundamentally databases with the following operations: subtract X units from A and add X units to B, provided that (1) A has at least X units before the transaction and (2) the transaction is approved by A. Implementing a token system is to implement such logic into a contract.
The basic code for implementing a token system in Serpent language is as follows:
Def send (to, value):
If self.storage [from] > = value:
self.storage [from] = self.storage [from] - valueself.storage [to] = self.storage [to] + value
This is essentially a minimal implementation of the "banking system" state transition function that will be further described in this article. Some additional code needs to be added to provide the function of distributing currency in initial and other edge cases. Ideally, a function will be

added to allow other contracts to query the balance of an address. Sufficient. In theory, an Ethereum-based token system that acts as a sub-currency may include an important feature that a Bitcoin-based on-chain token lacks: the ability to directly pay transaction fees with this currency. The method of achieving this capability is to maintain an Ether account in the contract to pay transaction fees for the sender. By collecting internal currency used as transaction fees and auctioning them off in a constantly running auction, the contract continuously funds the Ether account. This way, users need to "activate" their account with Ether, but once there is Ether in the account, it will be reused because each contract will recharge it.

Financial derivatives and stable currencies

Financial derivatives are the most common application of "smart contracts" and one of the easiest to implement with code. The main challenge in implementing financial contracts is that most of them need to refer to an external price publisher; for example, a very demanding application is a smart contract used to hedging the price fluctuations of Ether (or other cryptocurrencies) relative to the US dollar, but the contract needs to know the price of Ether relative to the US dollar. The simplest method is to use a "data provision" contract maintained by a specific institution (such as NASDAQ), which is designed to allow the institution to update the contract as needed and provide an interface for other contracts to obtain replies containing price information by sending a message to the contract.
When these key elements are in place, the hedging contract will look like the following:

1. Wait for A to enter 1000 Ether..
2. Wait for B to enter 1000 Ether.
3. By querying data to provide a contract, the dollar value of 1000 Ether, such as x dollars, is recorded in storage.
4. After 30 days, A or B is allowed to "reactivate" the contract to send x dollars worth of ether (re-query the data provider contract to obtain the new price and calculate) to A and send the remaining ether to B.

Such contracts have extraordinary potential in cryptographic commerce. One problem that cryptocurrency is often criticized for is its price volatility; although a large number of users and merchants may need the security and convenience brought by cryptographic assets, they are unlikely to be willing to face a situation where the asset loses 23% of its value in a day. Until now, the most common recommended solution is for publishers to endorse assets; the idea is that publishers create a seed currency, and they have the right to publish and redeem this seed currency, giving (offline) people who provide them with a specific unit of related assets (such as gold, US dollars) a unit of sub-currency. The publisher promises to return a unit of related assets when anyone returns a unit of cryptographic assets. This mechanism can allow any non-cryptographic asset to be "upgraded" to a cryptographic asset if the publisher is trustworthy.

However, in practice, publishers are not always trustworthy, and in some cases, the banking system is too fragile or not honest enough to make such services impossible. Financial derivatives provide an alternative. There will no longer be a separate publisher providing reserves to support an asset, but a decentralized market composed of speculators betting that the price of a cryptographic asset will rise. Unlike publishers, speculators have no bargaining rights because hedging contracts freeze their reserves in contracts. Note that this method is not completely decentralized, as a trusted data source providing price information is still needed, although it is still controversial. This is still a huge progress in reducing infrastructure requirements (unlike publishers, a price publisher does not require a license and seems to be classified as free speech) and reducing potential fraud risks.

Identity and reputation systems

The earliest alternative currency, Domain Name Coin, attempted to use a Bitcoin-like blockchain to provide a name registration system, where users could register their names and other data in a public database. The most common use case is the Domain Name System corresponding to an IP Address with a domain name like "bitcoin.org" (or in Domain Name Coin, "bitcoin.bit"). Other use cases include email verification systems and potential more advanced reputation systems. Here is the basic contract for providing a name registration system similar to Domain Name Coin in Ethereum.

```
Def register (name, value):
If! self.storage [name]:
self.storage [name] = value
```

The contract is very simple; it is a database in the Ethereum network that can be added but cannot be modified or removed. Anyone can register a name as a value and never change it. A more complex name registration contract will include "functional terms" that allow other contracts to query, as well as a mechanism for the "owner" of a name (i.e., the first registrant) to modify data or transfer ownership. Reputation and trust network functions can even be added to it.

Decentralized storage

In the past few years, some popular online file storage startups have emerged, the most prominent of which is Dropbox, which seeks to allow users to upload their hard drive backups, provide backup storage services, and allow users to access them for a monthly fee. However, at this point, the file storage market is sometimes relatively inefficient; a rough look at existing services shows that, especially at the level of "Mystic Valley" 20-200GB, which has neither free space nor enterprise-level user discounts, the mainstream file storage cost per month means paying the cost of the entire hard drive in a month. Ethereum contracts allow for the development of decentralized storage ecosystems, so that users rent out their own hard drives or unused network space for a small profit, thereby reducing the cost of file storage.

The basic building block of such a facility is what we call a "decentralized Dropbox contract". The working principle of this contract is as follows. First, someone divides the data that needs to be uploaded into blocks, encrypts each piece of data to protect privacy, and constructs a Merkel tree based on this. Then create a contract with the following rules. For every N blocks, the contract will extract a random index from the Merkel tree (using the hash of the previous block that can be accessed by the contract code to provide randomness), and then give the first entity X ether to support a proof of ownership of a block at a specific index in the tree with a simplified verification payment (SPV). When a user wants to redownload his file, he can use a micropayment channel protocol (such as paying 1 Saab per 32k bytes) to restore the file; the most cost-effective method is for the payer not to publish the transaction at the end, but to replace the original transaction with a slightly more cost-effective transaction with the same random number after every 32k bytes.
An important feature of this agreement is that although it looks like a person trusting many random nodes that are not prepared to lose files, he can divide the files into many small pieces through secret sharing, and then monitor the contract to know that each small piece is still being saved by a certain node. If a contract is still making payments, it provides evidence that someone is still saving files.

Decentralized Autonomous Organization

Generally speaking, the concept of "Decentralized Autonomous Organization (DAO) " refers to a virtual entity with a certain number of members or shareowners, relying on, for example, a 67% majority to decide how to spend money and modify code. Members will collectively decide how the organization distributes funds. The method of distributing funds may be rewards, salaries, or more attractive mechanisms such as rewarding work with internal currency. This fundamentally replicates the legal meaning of traditional companies or non-profit organizations using cryptographic blockchain technology to achieve enforcement. So far, many discussions around DAO have revolved around the "capitalist" model of a "decentralized autonomous corporation (DAC) " with shareowners who accept dividends and tradable stocks; as an alternative, an entity described as a "decentralized autonomous community" will give all members equal rights in decision-making and require 67% majority approval when adding or subtracting members. Each person can only have one membership, which needs to be enforced by the group.
Here is an outline of how to implement DO with code. The simplest design is a piece of code that can be self-modified if two-thirds of the members agree. Although the code is theoretically immutable, by placing the code backbone in a separate contract and pointing the address of the contract call to a changeable storage, it is still easy to bypass obstacles and make the code modifiable. In a simple implementation of such a DAO contract, there are three types of transactions, distinguished by the data provided by the transactions.

- `[0, i, K, V]` Proposed changes to storage address indexes K to v with registration index i.
- `[1, i]` Register to vote on Proposal i.
- `[2, i]` confirm proposal i if there are sufficient votes.

Then the contract has specific terms for each item. It will maintain a record of all open storage changes and a table of who voted. There is also a table of all members. When any change to the stored content is approved by a two-thirds majority, a final transaction will execute the change. A more complex framework will add built-in election functions such as sending transactions, adding or subtracting members, and even providing voting representatives such as delegation democracy (that is, anyone can delegate another person to vote on their behalf, and this delegation relationship is transitive, so if A delegates B and then B delegates C, then C will decide A's vote). This design will allow DAO to grow organically as a decentralized community, allowing people to eventually delegate the task of selecting suitable candidates to experts. Unlike the current system, experts will easily appear and disappear over time as community members change their positions. An alternative model is a decentralized company, where any account can have 0 to more stocks, and decisions require a two-thirds majority of stocks. A complete framework will include asset management functions - the ability to submit orders to buy and sell stocks and accept such orders (provided there is an order matching mechanism in the contract). Representatives still exist in a democratic form of appointment, giving rise to the concept of a "board of directors".
More advanced organizational governance mechanisms may be implemented in the future; now a decentralized organization (DO) can be described starting with a Decentralized Autonomous Organization (DAO). The difference between DO and DAO is blurred, and a rough dividing line is whether governance can be achieved through a political process or an "automatic" process. A good intuitive test is the "no common language" standard: if two members do not speak the same language, can the organization still operate normally? Obviously, a simple traditional shareholding company will fail, while something like the Bitcoin protocol is likely to succeed. Robin Hansen's "futarchy", a mechanism that achieves organized governance through predictive markets, is a good example of what "autonomous" governance may look like. Note that one does not need to assume that all DAOs are superior to all DOs; autonomy is just a paradigm that has great advantages in some specific scenarios, but may not be feasible elsewhere, and many semi-DAOs may exist.

Further applications

1. **Savings Wallet** . Suppose Alice wants to keep her funds safe, but she is worried about losing or having her private keys stolen by hackers. She puts Ether into a contract signed with Bob, as shown below. This contract is a bank:

- Alice can withdraw up to 1% of the funds per day alone.

- Bob alone can withdraw up to 1% of the funds per day, but Alice can create a transaction with her private key to cancel Bob's withdrawal permission.
- Alice and Bob can withdraw funds at will. Generally speaking, 1% per day is enough for Alice. If Alice wants to withdraw more, she can contact Bob for help. If Alice's private key is stolen, she can immediately find Bob to transfer her funds to a new contract. If she loses her private key, Bob can slowly withdraw the money. If Bob shows malice, she can turn off his withdrawal permission.

1. **Crop insurance** . One can easily create a financial derivative contract based on weather conditions rather than any price index as data input. If an Iowa farmer buys a financial derivative that pays out in reverse based on Iowa's rainfall, the farmer will automatically receive the payout if there is a drought and will be happy if there is enough rain because his crop will be good.
2. **A decentralized data publisher** . For financial contracts based on differences, it is actually possible to decentralize the data publisher through the "Schelling point" protocol. The working principle of the Schelling point is as follows: N parties provide input values to the system for a specified data (such as ETH/USD price), all values are sorted, and each node that provides values between 25% and 75% will receive rewards. Everyone has an incentive to provide answers that others will provide. The answer that a large number of players can truly agree on is obviously the correct answer by default. This constructs a decentralized protocol that can theoretically provide many values, including ETH/USD price, Berlin temperature, and even the result of a particularly difficult calculation.

5. **Cloud Service** . EVM technology can also be used to create a verifiable computing environment, allowing users to invite others to perform calculations and optionally request evidence that the calculations were done correctly at certain randomly selected checkpoints. This makes it possible to create a Cloud Service marketplace where any user can participate with their desktop, laptop, or dedicated server, and on-site inspections and security guarantees can be used to ensure that the system is trustworthy (i.e., no node can profit from fraud). Although such a system may not be suitable for all tasks; for example, tasks that require advanced Inter-Process Communication are not easily completed on a large node cloud. However, some other tasks are easily parallelized; projects such as SETI@home, folding@home, and genetic algorithms are easily carried out on such platforms.

6. **Peer-to-peer gambling** . Any number of peer-to-peer gambling protocols can be moved to the Ethereum blockchain, such as Cyberdice by Frank Stajano and Richard Clayton. The simplest gambling protocol is actually a simple contract that is used to bet on the difference between the hash value and the guessed value of the next block. Based on this, more complex gambling protocols can be created to achieve almost zero fees and no fraud gambling services.

7. **Prediction Market** . Whether there is an oracle or Sherin, prediction markets will be easy to implement. Prediction markets with Sherin may prove to be the first mainstream "futarchy"

application as a decentralized organization management protocol.

8. On-chain decentralized markets, based on identity and reputation systems.

Miscellaneous and attention

Implementation of Improved Ghost Protocol

The "Greedy Heaviest Observed Subtree" (GHOST) protocol is an innovation introduced by Yonatan Sompolinsky and Aviv Zohar in December 2013. The motivation behind the proposed GHOST protocol is that the current fast-confirming blockchain is troubled by low security due to the high invalidation rate of blocks; because blocks take a certain amount of time (set to t) to spread to the entire network, if miner A mines a block and miner B happens to mine another block before A's block spreads to B, miner B's block will be invalidated and will not contribute to cyber security. In addition, there is a centralization issue here: if A is a mining pool with 30% of the network's computing power and B has 10% of the computing power, A will face the risk of producing invalidated blocks 70% of the time and B producing invalidated blocks 90% of the time. Therefore, if the invalidation rate is high, A will simply be more efficient because of the higher computing power share. Taking these two factors together, a blockchain with fast block generation speed is likely to lead to a mining pool having a computing power share that can actually control the mining

As described by Sompolinsky and Zohar, the ghost protocol solves the first problem of reducing cyber security by including obsolete blocks when calculating which chain is "longest"; that is, not only the parent block and earlier ancestor blocks of a block, but also the obsolete descendant blocks of the ancestor block (referred to as "uncle blocks" in Ethereum terminology) are added to calculate which block has the maximum proof of work supporting it. We go beyond the protocol described by Sompolinsky and Zohar to solve the second problem - centralization tendency. Ethereum pays 87.5% of the reward to obsolete blocks that contribute to the confirmation of new blocks as "uncle blocks", and the "nephew block" that includes them in the calculation will receive 12.5% of the reward. However, transaction fees are not rewarded to uncle blocks. Ethereum implements a simplified version of the ghost protocol that only descends to the fifth layer. Its characteristic is that obsolete blocks can only be included in the calculation as uncle blocks by the second to fifth generation descendants of their parents, rather than more distant descendants blocks (such as the sixth generation desc Firstly, the unconditional ghost protocol will bring too much complexity to calculating which uncle block of a given block is legitimate. Secondly, the unconditional ghost protocol with compensation used by Ethereum deprives miners of the incentive to mine on the main chain rather than a public attacker's chain. Finally, calculations show that the five-layer ghost protocol with incentives achieves over 95% efficiency even when the block production time is 15 seconds, while miners with 25% computing power benefit less than 3% from centralization.

Cost

Because each transaction published to the blockchain occupies the cost of downloading and verification, there needs to be a standardized mechanism including transaction fees to prevent spam. The default method used by Bitcoin is a purely voluntary transaction fee, relying on miners to act as gatekeepers and set dynamic minimum fees. Because this method is "market-based", it allows miners and transaction senders to determine prices based on supply and demand, so this method has been smoothly accepted in the Bitcoin community. However, the problem with this logic is that transaction processing is not a market; although it is attractive to interpret transaction processing as a service provided by miners to senders based on intuition, in fact, the transactions collected by a miner need to be processed by every node in the network, so the largest part of the cost of transaction processing is borne by third parties rather than miners who decide whether to include transactions. Therefore, it is very likely that a tragedy of the commons will occur.
However, when a special and imprecise simplification assumption is given, the loophole in this market-based mechanism magically eliminates its own impact. The argument is as follows.
Assumption:

1. A transaction brings k steps of operation, providing a reward kR to any miner who includes the transaction. Here, R is set by the transaction publisher, and both k and R are visible to miners in advance (roughly).
2. The cost of each node processing each step is C (i.e., the efficiency of all nodes is consistent).
3. There are N mining nodes, each with the same computing power (i.e. 1/N of the total network computing power).
4. There is no full node that does not mine.

When the expected reward is greater than the cost, miners are willing to mine. In this way, because miners have a 1/N chance to process the next block, the expected return is kR/N, and the miner's processing cost is simply kC. In this way, when kR/N > kC, that is, R > NC, miners are willing to include transactions. Note that R is the fee per step provided by the transaction sender, which is the lower limit for miners to benefit from processing transactions. NC is the cost of processing an operation on the entire network. Therefore, miners only have the motivation to include transactions that have benefits greater than costs. However, there are several important deviations between these assumptions and the actual situation.

1. Because the additional validation Time Lag increases the chance of the block becoming a scrap block, miners who process transactions pay higher costs than other validation nodes.
2. Full nodes that do not mine do exist.
3. In practice, the distribution of computing power may end up being extremely uneven.

4. Speculators, political enemies, and lunatics who take it upon themselves to destroy the network do exist, and they can cleverly set up contracts that make their costs much lower than other verification nodes. Point 1 above drives miners to include fewer transactions, while point 2 increases NC; thus, the effects of these two points at least partially offset each other. Points 3 and 4 are the main problems; as a solution, we simply establish a floating upper limit: no block can contain more operations than BLK_LIMIT_FACTOR times the long-term exponential moving average. Specifically:

```
blk.oplimit = floor((blk.parent.oplimit * (EMAFACTOR - 1) + floor(parent.opcount * BLK_LIMIT_FACTOR)) /EMA_FACTOR)
```

BLK_LIMIT_FACTOR and EMA_FACTOR are constants temporarily set to 65536 and 1.5, but may be adjusted after more in-depth analysis. Reply

Computation and Turing completeness

It should be emphasized that the Ethereum virtual machine is Turing complete; this means that EVM code can perform any imaginable computation, including infinite loops. There are two ways in which EVM code implements loops. Firstly, JUMP instructions can make the program jump back to somewhere in front of the code, and there are also JUMPI instructions that allow conditional statements such as `while x < 27: x = x * 2` The same conditional statement implements conditional jumps. Secondly, contracts can call other contracts, with the potential to achieve loops through recursion. This naturally leads to a question: can malicious users force miners and full nodes into an infinite loop and have to shut down? This problem arises from a problem in computer science called the shutdown problem: in general, there is no way to know whether a given program can end running in a limited time.

As described in the state transition section, our scheme solves the problem by setting the maximum number of calculation steps for each transaction to run, and if it exceeds, the calculation is restored to its original state but still requires payment. Messages work in the same way. To show the motivation behind this scheme, consider the following example:

- An attacker created a contract that runs an infinite loop and then sent a transaction that activates the loop to the miner. The miner will process the transaction and run the infinite loop until the gas runs out. Even if the gas runs out and the transaction stops halfway, the transaction is still correct (back to its original location) and the miner still earns a fee for each step of calculation from the attacker.
- An attacker creates a very long infinite loop intending to force miners to calculate for a long time, causing several blocks to be generated before the calculation ends, so miners cannot record transactions to earn fees. However, the attacker needs to publish a STARTGAS value to limit the number of executable steps, so miners will know in advance that the calculation will take too many steps.

- An attacker sees a contract containing a format such as send (A, self.storage); self.storage = 0 and then sends a transaction with a fee that is only enough to execute the first step and not enough to execute the second step (i.e. withdraw without reducing the account balance). The contract author does not need to worry about defending against similar attacks, because if execution stops midway, all changes are reverted.
- A financial contract works by extracting the median of nine dedicated data publishers to minimize risk. An attacker takes over one of the data providers and then designs the variable address call mechanism described in the DAO chapter as a changeable data provider to run an infinite loop in an attempt to force any attempt to claim funds from this financial contract to be aborted due to gas depletion. However, the financial contract can set gas limits in the message to prevent such problems. An alternative to Turing completeness is Turing incompleteness, where JUMP and JUMPI instructions do not exist and only one copy of each contract is allowed to exist in the call stack at a given time. In such a system, the above fee system and the uncertainty surrounding the efficiency of our scheme may not be necessary, because the cost of executing a contract will be determined by its size. In addition, Turing incompleteness is not even a big limitation. Of all the contract examples we have envisioned internally, only one requires a loop so far, and even this loop can be replaced by repeating 26 single-line code segments. Given the serious troubles and limited benefits of Turing completeness, why not simply use a Turing incompleteness? In fact, Turing incompleteness is far from a concise solution. Why? Please consider the following contract:

C0: call (C1); call (C1);
C1: call (C2); call (C2);
C2: call (C3); call (C3);
...
C49: call (C50); call (C50);
C50: (Calculate and record the results of a Turing machine step in the long-term storage of the contract)
Now, send such a transaction to A, so that out of 51 transactions, we have a contract that takes 2 ^ 50 steps to calculate. Miners may try to pre-detect such logical bombs by maintaining a maximum executable step for each contract and calculating the possible execution steps of other contracts for recursion calls. However, this will prevent miners from creating contracts for other contracts (because the creation and execution of the above 26 contracts can easily be placed in a single contract). Another problem is that the address field of a message is a variable, so it may not even be possible to know in advance which contract a contract will call. So, in the end, we have an amazing conclusion: Turing-complete management is surprisingly easy, while Turing-incomplete management is surprisingly difficult without the same control - so why not make the protocol Turing-complete?

Currency and publishing

The Ethereum network includes its own built-in currency, Ether. Ether plays a dual role, providing the main liquidity for various digital asset transactions, and more importantly, providing a mechanism for paying transaction fees. To facilitate and avoid future disputes (see the current mBTC/uBTC/Satoshi debate), the names of different face values will be set in advance.

- 1: Wei
- 10 ^ 12: Saab
- 10 ^ 15: Finney
- 10 ^ 18: Ether

This should be seen as an extended version of the concepts of "yuan" and "fen" or "bitcoin" and "cong". In the near future, we expect "ether" to be used for ordinary transactions, "fenny" for microtransactions, and "saab" and "wei" for discussions about fees and protocol implementation.
The publishing model is as follows:

- Through the sale activity, Ether will be sold at a price of 1337-2000 Ether per BTC. A mechanism aimed at raising funds for the Ethereum organization and paying developers has been successfully used on other cryptocurrency platforms. Early buyers will enjoy significant discounts, and the BTC obtained from the sale will be used entirely to pay the salaries and rewards of developers and researchers, as well as to invest in projects in the cryptocurrency ecosystem.
- 0.099X (x is the total amount sold) will be allocated to early contributors who participated in the development before the success of BTC financing or other deterministic financing, and another 0.099x will be allocated to long-term research projects.
- Every year from the launch, 0.26x (x is the total amount sold) will be mined by miners.

Publishing decomposition

The permanent linear growth model reduces the risk of excessive wealth concentration in Bitcoin and gives people living in the present and future a fair opportunity to acquire currency, while maintaining incentives to acquire and hold Ether, as the "money supply growth rate" tends to zero in the long run. We also infer that the loss of coins due to carelessness and death will occur over time. Assuming that the loss of coins is a fixed proportion of the annual money supply, the total circulating money supply will eventually stabilize at a value equal to the annual money publishing volume divided by the loss rate (for example, when the loss rate is 1%, when the supply reaches 30x, 0.3x are mined and 0.3x are lost each year, achieving an equilibrium).

In addition to the linear publishing method, like Bitcoin, the supply growth rate of Ether tends to zero in the long run.

Centralization of mining

The Bitcoin mining algorithm basically allows miners to slightly change the block header millions of times until the hash of the modified version of a node is less than the target value (currently around 2190). However, this mining algorithm is vulnerable to two forms of centralized attacks. The first is that the mining ecosystem is controlled by ASICs (application-specific integrated circuits) and computer chips that are specially designed to be thousands of times more efficient at this particular task of Bitcoin mining. This means that Bitcoin mining is no longer highly decentralized and egalitarian, but requires the effective participation of huge amounts of capital. The second is that most Bitcoin miners no longer perform block verification locally; instead, they rely on centralized mining pools to provide block headers. This problem can be said to be serious: at the time of writing, the two largest mining pools indirectly control about 50% of the computing power of the entire network, although the fact that miners can switch to other mining pools when one pool or consortium attempts a 51% attack mitigates the severity of the problem.

The current goal of Ethereum is to use a mining algorithm based on a function that randomly generates a unique hash for every 1000 random numbers, with a wide enough computing domain to eliminate the advantage of dedicated hardware. This strategy will not reduce the benefits of centralization to zero, but it is not necessary either. Note that each individual user can complete a certain amount of mining activities almost for free using their private laptop or desktop, but when the CPU usage reaches 100%, more mining will require them to pay for electricity and hardware costs. ASIC mining companies need to pay for electricity and hardware costs from the first hash. Therefore, if the centralized benefits can remain below (E + H) /E, even if ASICs are created, ordinary miners will still have room to survive. In addition, we plan to design the mining algorithm so that mining requires access to the entire blockchain, forcing

miners to store completed blockchains or at least verify each transaction. This eliminates the need for centralized mining pools; although mining pools can still play a role in smoothing the randomness of revenue distribution, this function can be performed equally well by P2P mining pools without centralized control. This way, even if most ordinary users still prefer light clients, increasing the number of full nodes in the network can help resist centralization.

Scalability

Scalability is a common concern for Ethereum. Like Bitcoin, Ethereum also suffers from the dilemma of requiring every node in the network to process every transaction. The current blockchain size of Bitcoin is about 20GB, growing at a rate of 1MB per hour. If the Bitcoin network processes Visa-level transactions of 2000tps, it will grow at a rate of 1MB every three seconds (1GB per hour, 8TB per year). Ethereum may also experience a similar or even worse growth pattern because there are many applications on top of the Ethereum blockchain, rather than being just a simple currency like Bitcoin. However, the fact that Ethereum full nodes only need to store state instead of the complete blockchain history has improved the situation.
The problem with large blockchains is centralization risk. If the size of the blockchain increases to, say, 100TB, the possible scenario will be that only a very small number of large merchants will run full nodes, while regular users will use light SPV nodes. This will increase concerns about the risk of full-node partnership fraud (such as changing block rewards and giving themselves BTC). Light nodes will not be able to detect this fraud immediately. Of course, there may be at least one honest full node, and information about the fraud will be leaked through channels like Reddit a few hours later, but it is already too late: no matter how hard ordinary users try to abolish the blocks that have already been generated, they will encounter a huge unfeasible coordination problem of the same scale as launching a successful 51% attack. In Bitcoin, this is now a problem, but a change suggested by Peter Todd can alleviate this problem.
Recently, Ethereum will use two additional strategies to deal with this problem. Firstly, due to the blockchain-based mining algorithm, at least each miner will be forced to become a full node, which ensures a certain number of full nodes. Secondly, and more importantly, after processing each transaction, we will include the root of an intermediate state tree in the blockchain. Even if block verification is centralized, as long as there is an honest verification node, the centralization problem can be avoided through a verification protocol. If a miner publishes an incorrect block, the block is either malformed or the state S [n] is incorrect. Because S [0] is correct, there must be a first error state S [i], but S [i-1] is correct. The verification node will provide index i, along with a subset of Patricia tree nodes required to process APPLY (S [i-1], TX [i]) - > S [i]. These nodes will be instructed to perform this part of the calculation to see if the generated S [i] is consistent with the previously provided value.
In addition, the more complex issue is that malicious miners release incomplete blocks for attack, resulting in insufficient information to determine whether the block is correct. The solution is the challenge-response protocol: the verifying node questions the target transaction

index, and the light node that receives the challenge information will untrust the corresponding block until another miner or verifier provides a subset of Patricia nodes as correct evidence.

Overview: Decentralized Applications

The above contractual mechanism allows anyone to establish a command-line application through network-wide consensus on a virtual machine (fundamentally), which can change a network-accessible state as its "hard disk". However, for most people, the lack of sufficient user-friendliness of the command-line interface used as a transaction sending mechanism makes decentralization an attractive alternative. Finally, a complete "decentralized application" should include underlying business logic components (whether fully implemented on Ethereum, using a combination of Ethereum and other systems (such as a P2P messaging layer, one of which is planned to be placed in an Ethereum Client) or only other systems) and upper-level graphical user interface components. The Ethereum Client is designed as a web browser, but includes support for the "eth" Javascript API object, which can be used by specific web pages seen in the Client to interact with the Ethereum blockchain. From the perspective of "traditional" web pages, these web pages are completely static content, as blockchain and other decentralized protocols will completely replace servers to handle user-initiated requests. Finally, decentralized protocols have the hope of using Ethereum to store web pages in some way.

Conclusion

The Ethereum protocol was originally conceived as an upgraded cryptocurrency that provides advanced features such as on-chain contracts, withdrawal restrictions and financial contracts, gambling markets, etc. through a highly universal language. The Ethereum protocol will not directly "support" any application, but the existence of a Turing-complete programming language means that any contract can be created for any transaction type and application. However, what is more interesting about Ethereum is that the Ethereum protocol goes further than simple currency. Protocols and decentralized applications built around decentralized storage, decentralized computing, decentralized prediction markets, and dozens of similar concepts have the potential to fundamentally improve the efficiency of the computing industry and provide strong support for other P2P protocols by adding an economic layer for the first time. Eventually, there will also be a large number of applications that have nothing to do with money.

The concept of arbitrary state transitions implemented by the Ethereum protocol provides a platform with unique potential; unlike closed protocols designed for single purposes such as data storage, gambling, or finance, Ethereum is open by design, and we believe it is extremely suitable as a foundation layer to serve the extremely large number of financial and non-financial protocols that will emerge in the coming years.