Ether Data (ETD)
White Paper

July 2021 v.5.2

Contents

1. Project Background

The centralized society has played a great role in promoting the rapid development of human civilization for thousands of years. However, with the progress of mankind and economic development, the class conflicts caused by the gap between the rich and the poor have become more and more intensified, thus limiting the increase in total productivity, directly affecting the further development of civilization. The main reason is the lack of transparency in a centralized society, and a lack of trust will result in the failure to reach a consensus.

The emergence of blockchain allows us to find the direction to a solution. The consensus system generates passive trust through technical means and forms a consensus mechanism that cannot be tampered with, thereby achieving the highest level of trust so far—decentralization. Through this new technology, people realized that most of the current social conflicts are being caused by centralization. Blockchain perfectly solves this global crisis of trust, and cryptocurrency has found a way out for the safety of our assets.

1.1 Market Environment

Blockchain has the most potential to trigger the fifth wave of technological revolution since the creation of the steam engine, electricity, and information and internet technology. The digital currency concept in development, Bitcoin, was first

proposed by Satoshi Nakamoto in 2009. It is an electronic cash system implemented through peer-to-peer technology. The core idea of Bitcoin is embodied in the underlying blockchain technology. The blockchain can establish decentralized trust from the technical level, which is vastly different from the institutional foundation of the existing financial system. With the ever-growing usage and recognition of Bitcoin by the public, the digital currency industry has been booming.

1.2 What is mining

Mining is a process of increasing Bitcoin's money supply. Mining also protects the security of the Bitcoin system, prevents fraudulent transactions, and avoids "double payment". "Double payment" refers to spending the same bitcoin multiple times. Miners provide computing power for the Bitcoin network in exchange for the opportunity to obtain Bitcoin rewards. The process of mining is simply the process of issuing coins by banks. In addition to issuing coins, miners also undertake the work of packaged transaction accounting.

The miners verify each new transaction and record them in the general ledger. Every 10 minutes, a new block will be "mined". Each block contains all the transactions that occurred during the period from the creation of the previous block to the present, and these transactions are sequentially added to the blockchain. We refer to the transactions included in the block and added to the blockchain as "confirmed" transactions. After the transaction is "confirmed", the new owner can spend the bitcoins he got in the transaction.

Miners receive two types of rewards during the mining process: new currency rewards for creating new blocks, and transaction fees for transactions contained in the blocks. In order to obtain these rewards, miners rush to complete a mathematical puzzle based on cryptographic hashing algorithms. The answers to these puzzles are included in the new block as a proof of the miner's computational workload, which is called "proof of work." The competition mechanism of the algorithm and the mechanism by which the winner has the right to record transactions on the blockchain are the cornerstones of Bitcoin security.

Simple understand this: Bitcoin is a bank in the blockchain world, and the miners are the staff of the Bitcoin bank. During the mining process, the miners have completed all the work of the Bitcoin bank minting (issuing Bitcoin) and bookkeeping (packaging transactions). If someone works, someone has to pay the fees. Block rewards and transaction fees pay all the miners' work costs. The mining mode ensures the safe, decentralized and automatic operation of the Bitcoin system.

1.3 Evolution of mining power

At the very beginning, Bitcoin could be mined with an ordinary computer. As the price of Bitcoin exceeded $1,000 at the end of 2013, more people joined the mining industry and the difficulty of mining became more and more difficult. At this time, mining started to become a full-time job. Mining personnel and large mining

machine rooms are called mines. In this era of large-scale mining, the computer rooms consist of thousands of mining machines with 24-hour full-time maintenance personnel and air/water-cooled to a constant temperature and humidity to ensure the continuous operation of the machines. The current Bitcoin mining has entered the era of large-scale mining farms.

1.4 The market environment of the mining industry

Initially, Bitcoin was mined using a CPU. In January 2009, the founder of Bitcoin, "Satoshi Nakamoto", used his computer's CPU to mine the first founding block. With the rise in the price of Bitcoin, mining participants increased, GPU mining began to gain the upper hand, and CPU mining withdrew from the stage of history. At the beginning of 2013, the first FPGA mining machine appeared in the market, replacing the original GPU mining. In July of the same year, ASIC mining machines appeared, with chips from 110nm to 55nm, from 55nm to 28nm, from 28nm to the current 16nm. Step by step, the development until now, with the emergence of professional bitcoin mining machines, has put the bitcoin mining capital in a competition between a small group of people with the resources to do so.

2. Market weaknesses

Computing power monopoly: In order to resist over-concentration of computing power, people constantly try to change new algorithms. There are hopes to be able to resist ASIC attacks by changing the algorithm and maintaining a relatively low mining cost. This method is often effective in the early stage, but once the market value of this new type of cryptocurrency reaches a certain height, driven by profits, ASIC developers will still find ways to crack these new algorithms, and the interests of ordinary miners will suffer huge losses.

Miners have no right to speak: The essence of decentralization is that everyone can participate. Everyone has the right to participate in the ecological construction of cryptocurrency, and every miner has certain rights to ecological construction. However, the emergence of computing power monopoly has caused more and more miners to lose their original rights. It is difficult for ordinary miners to obtain large computing power, mining costs are high, it is difficult to obtain profits, and it is difficult to participate in the ecological construction of digital currency.

Unconscious smashing: Based on the POW consensus chain, maintaining its security requires the consumption of a lot of electricity. When the market is in a downturn, electricity is the foundation of the cost of POW, which far exceeds the resource consumption caused by the hardware itself. Miners have to sell coins to pay electricity fees. Mining, selling and withdrawal have become a method that many miners have to choose, making it difficult for cryptocurrencies to be held for a long time. Little do they know that this kind of behavior is actually an unconscious smash, and the miners are unable to establish a sense of consistency and identity of interests. Instead, a malicious competition is formed, which ultimately harms the interests of the miners themselves.

2.1 The mining threshold is too high

Individual investors involved in the mining industry do not have any bargaining power in any aspects of production factors (mining machine + electricity fee + maintenance cost + site), and retail investors are basically unable to participate in low-cost mining. Secondly, the speculative nature of the digital currency trading market determines its own price fluctuations. Even when the overall market price rises, it is often impossible to obtain high and stable returns. With the skyrocketing currency price, the output of mining machines cannot meet market demand, and orders for mining machines cannot be shipped on time, which will cause certain economic losses to users.

2.2 The speculative nature of digital currency

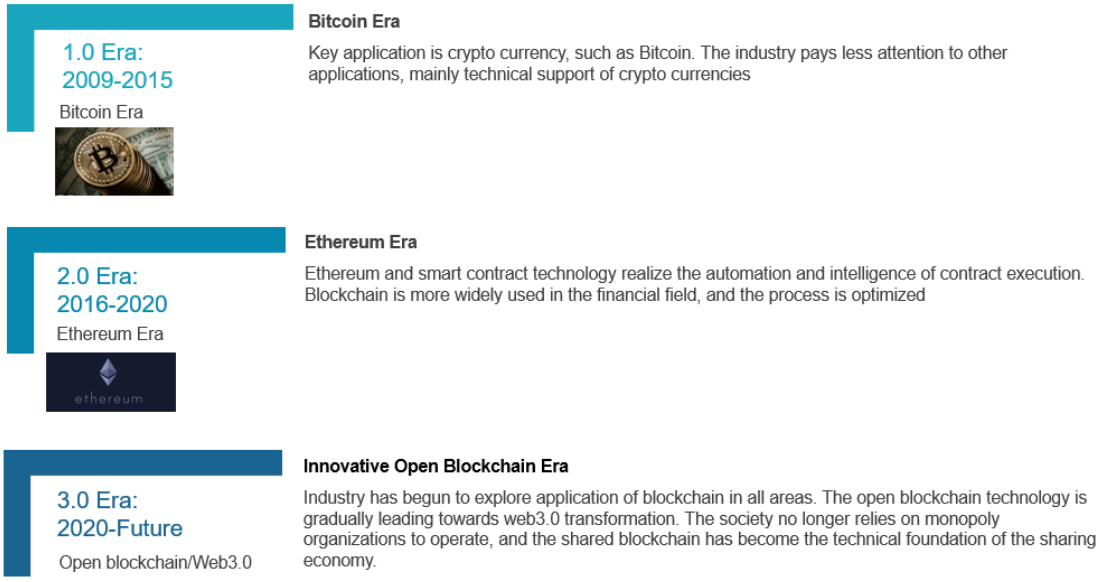
The digital currency market is not only under large speculation, but also has large fluctuations due to the T+0 arrival, as there are no limits on the rise and fall, the high circulation of funds, and the large coverage. Retail transactions often follow the distribution law of "one gain, two equals and seven losses". Most people will withdraw halfway due to the fluctuations in currency prices and fail to maximize their benefits. In the long run, with the continuous development of the digital currency industry, And the irreversible historical process of asset listing, long-term currency holding is the best choice.

2.3 Exit barriers to mining

The mining industry’s computing power and time means everything to profit. When the profit is high, there is no delisting. In the period of low profit, when the miners need to sell the mining equipment such as mining machines, it is often impossible to trade because of the chaos in the second-hand mining machine market. An appropriate price often fails to be reached in time, and mining capital will also depreciate. The relatively heavy asset operation attribute of mining determines that it cannot be circulated in real time, resulting in the failure to guarantee a profit when selling the mining machine.

3. Opportunities and Challenges

3.1 Opportunities in the digital economy



Milestones in the development of blockchain technology

The birth and development of blockchain technology has experienced the Bitcoin era and the Ethereum era and has entered the innovative era of an open blockchain. In the era of blockchain 1.0 represented by Bitcoin BTC, the first layer of "monetary value shaping" of the mining mechanism was introduced. In the era of blockchain 2.0 represented by Ethereum ETH, the second layer of "application value landing" of smart contracts was introduced by changing the production method of encrypted currency. However, the huge energy consumption caused by BTC and ETH mining, as well as the bottleneck of its platform performance, have greatly restricted the large-scale application and development of blockchain technology.

Blockchain is essentially a distributed accounting technology used to maintain a growing list of records (called blocks). Each block contains a timestamp and a link to the previous block. The information on the chain is encrypted by asymmetric encryption methods (such as keys and hash algorithms). Once the blockchain is recorded, it can prevent data from being modified. The data stored in any given block cannot be changed retrospectively without changing the consensus of all subsequent blocks and the majority of nodes in the network. This means that all participants should agree on the order of the blocks and have the same consensus on the blockchain of the system. Therefore, to solve the core bottleneck problems of 1.0 and 2.0 in the blockchain era, it is necessary to solve the bottleneck problems that restrict the current Internet development and core infrastructure such as computing, storage, and network communications. Innovative applications are needed in the era of blockchain 3.0, web 3.0-based network technology development, through technologies such as big data processing algorithms, distributed cloud storage, IoT, P2P networks, intelligent perception, 5G communication networks, etc., to achieve decentralization, safety and reliability. The distributed blockchain cloud platform can provide open blockchain distributed cloud services for various computing scenarios. Combined with the Token incentive mechanism of the open blockchain, through the use of a record token called Ether Data that supports smart contracts and distributed computing, it provides ETD token incentives for service-providing nodes to drive

shared cloud computing platform resources.

The distributed intelligent data computing platform supported by ETD can support the "community value autonomy" and "cross-chain value transfer" of node voting. The "consensus value network" of the smart contract consensus network can build a brand-new digital economy in different real economic fields. When economic development encounters a growth bottleneck, finding new growth points becomes a top priority. In the face of increasingly complex market changes and higher consumer demand, the way out is bound to be changes in new technologies. However, the current revolution is to find new technological breakthroughs, starting from the real demands of consumers, with the help of new technologies and new models, to re-excavate the value of people and products. ETD is empowered by blockchain technology and builds a smart contract consensus network to make it possible to solve the rediscovery of the value of people and commodities.

The concept of smart contracts was first proposed by Nick Szabo in 1994. A smart contract is a computer protocol designed to spread, verify or execute a contract in an information-based way. Smart contracts allow for trusted transactions without a third party, which are traceable and irreversible. ETD has an independent smart contract system. It is a micro-core smart contract execution environment that provides a set of instructions including stack operations, process control, logical operations, arithmetic operations, cryptographic operations, string operations, and array operations. ETD can create independent virtual hardware and open it to smart contracts for use in the form of interfaces, so that the contract can obtain platform-related data, persistent storage, and access to the Internet at runtime. Because ETD has a hardware-level security mechanism, it can ensure that the behavior of the contract is safe and controllable, and security can be improved by reasonably programming virtual hardware.

3.2 Opportunities after the internet traffic dividend disappears

With the rapid development of e-commerce for more than a decade, the dividends of internet traffic have gradually disappeared, and the cost of online customer acquisition has become higher and higher. E-commerce companies have begun to gradually shift from online to offline and conduct retail O2O attempts. In the retail O2O model, consumers can browse product information online and pay for purchases, and experience products and services offline. Entering 2016, the integration of online and offline has gone further, and new retail models such as unmanned vending stores have initiated a new round of changes. Internet traffic is essentially human traffic. Whoever has greater access to traffic will have the opportunity to monopolize wealth. This concept is becoming a reality. The development of the Internet has proven that wealth is converging on some giants, causing the gap between the rich and the poor to grow. There is a possibility that the digital economy is gradually migrating from the flow of people to the flow of data. Whoever masters the flow of data is likely to seize new wealth, and the degree of monopoly of this wealth will exceed everyone’s imagination and speed. Soon, the gap between the rich and the poor will be greater, and mankind is facing

unprecedented threats and challenges. ETD is carrying out this great experiment, which is to make data no longer monopolized by a few people or institutions, resulting in greater wealth exploitation and thus realizing the redistribution of wealth.

3.3 The solution to the incomplete integrity mechanism

Due to the liquidity and fictitious nature of e-commerce transactions, both parties of the transaction cannot confirm the identity information of the other party during the entire process of searching for trading partners, consulting and negotiating, and then paying online. The buyer cannot know the identity of the product when purchasing the product. The real situation can only be judged based on the image information provided by the seller, and the two parties in the transaction cannot be trusted with each other in a short time, which seriously affects the security and reliability of the transaction. The imperfect integrity mechanism hinders the development of e-commerce, especially the development of cross-border e-commerce. ETD uses a complete user privacy protection and identity authentication mechanism, based on the low-cost and high-efficiency PoW+DSB consensus algorithm, and customized smart contracts to quickly establish a decentralization, resource sharing and self-development for authentication entities and applications with different identities. The smart contract consensus network: as long as all contributions are generated by the user's authentication entity network, you will be rewarded with equivalent value. The data will be on the chain, truthful, open, and transparent, so as to establish a new integrity mechanism network, which will benefit everyone for life. Start with the smart contract consensus network.

3.4 Challenges to user data security risks

Nowadays, mobile payment is ubiquitous and has become the norm of daily consumption, but in the era of big data, personal privacy has nowhere to hide. Everyone is almost transparently exposed to the supervision of the big data system. As long as you search a little in a big data system, you will find all kinds of information, materials and data about a person. The information and data that can be found is extremely comprehensive - more so than the personal information managed by the police station's household registration system. If the data is leaked, the harm could be beyond imagination. The problem of data security has become one of the most urgent problems to be solved at the moment.

4. Blockchain core technology and principal mechanism

The core of blockchain technology is that all currently participating nodes jointly maintain the transaction database. It makes it so that the transaction is based on cryptographic principles rather than trust, so that any parties who have reached an agreement can directly conduct payment transactions without the need for a third party to participate. Technically speaking, a block is a data structure that records transactions and reflects the flow of funds for a transaction. The blocks of transactions that have been reached in the system are connected together to form a

main chain, and all nodes participating in the calculation record the main chain or part of the main chain. A block contains the following three parts: transaction information, the hash formed by the previous block, and a random number. Transaction information is the task data carried by the block, which specifically includes the private keys of both parties to the transaction, the number of transactions, the digital signature of electronic currency, etc.; the hash formed by the previous block is used to connect the blocks to realize the past order of transactions arranged; the random number is the core of the transaction. All miner nodes compete to calculate the answer to the random number. The node that gets the answer the fastest generates a new block and broadcasts it to all nodes for update, thus completing a block.

4.1 What is blockchain technology

Blockchain is an organic combination of a series of existing mature technologies. It uses chain or directed acyclic graph data storage structure, supporting consensus algorithms, P2P distributed interconnection technology, and game theory design ideas. The combination of cryptography technology is called blockchain technology.

In a typical blockchain system, data is generated and stored in units of blocks and connected into a chain data structure in chronological order. All nodes jointly participate in the data verification, storage and maintenance of the blockchain system. The creation of a new block usually needs to be confirmed by a majority of nodes in the entire network (the number depends on different consensus mechanisms), and broadcast to each node to achieve synchronization across the entire network, and cannot be changed or deleted afterwards. Although blockchain technology originated from Bitcoin, the underlying technology used in Bitcoin technology cannot be directly equated with blockchain technology.

4.2 The core technology of blockchain

Public ledger: The ledger recorded by the blockchain system should be in a state where all participants are allowed to access. In order to verify the validity of the information recorded by the blockchain, the accounting participants must have the ability to access the information content and ledger history. However, the public ledger refers to the disclosure of accessibility, and does not represent the disclosure of the information itself. Therefore, the industry expects to apply many privacy protection technologies, such as zero-knowledge proof, homomorphic encryption, and threshold encryption, to the blockchain Field to solve the problem of verifying the validity of information through ciphertext operations.

Multi-party consensus: Blockchain is a distributed ledger system that is maintained by multiple parties. The participants need to agree on rules for data verification, writing, and conflict resolution. This is called a consensus algorithm. Bitcoin and Ethereum, as public chains, currently use Proof of Work (PoW) algorithms. The consensus algorithms applied in the consortium chain field should be more flexible and diverse, and be closer to business needs.

Weak centralization: The blockchain should be a system that does not rely on a single trust center. When processing data that only involves the closed system within the chain, the blockchain itself can create trust between participants. However, in some cases, such as identity management and other scenarios, it is inevitable that external data will be introduced, and these data need the trust endorsement of a trusted third party. At this time, for different types of data, the trust should come from different trusted sources. A third party instead of relying on a single trust center. In this case, the blockchain itself does not create trust, but serves as a carrier of trust.

Information cannot be tampered with: Important information recorded in the blockchain system is covered by the digest algorithm. The longer the chain, the more times the information is confirmed, and all nodes participating in the bookkeeping will store a copy of the data. The tampering of data by a small number of nodes is not recognized, nor can it affect the overall operation of the system.

Smart contract: The internal information of the blockchain system cannot be tampered with and all participating nodes store a copy of the ledger data, which provides a platform for the realization of smart contracts. Smart contracts are a powerful weapon for blockchain technology to reduce trust costs and subvert third-party intermediaries. It is also a tool for companies to use blockchain to achieve value transfer and efficient collaboration. It is also the ultimate value of blockchain technology to achieve social governance.

Cryptography: Information security and cryptography technology are the cornerstones of the entire information technology. In the blockchain, a large number of modern information security and cryptography technical achievements are also used, mainly including: hash algorithm, symmetric encryption, asymmetric encryption, digital signature, digital certificate, homomorphic encryption, zero-knowledge proof, etc.

4.3 Consensus mechanism

The consensus mechanism is a mechanism to maintain the operating sequence and fairness of the system. It determines that the blocks in the blockchain system are accurately added to the chain to ensure the consistency of the entire block content across the network. Because there is no centralized bookkeeping institution like a bank in the blockchain world, which guarantees the consistency of each transaction on all bookkeeping nodes, that is, allowing the entire network to reach a consensus. The consensus mechanism solves this problem. At present, the main consensus mechanisms include workload proof mechanism PoW, equity proof mechanism PoS, and authorization proof mechanism DPOS.

According to the size of the rights of the nodes in the digital asset system network, the consensus protocol can be divided into permissionless protocols and permissioned protocols. The unlicensed protocol is typically that all nodes in PoW have equal rights. The degree of authorization is different, the more typical ones are

PoS and DPoS.

4.3.1 PoW mechanism

PoW: proof of work is a consensus mechanism adopted in the Bitcoin system. The legality of Bitcoin transactions is verified by the entire network. Only when most participants agree with a transaction can the transaction be considered valid. However, under this mechanism, the problem of false identities is highlighted, that is, the adversary may launch an attack, and the transaction initiator can forge multiple identities and then confirm its own transaction. Since "most people" agree with this transaction, even if it is a double payment, the recipient will believe and accept the transaction. Before confirming the transaction, participants need to do some work to prove their true physical identity. This work is to solve a cryptographic problem and artificially increase the computational cost of confirming the transaction. Therefore, the ability to verify transactions depends on computing power, not the number of entity identities. In the Bitcoin system, new transactions are constantly generated. Nodes need to put legal transactions into a block. The block header is hashed by the version number and the previous block. The value, Merkle root, timestamp, difficulty target and random number are composed of six parts. Participants need to find a random number to make the hash value of the block header less than or equal to the difficulty target. The SHA-256 hash algorithm is used in the Bitcoin protocol. Unless the algorithm is compromised, the most effective method is to try different random numbers until the goal is met.

Solving the problem of proof of work requires computing power, which is actually spending money. In order to encourage nodes to participate in the maintenance of network security, the Bitcoin protocol provides an incentive mechanism to give the first node that solves the mathematical problem a reward, including mining Mine rewards and transaction fees. The first transaction of a Bitcoin block is called a coinbase transaction, in which the system sends a certain amount of Bitcoin to the miner's account that solves the problem of proof of work. The mining reward was initially set to 50 Bitcoins, and the rewards were halved every 210,000 blocks (i.e. nearly four years). It is estimated that Bitcoin mining will be completed around 2140. The subsequent maintenance of network security depends on transaction fees. The mined bitcoins circulate in the system. The incentive mechanism is not only a means of currency issuance, but also guarantees the network security of the system. The main chain in the Bitcoin system is defined as the blockchain that has accumulated the most difficulty. In general, it is also the chain that contains the most blocks. When a block is mined in a short interval, the main chain will fork. At this time, the system will keep the branch. If at some point in the future one of them is extended and the difficulty value exceeds the main chain, then subsequent blocks will reference them.

The proof-of-work mechanism guarantees the safe operation of the Bitcoin system from four aspects: money supply, prevention of double payments, incentive measures to ensure safety, and agreement on transactions within a limited time, and provides a solution to the Byzantine Generals problem.

4.3.2 PoS mechanism

The security of the Bitcoin network is guaranteed by scarce physical resources, including the physical hardware and electricity that perform hash operations. In order to increase mining rewards, miners have to participate in the increasingly fierce mining arms race, so from an energy perspective, proof-of-work is an ecologically unfriendly consensus mechanism, which has also led to the emergence of a consensus mechanism with less energy consumption-proof of equity. Proof of equity is PoS. At present, Peercoin and Nextcoin, and many other cryptocurrencies have used this consensus mechanism, and its starting point is to solve the energy waste problem of proof-of-work. Proof of equity is based on the concept of currency age, which is defined as the product of currency quantity and currency holding time.

The idea behind the proof of rights is that the blockchain should be protected by those who have economic rights in it. PoS mining was implemented for the first time in the Peercoin released by the anonymous developer SunnyKing in 2012. In the Peercoin block, there is a transaction called coinstake, whose name is similar to the coinbase transaction in the bitcoin block. In the coinstake transaction, it is stipulated that currency owners send the currency they hold to themselves (guaranteeing that the currency age will return to zero after the equity block is generated), which is used to generate a bit of currency block and get some interest. The cost of getting interest currency is the consumption of currency age. Similar to the Bitcoin system, the Peercoin block also requires participants to find a random number to make the hash value of the block header meet the target difficulty. The difference is that each participant in the Peercoin system has a different difficulty target value for the block generated. It is not the same. The difficulty target is inversely proportional to the coin age consumed in the coinstake transaction. The more coin age participants accumulate, the greater the probability of generating a block.

The concept of coin age in PoS can be imagined as the computing power in PoW. If someone holds a large sum of money for a long period of time, he will have an opportunity to use a powerful ASIC mining machine in the next mining, but this opportunity does not depend on the purchase of hardware facilities and electricity. The consumption depends on the user’s deposit and savings time in the system. Unlike the nature of the PoW mining competition, PoS is more like a lottery. The more coins you accumulate, the more you have the chance to win. If it is consumed, the probability of winning again is reduced, avoiding the occurrence of "the rich get richer".

In PoS, the main chain is defined as the chain that consumes the highest coin age, and each block transaction will submit its consumed coin age to the block to increase the block score. In this case, if an attacker wants to launch an attack on the main chain, he must have a large amount of money and have to accumulate enough currency. The attacker gets a large amount of money in the PoS system. It is more expensive than mastering most of the computing power in the Bitcoin system, and once an attack is carried out, the currency system will be destroyed while the large

amount of currency owned by itself will also be damaged. This may reduce the attacker's motivation from the beginning, but once the coin age is cleared immediately after the block is generated, which also ensures that the attacker cannot carry out continuous attacks.

After the emergence of PoS, some new protocols that were born by modifying one of the shortcomings were called PoS derivatives, such as PoSV and PoA. PoSV addresses the problem that the coin age is a linear function of time in PoS, and is committed to eliminating the phenomenon of currency holders. PoSV means proof of rights and activity frequency. It is the consensus mechanism currently used by Reddcoin. Reddcoin uses POW in the early stage for currency distribution, and later uses PoSV to maintain long-term network security. PoSV modifies the linear function of coin age and time in PoS to an exponential decay function, that is, the growth rate of coin age gradually decreases with time and finally tends to zero. Therefore, the age of new coins grows faster than old coins until it reaches the upper limit. Limit. This alleviates the phenomenon of currency holders tuning the currency to a certain extent.

PoA means proof of action, and it is also an improvement scheme of PoS. Its essence is to maintain system security by rewarding currency holders with a high degree of participation rather than punishing passive participants. PoA combines PoW and PoS. The main idea is to distribute a part of PoW mining coins to all active nodes in a lottery, and the stake held by nodes is proportional to the number of lottery tickets, that is, the probability of winning.

4.3.3 DPoS mechanism

In order to further accelerate the transaction speed, and at the same time solve the security problem that nodes in PoS can accumulate currency age when they are offline, Daniel Larimer proposed DPoS in April 2014. DPoS is a derivative of PoS, which means a share authorization certification mechanism. Shareholders grant rights to a certain number of delegates, who are responsible for maintaining the operation of the currency system. This is similar to a representative system to some extent. The real difference between members of parliament is that voters have the right to re-elect according to the performance of the trustee after a certain period of time. If they are not satisfied with their work performance, they can also request the removal of the trustee. DPoS is currently a consensus mechanism built into the BitShares and Crypto platforms.

In DPoS, shareholders vote for a certain trustee, and the system calculates a certain number of trustees with the highest number of votes based on the proportion of shareholders' equity in the system. The trustees take turns responsible for generating blocks in a predetermined order, and all shareholders vote. Later, the trust in the system has been concentrated from all participants to a small number of participants. After the node initiates a transaction, there is no need to wait for a considerable number of untrusted nodes to confirm, but only the trustee needs to verify the transaction, which greatly shortens the transaction. For example, BitShares can achieve a block generation speed of 10 seconds per block, which is a significant

improvement compared to Bitcoin's average generation time of nearly 10 minutes per block.

In some DPoS protocol versions, a node must first pay a certain price in order to be eligible to compete as a trustee, such as paying a deposit to a certain security account. If the node does evil, the deposit will be confiscated, and the trustee will be paid for maintaining the system operation. The block transaction fee will be shared with other trustees, and the reward will form a positive feedback on them to encourage the trustee to work harder to maintain the security of the system. Since the block is signed by the trustee in turn, if a trustee misses the signing of the block due to offline, he will face the risk of being replaced by other candidate trustees. Therefore, in order to make a profit, the trustee must guarantee sufficient online time and pay a deposit This DPoS protocol is also called Deposit-based Proof of Stake.

5. Ether Data

As the blockchain industry matures and grows, people working in the business generally abandon the dichotomous narrative structure of centralization vs decentralization, regulation vs democratic teamwork, and waste of resources vs environmentalism, and have turned to explore the diverse practical value of blockchain. Among these people, some pioneers set their sights on the scientific community, as it is intrinsically characterized by borderlessness, mechanism of mutual consensus, wide dissemination, and free flow of its product (i.e., knowledge), and so forth, which are extremely similar to many basic characteristics of the blockchain. The two undoubtedly have the premise of cooperation in terms of the underlying mutual understood ideology.

Donating Bitcoin to scientific research institutions is one of the easiest methods, but we now believe that this is a rather primitive and inefficient means of bringing science and blockchain together, as a new set of open, transparent solutions for members of the blockchain community to participate in real world scientific research has emerged. It not only solves all the major technical difficulties, but also builds sustainable ecological processes in line with economic logic. This is Ether Data (ETD).

The idea of ETD comes from integrating two concepts: distributed computing, and time-based banking. Time-based banking was first proposed in the nineteenth century, the core idea being that everyone’s time has equal value, and therefore, a time-based currency exchange certificate issued by a bank only recorded the time, not the price. As a result, anyone could contribute their two hours in exchange for the same value of two hours from others in the future. In distributed computing, the value of a unit of processing power contributed by each node is also equal. Large numbers of nodes communicate with each other and pool their resources to form a cluster that rivals even supercomputers in terms of processing power. In other words, a decentralized supercomputer is formed by being installed in various locations around the world. Meanwhile, of all human undertakings in today’s world, science is the one that can best unite people across geographical and cultural barriers to share

their computing power voluntarily.

In humanity’s several scientific paradigms shifts so far, the status of “computing” has continuously improved, its significance has also evolved, and it has even become one of today's dominant doctrines in itself. Since the digital revolution, scientists can no longer make world-class ground-breaking discoveries through manual calculations, as was typically the case in the first and second industrial revolutions. Moreover, after the arrival of the big data era where everything is connected, a typical research team composed of dozens of people and computers is also doomed to fail due to its limited processing power, in both the human brains and the computers. To put this in perspective, GPT-3, an artificial intelligence developed by OpenAI, had to collect 45 TB of textual data from the entire internet before it was trained to become today’s top natural language processing neural network.

At the same time, the spirit of sharing since the early years of the internet has been in decline. The trend of information fragmentation and oligarchy in cyberspace has also affected the scientific community. Websites that provide free access to research papers like Sci-Hub are being hunted down by monopolistic academic publishers and are facing shutdown. This not only causes scholars to pay extortionately high publishing fees, but it also creates artificial barriers in the process of disseminating scientific discoveries to the public and potential investors. The Internet is no longer interconnected, and the scientific community needs the next generation of the Internet - a computing platform with powerful processing power at affordable prices; an open, transparent, and accessible platform with free flow of information. It means that the public also needs the next generation of the Internet - if humanity's scientific endeavors are to be treated as a listed company, then everyone would be a shareholder, because science shapes reality in every way, even for those who are indifferent to it.

By integrating smart minds and computational resources scattered around the world through distributed computing, and by ensuring each scientific research team and all resource contributors are reasonably paid through financial technology based on time banking, we can achieve a win-win situation consistent with the economic theory of incentives and in return, the long-term interests of mankind will be developed. This future is the vision of ETD.

5.1 Introduction to Ether Data

ETD (Ether Data) is a distributed general-purpose computing system based on the Ethereum smart contract and DSB (Disk Storage Banking) distributive storage and secure computing technologies to contribute public computing power to Berkeley Open Infrastructure for Network Computing (BOINC) and other scientific computing platforms. By adopting a new PoW+DSB PoS consensus mechanism, the architecture is positioned as an easy-to-use high-performance blockchain platform that aims to achieve flexible expansion of distributed applications to meet the performance requirements of scientific research institutions, the storage and computing

requirements for web applications, and the economic requirements for contributors to get rewards.

Why use ETD instead of Ethereum? First of all, for the existing blockchains such as Ethereum and Bitcoin, the purpose of consensus is only to keep accounts. ETD reaches a consensus while also solving scientific calculation problems, giving consensus value beyond accounting. Secondly, Ethereum can only execute smart contracts and cannot directly solve the problems of storage and computing. Therefore, it costs three sums to perform a scientific calculation: gas fee, possibly prohibitive cost of cloud storage service, and payments to computing power providers. In contrast, the technical architecture of ETD integrates computation and data storage functions with lower cost and higher efficiency, has a more complete mechanism of user privacy protection and identity authentication, and an Ethereum-based smart contract system more suitable for diversified computing needs, so that it can quickly establish a decentralized, resource-sharing and self-organizing ecological network for authenticated entities and applications of multitudinous identities.

5.2 Introduction to BOINC

BOINC (Berkeley Open Infrastructure for Network Computing), mainly developed by the Department of Computer Science at the University of California, is an open-source middleware system for voluntary computing and grid computing. BOINC was originally developed to support the SETI@home project, and later became a widely used distributed computing platform, covering areas which include mathematics, linguistics, medicine, molecular biology, climatology, environmental science, and astrophysics.

BOINC aims to draw together the personal computers of volunteers scattered around the globe to form a huge amount of computing resources for scientific research personnel. As of June 3rd, 2021, BOINC has 73,006 volunteers and 636,158 active hosts around the world, with an average 24-hour pooled processing power of 26.185 Petaflops. At its peak in March 2020, due to the public's enthusiasm for scientific research triggered by the COVID-19 pandemic, BOINC’s 24-hour average computing power reached 41.548 Petaflops, which means its maximum processing power rivals the world’s fifth to ninth single supercomputers.

Rank	System	Cores	Rmax (TFlop/s)
1	**Supercomputer Fugaku -** Supercomputer Fugaku, A64FX 48C 2.2GHz, Tofu interconnect D, ***Fujitsu*** RIKEN Center for Computational Science **Japan**	7,630,848	442,010
2	**Summit -** IBM Power System AC922, IBM POWER9 22C 3.07GHz, NVIDIA Volta GV100, Dual-rail Mellanox EDR Infiniband, ***IBM*** DOE/SC/Oak Ridge National Laboratory **United States**	2,414,592	148,600.0
3	**Sierra -** IBM Power System AC922, IBM POWER9 22C 3.1GHz, NVIDIA Volta GV100, Dual-rail Mellanox EDR Infiniband, ***IBM / NVIDIA / Mellanox*** DOE/NNSA/LLNL **United States**	1,572,480	94,640.0
4	**Sunway TaihuLight -** Sunway MPP, Sunway SW26010 260C 1.45GHz, Sunway, ***NRCPC*** National Supercomputing Center in Wuxi **China**	10,649,600	93,014.6
5	**Selene -** NVIDIA DGX A100, AMD EPYC 7742 64C 2.25GHz, NVIDIA A100, Mellanox HDR Infiniband, ***Nvidia*** NVIDIA Corporation **United States**	555,520	63,460.0
6	**Tianhe-2A -** TH-IVB-FEP Cluster, Intel Xeon E5-2692v2 12C 2.2GHz, TH Express-2, Matrix-2000, ***NUDT*** National Super Computer Center in Guangzhou **China**	4,981,760	61,444.5
7	**JUWELS Booster Module -** Bull Sequana XH2000 , AMD EPYC 7402 24C 2.8GHz, NVIDIA A100, Mellanox HDR InfiniBand/ParTec ParaStation ClusterSuite, ***Atos*** Forschungszentrum Juelich (FZJ) **Germany**	449,280	44,120.0
	BOINIC Distributed, Global Volunteers	_	41,548.0
8	**HPC5 -** PowerEdge C4140, Xeon Gold 6252 24C 2.1GHz, NVIDIA Tesla V100, Mellanox HDR Infiniband, ***Dell EMC*** Eni S.p.A. **Italy**	669,760	35,450.0

Figure: Supercomputer Global Ranking (November 2020)

Projects that have used BOINC for the purposes of computing are listed on its official website, and some of the prominent ones include:

Rosetta@home: Research on protein folding, recently committed to finding an effective, safe treatment for the COVID-19 pandemic.
Docking@Home: In-depth study of atomic-level construction and details of protein bonding and reactions for the development of medicines.
GPUGRID.net: Molecular Dynamics.
Climateprediction.net: Climate Prediction.
Einstein@Home: Searching for gravitational waves from pulsars.

LHC@home: Simulate particle acceleration, assisting in the design and improvement of LHC particle accelerators.
SETI@home: Search for civilizations in outer space.
ABC@Home: Trying to solve the ABC Conjecture.
World Community Grid: Hosted by IBM, its main purpose is to use distributed computing to help find treatments for human diseases, improve the standard of human life, and other research related to improving human life.
SZTAKI Desktop Grid: Search Generalized Binary Number System

These projects operate independently; some are located at universities and research laboratories, and some are run by private groups or individuals. Contributors (Crunchers) can choose the projects which they wish to contribute to. There are currently 34 projects that have been verified and maintained as whitelisted on the BOINC website. Contributors can also fill in specific project URLs to join other projects.

BOINC consists of a server system and client software that communicate with each other to distribute and process work units and return the results. A complete task process is divided into five steps:

- Your PC gets a set of tasks from the project's scheduling server. The tasks depend on your PC: for example, the server won't give it tasks that require more RAM than you have. Projects can support several applications, and the server may send you tasks from any of them.
- Your PC downloads executable and input files from the project's data server. If the project releases new versions of its applications, the executable files are downloaded automatically to your PC.
- Your PC runs the application programs, producing output files.
- Your PC uploads the output files to the data server.
- Later (up to several days later, depending on your preferences) your PC reports the completed tasks to the scheduling server, and gets new tasks.

5.3 From BOINC to ETD

BOINC itself has a point-earning system: each unit of contribution is called 1 Cobblestone. Since BOINC is one of the most mainstream distributed scientific computing platforms, with huge capital injections from IBM and other organizations, there is no need to look for ways to make profit. Therefore, its official documentation emphasizes the fact that Cobblestone has no monetary value or other intrinsic value: its only function is to record the amount of processing power contributed by each host. Cobblestone cannot be used to exchange processing power for other volunteers, nor can it be circulated across platforms.

The contradiction between the open-source nature of BOINC and the fully closed

nature of its own point-earning system creates a huge space, theoretically allowing any sub-network contributing processing power to BOINC to be able to adopt blockchain technology and develop a decentralized authentic point-earning system that is positively related to Cobblestone. The system is outside of BOINC, so that contributors can obtain certified and freely tradable tokens. However, due to the massive and non-homogeneous characteristics of scientific computing tasks, each task the host receives from the BOINC server is composed of different types of operations, and the amount of operation is extremely large. Therefore, it is difficult for any existing blockchain platforms (including Ethereum) to meet this demand in terms of both the hardware and software requirements. ETD was developed specifically to fill this gap. Its unique distributed computing technical architectures, token issuance rules, and ecological construction principles, can provide BOINC with additional processing power and obtain Cobblestone while simultaneously generating ETD tokens in relative proportion. Through the time-banking mechanism and ecosystem composed of dApps (Decentralized Application) relying on ETD public chain, the free circulation and empowerment of value is realized in both time and space, as are the in-depth sharing and optimal roll out of computing resources.

The computing and storage resources that users donate to BOINC and other distributed scientific computing platforms through ETD will all obtain tokens permanently recorded in the chain, which are genuine, open, transparent, and verifiable. Free flow of value carried by tokens will lead to well-proportioned sharing and redistribution of processing power among volunteers around the world, becoming one of the driving forces of scientific progress. A user who accesses BOINC through ETD and completes computing tasks to obtain contribution credentials (tokens) will automatically become an ETD Processing Power Contributor with a Time Bank account. The tokens can be deposited in the Time Bank to earn interest, which can be withdrawn in the future if needed and is used to exchange for computing resources for yourself. Tokens can also circulate freely among all contributors through the public processing power pool, bridging the divide between those inside and outside of the scientific community, achieving an optimal allocation of global computing resources. Individuals and organizations can build dApps with specific functions on the ETD Platform to provide various Internet services, to explore different ways of using credentials, and to attract more people to join the global volunteer community and become one of the active hosts, getting rewards for helping solve scientific problems.

ETD is designed to achieve high speed, stability, strong security, and ease of use through a brand-new system architecture, making it particularly suitable for distributed scientific computing. This also enables blockchain technology-based dApp developers to enjoy a wider scope for innovation and greater efficiency. The system also provides a rich combination of modular templates and plug-ins to provide various functional requirements for scientific and enterprise application scenarios with simple installation and convenient operation, enabling users from various industries to do application development, operation, trading and customer acquisition at low cost.

The ETD ecological network has the following three important characteristics:

- Instant confirmation:
    - If a transaction is executed in accordance with the agreement of the smart contract, the transaction will be confirmed immediately.

- Value confirmation:
    - The use of crypto assets via loyalty points obtained by users for trading physical products can be determined by the merchant and can be adjusted due to market conditions, reducing the uncertainty of using crypto assets.

- The establishment of a variety of TOKEN circulation pools:
    - ETD ecology welcomes token holders to contribute tokens to the token circulation pool. The design principle of the ETD ecological network is to allow cooperative institutions and developers to integrate the ETD ecological network into their system, and through the ETD ecological public capital circulation pool, it is convenient for all enterprises and individuals in the ETD ecosystem to convert tokens.

The platform adopts the underlying architecture of the shared blockchain, and a professional team is responsible for the construction, testing and maintenance of the source code of the underlying architecture. The ETD ecological network will not control any user's wallet account at any time, and all operations and transactions can be queried on the blockchain. Therefore, even if the platform is hacked, the user's funds will not be affected.

Third-party developers can use the public API interface of the ETD ecological network to implement transactions and information in their own system by calling the smart contract interface of the ETD ecological network. Compared with the common off-chain protocol interfaces and hybrid interfaces on the market, the on-chain protocol interfaces will make the processing of data and information more efficient. At the same time, the entire process does not require the participation and trust endorsement of a third-party organization, which improves the efficiency of the entire operation and simplifies the access process.

5.4 Design Philosophy

The design philosophy of ETD supports the following multiple target requirements.

- The technical architecture ensures that the generation of tokens simultaneously contributes processing power to scientific computing tasks, creating real value and avoiding speculation and energy waste.
- ETD machines serve multiple functions of distributed computing and data storage applications across domains.
- The average power of each machine is only 36W, which is equivalent to a table lamp, leaving less carbon footprint.

- Zero to low entry barrier for individuals. Applications can run at home, office, or mobile phones so that everyone can participate
- Zero barrier for enterprises or merchants to get onto the ecosystem with rapid one-click chain deployment
- Fully support smart contracts to meet the requirements of various applications
- On-chain pledge system to ensure stable operation of distributed computing
- Global coalition and ecosystem of volunteers/contributors

ETD relies on distributed computing (Ethereum) and storage banking (Data) resources to achieve the means of circulation for digital assets. It feeds back the real world through scenario applications and promotes the virtuous circular co-development with the real-world economy. All contributions generated by the network resources of the certified entity will be rewarded with ETD of the equivalent value. Application data is on the chain, immutable, open-access, transparent, and verifiable. ETD is designed to achieve high speed, high stability, strong security and ease of use through a brand-new system architecture, making distributed applications based on blockchain technology more innovative and more efficient. The system also provides a rich combination of modular templates and plug-ins to provide various functional requirements for enterprise application scenarios with simple installation and convenient operation, enabling merchants to do application development, operation, trading and customer acquisition at low cost.

5.5 Technology Architecture

ETD maintains a shared public blockchain based on the Ethereum smart contract and distributed DSB storage banking platform for authenticating data and computation. By adopting a new PoW+DSB PoS consensus mechanism, the architecture is positioned as an easy-to-use high-performance blockchain platform that aims to achieve flexible expansion of distributed applications to meet the performance requirements of real-world computing and business needs. Through a complete user privacy protection and identity authentication mechanism, low-cost and efficient PoW+DSB PoS consensus algorithm, and customizable smart contracts, ETD can quickly establish a decentralized, resource sharing, and intelligent ecological network of collaborative development for corresponding authentication entities and applications.

ETD covers a broad range of technologies such as the efficient implementation of the underlying consensus algorithm, the computing power operation layer of distributed storage, computing, and verification, the embedded system support of Internet of Things, the blockchain operating system, the distributed storage system, the distributed security system, the smart contract, the big data analysis computation, as well as complete systems for scientific computing and dApps. ETD solves the core technical problems of trust, performance, and security in blockchain applications, forming a co-evolutionary relationship among all the on-chain Internet applications and the global scientific community that transcends national borders.

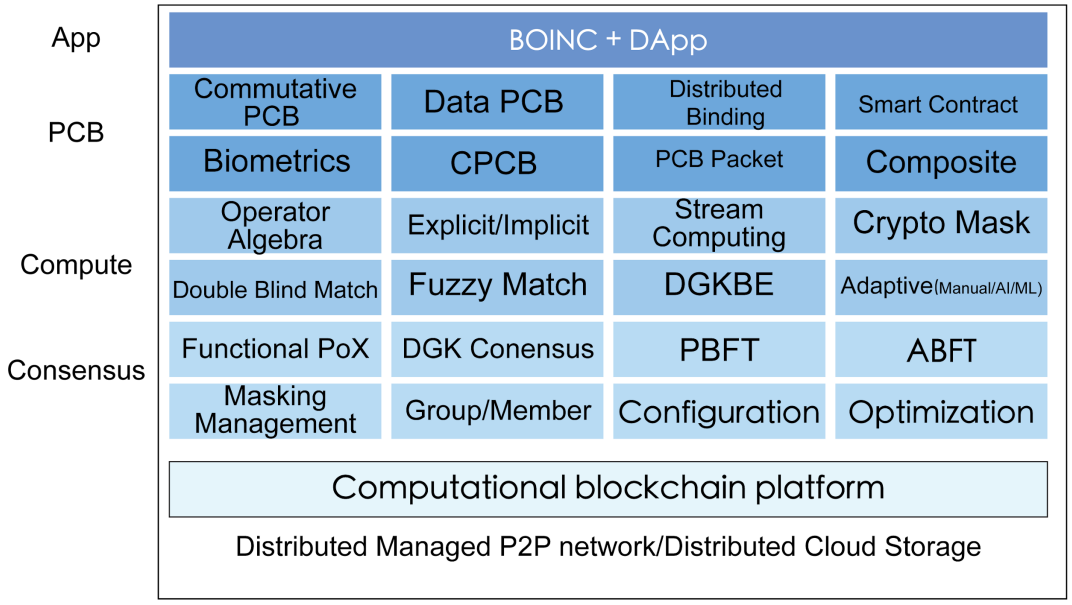
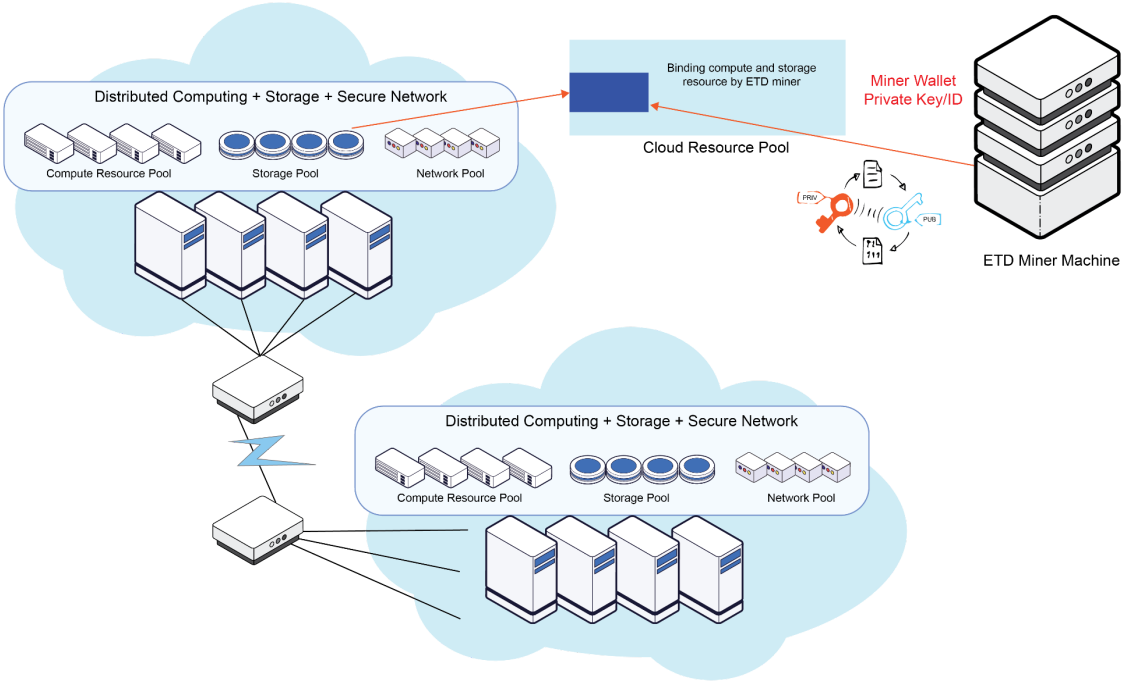


Figure: ETD Overall Technology Framework



ETD distributed computing model architecture:

(1) Decouple the programs executed by the distributed applications through the key and identity binding for distributed computing/storage signaling transmission which is coordinated by the ETD mining hardware to maintain an object-oriented encapsulation.

(2) The internal state of the ETD system can only be changed by passing messages, and only one message will be processed at the given time, which eliminates the problems caused by thread contention in traditional programming and improves system efficiency.

(3) The transmission of data and the sender of the message will not be blocked. Parallel computations and applications can be effectively arranged in parallel. It

achieves the optimized combination and efficient operation of the hybrid computing resources of the CPU and GPU in the distributed cloud ETD platform.

5.5.1 EMP2P Network

Distributed MP2P (Managed P2P) peer-to-peer network is a controllable logical network. Through community super node election and community management, it can be extended to support the entire Internet of massive users. ETD's distributed MP2P network runs a unique EMP2P (ETD Managed P2P) protocol, including multiple high-performance network protocol stacks: EMP2P PCB capability exchange protocol stack (PMC/PCB list, Mask, Coordination); EMP2P peer node discovery protocol stack (TS-Tracker Service); EMP2P performance monitoring protocol stack (MS-Monitoring Service), etc.

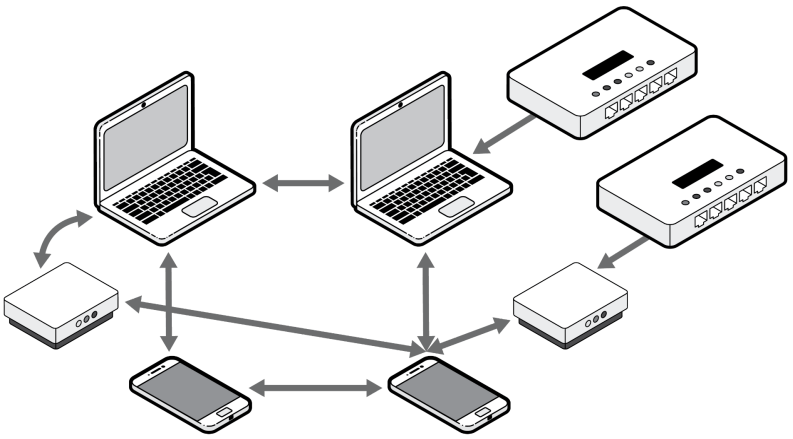


Figure: ETD Managed P2P Protocols

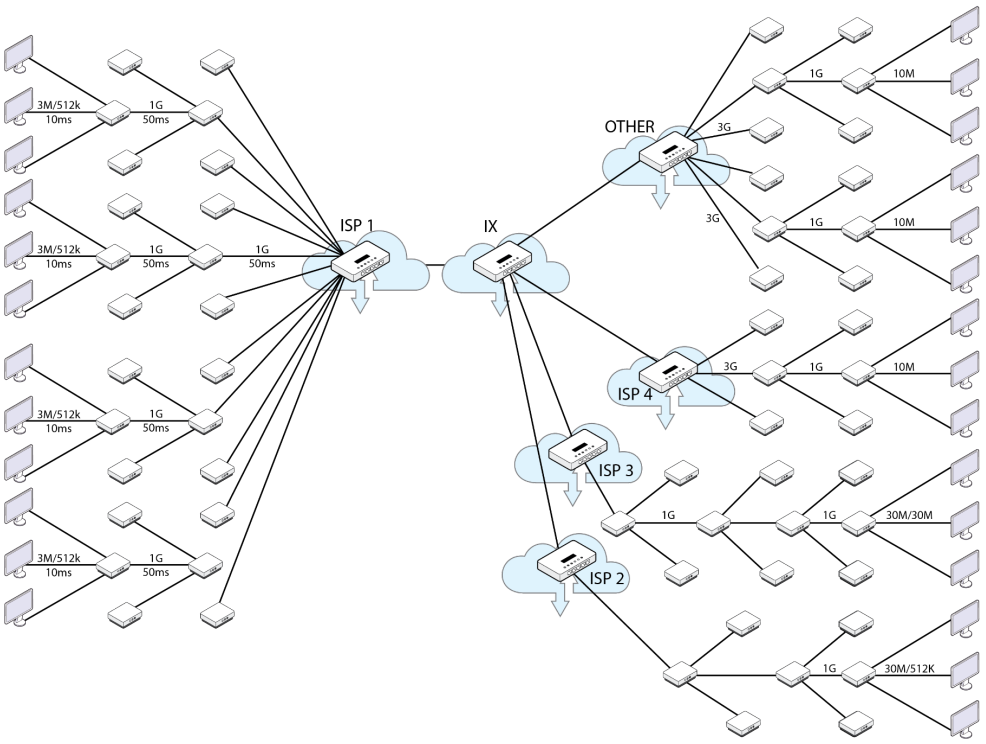


Figure: ETD MP2P Peer-to-Peer Network Users

The EMP2P protocol combines the characteristics of a general P2P peer-to-peer network with the safe Projective Crypto Biometrics (PCB) computing function for ETD applications, and provides a practical, optimizable, and manageable network platform for double-blind matching applications. It has the following significant advantages:

- Compatibility: Support any user terminal (software/hardware)
- Scalability: easy to expand, can support massive applications, is not restricted by the encryption method bottleneck, the system capacity is proportional to the number of participating nodes (computation/storage/bandwidth)
- High efficiency: Low latency controllable for dApp
- Robustness: Robust to node crashes and malicious attacks (the attack cost is extremely high); super nodes have error recovery function
- Interactivity: Support users to participate in the construction of the ecological network through manual, automatic, machine learning, etc.

5.5.2 Double-Blind Matching Algorithm

ETD pioneered the application of double-blind matching technology to deal with data security issues in distributed computing and big data applications. Since each node only contains the distributed data of some nodes, the calculation/index can only be based on the data it sees, and all nodes are required to perform coordinated operations to solve the matching problem. At the same time, the auxiliary computing node, as an intermediate computing node, is bidirectionally encrypted (double-blind) for the data of the matching parties. The double-blind data PCB is CPCB (that is, the commutatively encrypted calculation PCB, Commutative PCB), and the consensus verification algorithm uses differential group key broadcast encryption.

Compared with any existing public chain, the huge advantage of CPCB is that it can encrypt/decrypt PCB data with user biological characteristics (such as fingerprints, voiceprints) or unique hardware characteristics (such as camera CMOS photosensitive elements) without using/storing related secret key and public key. It is more secure and practical. At the same time, the unique and non-cloneable built-in user identity binding secret key and hardware modules are used to make the identification key hence the security mechanism more reliable, greatly reducing the opportunity for user data exposure to the external network and environment and providing hardware-level protection.

Figure: Cryptographic Biometrics for Encryption and Decryption

- Double blind matching system framework:

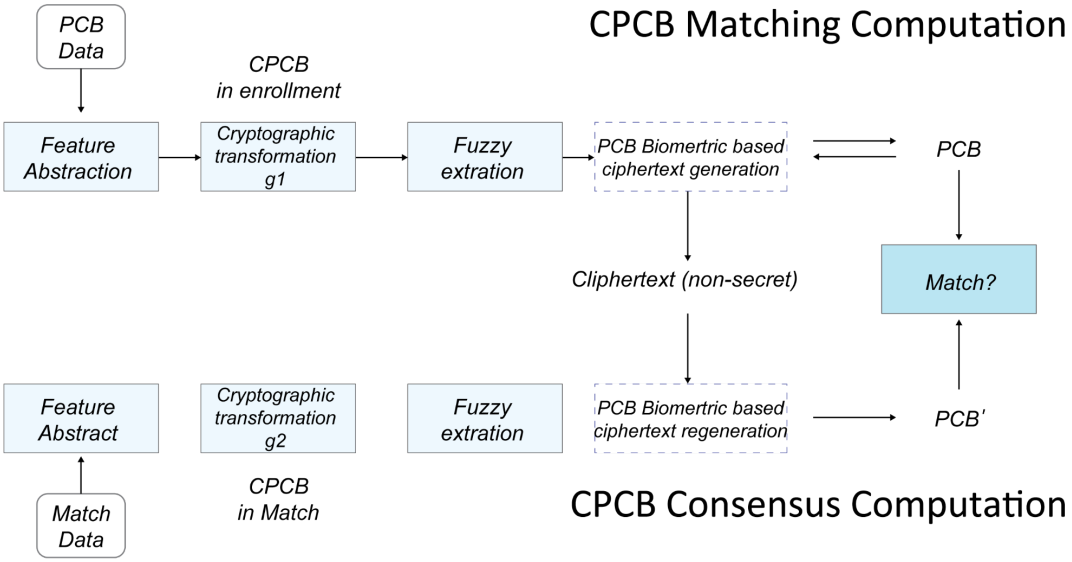


Figure: Double blind matching system framework

- CPCB Matching Computation :

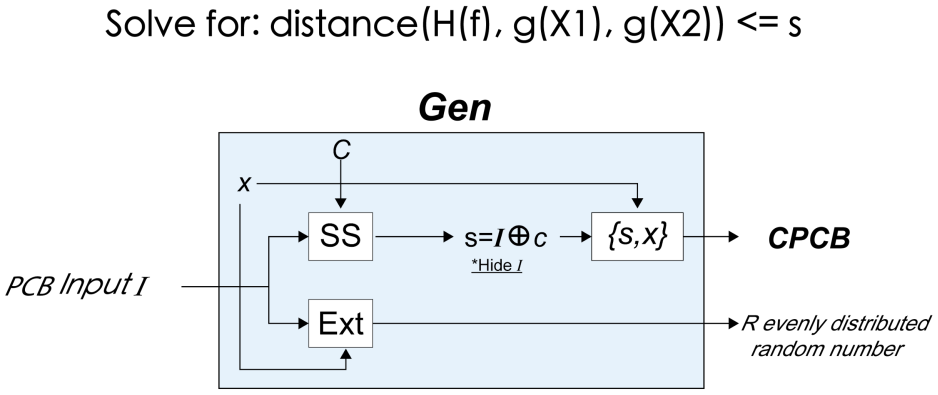


Figure: CPCB Matching Computation

- CPCB Matching Verification :

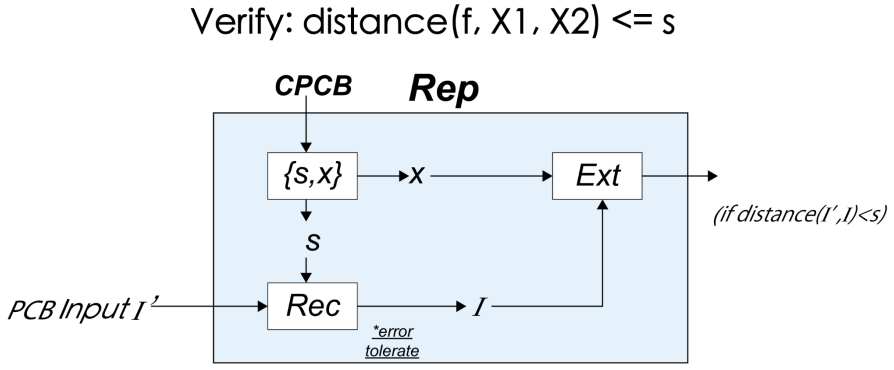


Figure: CPCB Matching Verification

- CPCB Consensus Computation:

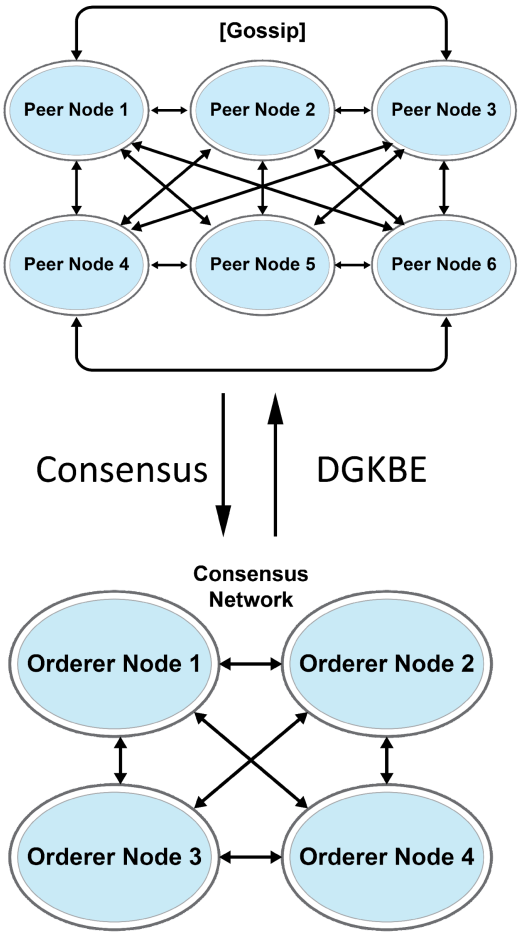


Figure: CPCB Consensus Computation

The distributed CPCB double-blind matching operation model is divided into three layers:

- The top layer is a dApp - a distributed dApp that realizes double-blind matching of encrypted PCBs, such as search, pairing, exchange, ads, etc.
- The second layer is the encrypted PCB double-blind matching calculation layer: distributed nodes exchange calculation requirements (smart contracts) and related node data lists through gossip protocol and perform double-blind matching calculations. Matching pairs that meet the matching rules are passed to the consensus mechanism layer.
- The consensus mechanism layer receives double-blind matching pair data and runs the Proof of Computation-Storage consensus algorithm.

ETD sets up an independent computing layer and consensus mechanism layer to solve the problem of decentralized data storage. The existing public chain contains all the data (full node) in the local node, which is unrealistic for the massive user data in the large-scale scientific computing of double-blind matching. ETD disperses and stores massive user data in the P2P network through CPCB.

- Consensus Mechanism

ETD adopts the Proof of Computation-Storage consensus algorithm that combines Proof of Computation (PoC) and Proof of Existence (PoE).

The choice of consensus mechanism is determined by the requirements of the double-blind matching problem-it is a general distributed computing platform whose goal is to optimize the use of core resources, including distributed computing models, distributed storage models, and P2P peer-to-peer Logical network communication (bandwidth) model, and two-way data privacy protection requirements. In order to realize general PCB matching, the operation of double-blind matching is the core. In essence, PCB consensus is a proof of work (pairing is obtained/discovered through certain calculations). But calculations require data and the network bandwidth to transmit the data, unless all the data is in the local node. Therefore, the provision of data resources is as important as the calculation workload (PoC) (otherwise the calculation will be impossible). In order to ensure the safety of the data source of the double-blind matching operation, the PCB data storage adopts the Proof-of-Existence mechanism. The pairing data can be provided by the node (PoE); or the data fragments are provided by the local or other nodes, and then the required PCB data (combined PoC and PoE) can be obtained through calculation. Encrypted biometric PCB can effectively obtain proof in PoE without decrypting all encrypted data.

- Differential Group Key Broadcast Encryption (DGKBE)

Since the current public key infrastructure cannot cope with the massive P2P encrypted data computing requirements, such as the large number of users, multiple concurrencies, multi user types, real-time, and cross-platform, ETD adopts the differential group key broadcast encryption (DGKBE) technology to achieve the following performance:

- High speed (can be used for massive distributed P2P, such as PCB)
- Security (160-bit DGK=1024-bit RSA)
- Large-scale scalability (processing 100 million level)
- Fixed storage capacity (only 60 bits on the client side)
- Low CPU requirements (as low as 10MHz)

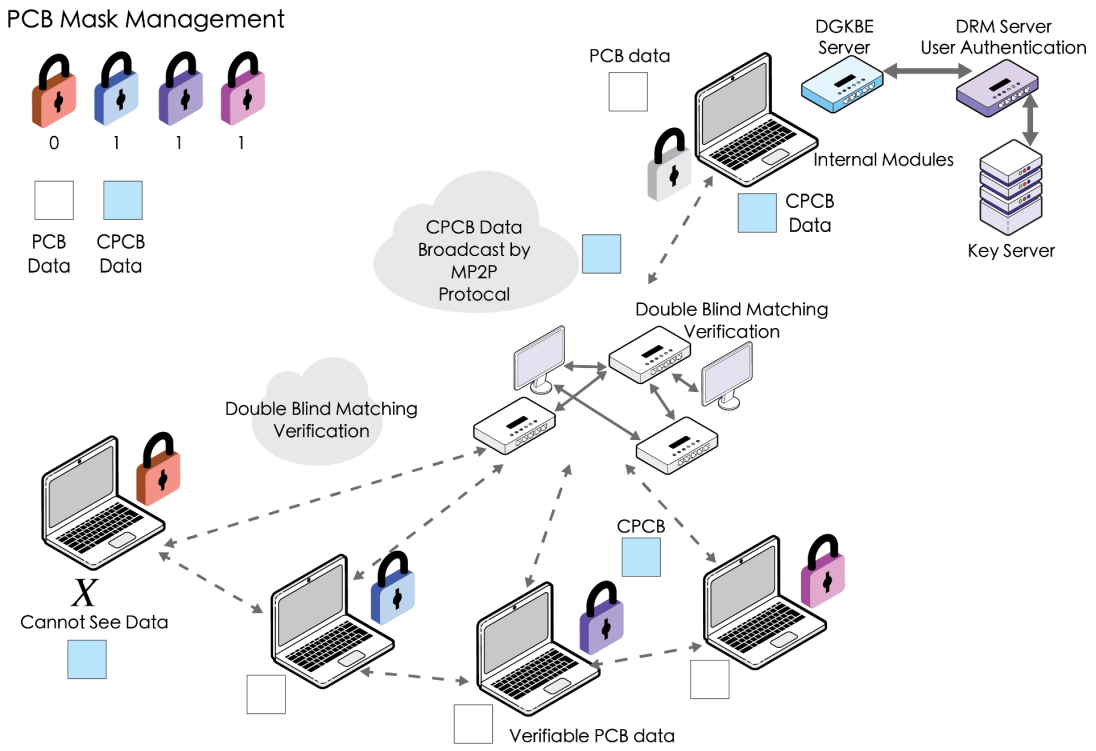


Figure: Differential Group Key Broadcast Encryption

DGKBE implements safe, reliable and efficient processing of user data for dApps (such as IoT/computers/mobile phones) on the blockchain platform. It enables CPCB data secure operations and can become an effective part of the chip solution to support the broad range of applications at the networking level.

DGKBE Security Model

A *Group Key Broadcast Encryption (GKBE)* is a tuple (Setup, ServEnc, Dec) where

1. Setup accept security parameter 1^{λ_s} to output public-domain parameters param which includes at least n the number of clients. Also it outputs the server secret $ServS$ which includes at least S_0 the initial list of clients, t_0 the initial randomness. It also outputs the client private keys $\mathbf{d}_1, \cdots, \mathbf{d}_n$.
2. ServEnc, the server encryption algorithm, accepts inputs param, $ServS$, $\mathbf{d}_1, \cdots, \mathbf{d}_n$, the list of valid broadcast receiving clients $S \subset \{1, \cdots, n\}$, randomness t, plaintext ptxt, to output ciphertext ctxt.
3. Dec accepts as input $i \in \{1, \cdots, n\}$, $\mathbf{d}_i$, ctxt to putput ptxt provided

$$\text{ctxt} = \text{ServEnc}(\text{param}, ServS, \mathbf{d}_1, \cdots, \mathbf{d}_n, S, t, \text{ptxt})$$

for some $S \subset \{1, \cdots, n\}$ and some randomness t. Its output is unspecified otherwise.

The GKBE (Setup, ServEnc, Dec) is correct provided the following holds

1. ServEnc (resp. Dec) can complete its computations to produce outputs with the specified inputs.
2. $\mathsf{Dec}(i, \mathbf{d}_i, \mathsf{ctxt}) = \mathsf{ptxt}$ when

$$\mathsf{ctxt} = \mathsf{ServEnc}(\mathsf{param}, ServS, \mathbf{d}_1, \cdots, \mathbf{d}_n, S, t, \mathsf{ptxt})$$

and $i \in S \cap S_0$.

Algorithmic Implementation :

Setup Upon input the security parameter 1^{λ_s}, it outputs finite field F_p where p is a prime power, elliptic curve $\mathcal{C}$, a rational point $g_0 \in \mathcal{C}$, $\mathrm{order}(g_0) = r$ which is a prime, group $G_1 = \langle g_0 \rangle$, pairing $\hat{\mathbf{e}} : G_1 \times G_1 \to G_T$, n the number of clients, server secret

$$ServS = \{g, \alpha, \gamma, S_0, t_0\}$$

client private key $\mathbf{d}_i = (d_{1,i}, d_{2,i}, d_{3,i})$ where $i \in \{1, \cdots, n\}$, $g_i = g^{\alpha^i}$, $v = g^{\gamma}$,

$$\begin{aligned} d_{1,i} &= g_i^{\gamma} \\ d_{2,i} &= g_i \\ d_{3,i} &= \prod_{j \in S_0, j \neq i} g_{n+1-j+i} \end{aligned}$$

ServEnc : Upon inputs param, $ServS$, $\mathbf{d}_1$, $\cdots$, $\mathbf{d}_n$, $S \subset \{1, \cdots, n\}$, randomness t, ptxt, it outputs $\mathsf{ctxt} = (C_0, C_1, C_2)$ where

$$\begin{aligned} C_0 &= g^t \\ C_1 &= (v \prod_{j \in S} g_{n+1-j})^t \\ C_2 &= (\prod_{j \in S \setminus S_0} g_{n+1-j})^{t/\gamma} (\prod_{j \in S_0 \setminus S} g_{n+1-j})^{-t/\gamma} \end{aligned}$$

Dec Upon inputs param, i, $\mathbf{d}_i = (d_{1,i}, \cdots, d_{3,i})$, $\mathsf{ctxt} = (C_0, C_1, C_2)$, it outputs

$$\mathsf{ptxt} = \hat{\mathbf{e}}(d_{2,i}, C_1) \hat{\mathbf{e}}(d_{1,i} d_{3,i}, C_0)^{-1} \hat{\mathbf{e}}(C_2, d_{1,i})^{-1}$$

Assume $i \in S_0 \cap S$, te output of Dec equals

$$\hat{e}(d_{2,i}, C_1)\hat{e}(d_{1,i}d_{3,i}, C_0)^{-1}\hat{e}(C_2, d_{1,i})^{-1}$$
$$= \frac{\hat{e}(g_i, (v\prod_{j\in S} g_{n+1-j})^t)}{\hat{e}(g_i^\gamma \prod_{j\in S_0, j\neq i} g_{n+1-j+i}, g^t)\hat{e}((\prod_{j\in S\setminus S_0} g_{n+1-j})^{t/\gamma}(\prod_{j\in S_0\setminus S} g_{n+1-j})^{-t/\gamma}, g_i^\gamma)}$$

The numerator equals

$$\hat{e}(g,g)^{t\alpha^i(\gamma+\sum_{j\in S}\alpha^{n+1-j})}$$

the denominator equals

$$\hat{e}(g,g)^{t\alpha^i(\gamma+\sum_{j\in S_0, j\neq i}\alpha^{n+1-j}+\sum_{j\in S\setminus S_0}\alpha^{n+1-j}-\sum_{j\in S_0\setminus S}\alpha^{n+1-j})}$$
$$= \hat{e}(g,g)^{t\alpha^i(\gamma+\sum_{j\in S_0, j\neq i}\alpha^{n+1-j}+\sum_{j\in S\setminus S_0, j\neq i}\alpha^{n+1-j}-\sum_{j\in S_0\setminus S, j\neq i}\alpha^{n+1-j})}$$
$$= \hat{e}(g,g)^{t\alpha^i(\gamma+\sum_{j\in S, j\neq i}\alpha^{n+1-j})}$$

Therefore, the output of Dec equals

$$\frac{\text{numerator}}{\text{denominator}} = \hat{e}(g,g)^{t\alpha^{n+1}}$$

5.5.3 Matching Computation Optimization

- Distributed M:N double blind matching problem

Suppose we have M research groups and N users. The research group collects computing power/funds/volunteers/product testers for scientific research projects based on user data matching. When the research group data and user data are double-blind to each other, how to conduct distributed double-blind matching calculation through distributed application on the ETD chain, so that the research teams can find the right users by using the help of all the ETD nodes for the M-by-N matching problem (computation, storage, and communication bandwidth resources) without data leakage of both parties?

- Double blind matching function assumptions

Matching optimization function conditions

- The matching distance function is logically separable and can use parallel algorithms (peer-to-peer distributed network computing model)
- Any complex function can be decomposed into a combination of basic logic operators of finite logic operators, such as sequence (E1; E2), parallel (E1∨E2), at the same time (E1∧E2), restriction (Any(n) E1) Etc., these logical operators are expressed by the function f, which can be the explicit function y=f(x) when the

causality is clearly known, or the implicit function f(x,y) = 0 when the causality is unknown

Matching optimization function data

- User data can be split and combined infinitely (arbitrarily). The computation of data splitting is relatively very small compared with the matching calculation or the network bandwidth resource (or even negligible), so user data can be split and combined arbitrarily or randomly
- PCB operators of the matching function for the arbitrarily split user data satisfy the commutative property of the operators under the double-blind matching condition. If this commutative condition is not met, there is a need to define the function of the composite operators for the data splitting computation, achieving data protection at extra computational cost, such as Weak Commutative Computability matching
- Compared to the complexity of double-blind matching, the amount of calculation for the authentication of the reverse verification of matching result is small. ETD uses an efficient differential group key broadcast encryption algorithm (DGKBE) to achieve the best O(1) verification algorithm.

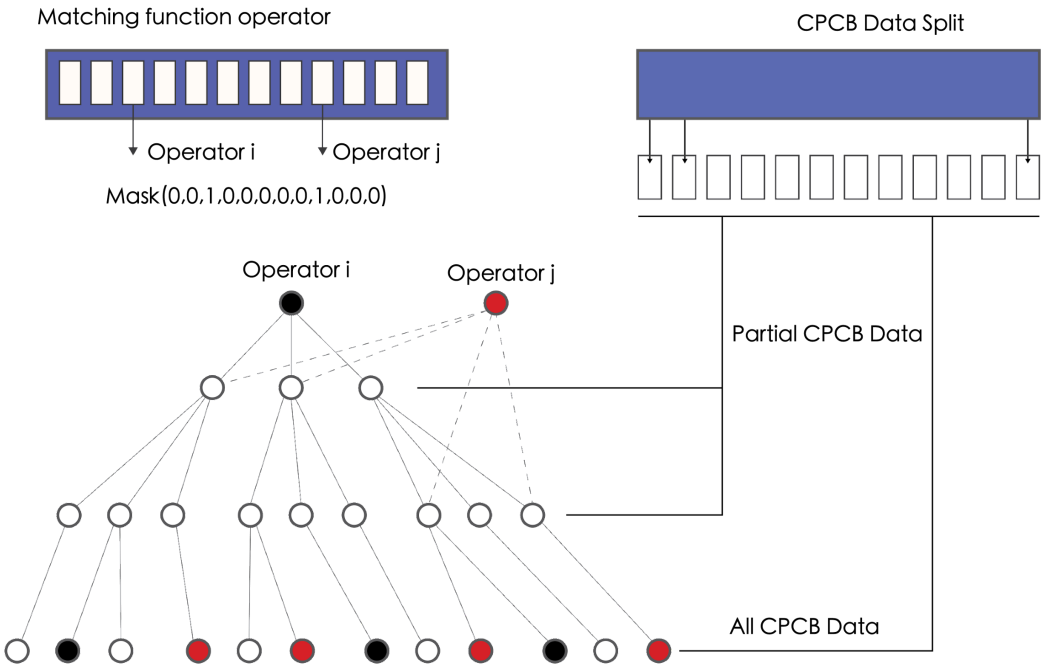


Figure: Double Blind Matching Operators

In the figure, operator i (black) has three double-blind matching, and operator j has four matching (red); all data are CPCB double-blind. The verification of the matching result is completed by the distributed calculation of the differential group key over the EMP2P network.

5.5.4 Technical Advantages

Through computing node resource control and distributed storage node data splitting, ETD decomposes the computing tasks of the distributed applications into exchangeable CPCB operator calculations, enabling the asynchronous data-oriented consensus computation. The internal state of the ETD node can only be changed by passing smart contract messages. The transmission of data and the sending of messages will not be blocked. Distributed calculations and applications can be effectively arranged in parallel on multiple threads over different machines, giving efficient utilization of the CPU and GPU resources in the distributed cloud of computing nodes and storage nodes.

ETD public chain has higher performance:

- Improve storage read and write performance: calculation/storage is the computing mechanism. Distributed calculation/storage realizes an efficient matching operation under the protection of encrypted PCB, instead of complex calculation (encryption operation + propagation + decryption operation + matching operation) multiplied by N*M, ETD realizes (O(1) cryptographic matching operation) * logN * logM calculation. Data storage changes from N *Size L * replication factor K (generally K is the range of tens such as in IPFS) to CPCB's (logN)^2 * (logL)^2 * k (here k is greater than 1 but less than 1.2 ~ 1.3).
- Improve communication performance: The improvement of communication performance is achieved under the condition of ensuring data protection. Merkel tree cannot provide adequate support for encrypted data computation (e.g. sub-tree branch search and comparison). Crypto PCB uses a differential group key broadcast encryption algorithm to bind data encryption and data structure optimization to achieve O(1) data communication requirements (compared to data structure of other blockchains using Merkel tree or DAG diagram with O(logN) requirements).
- Improve public chain data computing performance: 1) Comprehensive optimization goals of computing/storage/communication; 2) Crypto PCB's key distribution mechanism avoids the transmission and distribution of keys, and improves security and computing efficiency; 3) Customizable computation and storage/communication modules; 4) Composite PCB algorithms resistant to statistical learning; 5) Parallel subdivision operators of matching functions, supporting parallel algorithms and intermediate/partial matching results; 6) Random/arbitrary subdivision of PCB data for distributed storage supporting recombination and composite operators for data in encrypted state, with tradeoff of calculation and storage; 7) Support PoC/PoE consensus mechanism, and generic or customizable consensus algorithms.

Only the result of the double-blind matching operation is written to the chain, and the matching functions use crypto PCB cipher text *ctxt* and related parameters such as matching mask *S_i* for request *i*, where *S_i* is binary mask of size N (of total N users). *ctxt* and *S_i* info will be included in the block data. Any users whose corresponding binary value is "*True*" at the corresponding position in *S_i* will be able

to decrypt cipher text using his crypto biometric input data and verify the request i satisfy his condition. At the same time, other nodes whose binary value are "*False*" will not be able to decrypt the cipher text, hence will not know the content of the request *i*, nor will he be able to see other users' private data.

Due to the data encryption feature of the double-blind PCB matching, the ETD computing platform can effectively resist malicious attacks from the network (the cost of the attack not only consumes computing resources, but also consumes network bandwidth and storage resources. Because of the data encryption characteristics, it is difficult to launch a targeting attack on a specific node or application/service, unless the data is decrypted first). Therefore, the distribution of the computing resources can be adaptively set for the distributed applications. In the computing environment of double-blind matching, nodes can accumulate and analyze historical data. Even in the case of double-blind, they can still store high-frequency service requests or high-frequency paired users through machine learning (although they do not know the exact data of the service or username due to the data encryption). If nodes only store high-frequency data or requests, the system will lose fairness as the performance for low-frequency services and users may be reduced. To ensure service quality, the reward for low-frequency data can be improved, or the computing resources are set to fluctuate within a given range (for example, between 30%-50%) to ensure sufficient computing power and storage for any high and low frequency matching calculation needs. In addition, nested PCB (composite PCB, or PCB of PCB, i.e., PCB (PCB) algorithms) can be introduced. Since PCB function f is a double-blind operation for user data, another double-blind function g is introduced to generate $g(f(X)+p)$, where p is a system random parameter. It will make it meaningless for any node's historical big data analysis or machine learning of the PCB function f (similar to asynchronous randomization algorithms).

ETD has an independent smart contract system, which is compatible with Ethereum smart contracts in general, and provides a set of instructions including stack operations, process control, logical operations, arithmetic operations, cryptographic operations, string operations, and array operations etc. ETD can create independent virtual hardware and open it to smart contracts in the form of interfaces, so that the contract can obtain platform-related data, distributed storage, and other network resources at runtime. Since the PCB has a hardware-level security mechanism, it can ensure that the behavior of the contract is safe and controllable, and the security can be improved by properly programming virtual hardware.

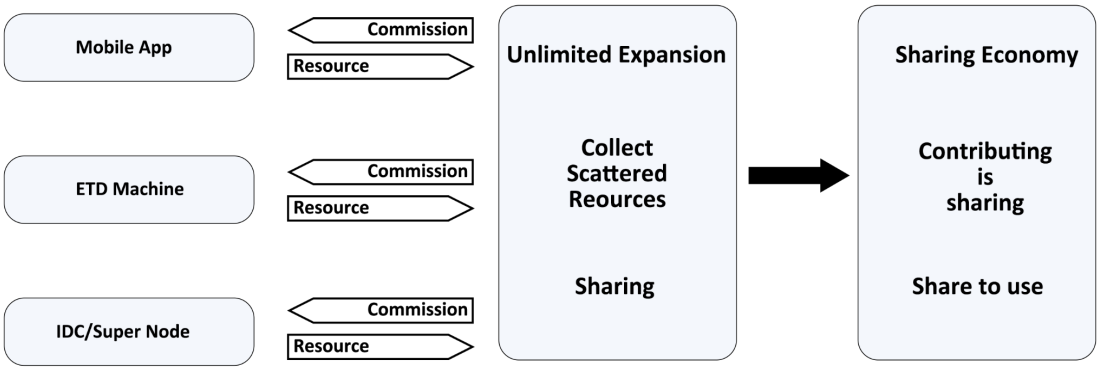


Figure: ETD Sharing Distributed Cloud

5.6 ETD Computing Node

ETD adopts a distributed network architecture. The network is built on a concurrency framework and consensus mechanism based on the sharing public blockchain platform with distributed intelligent computing model. The nodes are running a point-to-point (P2P) network structure. There are two types of nodes in the network, computing nodes and committing nodes. Computing nodes can run programs, perform calculations, broadcast, receive and forward transactions, synchronize blocks, etc., while committing nodes participate in distributed consensus and create blocks. The committing node is the core role of the blockchain, which saves complete historical data and listens to broadcast transactions. The committing nodes in the ETD system are distributed to many mining pools with mining power around the world.

The ETD computing nodes from the sharing contributors are crucial to maintaining the system computing power and overall security. On public chain platforms such as Bitcoin and Ethereum, mining contributors obtain accounting rights and ledger rewards through PoW or PoS mechanism (equivalent to ETD's PoC and PoE). The consensus mechanism is to ensure the security, reliability and consistency of the ledger. The public chain itself does not provide any complex or useful computation services at the application layer. Although Ethereum has simple smart contract calculations, complex computation will be extremely expensive because of the replication of calculations over all the nodes. For example, GAN or neural network learning algorithms cannot be supported. The data source is severely limited and must be provided by on-chain nodes, or third-party Oracle services. It does not support the P2P distributed storage network model. The PoC/PoE mechanism of the ETD unifies the distributed computing and storage model on the public ETD chain. The matching calculations of computing resource contributors solve the computing and storage problem of distributed applications, and at the same time they provide the consensus mechanism ensuring the security, reliability and consistency of the calculation and storage ledger. Therefore, any valuable computing/storage/network resources are not only used to generate ledger but are also used to solve actual application problems and provide accounting functions. Each node is both a user, and a contributor to the computing power of the overall system. User can choose any distributed computing strategy, distributed storage strategy, and peer-to-peer network communication strategy to maximize his computing efficiency and financial

return, and at the same time achieve the effective matching with the required distributed calculation and data storage.

For example, user A has an advantage over matching apps promoted by online e-commerce merchant B (A may have marketing resources or excellent customer networks), A can optimize the use of his limited computing and storage resources to support the matching strategy function f promoted by the merchant B. A can widely promote the matching strategy f to the ETD chain and receive double-blind matching results quicker and broader.

The computing power of ETD hardware depends on the number and types of node's computing cores, as well as the size of memory and data storage space. Since storage space can be used to store intermediate or temporary calculation results, therefore, the storage space can be used as a tradeoff for a certain amount of computing power, and vice versa. Since the stored data may be used by multiple computing units (like multiple read), but the computing resource once used for one specific computing task, in general it cannot be used for another computing task at the same time (like Proof of Work), hence the storage capacity is a more flexible and versatile recording unit when denominating resources and capabilities for the static computing power of the ETD nodes. The actual dynamic computing power of a node machine is comprehensively determined by the storage (the total amount of hardware, access speed, and network location etc.) and the computing unit bound to it, and usually is determined at the runtime. Nevertheless, such value can be estimated from historical data. Because the blockchain's ledger is immutable, the estimated value can be easily verified by every node on the blockchain. In general, an all-purpose ETD node uses static 4T storage as a unit, and can have three configurations of 4T, 8T, and 16T. The computing power of 4T machines at the user's premises is bound by its dedicated hardware CPU/GPU. The 8T and 16T machines can be remotely paired with any CPU or graphics card scattered in the network to perform general computing tasks. The greater computing power a node has, in general the more tokens it may generate.

6. Token Issuance

6.1 Token (ETD Coin) Referred to as ETD

ETD is the native token on the Ether Data Blockchain, and the ways to obtain it include:

- Complete scientific computing tasks through environmentally friendly ETD machine
- Within the ETD ecosystem, it can be obtained through voluntary circulation channels such as transfer from others, dApp rewards, etc.
- Transfer via other crypto exchanges or e-wallets

6.2 Block Generation Rules

The planned mining volume of ETD (Ether Data) is 2,100,000,000 (2.1 billion) coin units, which is halved every 2100 days. In theory, it can be mined for more than 100 years.

Mining rule plan:

Year	Block/ day	Block output	Daily output	Annual output	Total output
1	8640	57.87	500000	182500000	182500000
2	8640	57.87	500000	182500000	365000000
3	8640	57.87	500000	182500000	547500000
4	8640	57.87	500000	182500000	730000000
5	8640	57.87	500000	182500000	912500000
6 (7.5 months)	8640	57.87	500000	112500000	1025000000
6 (4.5 months)	8640	28.935	250000	35000000	1060000000
7	8640	28.935	250000	91250000	1151250000
8	8640	28.935	250000	91250000	1242500000
9	8640	28.935	250000	91250000	1333750000
10	8640	28.935	250000	91250000	1425000000
11	8640	28.935	250000	91250000	1516250000
12 (5 months)	8640	28.935	250000	37500000	1553750000
13	/	/	/	/	/
14	/	/	/	/	/
15	/	/	/	/	/
16	/	/	/	/	/

1 block every 10 seconds. The system generates 8640 blocks per day. There is 0 pre-issued ETD coins. All coins are generated through the mining process. Mining machines are divided into three types, namely, the household mining machines with a hashrate of 4T, mining pool machines with a hashrate of 8T, and merchant mining machines with a hashrate of 16T. In the first 5.75 years, it is planned to invest 500,000T of hashing power every year, and it is estimated that 1T hash power can mine one coin per day. Subsequent annual plan for investment computing power will be halved for every 5.75 years.

6.3 Distribution Rules

- In order to promote the ecological operation of ETD, the total supply of ETD is 2.1 billion, and there will never be additional issuance. The number of coins each block produces will be halved every 2100 days. The specific distribution rules are as follows:

- 75% for processing power contributors
- 15% for application value contributors
- 5% for the ETD global science and research foundation (allocated by the Community Governance Committee)
- 5% for operation infrastructure construction and maintenance

- Contribution will start whenever the machine is connected to the ETD network. To protect the stable operation of ETD as a globally distributed supercomputer and to avoid exploitation by speculators, machine owners are required to pledge according to the following rules:

- Pledge 100 tokens per T to get normal computing power.
- Lock-up period is 540 days.
- Every time the production is halved, the pledge is doubled. If the pledge is not increased, the mining income will be reduced by 50%.

6.4 Governance Mechanism

In the ETD ecology, all contributions will be incentivized by ETD coins, and at the same time, all the use of resources needed to consume ETD coins. ETD incentive rewards are distributed by the consensus mechanism according to the contribution weighting factor, while the consumption of ETD is measured by the specific use of resources.

ETD is a standard for measuring value transmission, and it is also a basic asset for measuring other derived assets in the ETD ecology. ETD should encourage contributors to develop better applications and innovations to maximize the value of the entire ETD ecosystem, and to guarantee the value of assets of those contributors who have lost the ability to continue contributing.

6.5 Locking Mechanism

The processing power contributors and application value contributors can obtain 20% release of the ETD earned on the same day, and the rest will be released at the rate of 1/180 per day. When releasing holdings, all ETD tokens are automatically distributed by smart contracts without human intervention.

The lock-up period of ETD obtained by the ETD science foundation and operation infrastructure maintenance is 1 month. After 1 month, the tokens are released at the rate of 10% each month. When releasing holdings, all ETD tokens are automatically

distributed by smart contracts without human intervention.

7. Ecosystem Construction

ETD is the underlying technical infrastructure of distributed computing clusters, which provides strong technical support for the development of decentralized applications and will eventually develop into an ETD ecosystem. The global ETD community of scientific and research collaboration ecology and continuous talent training are important factors for realizing the ETD ecosystem.

7.1 Construction of ecological network

The ETD public chain system aims at the pain points of the industry and provides innovative solutions for enterprises and application developers based on public chain technology, which can build and develop system applications to serve the real economy. It is consistent with the industry trend in terms of combining industry applications, talent training, open-source system, incubation accelerator, etc., making the use of blockchain systems more convenient, lower cost, and more flexible to choose application modules.

ETD is committed to building a public ecological chain, through talent, funds, and other communities to provide full support of the industry needs. ETD is committed to accelerating the implementation of blockchain applications and boosting the high-quality development of traditional industries. In terms of application areas, ETD will combine high-tech science and technology such as artificial intelligence, big data, virtual reality, robotics, Internet of Things, cloud services, etc., for applications in intelligent manufacturing, health care, transportation, intellectual property protection, new energy vehicles, organic agriculture, distributed energy, food, commerce, finance, and other industries, to provide a solid blockchain infrastructure for these application scenarios, and support enterprises to move onto the blockchain, realize the deep integration of blockchain technology and industrial applications to improve the efficiency and reduce the operating cost.

The ETD public chain adopts the new PoW+DSB PoS blockchain architecture and is positioned as an easy-to-use high-performance blockchain platform, aiming to achieve performance expansion of distributed applications to meet the needs of the real world. The high cost of enterprise R&D and application development is one of the bottlenecks restricting the industrial adoption of blockchain technologies, especially the public blockchain. The ETD public chain enables enterprises to develop various applications and services based on the ETD ecological network by providing stable and efficient infrastructure, standardized and modular application plug-ins, and full-process technology and business model consultation.

7.2 Chain Delegation and Chain Settlement

The trust mechanism is an important part of the underlying technology of the blockchain. ETD uses this as the cornerstone in the process of digitizing value assets

to build the entire ETD ecology. Equity custody (chain custody), a qualified third-party institution is used to custody equity assets and all data is written to the blockchain. Equity settlement (chain settlement), using qualified third-party institutions to settle equity assets and write all data to the blockchain.

7.3 Cross-chain Payment and Circulation

The ETD obtained by users from any channel (including contributing processing powers, consumer terminals and applications, trading platforms, etc.) can be freely traded in the ETD ecosystem, and seamlessly connected to other trading platforms for cross-chain digital assets to achieve free exchange and circulation.

7.4 ETD Committing Node

The ETD committing node is a multi-crypto mining pool based on the PoW+DSB PoS consensus mechanism, which supports the computing and storage functions running of the ETD public chain to provide one-stop general computing services.

ETD main chain has the potential for diversified uses, and the value of processing power is further enhanced through technology to bring higher returns to users. In other words, the computing resource can be used to do multiple things. Contributors can participate in the pools through delegated voting to obtain mining rewards. Contributors can become ETD committing node candidates through election. In future, after more general computing services based on PoW+DSB PoS consensus mechanism come online, contributors can also participate in computing through delegated voting to obtain tokens.

7.5 Incentives

The traditional peer-to-peer communication network focuses on information transmission. It is a bit like the applications on the Internet 1.0 era. They are all open and shared. However, they have not achieved the striking effect of blockchain technology. Blockchain’s effective consensus mechanism renders the distributed nodes to work collaboratively. And more importantly, because the behaviors of nodes are driven by the economic rationale behind, an invisible binding force on individual nodes is established for them to achieve the common goals together.

The Bitcoin network uses the PoW (Proof of Work) consensus mechanism to incentivize nodes to participate in the mining process by obtaining accounting rights through contributing mining calculations to obtain Bitcoin rewards. The token economic model is the core value of the blockchain. Ethereum is based on the same underlying consensus mechanism, allowing smart contract developers to issue their own tokens and use ETH as the GAS fee to pay for consensus computing costs, which not only unifies the measurement of consensus costs, but also allows for the same consensus cost to benchmark different value outputs according to the application ecology used by the token. The application users can estimate the best balance point of investment and return.

From the perspective of ETD, all services have a source from which its value is derived. Because the essence of the blockchain platform is a fair value exchange and circulation market, the fundamental layer of all economic activities lies in the transaction costs. ETD is the carrier of transaction costs. At this level, ETD tokens will be used for the following incentive purposes:

- Committing rewards
- Computing contribution rewards
- Processing roles involved in the operational incentives for algorithm providers (in the form of issuing smart contracts)
- Developers in the ETD ecosystem will receive ETD rewards for the actual value generated by their developed applications. Such rewards are used to actually subsidize their consensus accounting work or computing cost in supporting the applications.
- Users can also add various application requests or computing targets to the ETD ecosystem.

The operation of the ETD ecosystem is inseparable from the support of each node to the network. In a fully decentralized network, the ETD system hopes to create more nodes to maintain the stable operation of the ETD network.

The ETD node is a full node that provides continuous services for the entire network. It is necessary to deposit 100 ETD units into the ETD address as a binding for every 1T hash power, as a deposit for participating in the construction of mining nodes, in order to participate in node mining reward generation. The deposit can be kept in the local offline wallet to completely ensure the safety of funds. Both ordinary addresses and multi-signature addresses can be used. When a node is activated, it can provide various data services for the network, and get reward in the process. The increase in the number of nodes will generate a demand for ETD to be used as deposit, which effectively balances the supply of ETD in the trading market and provides support for the continuous appreciation of ETD.

8. Token Application Scenarios

8.1 Time Banking

Following the traditional value of time-based currency, ETD is a distributed universal computing cluster with the core concept that the price per unit of computing power from each contributor is equal. ETD Time Bank offers a more diversified and cheaper service than traditional banks for contributors, including three categories of services:

- Wallet - Retail banking services including token deposit and withdrawal, quick transfer, collection and receipt of bills, exchanging ETD and other cryptocurrencies.

- Financial Service - any business models in traditional financial markets can be implemented in the ETD ecosystem, such as financial management, lending, payment, insurance, quantitative trading, disposal of non-performing assets, installment loans, crowdfunding, M&A or asset restructuring of listed companies, market value management, etc.
- Fintech on Chain - Uploading financial data to the blockchain, risk control models on the chain, ecological system credit scoring on the chain, and financial assets on the chain.

8.2 Smart City

- Industrial Clusters - Massive dApps based on the cutting-edge smart contract tools provided by the public chain will organize themselves into an industrial cluster that can promote online and offline integration, improve multi-domain collaboration and service experience.

- Fundraising and Investment - Projects in the planning stage can publicly raise tokens, which can be used to exchange for processing power or for various services provided by ETD platform, such as cloud computing, data hosting, financial services, etc., with fewer red tape and lower costs to start a business. At the same time, it will be easier for investors to inject capital into projects. Contributors will also be able to exchange ETD tokens for other currencies they need.

- Enterprise Blockchain Reform - Compared with other blockchain platforms, ETD has significant advantages in terms of security, reliability, efficiency, and flexibility. Enterprises will benefit from transforming their existing business models with ETD technologies to form an interconnected, interoperable and mutually supportive ecosystem on blockchain.

9. ETD Foundation

The Foundation will engage in ecological construction and investment activities with ETD blockchain at its center, including the issuance and management of financial products, publication of community news, blockchain IPOs, equity investments, and doing research on token economy to guarantee that tokens held by all the contributors is stable in value and free in circulation. The Foundation will also be responsible for the future expansion of ETD open-source software architecture and meeting the requirements of ESG standards (environmental, social and corporate governance).

9.1 ETD General-Purpose Computing Lab

We plan to cooperate with universities and their affiliated scientific research institutions around the world to establish ETD General-Purpose Computing Labs, in

which ETD machines and a full node of blockchain will be allocated, so that research teams who cannot afford to purchase/rent supercomputers on their own can now connect to ETD platform through the node to get computing and storage power equivalent to accessing a supercomputer. The labs will share each other's computing power. The tokens obtained in this process will go directly into the Lab's processing power pool for further R&D activities and the commercialization of corresponding technologies and inventions.

Labs can use ETD modular tools to easily transform their inventions into user-friendly online applications that provide service to the general public (paid or free). Scientists no longer need to bear the cost of hiring software developers, marketing personnel, and financial personnel to commercialize their knowledge and get rewards that match their efforts. At the same time, collected user data can in turn help scientists to continuously improve and optimize their research work, which means that if a research team needs a lot of data/volunteers (such as natural language processing; medical, historical and social science subjects related to human genome database, etc.), then they can pay ETD tokens to collect data or recruit volunteers around the world at a lower cost compared to traditional methods. Because ETD has extraordinarily good privacy protection and anonymity mechanisms, volunteers do not need to worry about the potential leakage of their data.

As a responsible manager, the ETD foundation will examine and select the partner universities based on three criteria: comprehensive research strength, research capabilities in chosen fields, and the ability to make breakthroughs in current and emerging areas.

9.2 Innovation Incubator

We will adopt the Silicon Valley model to build a world-class tech-startup incubator -- a decentralized, distributed and self-organized virtual Silicon Valley which is scattered around the world and is no longer limited by the constraints of physical space. Its function is executed through the blockchain's smart contracts and DAOs, which greatly improves efficiency and reduces costs. Its economic value is reflected in the collaborative sharing platform of participants and ultimately leads to a win-win situation. In the long-term, this may have a chance to become a global model for scientific research discoveries via more affordable and readily available technologies.

The ETD foundation connects the scientific community with professional investors, including venture capitals and investment departments in technology corporations. Investors can choose to donate or invest together with the foundation to set up a general-purpose computing lab, or they can invest in specific research projects. They will save legal fees and access more opportunities at a much earlier stage. If an incubated project is commercially successful, profits may be distributed among the research team, the investors, and the foundation (for further incubation investment).

It is worth mentioning that we pay special attention to environmental and climate

sciences. Firstly, because its object of study is the foundation of the entire human economy and civilization. Secondly, indicators such as the diversity of marine life and the cleanliness of the atmosphere are difficult to measure and cannot be traded. It is difficult to find a prototype in the traditional financial world to help with the practical application of its research results. The foundation will cooperate with scientists in the field to explore the feasibility of natural resource token economy, to design a special financial incentive mechanism, and to make natural resources (or specific indicators) crypto assets on the blockchain, so as to obtain open and credible quality assessment, transparency and tradability, to avoid the tragedy of the commons.

10. Team members

Nikolay Tasev, Co-founder of the Ether Data Foundation. Nikolay is a programmer, cryptologist, cryptographer and cypherpunk. Nikolay dedicated his effort in advocating widespread use of strong cryptography and privacy technologies to enhance the welfare of individuals and society. At a very young age, he won two-time hackathon titles and one of his apps was adopted by a leading social network company which valued it over $50 million. He was the core system programmer for an early open-source mobile operating system way before Android became the industry monopoly. Nikolay pioneered the security work by binding physical unclonable functions with public-key cryptography which has contributed to the development of pseudo randomness, zero knowledge proofs, secure random functions, and other areas in the practical implementations of the cryptography algorithms. His research interests lie within the interplay of computational complexity, cumbersome security, substance randomness and inconsistent human nature of fallacy and imagination.

Robert Bo Collins, Advisor of the Ether Data Foundation. Collins is an active entrepreneur and blockchain practitioner, currently serving as Chairman of MGH Group (Mercantile Global Holdings) and CEO of its bank, Mercantile Bank International. He founded the San Juan Mercantile Exchange and its partner bank San Juan Mercantile Bank & Trust International in 2019 to provide cryptocurrency and fiat currency trading and custody services to institutional clients. Collins is also the former president of the New York Mercantile Exchange (NYMEX). He led NYMEX to obtain the S&P credit rating of A++ and was named the "Deal of the Year'' in 2004 by "Energy Risk" magazine. NYMEX went public in November 2006. Collins also established MotherRock' energy trading hedge fund in 2005, which has conducted several highly leveraged transactions in the natural gas market. Collins is also the head of the International Derivatives Clearing Group (IDCG). Before joining NYMEX, Collins was the senior vice president of natural gas trading at El Paso Corp. He has worked at Federal Reserve.gov in Dallas.

Michael Gaard, Co-founder of the Ether Data Foundation. Michael has extensive experience in IT strategy, business transformation, software development and service delivery. Mike was a financial services partner of Andersen Consulting (NYSE: ACN Accenture.com) and PWC (PWC PwC) and was responsible for the North American

Retail Banking Advisory Services Group. As a member of the Information Advantage management team, he has gained leading software development and deployment experience, which is responsible for data warehouse practices in the healthcare and financial services industries. Mike leads Unisys' North American financial services business as the general manager of the retail banking department. He is currently the head of Contata Solutions' corporate marketing services team.

Hans-Arno Jacobsen, Advisor of the Ether Data Foundation, IEEE Fellow, Professor of Computer Engineering. He directs and leads the research activities of the Middleware Systems Research Group (msrg.org). His research aims to ease the development of scalable, reliable, and secure ultra-large-scale distributed applications. In pursuit of these objectives, he engages in basic research on event processing, publish/subscribe, service-orientation, aspect-orientation, and green middleware. In research and development engagements with various companies, he pursues projects on large-scale business process management, service delivery models, service and infrastructure management, and e-energy.

Timothy Parez, Technical Advisor of the Ether Data Foundation, Inventor of QBKEY. Parez is from Belgium and started working with computer hardware devices at the age of 7 and wrote his first software at 13. He is an expert in data and network security and a leader in the field of cryptography. He has worked as a security consultant for companies such as Microsoft, Adobe, Ubisoft and Canonical, specializing in communication protocol design, embedded systems and cross-platform software solutions. He designed QBKEY, a portable biometric data encryption device with an embedded fingerprint sensor for individuals and businesses to encrypt and manage data, securely share and browse files, and support any local storage device and cloud storage services. His current company provides OEM service for Apple, Dell and other technology giants and automotive brands.

11. Risk warning and disclaimer

11.1 Risk warning

Systemic risk: refers to the possible changes in returns due to the overall common factor, which affects the returns of all securities in the same way. For example, policy risk-digital assets have entered supervision in some countries in the world. If the judicial institution's policy changes, there is a certain possibility that participants will lose due to policy reasons; in the market risk, if the overall value of the digital asset market is overestimated, Then the investment risk will increase, and participants may expect the project to grow too high, but these high expectations may not be realized. At the same time, systemic risks also include a series of force majeure factors, including but not limited to: Natural disasters, large-scale failures of computer networks worldwide, political turmoil, etc.

Risks between teams: There are many teams and projects in the current blockchain technology field, and the competition is fierce. There is strong market competition and project operation pressure. Whether the ETD project can break through many

excellent projects is widely recognized, not only linked to its own team capabilities, vision planning, etc., but also affected by many competitors and even oligarchs in the market, and there is the possibility of facing vicious competition.

Project coordination and marketing risks: The ETD team will spare no effort to achieve the development goals set out in the white paper and extend the project's potential for growth. At present, ETD has relatively mature business model analysis. However, in view of the unforeseen factors in the overall development trend of the industry, the existing business models and overall planning ideas do not fit well with the market demand, resulting in unsatisfactory profitability. At the same time, since this white paper may be adjusted as the details of the project are updated, if the updated details of the project are not obtained in time by the participants, or the public is not aware of the latest progress of the project, the participants or the public may be concerned about the project due to asymmetric information. Insufficient cognition affects the follow-up development of the project.

Technical risks of the project: First, the project is constructed based on cryptographic algorithms, and the rapid development of cryptography is bound to bring potential risks of being cracked; secondly, technical support such as blockchain, distributed ledger, decentralization, and disapproval of tampering With the development of the core business, the ETD team cannot fully guarantee the implementation of the technology; again, in the process of project update and adjustment, vulnerabilities may be found, which can be compensated by issuing patches, but the extent of the impact caused by the vulnerabilities cannot be guaranteed.

Hacking attacks and crime risks: In terms of security, the amount of a single supporter is small, but the total number of people is large, which also puts forward high requirements for the security of the project. Electronic tokens have the characteristics of anonymity and difficulty in traceability, and are easy to be used by criminals, or attacked by hackers, or may involve criminal acts such as illegal asset transfers.

Other risks currently unknown: With the continuous development of blockchain technology and the overall situation of the industry, ETD may face some unforeseen risks. Participants are asked to fully understand the team background, understand the overall framework and ideas of the project, adjust their vision reasonably, and participate rationally before making participation decisions.

11.2 Disclaimer

The introduction and explanation of the basic situation of the ETD project in this white paper is not and cannot be regarded as an offer or promise for investment or cooperation with any specific or unspecified subject, and it is not and cannot be regarded as a commitment or guarantee of the project by the project team. The project team reserves all rights to modify, delete, add, repeal, explain and other related actions in this document. Those who have the intention of participating,

investing, or cooperating in this project must clearly understand all the risks of this project. Participants should enter into a written cooperation agreement to participate in this project, and the cooperation agreement should clearly, complete and clearly specify the cooperation, participation or investment matters. Participants shall indicate in written or verbal form that they have fully understood and accepted all the risks that the project has generated or may generate, and bear corresponding responsibilities.

Before you read and use this document, you should understand the following precautions: This document should not and cannot be regarded as the content, standard or condition of project cooperation, investment or any contract. The formation, change and elimination of any legal relationship between project participants and the project team shall be subject to the written contract. The ETD referred to in this project, as a digital asset that is not on the project team's server, has complete and independent value from the project team. Its value depends entirely on the recognition of its use value and exchange value by relevant market entities. It is not and should not be considered bonds, securities or any form of marketable securities, and it is not the equity, shares, ownership or control of the project team or the company. Based on the ETD generated by this project, the value of ETD is affected by the market environment and the degree of recognition of market entities, and the project team cannot and cannot guarantee the value of ETD. ETD has the risk of loss, tampering, theft, and deception. The project team cannot guarantee the custody, recovery, and modification of related virtual property. In view of the changes in the regulation of blockchain technology, encrypted currency or intangible property by governments around the world, the project team reserves the right to modify, delete, add, or abolish part or all of the contents of this document at any time in accordance with the laws and regulations of each region and actual conditions. You confirm that you can make your own judgment on the content of the project team and project services, and bear all risks arising from the use of the content of this document, including the risks arising from the reliance on the correctness, completeness or practicality of the content of this document. The project team cannot and will not be liable for any damages caused by your own actions.