



BFC (Bitfree Cash) white paper

A new type of CPoW digital currency system

Bitfree Core Team

CONTENTS

- ◆ Background
- ◆ Features
- ◆ About mining
- ◆ Problems in traditional mining
- ◆ BFC overview
- ◆ What is CPoW mining
- ◆ Problems BFC solved
- ◆ About faith
- ◆ Techniques
- ◆ Smart contract
- ◆ The future of BFC
- ◆ Problems in traditional business
- ◆ Commercial application
- ◆ Release details
- ◆ BFC mining
- ◆ CPoW mining rules
- ◆ The goal of CPoW mining
- ◆ BFC ecological route

Background

Centralization has significantly influenced the development of human society for thousands of years. However, with the progress of humankind and the development of the economy, the class contradictions caused by wealth gap are more and more intensified, which limits the total productivity of the human population and directly affects our further development. It is mainly caused by the lack of transparency in the centralized society which hardly to achieve consensus since no trust.

The emergence of the blockchain points us a way to solve the problem. With high-tech methods, the consensus system generates passive trust and forms a consensus mechanism which cannot be tampered, thus achieving the highest level of trust --- decentralization. Through this new technology, people realize that most of the current social conflicts are caused by centralization. The blockchain perfectly solves this global crisis of trust, and cryptocurrencies find a way out for our asset security.



Features

When we talk about cryptocurrencies, the first thing comes to mind is Bitcoin, then Ethereum, EOS, and many other well-known cryptocurrencies. The cryptocurrency is not issued by the legal currency institution and not controlled by the central bank. It uses computers in the world to calculate a set of open-source equation code, and then be generated by a large-scale arithmetic processing, after that, uses the password to ensure safe currency circulation in all aspects. It has the following characteristics:

1. Decentralization

This is the essential idea which is identified at the beginning of Bitcoin by Nakamoto. It makes the cryptocurrency out of regulation from the organization, the state, and any unit. No tax during transaction process, no freeze, no price control by a certain unit.



2. Open Source

The cryptocurrency will be published in parallel with the open-source code, as well as the mine pool protocol code. The cryptocurrency must be mined and mined. Without such info searched, it may be a fake cryptocurrency.



3. Limited

The circulation of cryptocurrencies can be viewed through open-source code. The circulation of cryptocurrencies must be quantitative, accurate, and unchangeable.



4. International

The cryptocurrency can be traded on international platforms. Different from other currencies, it can be circulated on the international platform to produce value.



About Mining



The cryptocurrency mining method includes PoW and PoS mining. Bitcoin is typical of PoW mining, yet EOS is more representative of PoS one. Among them, the PoW mining mode occupies the vast majority.

PoW mining

PoW mining is the workload proof mechanism. The reward criterion is that the computer in the network solves a very complicated mathematical problem and this process is called mining. The first who solves a block can get the token reward. In order to solve this mathematical problem, you need the necessary hardware, that is, the mining machine, and also have power and network to run the mining machine. The core of PoW is that who has stronger electricity and computing power, who gets more rewards.

PoS mining

PoS mining is equity proof, unlike the energy and computing power that PoW using. The PoS is the benefit verified by the verifier. Each verification rewards a certain percentage of the commission to the verifier with ratio based on the number of coins. The core of PoS is the more cryptocurrencies you have (if the encrypted currency supports PoS mining), the longer the holding time, the better record transaction chance, and the more record offering, that is, the more reward.

Problems in traditional mining



The original intention of Nakamoto to create Bitcoin is to make Bitcoin a completely decentralized cryptocurrency, and everyone can get Bitcoin. However, the interest drove the miners to continuously improve their equipment and increase their power. The most obvious is the emergence of ASIC mining machines, which makes the computing power increased exponentially, moreover the difficulty of mining is constantly improving. The computing power for Bitcoin is in the hands of a few miners. And the increase in equipment and electricity costs make it difficult for ordinary miners to obtain bitcoin by mining. Even if a few bitcoin is obtained, it is difficult to cover the cost. Besides, the monopoly of computing power is likely to cause 51% double attacks. These problems stand on the opposite side of the original concept of Nakamoto.

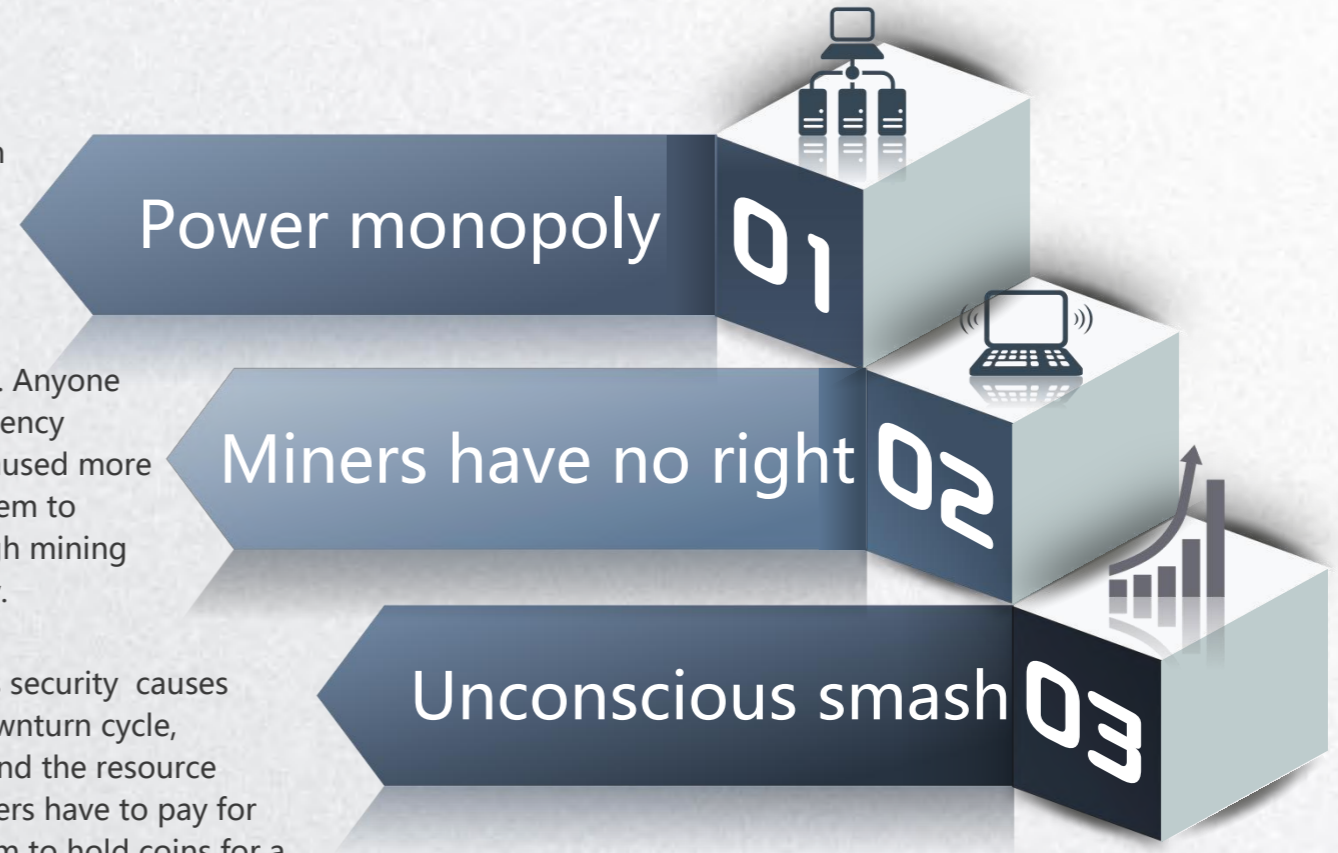
Although the PoS mining mode is not limited by mining equipment, it still cannot solve the monopoly problem. The more money you hold, the more you earn, and the vast majority of the proceeds are still divided by very few people. With the development of cryptocurrency, more and more problems have begun to emerge. The most prominent problems are the following:

Problems in traditional mining

In order to resist power monopoly, people are constantly trying to invent new algorithms. It is hoped that the algorithm can be used to resist ASIC attacks and maintain relatively low mining costs, which is often effective in the early stages. But once the market value of this new type of cryptocurrency reaches a certain level, under the driven of interests, ASIC developers will still try to crack these new algorithms, and the interests of ordinary miners will suffer huge losses.

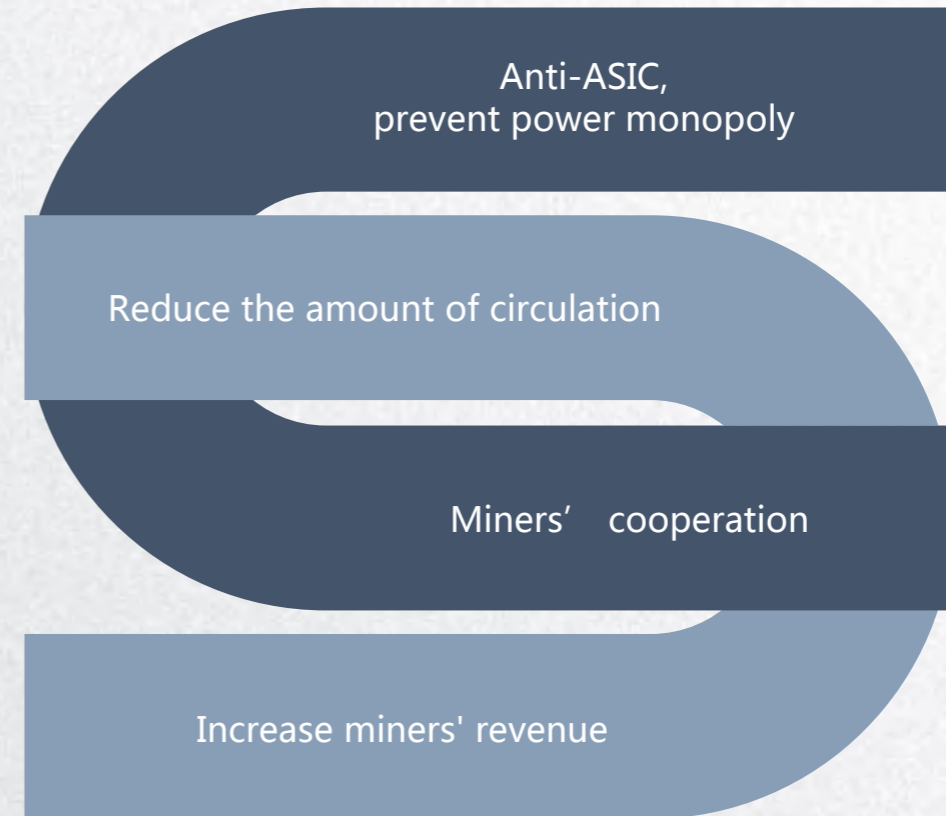
The essence of decentralization is that everyone can participate. Anyone has the right to participate in the construction of the cryptocurrency ecosystem. However, the occurrence of power monopoly has caused more and more miners to lose their original rights. It is difficult for them to obtain large computing power, hardly to make profit due to high mining cost, thus isolated by ecological construction of digital currency.

Based on the chain of PoW consensus, maintaining its security causes high power consumption. When the market is in a downturn cycle, electricity is the foundation of PoW cost. It is far beyond the resource consumption brought by the hardware itself. The miners have to pay for electricity with the coin that making it difficult for them to hold coins for a long time. It is not known that this kind of behavior is actually an unconscious smash. The miners cannot establish a sense of consistency and identity, but instead form a kind of malicious competition, which ultimately damages the miners' own interests. Therefore, PoW miners are precisely the biggest strength of shorting.

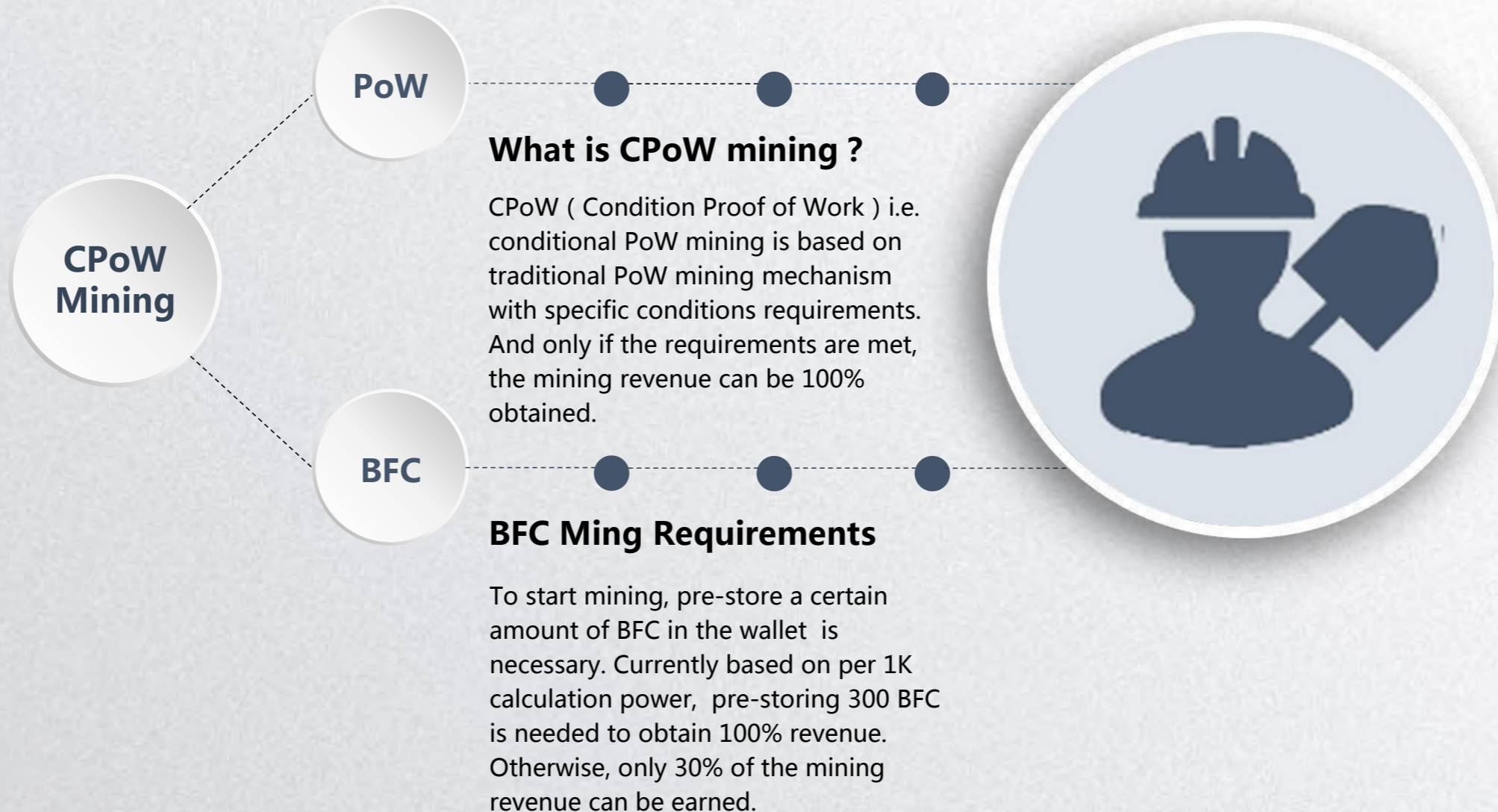


BFC Overview

Bitfree Cash(abbreviated as BFC) is a new cryptocurrency based on the improved Cuckoo Search algorithm, which can effectively resist ASIC and avoid concentration of computing power. BFC also adopts CPoW mining mechanism innovatively, which limits the mining participation entry. Through this mechanism, it could effectively avoid the power monopoly, reduce the amount of digital currency flowing into the market and increase the income of miners. There is no longer competition between minors, but cooperation, which makes BFC more secure and trustworthy to stimulate the sustained growth in quotation.



What's CPOW mining



Mortgage difficulty period

Every 4032 blocks in the entire network needs
Uniform coordination of mortgage difficulty
across the entire network

The mortgage difficulty
adjustment period is
Every 4032 blocks
(about 2 weeks)

The initial mortgage difficulty is 1K computing power
mortgage 300BFC (highest mortgage difficulty)

When the average computing power of the whole
network mortgage cycle reaches 6000K computing
power, the whole network will activate the dynamic
mortgage algorithm to reduce the difficulty value per
K mortgage.

The dynamic mortgage 1K computing
power mortgage number does not
exceed 300BFC at most, at least 1BFC

The handling fee of the mortgage is just like
transfer fee, applying to the unified whole
network accounting; The charge of each
mortgage refund is fixed to 0.01BFC.

Dynamic mortgage difficulty

The dynamic mortgage difficulty is calculated every 4032 blocks. The mortgage difficulty value will be used as the mortgage difficulty value in the next 4032 period.

The mortgage difficulty value is fixed in 4032 blocks, which is the mortgage difficulty value calculated in the previous 4032 period.

The difficulty cycle of the entire network mortgage reaches 6000K, which will activate the dynamic difficulty algorithm. If it is less than 6000K, it will return the standard of 1K mortgage 300BFC.

The dynamic mortgage difficulty algorithm uses the current liquidity as the calculation standard. The greater the computing power of the whole network, the smaller the difficulty value of the mortgage.

Dynamic mortgage difficulty reduces the amount of mortgages, helps increase BFC liquidity, and allows more users to participate in the BFC ecosystem.

Burst block address calculation



Any explosive block address, whether it is solo mining or mining pool mining, the explosive block address needs to meet 1K computing power mortgage 300BFC



The calculation principle of the explosive block address calculation power is that the current block height pushes forward 4032 blocks, and calculates the average calculation power of the explosion block address of 4032 blocks, that is, the average calculation power of calculating the explosion block address for about 2 weeks.



After the dynamic mortgage difficulty is activated, the 1K computing power needs to meet the mortgage value of the previous mortgage difficulty cycle.

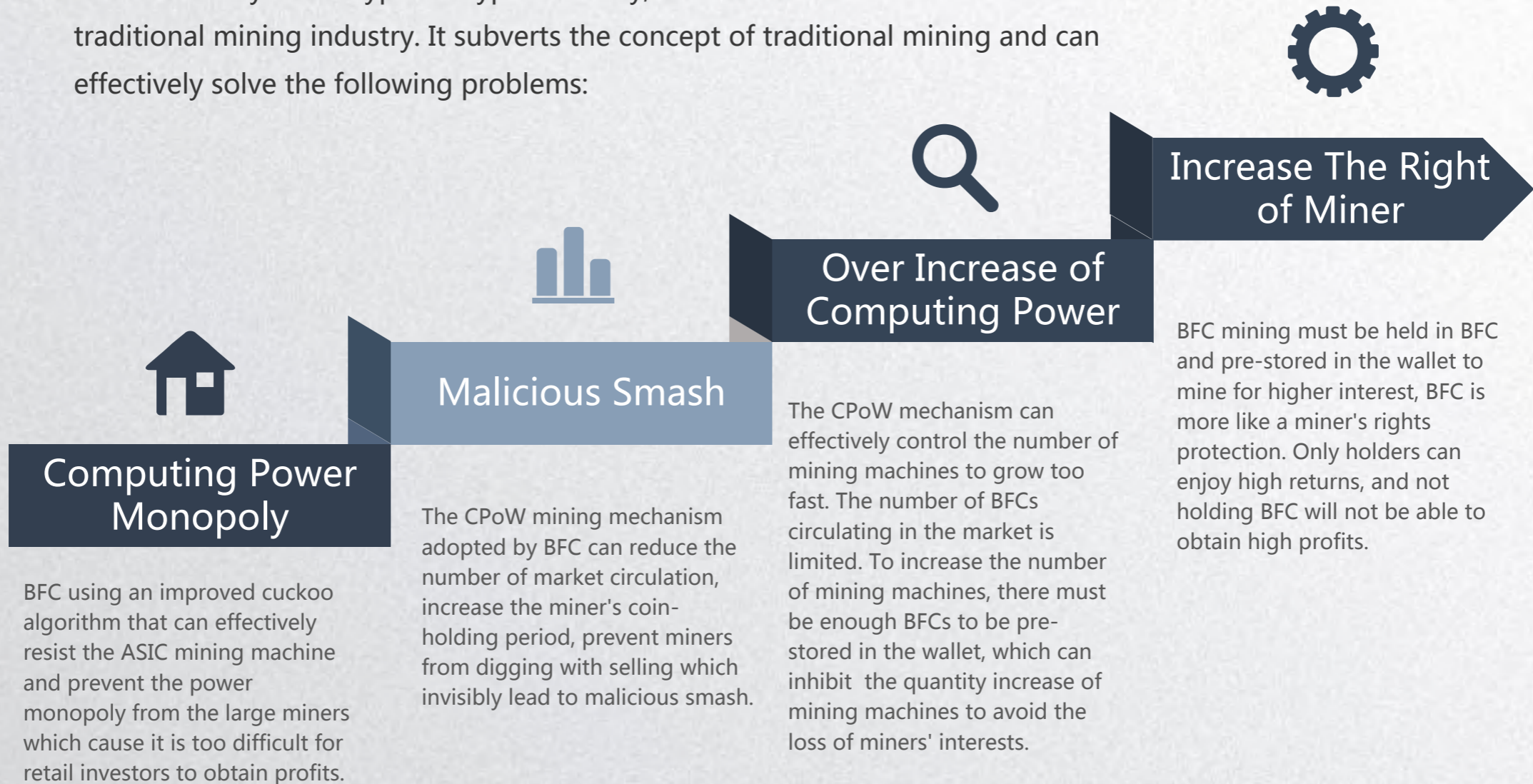


If it is a new explosive block address, it will be calculated according to the average calculation power of the previous 4032 full net mortgage.



Problems BFC solved

BFC is not only a new type of cryptocurrency, but also a reshuffle of the traditional mining industry. It subverts the concept of traditional mining and can effectively solve the following problems:



About Faith

**If you are given a chance to be financially free,
Will you stick to your beliefs for this
opportunity?**



Faith is an idea that all miners have. It is because of the belief that many talents have entered this circle. It is with faith that many talents dare to hold cryptocurrency for a long time and become rich overnight in the bull market. But the beliefs of many miners are not so firm. Once the market is turbulent, the faith will collapse and sell wildly. There are still many Buddhist miners whose consistent principle is to "dig and sell", selling whatever dug today. Once the bull market comes, there is no inventory in the hands, which has become an absolute "short".

Faith is priceless, but it is not enough to motivate more people to participate. In order for more participants to participate in BFC mining, we must provide all miners with more stable and profitable opportunities for revenue and rewards.

In fact, we are not lacking opportunities, just lacking faith.

Techniques

1. Using 8M as a large block, the technology of the generating block every 5 minutes greatly expands the efficiency of the network, which is 32 times the throughput of the BTC network.



2. Using the isolation witness technology, the second layer lightning network technology can be built on the main network technology to provide technical support for facilitating micro & quick payment in the future.



3. The next version will use zero-knowledge to prove, Mumblewimble has built a strong privacy anonymous transfer plan.



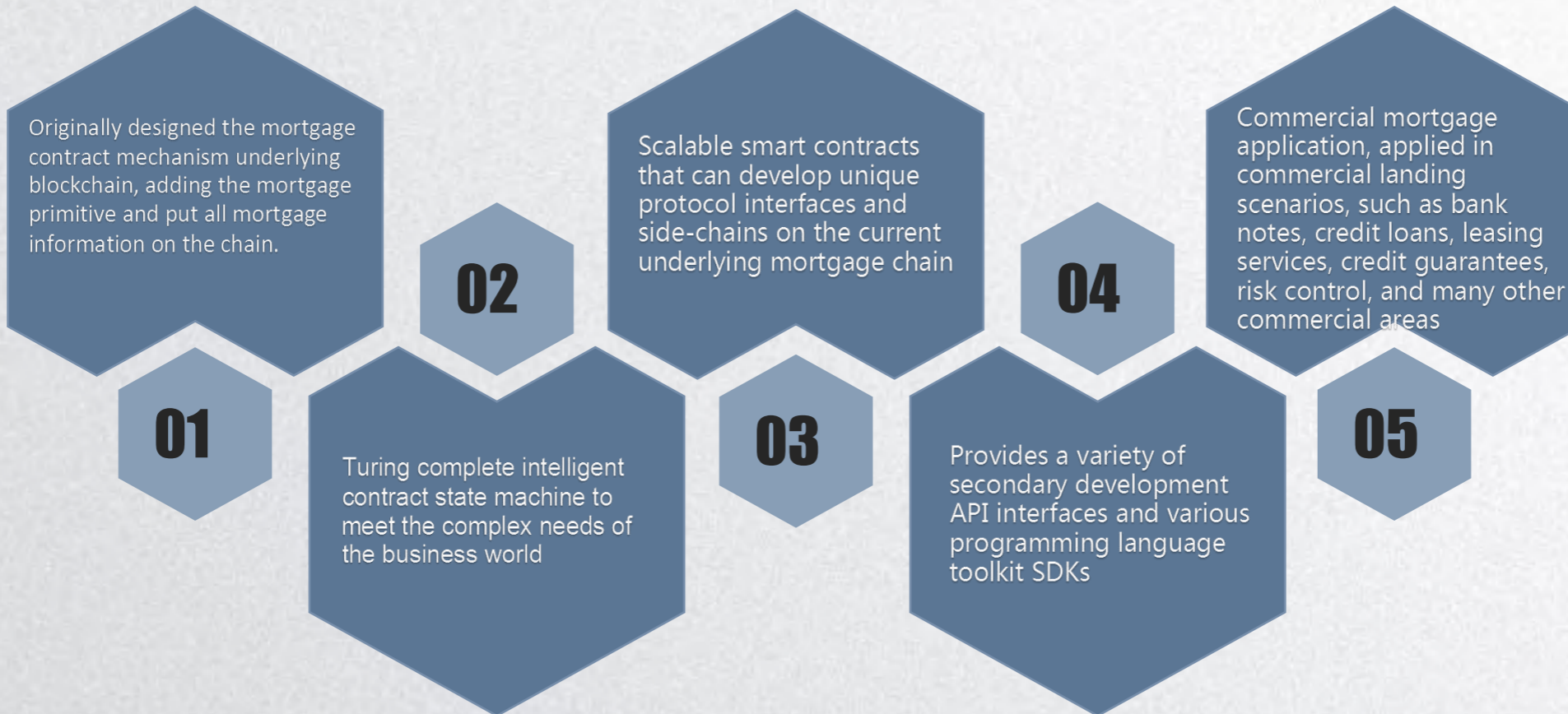
4. Based on CPoW / PoW mining model, which can ensure the security of the entire network data book



5. Innovatively designed mortgage primitives and anti-mortgage primitives, which will be widely used in the commercial field with mortgage demand in the future.

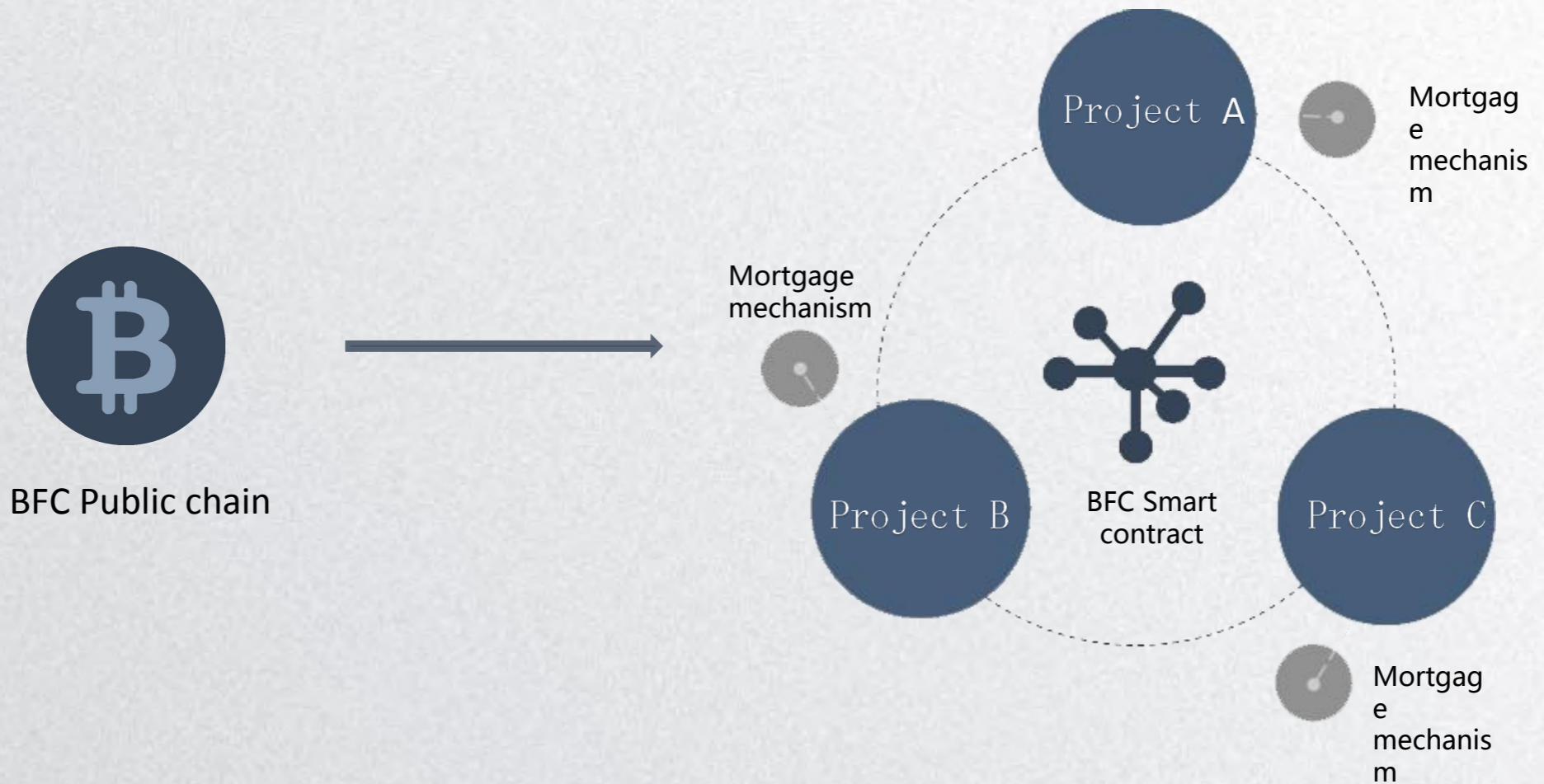


Smart contract



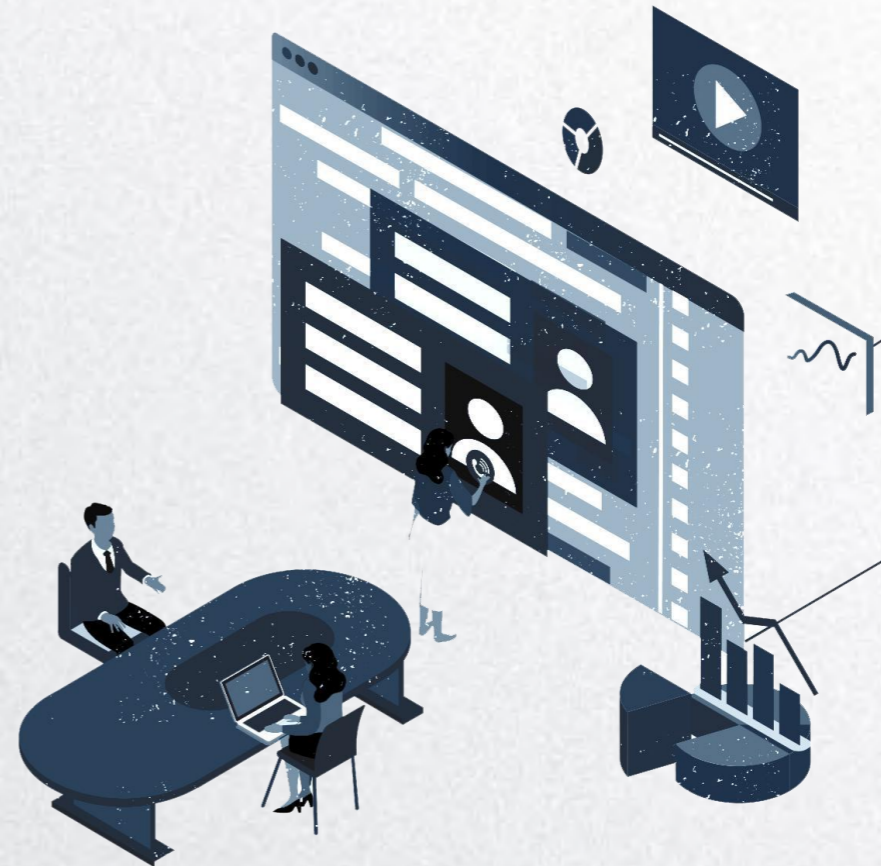
The future of BFC

BFC is not only a decentralized digital currency. In the future, we are committed to transforming BFC into a completely decentralized, new contractual system built with smart contracts to develop a blockchain ecosystem for commercial applications. To create a new business model with BFC's smart contracts that address the shortcomings of today's traditional business models.

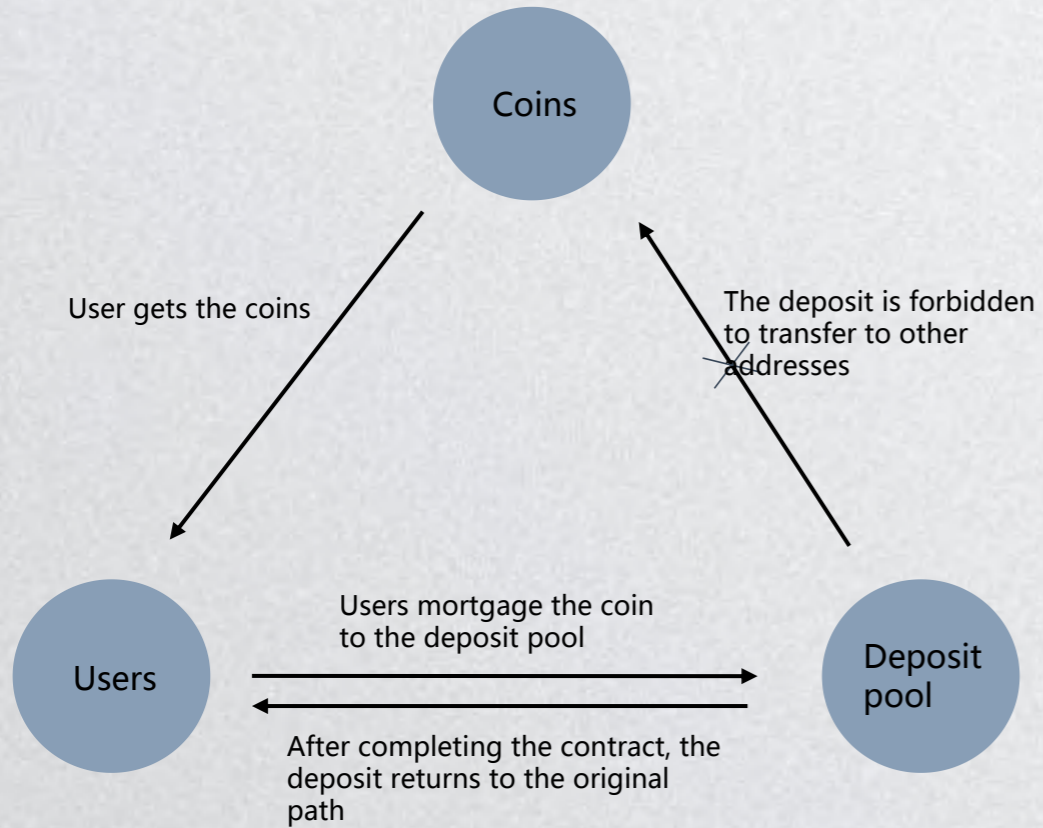


Problems in traditional business

Reputation is the foundation of the business. Once the credit is lost, the business cannot be established. The purpose of the deposit is to ensure that one party violates the agreement and the other party's interests will not be lost. This is based on the trust of both parties. However, this kind of trust is currently being severely challenged: the shared bicycle deposit cannot be returned to the user normally; the purchase of the house encounters the developer running, the prepayment is difficult to return; the tenant cannot get the rent deposit after the rent expires... What happened to us has caused many people to question the security and security of traditional mortgages.

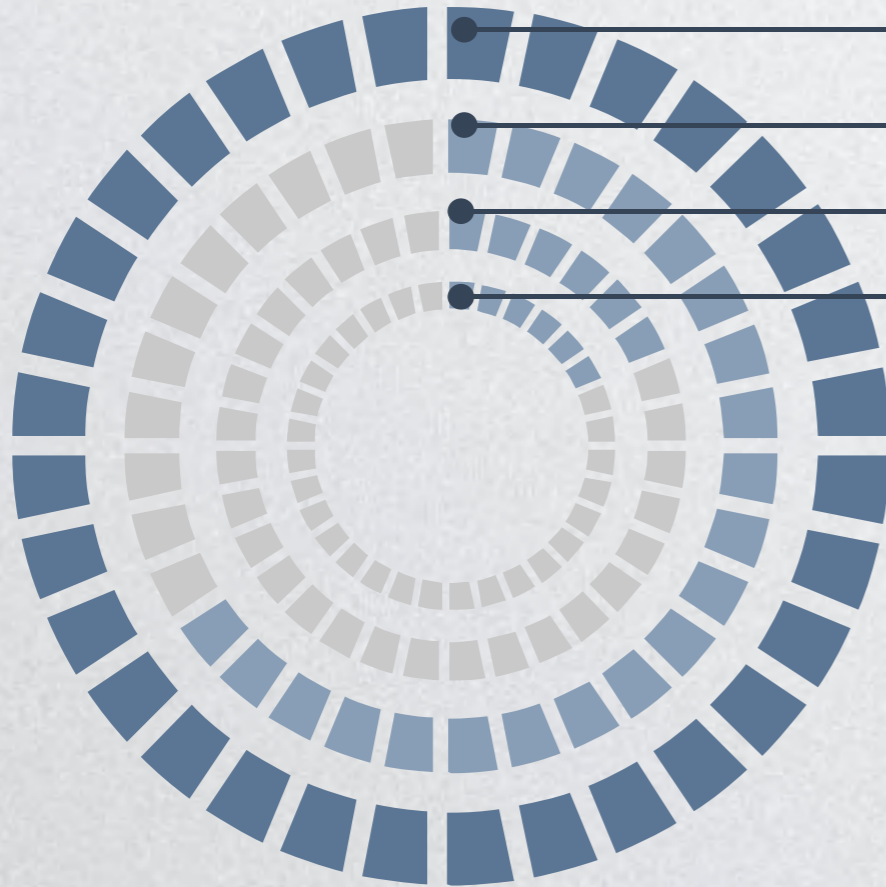


Commercial application



BFC's mortgage mechanism is an essential part of the smart contract. This mechanism stipulates that when the user meets the conditions to refund the deposit, the deposit can only be returned to the original route, and cannot be transferred to other places. That is to say, the project party cannot transfer the deposit to any address other than the original route, which ensures the security of the deposit. Relying on BFC's smart contract, the project party can develop its own coin on the BFC public chain. Users can use this coin as a deposit. During the mortgage, the mortgaged coin will be forbidden to transfer to any address other than the original mortgage path. The project party has no right to modify the deposit destination, and it is even more difficult to use the deposit for other purposes. The user and the project rely on this mechanism to establish a perfect trust relationship.

Release details



Total supply: 21 million pieces

Miners: 17.85 million pieces

Development team: pre-digging 2.1 million pieces, one-time block

Foundation and advertising team: 1.05 million, unlocked in proportion to each block of mining

Using improved Cuckoo algorithm

Block size is limited to 8M

Initialization reward 25 BFC

Mining difficulty adjusted block by block

Difficulty adjusted every 4032 block (about 2 weeks)

Mortgage strategy (300 BFC per 1K computing power, the higher computing power, the more mortgages are required)

When the computing power of the whole network reaches a threshold, the difficulty of mortgage will be reduced to reach dynamic mortgage

BFC mining



After the BFC online, the consensus mechanism of the main network is switched to the CPoW mining mode, and a total of 90% of the BFCs will be generated by the CPoW mining mode. Mining distribution is halved every four years until no new block rewards are generated.

CPoW mining rules



The CPoW mining mechanism requires the miners to pre-store a certain amount of BFC in the wallet to mine normally when mining, otherwise only 30% of the mining revenue can be obtained.

If the miner does not deposit BFC in the wallet and runs the mining program directly, then only 30% of the mining revenue will be obtained, and the remaining 70% of the mining revenue will be automatically transferred to the BFC Foundation.

The miner will receive a 100% return on the BFC specified in the specified address. When the miner does not want to mine, he can withdraw the mortgaged BFC at any time in real time.

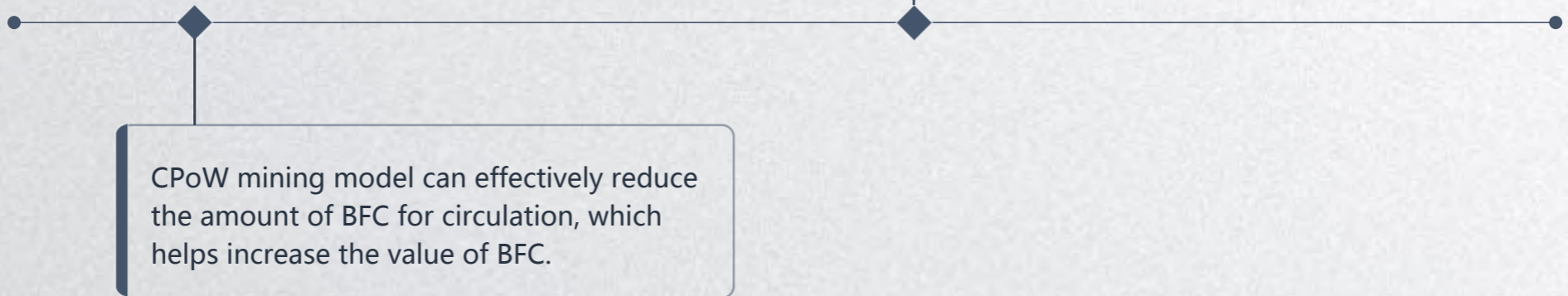
The SOLO mining miner needs to mortgage a certain amount of BFC at the block address. If the mine is mining, the miner needs to mortgage to the mine block address for mining.

Depending on the computing power, the number of BFCs that need to be pre-stored is different. The higher the computing power, the higher the amount of mortgages required. Pre-stored standard according to 300BFC per 1K computing power.

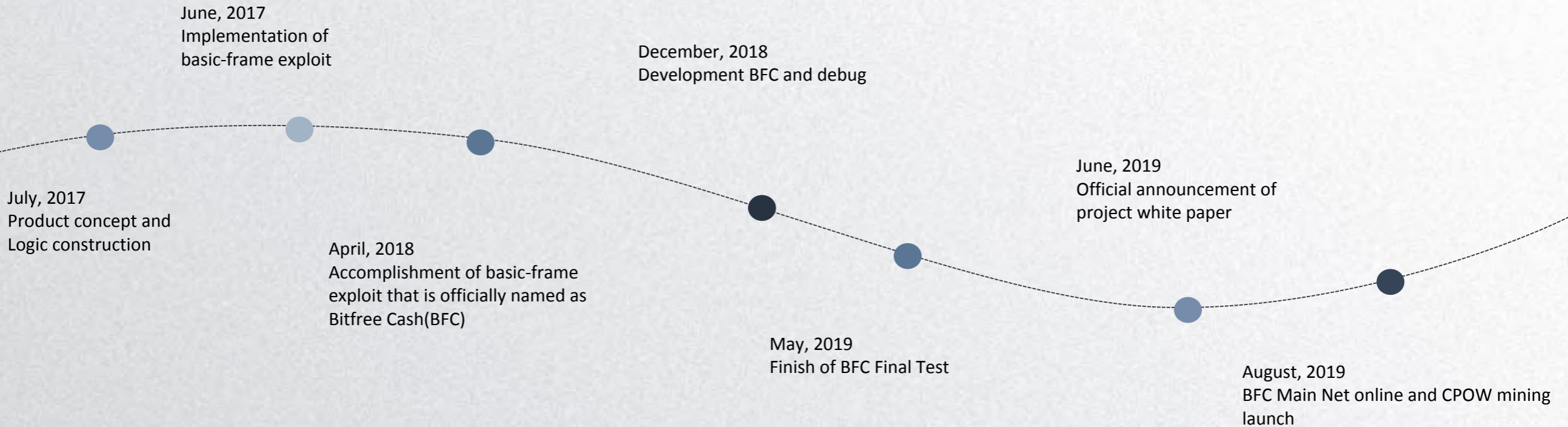
The goal of CPoW mining

The mechanism of CPoW mining is a key portion of BFC mining, and is also a guarantee for the healthy development of BFC.


Two main characteristics :



BFC Ecological Route



Summary



Due to an increasing number of cryptocurrency fans, the goal of decentralization is coming into reality. Each participant would like to participate and benefit, which cannot be achieved by the traditional PoW mining harder and harder. The CPoW mining model seems to increase the threshold of PoW mining, which is off the idea of decentralization. Virtually, it benefits the general cryptocurrency owners for more interests and makes the BFC a true decentralized encrypted currency. This is the original hope of Nakamoto.



Website : <https://www.bitfree.vip>



Github : <https://github.com/bitfreecash/bitfree>