Bit Ecological
Digital Asset

Bit Ecological Digital Asset

Bit Ecological Digital Asset

Abstract: Bitcoin, as a peer-to-peer electronic cash system, started a revolution in 2008. Her revolution started with the most basic value measurement and value storage of human society, overturning the existing economic system and financial system, and starting the journey of building a more open, fair, transparent and efficient value Internet. On the basis of the Bitcoin core-PoW consensus algorithm, subsequently amateurs and professionals have made explosive research progress, and the competition between all parties has promoted the prosperity of the encrypted digital industry. We propose Bit Ecological Digital Asset ("BED"), which uses a hybrid consensus algorithm of Proof of Work (PoW) and Proof of Stake (PoS) to ensure the security and fairness of the blockchain network, At the same time, anonymity technology development and off-chain transaction system development have been added to protect user transaction privacy and meet large-scale commercial micropayment needs.

Content

1 Foreword

Bitcoin's latest network-wide computing power is approximately 140 billion hash collisions (140E) per second, which is 140 times that of the beginning of 2016 and 1.4 trillion times that of the beginning of 2012. In the next 10 years, Bitcoin's computing power will reach a new order of magnitude, which will surpass everyone's imagination.

Behind the explosive growth of Bitcoin's computing power is the exponential jump in the performance of mining equipment. From the earlier FPGA mining machines, ASIC mining machines began to appear. The chip technology design has been continuously upgraded from 110nm, 55nm, 28nm, 16nm, and 7nm. The current 5nm competition, and the upcoming 3nm era.

So, why pursue such a powerful computing power? Speaking of ultimate meaning, from the nature of science, having more computing power is more meaningful than having more money. Computing power removes the weight of human nature in the entire ecosystem. In the future, it may go beyond carbon-based will and become a network protection net that we can't even imagine.

However, because of the inherent algorithm of Bitcoin, the equipment behind such a powerful computing power-the mining machine, once a new mining machine appears due to technological progress, the old equipment mining hardly benefits, it becomes a broken copper and broken iron. , Worthless. Because the chip technology of Bitcoin mining machines is developing rapidly, behind its exponential increase in computing power is a large number of old equipment being scrapped and rendered useless. This is a great waste of the human society.

Is there a way to increase the life cycle value of mining machines? We proposed the Bit Ecological Digital Assets (BED), which aims to design and develop an encrypted digital currency system with the second largest computing power in the encrypted digital ecosystem.

2 BED Vision and Mission

The blockchain relies on different consensus mechanisms and procedures to determine who will submit and verify each new block. The blockchains of crypto assets such as Bitcoin, Litecoin, Monero and Zcoin all rely on PoW consensus algorithms and specific consensus protocols, such as the Satoshi Nakamoto consensus of Bitcoin.

The competition of miners is crucial to the security of the blockchain protocol under the PoW consensus algorithm. Miners have limited resources and must allocate computing power to the blockchain with the highest expected income. Therefore, computing power has also become a very precious resource. As early as 2011, some people began to explore the issue of more effective use of computing power. At that time, there was also an attempt at hybrid mining (referring to the behavior of mining two or more cryptocurrencies at the same time without sacrificing the overall mining performance). Auxiliary computing power proof of work (AuxPoW) provided an implementation for hybrid mining Proof of work (AuxPoW) is the possibility of auxiliary computing power (AuxPoW): a kind between two blockchains that makes one blockchain believe that the workload of the other blockchain is its own, and accepts auxiliary workload proof blocks Relationship.

The first cryptocurrency to adopt a hybrid mining model was Domain Name Coin (NAME), which was launched in April 2011, and its hybrid mining took place at block 19,200 (October 2011). Since then, other cryptocurrencies have also adopted hybrid mining. Some cryptocurrencies even use multiple hash algorithms, such as Myriadcoin (XMY), which supports 5 different algorithms (SHA256, Scrypt, Myr-Groestl, Argon2d and Yescrypt).

Dogecoin (DOGE), launched in December 2013, made hybrid mining hot. Dogecoin adopted hybrid mining in block 317,337 (July 2014). Recent examples of encrypted assets such as Elastos (mixed mining with Bitcoin) remind people that mixed mining as a concept is not outdated and can be used for further research on existing and future PoW blockchains.

However, the hybrid mining method has not achieved great success in general. So far, there has not been a strong computing power and widely used cryptocurrency. The domain name coin (NAME) has long disappeared in the long river of history. Dogecoin (DOGE) is still just a plaything of a small number of people, most of the others have not even heard of it. The hybrid mining mechanism fails to give the mining machine greater life cycle value.

The fundamental reason behind it: Because computing power is selfish, only selfish computing power can guarantee the security of the blockchain and ensure the loyalty of miners.

To this end, we have proposed a brand-new concept, using mining machines eliminated from the Bitcoin network or brand new Bitcoin mining machines to maintain a new blockchain system-Bit Ecological Digital Assets (BED). She will learn from others and be tolerant Encrypted currencies are safe, open, transparent, and fair, and combined with anonymous transaction mechanisms and off-chain payment systems, they will be widely used in massive micropayment transactions and settlements in the future digital economy era.

Of course, such a vision poses a brand new challenge to the consensus algorithm of the blockchain system.

3 BED consensus algorithm and implementation mechanism

The consensus algorithm of the blockchain is used to ensure that participants agree on the current state of the blockchain. The consensus mechanism determines which nodes can add new transaction blocks, and one of its main goals is to ensure that the blockchain is not rewritten.

Consensus is to the blockchain, just like the idea of governing a country and governance mechanism, which determines the stability and development of the blockchain ecology. At present, the consensus mechanism design of many blockchain networks is "small wealth is safe", which has lost the vitality of development and failed to ensure sufficient security.

We propose that the consensus mechanism is best to be a dynamic unified consensus, a consensus of dynamic development, and a consensus of dynamic competition. The BED blockchain system innovatively proposes a consensus algorithm that mixes PoW consensus and PoS consensus.

3.1 Proof of Work Consensus (PoW)

In blockchains (such as Bitcoin) that use Proof of Work Consensus (PoW), new blocks can only be created by miners. Miners deploy hardware (mining machines) and calculate how to effectively solve a specific mathematical problem. Every time a miner completes an effective calculation, the blockchain network can accept the blocks they build, and the legitimate blockchain network with the most proof of work (that is, the most hashed or calculated) chain is regarded as the legal chain. This means that miners are incentivized to mine on the longest chain. When a transaction to send funds to the wallet appears in a block, and other blocks (confirmed) have been constructed on this block, the block (transaction) will not be rewritten.

An external attacker may purchase enough mining equipment until the 51% attack on the trusted network is completed. If the attacker controls enough hash power to attack the "real chain", it can rebuild (or refactor) the blockchain by rebuilding the "old" block to replace the latest block. The following is a brief description of this type of attack, also known as a 51% attack:

(1) The attacker first recharges the exchange, the transaction is recorded in block X, and then the attacker starts to build another parallel chain alone (not broadcasting the block to the network).

(2) When the number of confirmations required for the recharge transaction is reached, the attacker will exchange the token for other currencies and withdraw cash from the exchange.

(3) When the withdrawal transaction is completed, the attacker will release a parallel chain constructed independently, and if the blockchain has more PoW (blocks) than the original chain, the network will accept it as a legal chain, and the original area The blockchain (including the attacker's recharge transaction) will become a historical version and disappear. After that, the attacker can freely use these tokens again.

In the blockchain network using the PoW consensus algorithm, because miners are the only entities that can directly add blocks to the blockchain, this puts them in the highest position in governance. If the consensus rules need to be modified or upgraded in the blockchain network, it must be supported by most hashing power.

A "soft fork" requires enough miners to re-identify the new consensus rules so that users can conduct transactions and expect their transactions to be processed correctly, and package transaction data in blocks. The "hard fork" divides the original blockchain network into two parts, and the chain with the most PoW accepted by most miners is the legal chain. Therefore, miners will have the right to decide which chain is considered legal.

Is this mechanism reasonable? At the time of the network bifurcation, miners may not be able to represent the vast majority of the interests of the blockchain network (the coins held are relatively small), thus making actions that are not conducive to the entire ecology.

Because of this, the blockchain network using the PoW consensus algorithm must have a strong computing power protection, such as Bitcoin, if it is to be recognized by the society, otherwise it will be difficult to obtain sufficient security. Even if it is as strong as Bitcoin, it also forked BCH on November 13, 2017, and seized part of Bitcoin's computing power. In 2018, the computing power battle between BCH and BSV caused the Bitcoin network computing power to be greatly reduced, and the price of Bitcoin plummeted 50%.

As a new generation of encrypted digital currency system design, the pure PoW mechanism can no longer be successful.

3.2 Proof of Stake Consensus (PoS)

Proof-of-stake consensus (PoS) is another way to decide which miners can add new blocks and verify the current state of the blockchain. Proof-of-stake consensus (PoS) uses a mechanism to determine the next block producer based on the number of tokens (or "equity") in the wallet. The basic principle of the consensus algorithm is to believe that those who have the most benefits will make responsible and reasonable decisions for the entire network.This mechanism determines the next block producer. The basic principle of the consensus algorithm is to believe that those who have the most benefits will make responsible and reasonable decisions for the entire network.

Proof-of-stake consensus (PoS) eliminates the need for energy-intensive mining activities, but the lack of significant energy expenditure creates another problem, sometimes referred to as “irrelevant”. Take a fork as an example. Forged PoS ("forging" is usually used instead of "mining") will be mined on two chains separately, because the cost of creating another chain is very small, so they can be used at the same time. Gain revenue on both chains. This is a problem for blockchain networks, because the purpose of the consensus mechanism is to only recognize that there is a legal chain and only recognize the state of the legal chain.

Proof of Stake Consensus (PoS) has other problems in terms of token distribution. PoW miners have high costs (hardware, electricity) and usually need to sell most of the tokens they mine to meet these costs. Therefore, many mined coins can be purchased on the market without being hoarded by miners. The counterfeit cost of PoS is very low, and they do not need to sell the tokens they obtain in order to maintain network operations. Large equity holders participating in proof of equity tend to increase their share of tokens in circulation because they collect large amounts of rewards and transaction fees from network users. This is likened to feudalism, that is, the network is owned and manipulated by large token holders, and users need to pay a fee to them during use. In PoS, some restrictions are usually set so that ordinary users cannot directly participate in the proof of equity consensus.

3.3 BED consensus algorithm: PoW+PoS

Our goal is to combine the advantages of PoW and PoS, balance each other's weaknesses, and integrate a multi-factor and mixed consensus mechanism to serve as the consensus algorithm of BED.

BED adopts the PoW+PoS hybrid consensus algorithm mechanism.

BED's PoW consensus component is similar to other PoW-based projects (such as Bitcoin) and uses the HASH-256 hash function. BED’s PoW miners are responsible for proposing new blocks to the blockchain, but the PoS consensus node must verify the validity of the blocks before they can be added to the blockchain network.

The PoS component of BED and how it builds a blockchain is very unique and deserves further explanation.

To participate in BED's PoS consensus proof, token holders must lock their BED tokens in order to purchase "Tickets". When a user purchases a ticket (Ticket), the BED tokens they use will be locked (they cannot spend), and the lock-up period will last cycle their ticket (Ticket) is called by the network's pseudo-random function to complete the voting, which is a mining Cycle (1008 blocks).

Tickets bring opportunity costs to the PoS mechanism. In this way, it can ensure that PoS voters are fair in the game and can follow the best interests of the network.

Below we propose the PoS implementation mechanism of BED.

3.3.1 Secret voting mechanism

When BED's PoW miners find a valid block, they will broadcast it on the network. In order for the block to be considered valid, the block must be verified by most PoS holders, that is, every block All must be approved by 3/4 holders.

Specifically, in the PoS mechanism of BED, 1008 blocks are a cycle (approximately 7 days), corresponding to 1008 tickets (Tickets) and 1008 ticket holders. The currently purchased tickets (Tickets) can be used in the next block. Take effect. At each block time, 1008 vote holders are allocated to 21 voting groups based on a random function (48 votes for each voting group), and each group votes to elect a representative of the group, and then 21 voting groups are elected. A representative voted on the validity of the block submitted by the PoW miner. If the block is approved by 3/4 of the representatives, the block is added to the main network as a valid block; if the block does not get 3 /4 represents the approval of the person, the block is abandoned, and the PoW miners re-mine based on the previous block.

In each voting group, the representative must be approved by 3/4 of the group members (that is, 36 tickets (Ticket)). If the group cannot successfully elect a representative within the specified time, they cannot participate in the block of the round vote.

At the same time, in order to prevent PoW miners and PoS ticket holders from conspiring to attack the main network, all tickets (Tickets) will be encrypted, marked and grouped, concealing the identity of the ticket holder (but the network will encrypt and record the corresponding identity relationship), all The elected representatives are also encrypted to hide their identity.

In BED's PoS consensus algorithm, ticket holders represent the interests of most token holders in the entire network, and also represent the greatest interests of the BED network ecology. In this way, BED ticket holders are used to determine the validity of the block, contain the power of PoW miners, and achieve ecological balance.

There is a cooperative interest relationship between PoW miners and PoS ticket holders. When the block submitted by the PoW miner is valid, the miner and the ticket holder share the mining revenue and block reward; when the PoW miner submits an invalid block, the PoS holds the ticket They must be honestly deemed invalid, otherwise, as ticket holders, they will bear the greatest loss, and at the same time, PoW miners will not be able to gain profits, wasting time and computing resources. Therefore, only honest cooperation between PoW miners and PoS holders can obtain the greatest economic benefits.

3.3.2 Ticket pricing mechanism

The price of a ticket is determined by a market-like mechanism, and the goal of the system is to obtain a certain number (1008) of tickets. In each round of mining cycle, token holders start bidding for the next round of 1,008 tickets.

The bidding rules are: each round has 1,008 tickets (Tickets), and the holders will bid for them in BED tokens as a whole. In addition, the system sets the minimum price of the ticket. If the price of some tickets is less than the minimum price, the corresponding bidder must make up the difference, otherwise the ticket cannot be obtained. If the number of tickets participating in this round of auction is less than 1008, the next round of fares will be the minimum fare set by the system. If the number of votes involved in this round of auction is greater than 1008, then

The next round of fares is dynamically adjusted to a certain value. In addition, multiple people can entrust the mining pool to merge the bidding tickets together.

The tickets formed by participating in the auction will be released dynamically by the miners in the next round of mining.

3.4 BED PoS Pool

The new problem brought by the design of Proof of Stake Consensus (PoS) is: How to implement a mining pool similar to PoW mining during PoS mining?

In BED, it is allowed to have multiple inputs for the same ticket (Ticket) auction purchase transaction, and provide UTXO subsidy amount for each input in proportion, and also provide a new output public key for these proportional rewards or Script, which solves this problem.

This means that token holders can delegate their BED tokens to the PoS pool, and the PoS pool will participate in the ticket auction uniformly, and then share the rewards of the pool according to the proportion of the total pool of their token stations. In the future PoS ecosystem of BED, there will be multiple PoS pools, and PoS pools that can execute economic strategies well will gain the trust of token holders and obtain more agency rights. In order to prevent a few PoS pools from controlling the ticket market and PoS voting, a maximum proxy limit is set.

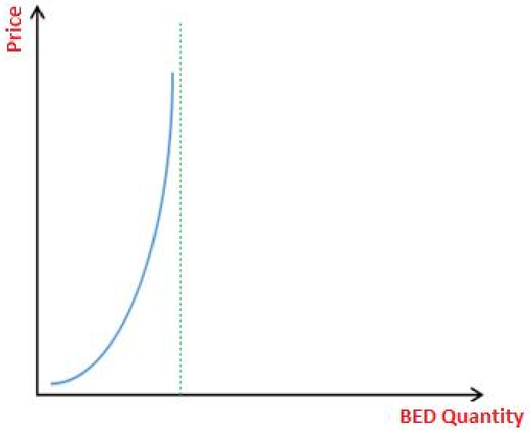
3.5 Miners and ticket holders

Under BED's PoW+PoS consensus algorithm, miners can participate in both PoW mining and PoS voting. In order to obtain higher mining revenue, miners have enough economic power to bid for 1,008 tickets. In each round of mining cycle, if the miner successfully bid for the ticket (Ticket), he can get all block rewards and handover fees; if the miner does not get the ticket (Ticket), he will only get part of the mining revenue. If other token holders successfully bid for a ticket (Ticket), they will receive a certain percentage of block rewards. If the ticket (Ticket) is provided virtually by the system, the corresponding percentage of block rewards will be automatically destroyed.

3.6 Attack cost

Miners participate in BED's PoW mining with obsolete Bitcoin mining machines or the latest Bitcoin mining machines. Ideally, miners can compare Bitcoin mining revenue with BED mining revenue and choose the one with the largest profit of the internet.

Under the PoS consensus mechanism, PoW miners cannot attack the BED network by suddenly switching most of the computing power, unless they control most of the tickets at the same time, which means that attacking miners not only need to prepare a large number of mining equipment, but also purchase A large number of BED tokens, and such behavior will cause the price of BED to soar, which greatly increases the cost of the attack.



BED price-quantity graph: Attacks cause the price of coins to skyrocket, and costs soar

4 Privacy and freedom: anonymous transactions

Many people think the demise of paper money is a good thing, but they are wrong.

It is not the criminals who need to hide, everyone deserves privacy. It's like you don't want a person to look at your window inadvertently, or on your shoulder, and read the email you sent to your best friend. You don't want anyone or organization to know all your financial records.

Nowadays, the digital trend of human society is unstoppable. The digital trails in life will always exist, allowing anyone in power, good or evil, to roll back time, pry into all the details of your life, and explore anything they want to know about you. .

When ordinary people wake up to danger, it is too late.

The only real hope is that cryptocurrencies with privacy protection mechanisms become popular in the real world. If we can build a decentralized, privacy-encrypted encrypted digital currency payment system, and ordinary people use it every day, then we are expected to achieve privacy and freedom.

This is our resonance: John Adams said: "There is absolutely no trust without a check." The death of cash is the death of freedom, and privacy encrypted digital currency may be the rebirth of freedom.

4.1 AnonymouslySend

We believe that in order to provide strong protection of user privacy on the client side, it is important to implement a standard non-trust system. Clients such as electrum, Android, and iphone will also directly embed the same anonymity layer, making good use of protocol scalability to ensure a good user experience while protecting user transaction privacy.

AnonymouslySend is an improved and extended version of CoinJoin (software that provides anonymous technology). In addition to having the core concept of CoinJoin, we have also made a series of improvements, such as decentralization, strong anonymity, and coin mixing technology.

Most cryptocurrencies in existence today have transparent and queryable blockchains, including Bitcoin and Ethereum, which means that anyone in the world can view any transaction. The addresses of coins can be associated with individuals in the physical world.

When improving privacy protection and the interchangeability of encrypted digital currencies, the biggest challenge is that the entire blockchain cannot be encrypted. In the Bitcoin-based encrypted digital currency system, you can see which outputs are not sent and which are sent, usually called UTXO, the full name is unspent transaction output. This allows each user to act as a guarantor of honest transactions in the public ledger.

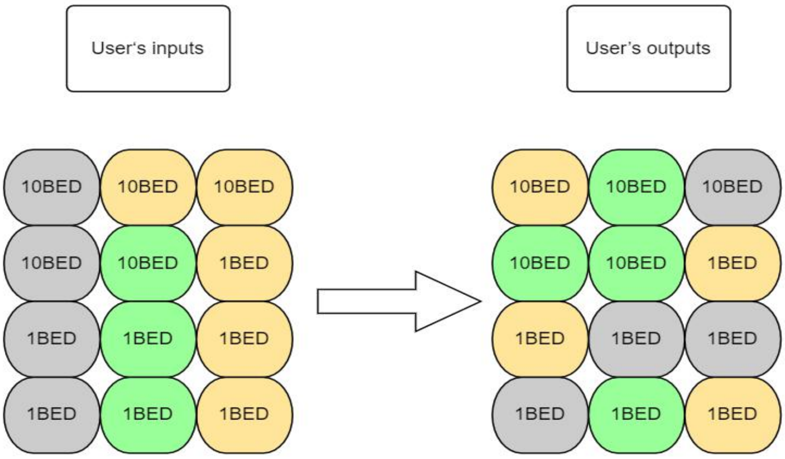
Bitcoin's protocol is designed without relying on the participation of third parties. Without the participation of third parties, it is vital that users can still read user information at any time through the public blockchain for auditing. Our goal is to improve confidentiality and interchangeability without losing these elements. We firmly believe that this is the key to creating a new and successful encrypted digital currency.

Using currency mixing technology, we can make the currency itself fully interchangeable, and interchangeability is an important attribute of currency. All parties involved in currency transactions must maintain an equal status. When you receive funds in the form of cash, the cash should not retain the previous user's use record, or the user can easily separate it from the previous use history. All currency transactions are equal. At the same time, any user guarantees that every transaction in the public ledger is honest without affecting the privacy of others.

In order to improve interchangeability and maintain the honesty of public blockchains, we propose to use advanced non-trusted, decentralized currency mixing technology. In order to maintain currency interchangeability, this service is directly integrated into this BED system. This is easy to use and safe for every user.

4.2 Enhanced privacy and DOS protection

AnonymouslySend combines multiple transactions into one transaction, and then sends them together, and the combined transaction cannot be split again. AnonymouslySend transactions are set up specifically for user payment. This system is highly secure and anti-theft, and user transactions are absolutely safe. At present, the use of AnonymouslySend's merger transaction technology requires at least three parties to participate.



Color denotes separate users

Figure 1: The funds of three users are merged into a common transaction, and users will export funds in a new disrupted form.

In order to enhance the privacy of the system as a whole, we propose to use the same face value of 0.1BED, 1BED, 10BED and 100BED. In each round of "coin mixing", all users should input and output funds with the same face value. In addition to using the same face value, all transactions will be broken down into scattered, independent, and unrelated small transactions.

The next step is to deal with possible DOS attacks. All users submit their transactions to the "mixed currency pool" in the form of deposits, and the transactions are finally output to the users, and at the same time they can pay a high reward to the miners. In other words, when a user makes a request to the mixed currency pool, he must provide a deposit from the beginning. If the user fails to cooperate at some point, such as refusing to sign, the deposit transaction will be automatically broadcast on the entire network. If a continuous attack is to be carried out on an anonymous network, the price paid is extremely high.

4.3 Passive funds and blockchain anonymity

AnonymouslySend is limited to 1000 BED per round of currency mixing, and multiple rounds of currency mixing can anonymously mix a considerable amount of funds. In order to make the user experience convenient and attacks difficult, AnonymouslySend runs in a passive mode. At the same time, the time interval is set, and the user's client must connect to other clients through the full node. Once entering the full node, the amount of face value required by the user to be anonymous will be queued up and broadcast across the entire network, but no information will expose the user's identity.

Each round of AnonymouslySend process can be regarded as an independent event that enhances the anonymity of user funds. However, each round is limited to only 3 participants, so observers have one-third of the opportunity to track transactions. In order to improve the quality of anonymity, a link is used Method, the funds are sent out sequentially through multiple master nodes.

Then, the number of users that may be involved in the N round of coin mixing:

X=n^r (n the number of participants in each coin mixing, r is the number of coin mixing)

In the BED system as follows:

Block depth	Number of possible users
2	9
4	81
8	6,561

16	43,046,721
32	1,853,020,188,851,840

4.4 Security considerations

Because the transactions are merged together, the node may "peep" when user funds flow through. Since the validity of each node block requires the PoS consensus to verify the validity, each ticket behind the PoS consensus corresponds to at least 1000 BED, and users randomly choose full nodes to deploy their funds, so the "peeping" impact is not big.

How to achieve "voyeurism"? Under BED's PoS consensus algorithm, 1,008 ticket holders are randomly assigned to 21 voting groups, and each voting group selects representatives to participate in the block validity voting. The attacker first needs to control more than 51% of the computing power; the ticket holders that the attacker needs to control are coincidentally distributed to 21 voting groups, and coincidentally, at least 16 people are selected as representatives in the 21 voting groups. And these 16 representatives coincidentally realized collusion; in order to achieve sustained attacks, the above-mentioned things must continue to occur within a certain period of time.

Since the PoS mechanism is secretly executed in a fully encrypted environment, there is absolutely no possibility that such a period will happen. Considering that the circulation of BED in the early days is very small and the liquidity in the market is very low, controlling so many tickets in continuous attacks means that the attack has become the representative of the best interests of the BED ecology. Attacking the BED network is attacking itself.

5 Instant transaction and off-chain payment system

5.1 BED off-chain payment system

In order to meet security and fairness, BED includes the PoW consensus algorithm, which means that there are several fundamental technical problems: in terms of processing power, the entire network currently only has 7 transactions per second; in terms of latency, it is roughly 10 minutes to generate a block; On the finality of the transaction, it is generally recommended to wait for the confirmation of 6 blocks as the finalization of the transaction, and for large transactions, it is recommended to wait more; on the capacity, each block is only 1M.

The emergence of the Lightning Network has led to an order of magnitude improvement in the transaction processing capabilities of the Bitcoin network, and at the same time fundamentally solved the problems of fast transaction verification and block capacity. With the Bitcoin blockchain as the backing, real peer-to-peer micropayment transactions are realized off-chain. The bottleneck of blockchain processing capacity is completely broken, and the problems of delay, finality, capacity and even privacy are also solved.

For this reason, the blockchain community even believes that the importance of the "Lightning Network" paper (The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments) to Bitcoin is only under Satoshi Nakamoto’s creation paper, ranking No. two.

In order for BED to be widely used in commercial payments and to develop the micropayment economy, we must develop BED's off-chain payment system with the help of the currently booming Lightning Network technology.

Backed by the BED blockchain network, real peer-to-peer micropayment transactions are realized under the chain. If both parties to the transaction have pre-installed payment channels on the blockchain, they can realize instant confirmation of micro-payments through netting multiple times , high-frequency and two-way; if the two parties do not have a direct point-to-point payment channel, as long as there is a connection in the network A payment path composed of multiple payment channels for both parties. The BED payment network can also use this payment path to achieve reliable transfer of funds between the two parties.

Therefore, the BED off-chain payment network satisfies the following characteristics:

- Low-latency payment: The main function of currency is payment. BED hopes to be a useful payment currency, and it must solve the problems of slow payment, high handling fees, and difficulty in small transactions.

- Deferred settlement: On the premise of ensuring security, minimize the number of transactions on the chain, reduce costs, and reduce the amount of data storage on the chain.

- Enhancing privacy: Through the off-chain payment system, transactions will only be recorded in the middle node, but not the off-chain transaction process, which is a powerful protection for privacy.

- Cross-chain atomic swap: If a merchant uses tokens on other blockchains, such as Bitcoin and Ethereum, atomic swaps can be realized in the BED off-chain payment system, and BED can be directly exchanged for other off-chain. Digital currency will make future payments very convenient and fast, and reduce costs.

5.2 Low-latency payment

Cryptocurrencies need to regularly create blocks in the blockchain, which limits the average time it takes to wait for confirmation that a transaction is valid. The average block time of BED is 10 minutes. For most commercial payments, the time it takes to confirm the transaction on the chain is too long, and this is still assuming that there is no accumulation of goods in the transaction on the chain. While keeping all transactions as on-chain transactions, the only way to solve this problem is to greatly shorten the average block time, but this still cannot fundamentally solve the dilemma of on-chain transaction congestion.

By supporting the BED offline payment system, BED will realize instant micro-payment technology. This means that BED can handle thousands of transactions per second, or even tens of thousands of transactions, and thus is accepted by merchants with physical retail business, and can even be used for micropayments in the Internet of Things, autonomous driving and other fields.

5.3 Deferred settlement

Banks regularly use netting procedures to minimize the number of transactions between banks and their counterparties. The typical process involves collecting all outbound payments from Bank A to Bank B within a given transaction day, which combines thousands of external payments from Bank A to Bank B into a single payment. By delaying inter-bank settlements, the number of inter-bank transactions has been drastically reduced.

The payment channel in the BED off-chain payment system is a delayed settlement path with limited value. Although there are upper limits on the amount of two-way flow, the settlement path is designed to be very similar to the net settlement process that occurs between banks, which means that there may be thousands of off-chain transactions, while the corresponding on-chain transactions are only a few .

Just as banks perform net settlement to simplify inter-bank transfers and save fees, the BED off-chain payment system can reduce the number of transactions on the chain and reduce fees accordingly. When not necessary, you should avoid storing data on the chain, which will allow users to avoid related transaction fees. The BED off-chain payment system will reduce the number of transactions on the chain, which helps minimize the growth rate of database record counts.

5.4 Enhanced privacy

Thanks to the AnonymouslySend transaction mechanism of BED, it can provide strong privacy protection for on-chain transactions. For the BED off-chain transaction system, the transaction can be completely off-chain, so there is no public data corresponding to the transaction, but the AnonymouslySend transaction mechanism can also provide privacy protection for settlement nodes, thereby further protecting the privacy of off-chain payments. The only record of transactions under the BED chain is the intermediate node that forwards the transaction between the sender and the receiver, and the privacy of the intermediate node will be protected by the main network, which is a major improvement in privacy protection.

5.5 Cross-chain atomic swap

Anyone who holds cryptocurrency knows how much they rely on centralized transactions in the process of buying cryptocurrency. Although the exchanges dealing with cryptocurrency are not prone to problems, they are still centralized, which not only have high transaction costs, but also have certain transaction risks. If an exchange must stop part or all of its business, it will have a very serious impact on the value of the cryptocurrency it trades. Decentralized exchanges do exist, but they rely on fund custody and decision-makers, and so far are difficult for ordinary people to use.

Both the BED main chain network and the off-chain payment system will allow atomic swaps. This means that trustless cross-chain exchanges can be carried out (provided that the exchange is supported by the counterparty chain). If the transaction amount is large and does not require a low settlement waiting time, then the on-chain atomic swap will have a good effect; if the transaction is frequent, the amount is small, and less waiting time is required, then off-chain atomic swap can be used. Creating liquidity through cross-chain atomic swaps will reduce the risks associated with trading BED.

5.6 Intermediate node

The BED off-chain payment network is separate from the BED blockchain network, which means that the nodes of the off-chain network are separate from the nodes of the main network. For end users (such as consumers or merchants), the requirements for running off-chain payment network nodes are very low. Just start the node, then fund a channel, and then it's set up. If you plan to run an intermediate node with frequent transactions that has many channels open to other nodes, you must lock some coins to open channels with various counterparties. When acting as an intermediate node, there are corresponding transaction fees as an intense mechanism to cover operating costs.

6 Incentive mechanism

Economic model design is a big problem and challenge for the new blockchain. A successful economic model is the biggest foundation for the rapid development and growth of the blockchain network. In BED, we design the following economic model to increase node computing power to support the BED network, to ensure that PoW miners and PoS nodes act honestly and more profitably, and then cooperate to maintain the network.

BED economic model	
Total number of tokens	21，000，000
Halving mechanism	The halving cycle is 4 years, and the halving block reward is 50%
Allocation mechanism	1. Miners holding tickets (Ticket) mining: PoW miners get full block rewards. 2. Miners do not hold tickets (Ticket) mining: PoW miners get 20% block rewards, and the remaining rewards are shared by the pos pool. 3．Foundation 5%， technical team 3%， community 7%

7 Application of BED

BED's vision is to become the currency of the digital age of human society, which is widely used in payment, transaction and settlement in economic activities. BED's security, privacy protection, and large-scale transaction processing capabilities are the basis of payment currency in economic life.

In the future, BED will become an important part of the encrypted digital currency field. BED's mining power will be second only to Bitcoin, which is the largest protection net for BED network security and the basis for the development of BED ecology.

We hope that through the continuous efforts of the broad community and the partners inside and outside the industry that are closely related to us, we will promote the development of the BED payment network in some important countries and regions, and become the payment system and financial infrastructure of these countries and regions for the public Providing safe and economical financial services makes it as easy and cheap as sending text messages to transfer money around the world. No matter where they live, what they do, and how much money they make, they will start a better life for them.

8 Conclusion

This white paper aims to introduce the blockchain protocol of BED. BED adopts the PoW+PoS consensus mechanism. New blocks proposed by PoW miners must be validated by PoS nodes before they can be added to the blockchain network, which means that the blockchain network will not appear. Forking situation. Through BED's anonymous transaction mechanism and off-chain payment system, the security and privacy protection of BED on-chain and off-chain transactions can be realized, and at the same time, it can meet the performance requirements of a large number of users, thereby providing a basis for BED to be widely used in commercial payments.

In addition, we use reasonable incentive mechanisms to effectively manage PoW miners and PoS nodes, and decide how to formulate and implement issues related to software upgrades, community management, and conflict resolution. Ultimately, the goal of BED is to build a secure and widely used encrypted digital asset to meet the needs of value storage and commercial payment applications.