White Paper

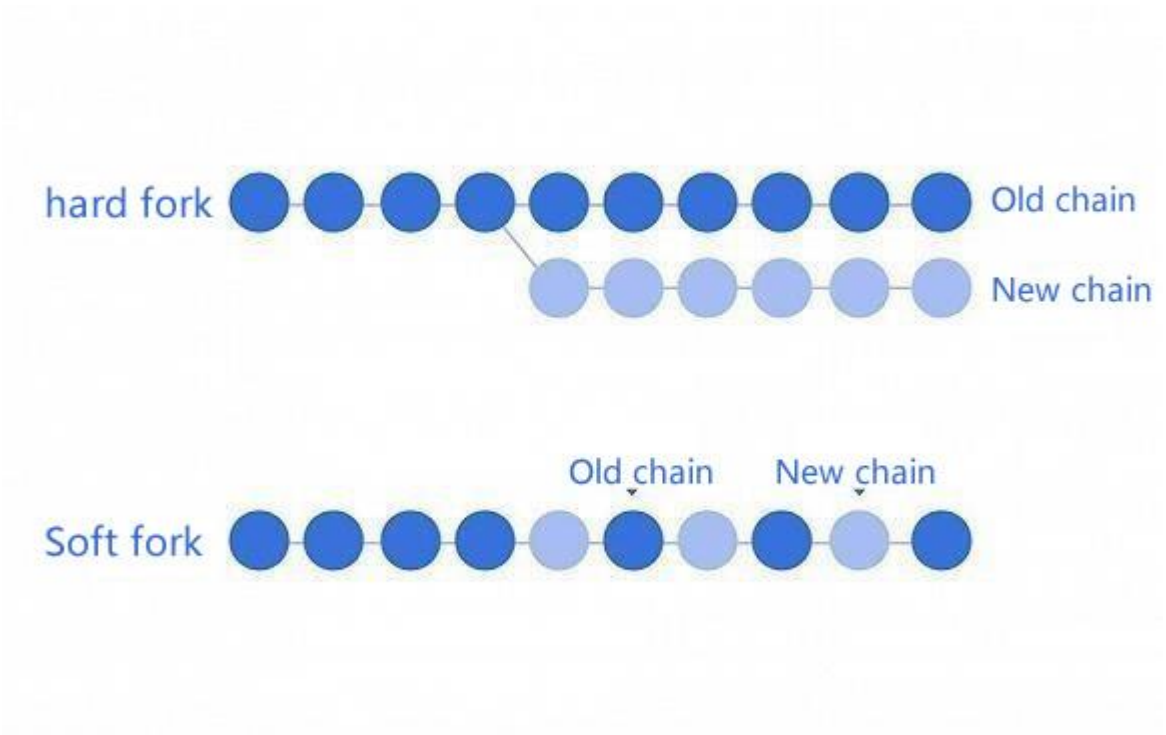
1 Blockchain digital currency

The first digital currency that uses blockchain technology was bitcoin. Bitcoin is a decentralized and globally universal electronic cryptocurrency that adopts blockchain as payment technology without any third-party organization or individual. Bitcoin was invented by Satoshi Nakamoto (alias) on January 3, 2009 based on a borderless peer-to-peer network using consensus-driven open-source software. Bitcoin is also the cryptocurrency with the highest visibility and highest market value.

Anyone can participate in bitcoin activities and issue bitcoin through a kind of computing named mining. The agreed maximum number of bitcoin is 21 million to avoid inflation. When using bitcoin, individuals are allowed to make payment directly to others based on their private keys as digital signatures without any third party such as banks, clearing centers, securities dealers to avoid high commissions, tedious processes, and regulatory issues. Any user who has access to digital devices with Internet connection can use bitcoin.

Bitcoin Cash (BCC, BCH) appeared on August 1, 2017 and is the first hard fork of bitcoin.

2 What is hard fork



Characteristics of hard fork: Re-upgrade the bitcoin system to completely change the height of the blocks through code form, using bitcoin unlimited as a mainstream solution. Such system has changed the block size of bitcoin networks and optimized the network's processing speed. However, the hard fork is not compatible with the original bitcoin system.

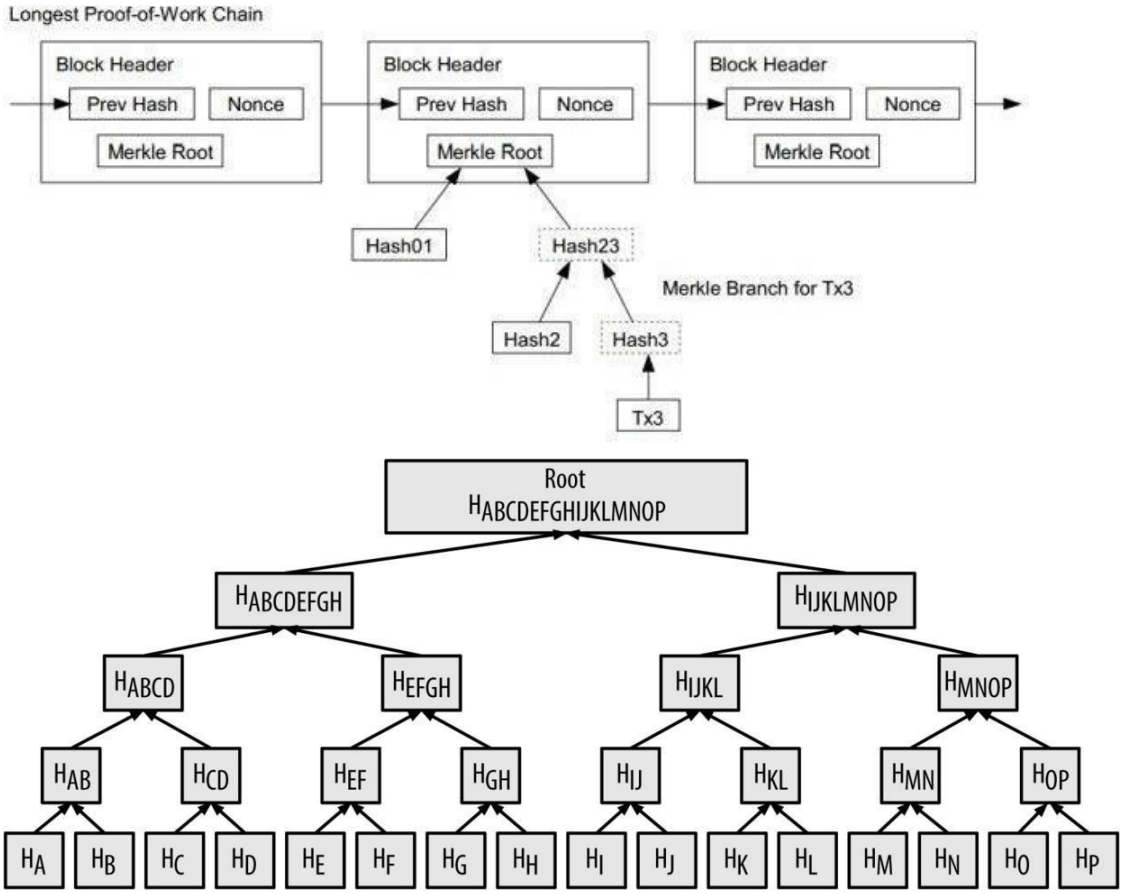
After hard fork, it is not compatible with the original bitcoin network. In this regard, all people using the bitcoin network need to support hard fork. If some people do not support the hard fork bitcoin network, there will be two versions and two bitcoins, giving rise to

competitions between two bitcoin blockchains. Such competitive relationship will lead to greater volatility in prices of bitcoin, but will also promote the healthy development of bitcoin ecology.

3 Why is hard fork necessary

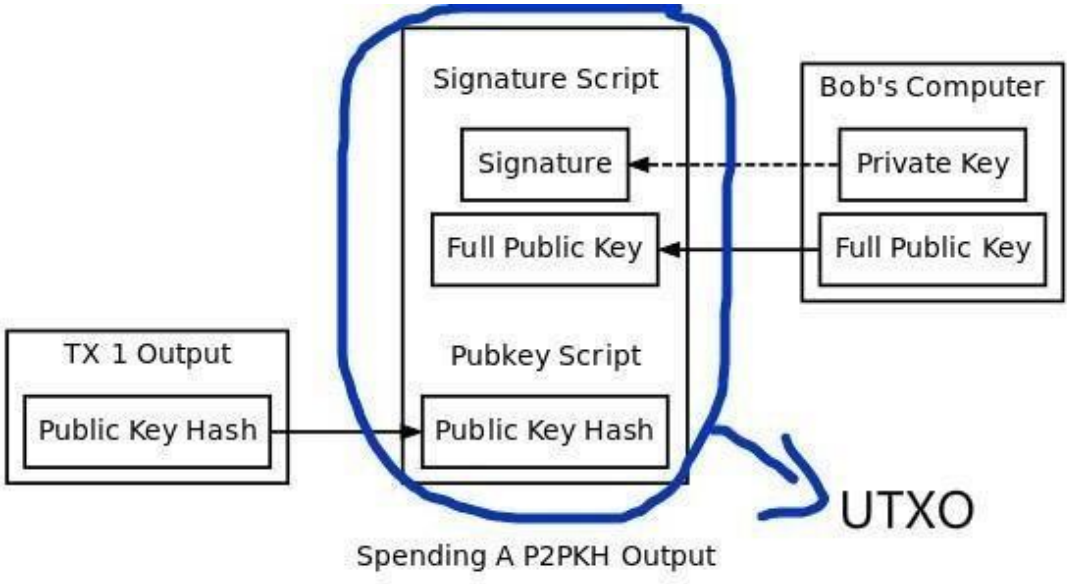
When Satoshi Nakamoto just started bitcoin, the bitcoin block size was 1M. Then, Satoshi Nakamoto sought to prevent DDos attacks. With the rapid development of bitcoin, the trading speed is becoming slower and slower. The core representing code power and the ore machine producers representing miners' power have different opinions on the future development of Bitcoin. The core insists on the solution of isolation verification being attached to small blocks, while the miners prefer the solution of large blocks. When there appears some sort of political stalemate and some people in the community stick to the old rules, problems will arise. The hash rate and network computing of the old chain will become outdated. Importantly, the data and rules of the old chain are still seen as valuable. Undoubtedly, miners hope to continue mining, while developers also hope to continue to offer support.

The following figure shows the data schematic diagram of bitcoin



UTXO represents Unspent Transaction Output. In the bitcoin community, transaction is referred to as TX, so the phrase above is abbreviated UTXO. UTXO is generally considered part of the design of the bitcoin blockchain.

The box that is circled with blue line is a "visualized" UTXO. The Public Key Hash for TX 1 Output is Hash for Bob's Full Public Key, and the address of bitcoin is BASE58 code (bidirectional) of the public key. The transaction chain of bitcoin can be imagined as a pipeline network with UTXO as a junction in the network. On this junction, there is a Pubkey Script that is off by default and water cannot flow from this junction to other pipelines. A key (Bob's private key) is required to open the valve to allow water to flow to another junction (UTXO).



Spending A P2PKH Output

Due to the special UTXO mode of bitcoin, this led to absence of smart contracts on bitcoin. The future will witness a digital society, in which programmability is an important feature. Although bitcoin is very stable, the lack of programmability is a soft spot in bitcoin, and the Ethereum blockchain is trying to solve this problem.

Ethereum is an open source public blockchain platform with smart contract function. It delivers decentralized virtual machines (referred to as "Ethereum Virtual Machines") to address point-to-point contracts through its proprietary cryptocurrency Ether.

Features of Ethereum include the following aspects when compared with a large number of other cryptocurrencies or blockchain technologies:

- Smart contract: It refers to the programs stored on the blockchain run by each node and requires the person running the program to pay a transaction fee to the node's miner or stakeholder.
- Proof-of-stake: Compared with proof-of-work, it can save a large number of computer resources wasted during mining and avoid the network centralization caused by Application Specific Integrated Circuit. (Not implemented yet)
- The development community is stable and growing, using hard fork.

The most important technical contribution of Ethereu is the smart contract. Smart contract is a program stored on block keys that assist with and validate the negotiation and operation of contracts. Ethereum's smart contracts can be written in Turing-complete programming languages. Although Ethereum improves the programmability of digital assets, and is faster than the bitcoin transaction, it also has its own shortcomings. In addition to scalability issues,

privacy, security, and blockchain governance are all the aspects that need to be improved before they can be implemented on a large scale. Privacy protection will affect a number of institutional applications, and it is less satisfactory when it comes to what Ethereum has done.

4 Bitclassic Coin

4.1 Advantages of Bitclassic Coin

To respond to the shortcomings of Bitcoin and Ethereum, we launch "Bitclassic Coin" in a great way.

Bitclassic Coin is a new generation of cryptocurrency, with a block size shifting from 1M to 8M and a faster transaction speed. The original bitcoin blockchain remains unchanged and the Bitclassic Coin is a new hard fork chain. The new branch has the same transaction history as bitcoin until a new chain emerges due to the fork. The birth of Bitclassic Coin mainly addresses a series of problems arising from the rapid development of bitcoin:

- Increase transaction speed

  A major upgrade is a wide expansion, with block size limit of Bitclassic Coin being raised to 8MB in order to process all transactions in each block in a more flexible manner. In addition, the transaction confirmation speed of Bitclassic Coin blockchain is significantly increased.

- Reduce transfer fees and user participation threshold

  The cost and threshold of participation is reduced to enable more users to engage in the trading activities of Bitclassic Coin more easily.

- Support zero-knowledge proof

  Zero-knowledge proof is a kind of interactive proof. In computational complexity theory, the interactive proof system (hereinafter referred to as interactive proof) is a type of computational model. Like other computational models, our goal is to determine whether x is in L for a language L and a given input x. The interactive proof system consists of two entities: Verifier and prover, both of which can be seen as some sort of Turing Machine. Its computing process is as follows: The input x is given and the information is exchanged between the verifier and the prover. Finally, the verifier decides whether the given input is in the language L based on the information given by the prover.

  Zero-knowledge proof has the following three traits:

  1) Completeness. If both the prover and the verifier are honest, follow each step of the proof process and conduct the right calculations, then the proof process must be successful and the verifier would be able to accept the prover.

  2) Rationality. No one can pretend to be the prover to make this proof successful.

  3) Zero knowledge. When the proof process is completed, the verifier only obtains the information that the "prover possesses this knowledge", and does not obtain any information about the knowledge itself.

  Advantages of zero-knowledge proof and related agreements:

  1) With the application of zero-knowledge proof, security would not be degraded as the proof is of a zero-knowledge nature.

2) High efficiency. The calculated amount of this process is small, and both parties exchange small amount of information.

3) Security depends on unresolved math problems such as discrete logarithms, large integer factorization, square root, and so on.

4) Technologies related to multiple zero-knowledge proof avoid the direct use of government-restricted encryption algorithms, which gives advantages to the export of related products.

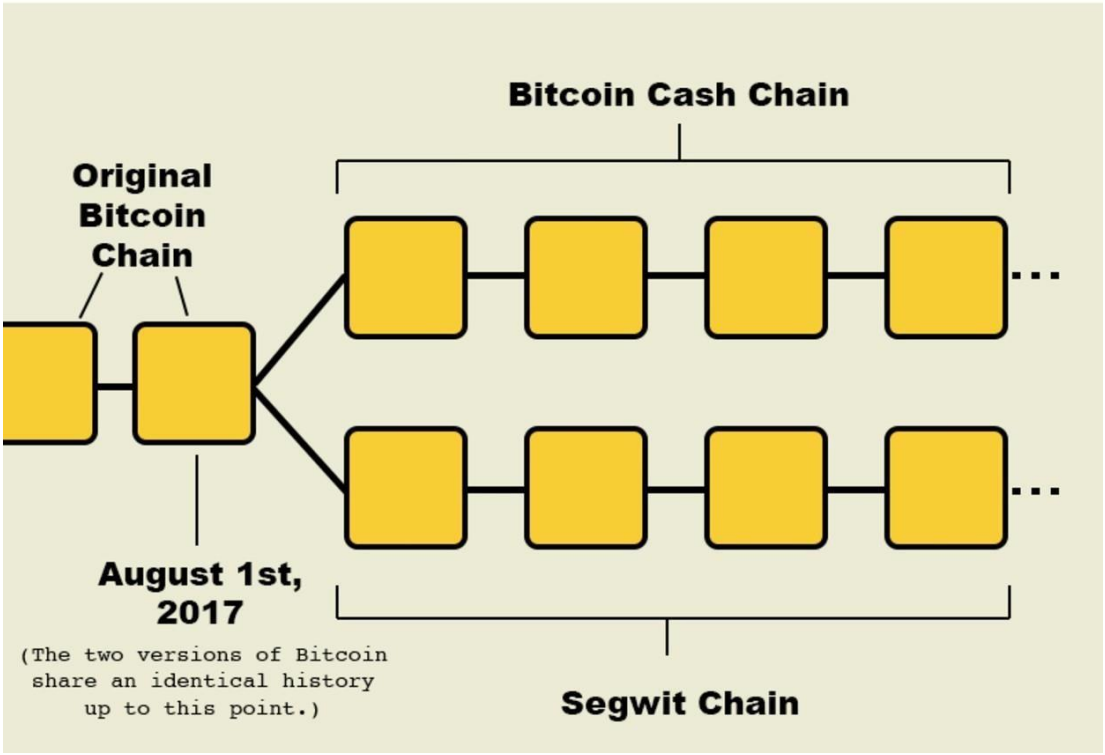
Zero-knowledge proof provides a way to prove the possessed knowledge without disclosing it. The process of zero-knowledge proof is widely applied in both identity authentication and NP problems.

The zero-knowledge proof of Bitclassic Coin will greatly protect the privacy of customers.

- Scalability:

Bitclassic Coin adopts the 8M block solution to greatly improve the transaction speed.

DIAGRAM OF THE BITCOIN CASH FORK

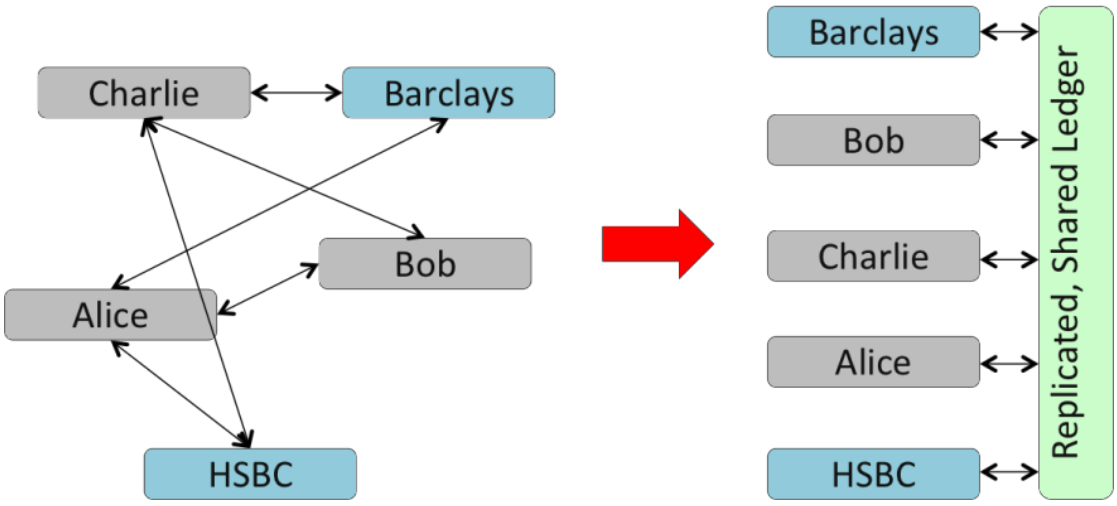


Bitclassic Coin, unlike the BCH solution, greatly enhances the privacy protection of user, and strictly abides by the spirit of Satoshi Nakamoto. Decentralized networks will facilitate the availability of the system greatly.

- Smart contract application:

Smart contract was proposed by Nick Szabo in the 1990s, as early as the birth of the Internet. Due to the lack of a trusted execution environment, smart contract was not applied to the real industries. Since the birth of Bitcoin, people gradually realize that the underlying blockchain

technology of Bitcoin could inherently provide a trusted execution environment for smart contracts.



A smart contract program is more than just a computer program that can be executed automatically: It is a system participant. It responds to received messages, receives and stores values, and sends out messages and values as well. Such program is like a trustworthy person who can hold assets on an ad hoc basis and always follow rules to be developed in advance.

The current smart contracts on the market are plagued by serious security risks, which can be described as follows

- Transaction order depends on contracts

  Transaction order dependency means that the execution of smart contracts varies according to the order in which the current transaction is processed. For example, there are two transactions T[i] and T[j], two blockchain states S[1] and S[2], and the state S[1] will shift to S[2] after the transaction T[j] is completed. Then, if the miners process the transaction T[i] first, the transaction T[i] calls the smart contract under S[1] state; if the miners process the transaction T[j] first, the contract state will shift to S[2] because of this. Finally, the transaction T[i] implements the smart contract under S[2] state.

- Timestamp depends on contracts

  When the miners process a new block, if the timestamp of the new block is larger than the last block and the difference between the timestamps is less than 900 seconds, such timestamp of the new block is legal. This is stipulated in the Ethereum agreement. Timestamp dependency means that the implementation of smart contracts rely on the timestamp of the current block. With different timestamps, the contract implementation results will vary.

- Reenterable assault

  In Ethereum, when a contract calls another contract, the current operation will stop till the call is completed. Then, problems will arise if the callee needs to use the caller's current state. Misoperation abnormalities

In Ethereum, a contract may call another contract by either sending an instruction or directly calling another contract's function. However, errors may occur during the call and the called

contract will fall back to the previous state. Then such abnormality may not be well known to the caller, depending on the method of call. For example, if a contract is called through the sent instruction, it should be verified whether it is correctly implemented by examining the returned value.

Bitclassic Coin will greatly change the above situations and enables smart contracts to be safer, more efficient and more user-friendly.

5 Technical parameters of Bitclassic Coin:

Total issue: 21.20 million Pre-dig 200,000 Allocation method: Mining Fork 1:1

Consensus mechanism: POW

Algorithm: SHA256

Mining equipment: ASIC

Block size: 8M

Replay protection: Supported

Block-out time: 10min

Project website: www.bicc.io

Project team: Top international teams in the world's blockchain field

6 Bitclassic Coin route map (Pacific time)

Established the team on June 1, 2017

Launched on the official website on August 10, 2017

Publicized on December 15, 2017

Fork the bitcoin blockchain at the height of 499888 on January 8, 2018

Traded on the exchange on February 8, 2018

Equipped with zero-knowledge proof on May 21, 2018

Smart contract will be available on October 30, 2018.