Bitcoin Classic

# Bitcoin Classic
## PROJECT WHITEPAPER

TABLE OF

# CONTENTS

TABLE OF

# CONTENTS

The existing Visa credit card network processes about 15 million Internet purchases per day worldwide. Bitcoin can already scale much larger than that with existing hardware for a fraction of the cost. It never really hits a scale ceiling."

Satoshi Nakamoto (April 2009)

Cryptocurrency is the future of economic, while Bitcoin Classic can be the best choice.

# ABSTRACT


## What is Bitcoin Classic (BXC) ?

Bitcoin Classic is a solution to the rising transaction fees and congestion on the Bitcoin network. With the growing popularity of Bitcoin, its main blockchain has experienced congestion, leading to higher fees and slower transaction times.

Bitcoin Classic addresses this challenge by providing a parallel network that leverages innovative technologies to reduce fees and increase transaction throughput. By offloading transactions from the main Bitcoin network onto our sidechain, users can enjoy seamless, cost-effective transactions while still benefiting from the security and immutability of the Bitcoin blockchain.

Bitcoin Classic with the symbol of “BXC”, is a digital currency set out by the great Satoshi Nakamoto , can be sent directly from person to person (peer-to-peer) via the net without need for a financial institution. Building a token economy that can be used by anyone, conveniently and naturally as part of daily life, replacing most international payment system in the world with a better user experience.

Bitcoin Classic brings a low-cost, safe and reliable payment method to merchants and users. It propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof- ofwork.

Bitcoin Classic (BXC) is a fork of Bitcoin that occurs at the block height of block 630,000 and therewith a new chain is generated as the BXC. Bitcoin Classic miners begins creating blocks with a new proof-of-work algorithm, and will consecutively develop and improve the transaction speed based on original features of BTC. This causes a hard fork of the Bitcoin blockchain. The original Bitcoin blockchain will continue on unaltered, but a new branch splits off from the original chain. Bitcoin Classic shares the same transaction history with Bitcoin until it starts branching and coming into a unique block from which it diverges.

# INTRODUCTION

The total amount of Bitcoin Classic is ten times that of Bitcoin which translates into a cost reduction for new participation and a reduction of necessary thresholds. Regardless of scalability, a chain is only as strong as its consensus. To reduce the danger of mining centralization, Bitcoin Classic uses an algorithm that makes it incredibly difficult for single entities to command large stakes of the processing power for block validation.

Total Issued Limited by

**210,000,000**

Block Size More Than

**8 MegaByte**

Block Creation Time

**1 Minute**

Faster Than BTC

**10X**

# BACKGROUND

**Bitcoin**

Bitcoin is a peer to peer electronic cash system created Satoshi Nakamoto. It was first detailed in the Bitcoin Whitepaper in October 2008, and the source code was released in January 2009. The Bitcoin ledger and Block chain were established with the generation of the Genesis block on the 3rd of January 2009 and the mining of Block 1 six days later on the 9th of January 2009.

Bitcoin allows electronic payments to be sent directly from one party to another, without requiring a central institution or server to process transactions and/or store funds.

The leaderless structure of the network is viewed as a resolution to The Byzantine Generals Problem allowing disconnected entities to follow a common direction without centralised instruction. This solves several issues previously seen as unsolvable in distributed networks, including the problem of preventing Double-spending of coins.

## BXC (Bitcoin Classic)

BXC raised the block size limit  to 8 MB as part of a massive on-chain scaling approach to create ample capacity for higher transaction storage. The transaction capacity of blocks will be increased and the ultimate goal is to improve transaction confirmation speed for the entire blockchain. With the addition of SegWit, transactions can now scale at a far greater pace than any Bitcoin chain before it. Bitcoin Classic also offers replay protection as the format for transactions that makes BTC transactions cannot be replayed in the BXC network as a way to steal user funds.

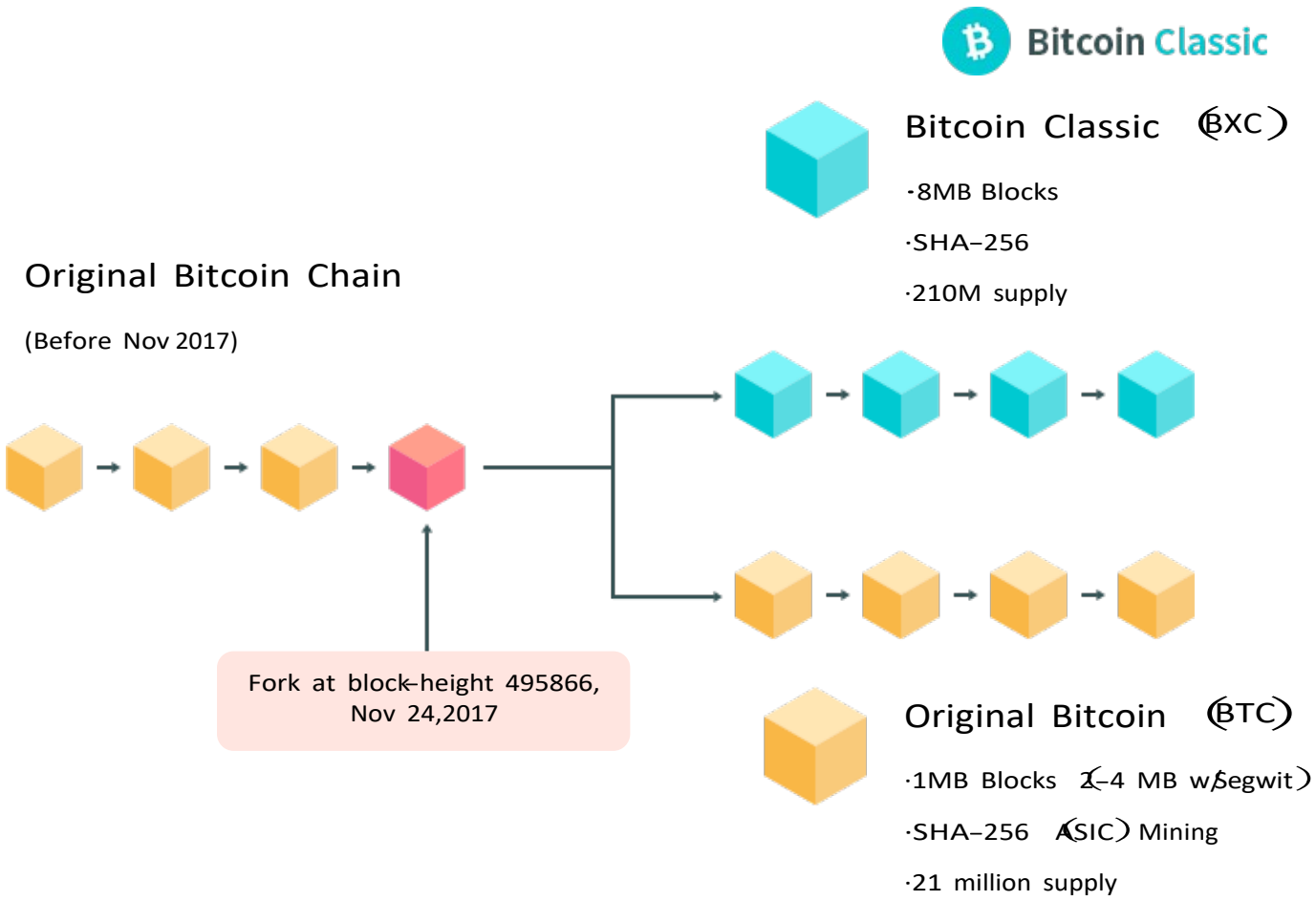
## Hard Fork

In blockchain, a hard fork is a change to a cryptographic protocol that causes a permanent divergence from the previous version. Users adopt the new protocol (fork to the new chain) with their own unique history, nodes and protocols.

Bitcoin Classic(BXC) nodes were once a part of the Bitcoin blockchain. Bitcoin Classic(BXC) is a fork of Bitcoin. BXC is a cryptocurrency with its own blockchain. It works as a POW network and new BXC is created through BXC mining.

The original Bitcoin remains unchanged, and the updated nodes split off from the original blockchain and create a new blockchain (like BXC) and the coins on the blockchain become separate and unique from the ones on the original blockchain.

Anyone holding the original coin at the time it was forked will automatically get the forked version of the coin they were holding. So, when Bitcoin forked to Bitcoin Classic(BXC), someone who had 10 BTC would automatically have received a certain number of BXC matching the value.




## Network

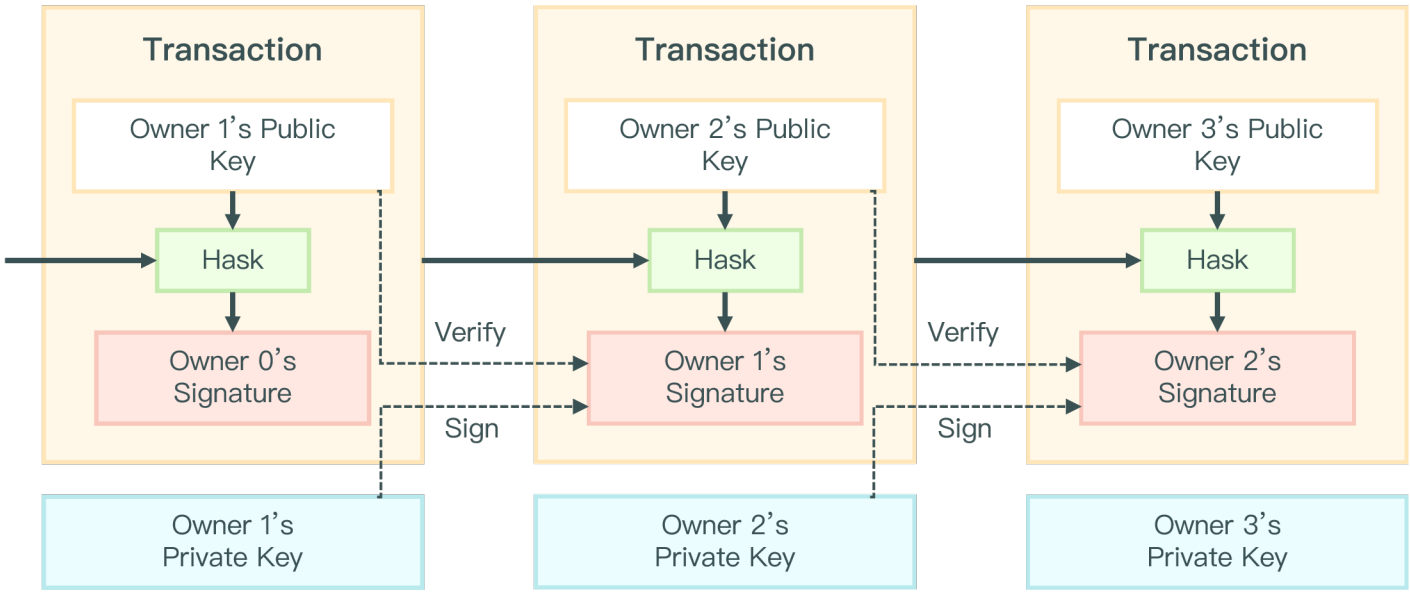
The Bitcoin Network is the network that all peers use to access the ledger. The network forms spontaneously over time as more peers access and use the system. There is no central governance that determines how peers on the network must connect, but the incentive structure that Bitcoin employs to bring enterprise miners into the system results in a spontaneously formed system which is simple and resilient.

Once the final restrictions on the protocol are removed in the Chronicle Update (expected early-mid 2021) network users will be able to create partitioned zones which employ specific rulesets particular to their requirements. This will be enabled by creating transactions that use OP_VER to give particular subsets of nodes specialised instructions, and will create the effect of layered network partitions over the core system which are referred to as Bitcoin Layered Networks.

## The Ledger

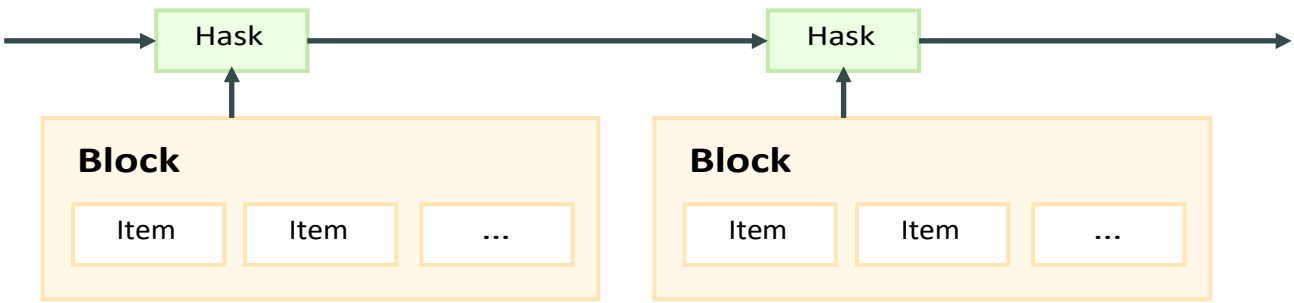
The Bitcoin ledger is a record of all valid transactions that have ever been transmitted to the network. The ledger is formed as a Directed Acyclic Graph (DAG) where each transaction is a node. The graph

starts at the Coinbase transaction of the first block ever found and via chains of digital signatures maps out the entire history of valid exchange actions, allowing the tracing of all Bitcoins back to their creation.



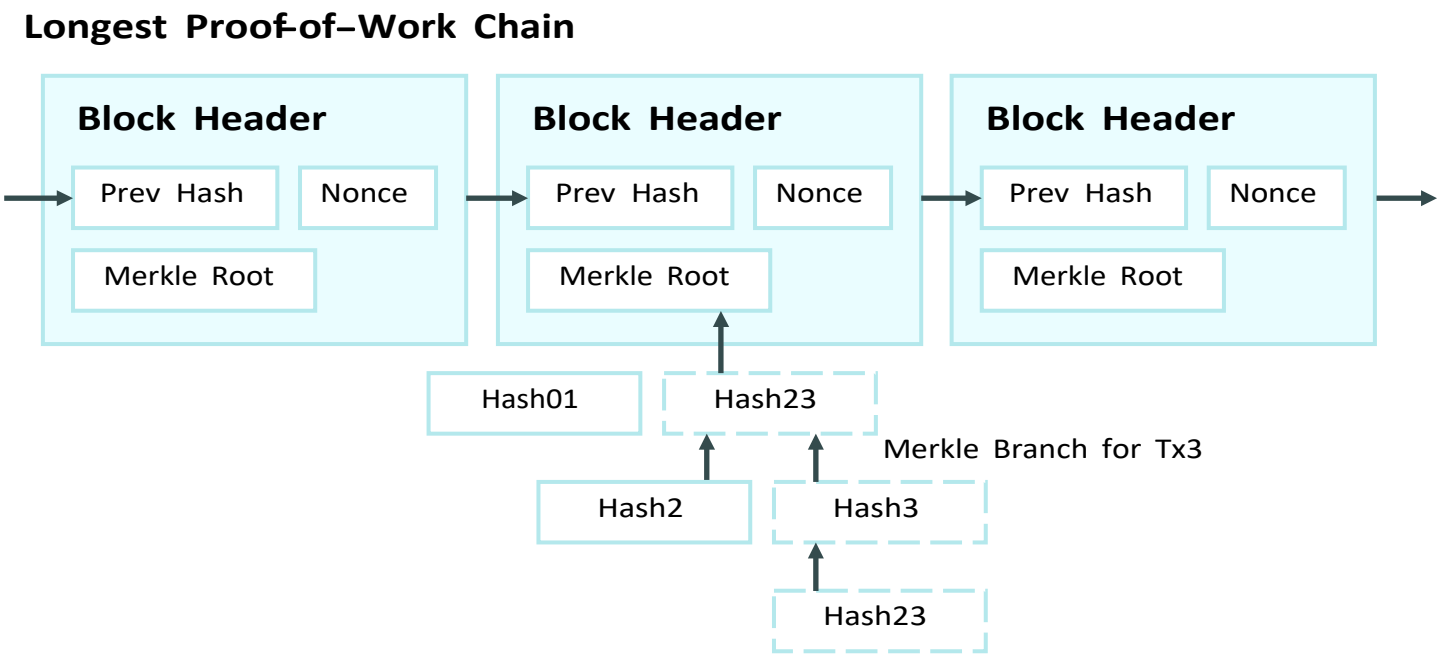

Valid transactions that are broadcast on The Bitcoin Network are committed to the ledger by miners in Blocks. A block consists of an ordered list of Bitcoin Transactions and a header which includes the root generated by hashing the listed transactions into a Merkle tree, a timestamp, a reference to the block it builds upon and the means to validate the Proof of Work needed for other miners to accept the block as valid.

Blocks form a second layer DAG called the Block chain which is built by network miners in a competitive process. Each block forms a node in the graph with a single incoming edge from the block it is built upon. A block may have more than one outgoing edge in a case where multiple blocks were built upon it, but only one of those edges can become part of the longest chain of proof of work. A block without an edge to the longest chain of proof of work is called an Orphan Block.



The structure of the block chain DAG means that there is a clearly traceable path back to the first block mined. Blocks are discovered just under every 10 minutes on average, with miners using a predefined mathematical algorithm to control the difficulty of the proof of work process to maintain that time frame.

Transactions can be exchanged peer to peer using Simplified Payment Verification (SPV) to manage trust. SPV involves sending accompanying information with a transaction input that proves it is from a transaction that has been timestamped on the ledger.



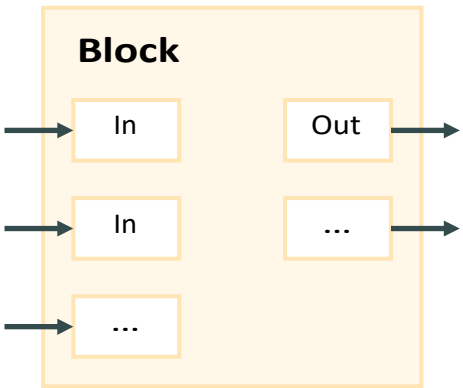

Users can exchange unfinalised transactions without sending them to the network to be mined creating what are called Payment Channels. Payment channels allow users to conduct information exchange within valid Bitcoin transactions, only broadcasting a finalised transaction including the full value exchange to the mining network once the information transfer is complete.

Once a transactions is sent to the network, global consensus can be reached on the validity in less than 2 seconds. If a transaction is not accepted by any miners and added to a block template, it is considered invalid. Transactions can be invalid for a variety of reasons such as being submitted with an invalid scriptSig, not adhering to network or miner rules, or not paying an adequate fee.

## Transactions

All Bitcoin Transactions are payments of some kind. Transactions are written in a flexible scripting language that is used to assign custodial control to each transaction output via the creation of arbitrary spending conditions defined by scripts.

Each transaction uses Bitcoins stored in 'unspent transaction outputs' as the transaction inputs. The transaction process aggregates the satoshis held in each input and spends them into a new set of unspent transaction outputs. When UTXOs are spent in a transaction they are consumed.



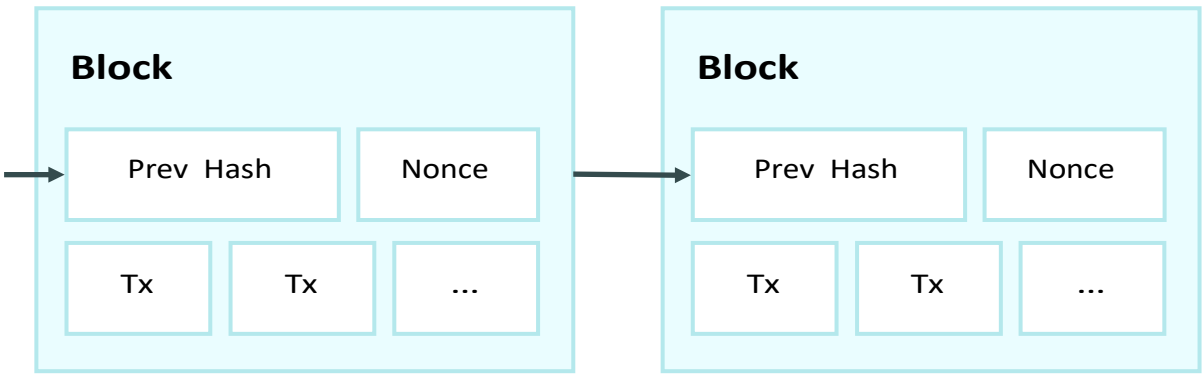

The Bitcoin scripting language can be used in a way that is Turing complete, creating a Turing machine that uses the Bitcoin ledger as a tape, reading to and writing from the transaction graph as needed.

The scripting language also includes opcodes that allow users to embed arbitrary data in transactions, providing for the creation of application layer protocols that use Bitcoin transactions as a transport layer.

Rewards paid to miners for the creation of a block are inscribed in what is called a Coinbase transaction. This transaction has a specific format and is always the first transaction in the block's Merkle tree.

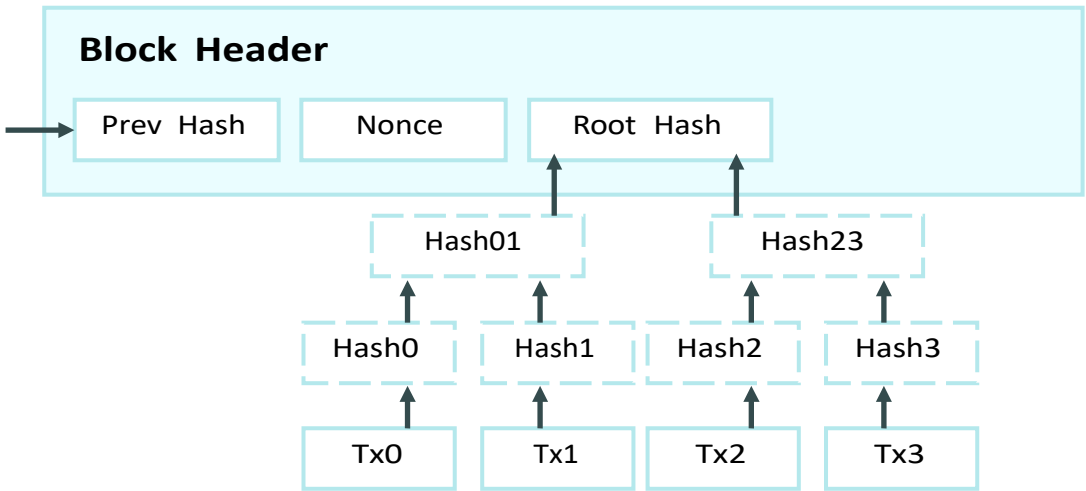
## Nodes and Mining

The ledger is held on a distributed network of nodes who use hash based Proof of Work to compete for the right to extend it and as a means to enforce network rules. The proof of work of each block in the longest chain of work is incorporated into its subsequent block to form the chain structure.




During the mining process, a node gathers transactions from the network on a first seen basis and evaluates whether they are profitable to mine before putting them into a block template. Block templates are created by calculating the root of a Merkle tree containing all of the transactions being mined. The order of transactions in the Merkle tree is not related to their position in the transaction DAG. As new transactions arrive, they are added to the tree, creating a new, updated template. Hash operators continuously request new block templates through the Getminingcandidate interface to ensure they are getting up-to-date block data to hash against. A block is found when a miner successfully discovers a value that generates a hash less than the difficulty target. The miner must then propagate the new block to the rest of the network who must then build an additional 100 blocks on top of it before the winner can claim the block reward.

## Block




Transactions Hashed in a Merkle Tree

Nodes are operated by the Bitcoin mining enterprises who build the network. Bitcoin's economic incentives are structured such that for the nodes to be most profitable at building the ledger they must be as closely connected to other well performing nodes as possible. This leads to miners forming a Small World Network which trends towards a Nearly Complete Graph where each miner is connected to most of the other miners. Miners gather transactions from users who connect in a layered network over the nodes at the core forming something that closely resembles a Mandala Network. Peers operating in these shell-like layers use Simplified Payment Verification to form a much less densely packed structure where information is exchanged in Payment Channels.

As Bitcoin scales, the nodes who comprise the network will be variously compartmentalised into specialised hardware. These clustered systems will be distributed globally, each being placed in a location optimised for its task.

As enterprise organisations, Bitcoin miners must operate as legal entities within a given jurisdiction and as such are bound to the laws and legal processes that exist in that jurisdiction. Through this, miners can be compelled to enact certain rules or perform certain actions in order to comply with the law.

## Unit of account

Satoshis are the ledger's native unit of account and 100,000,000 satoshis is abstracted to one Bitcoin. Satoshis are held in script puzzles called Unspent Transaction Outputs or UTXOs. These are transaction outputs which are held by miners in a quick access database called the UTXO set. During the spending process, UTXOs being used in a transaction are consumed and the solution to their puzzle script is recorded in the transaction.

Satoshis are distributed by miners to themselves as a subsidy payment during the network establishment phase. As the network matures, the subsidy dissipates forcing the miners to find alternate revenue streams. The payment allows miners to finance their operations through the payment of goods and services in Bitcoin, spreading it through the economy.

## Network rules

Bitcoin operates on a fixed ruleset. So-called consensus rules include things such as the operation of the opcodes in Bitcoin Script, the rate at which new Bitcoins are issued, the mathematical function used to

calculate the target for the Difficulty algorithm and more. The protocol is agreed upon by the miners who control network operation.

There are no limits in the Bitcoin protocol. Any limits imposed are put in place by miners who are incentivised to catch the largest profitable pools of transactions they can. Miners compete to offer better service to fee paying users by scaling their own capabilities.

Various kinds of problems have arisen in Bitcoin, which mainly consist of the following aspects :

1. Slow transaction confirmations.

2.High threshold for new members.

| | | |
|---|---|---|
| MAX SUPPLY | 21 M | 210 M |
| DISTRIBUTION | MINING | MINING |
| MINING ALGORITHM | SHA256(ASIC) | SHA256(ASIC) |
| BLOCKTIME | 10 MINUTES | 1 MINUTES |
| MAXBLOCKSIZE (SEGWIT) | 1 MB (2-4MB) | 8MB |
| DIFFICULTY ADJUSTMENT | 2 WEEKS | 33Hr |
| MAXTX/DAY | ~1.2 MIL | ~96 MIL |

| | | |
|---|---|---|
| SEGWIT | YES | YES |
| REPLAY PROTECTION | NOT NECESSARY | YES |
| ESTABLISHED SINCE | 2009 | May 20 |
| LIGHTNING NETWORK | YES | YES |

# WHAT PROBLEMS DOES Bitcoin Classic ATTEMPT TO SOLVE?

### Performance

The on-chain transaction processing capacity of the Bitcoin network is limited by the average block creation time of 10 minutes and the block size limit of 1 megabyte while Bitcoin Classic network's average block creation time of 1 minute and the block size limit of 8 megabyte.

| | |
|---|---|
| **Stability** | The BXC(Bitcoin Classic) is to provide assured stability with only a limited changes planned to enable innovation to occur on top of a stable base protocol.<br><br>Enable businesses and development teams around the world to create solutions on the Bitcoin Classic network, such as smart contracts, tokenisation and many more. Businesses, especially the biggest enterprises, require stability before they will operate on a technology platform. |
| **Scalability** | In order for Bitcoin Classic to truly act as a global money platform, it is necessary to demonstrate that the platform is ready to process transaction volume at the required scale. Bitcoin Classic primarily focussed on delivering capacity increases, through bigger default or miner configurable block sizes and performance improvements.<br><br>By enabling massive scaling, Bitcoin Classic is paving the way to support significantly higher transaction volumes.<br><br>Big blocks and large throughput capacity allow enterprises use Bitcoin Classic for their blockchain applications. |

| | |
|---|---|
| Security | BXC will be a global currency. To enable such a future, we need to be prepared to ensure a level of security commensurate with a global money system. To do this, the Bitcoin Classic has focused on rigorous Quality Assurance for mining node software.<br><br>This is achieved by implementing a rigid set of test phases with full traceability throughout the test pipeline, to assure users that changes pass through a formal and rigorous validation process before they are accepted. |

# Bitcoin Classic TRANSACTIONS

### Larger Blocks for Faster Transaction Confirmations

Bitcoin Classic (BXC) raised the block size limit to 8MB as part of a massive on-chain scaling approach.

There is now ample capacity for everyone's transactions to be processed. The transaction capacity of blocks will be increased five-fold and the ultimate goal is to improve transaction confirmation speed for the entire blockchain. With lightning fast transactions, highly diluted transaction fees, and ten times as much supply as other leading Bitcoin forks, Bitcoin Classic's blockchain prioritizes trust, accessibility, and affordability.

While there are concerns that large blocks may rapidly increase the blockchain's total size,the present number of transactions included in each block is still far from hitting the upper limit of the block size. In case of a future volume increase, additional mechanisms such as sharding are already being considered to reduce the problem of storing a colossal blockchain size.

### Lowering Transaction Costs with a Larger Supply

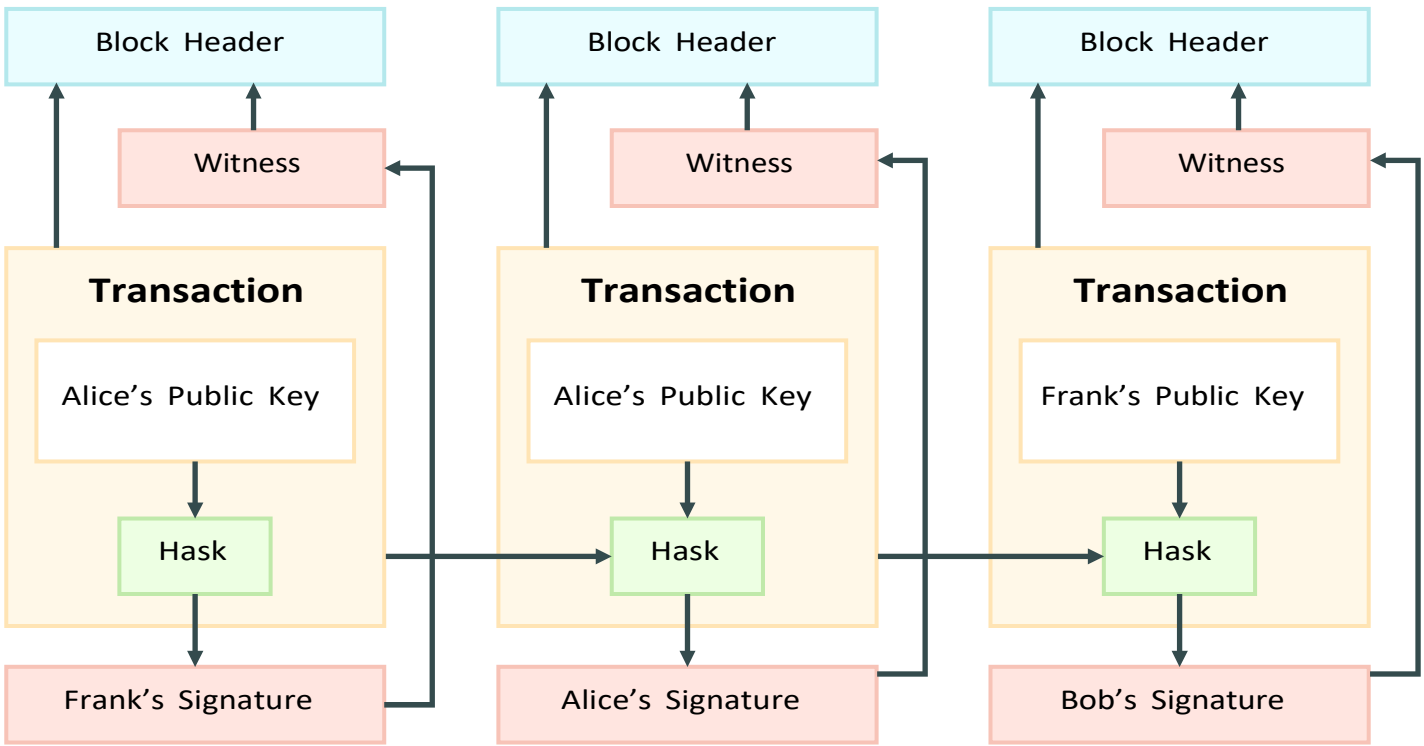
BXC (Bitcoin Classic) reduces the transaction fee and the cost of participation. The total amount of BXC is 210M that is 10 times of BTC so that it reduces the cost of participation.
Bitcoin Classic improves the situation of overpriced Bitcoin, increasing the total supply of

BXC and lowering the price. This supply change increases circulation and helps emphasizes the use of BXC for smaller transactions. With relatively low transaction fees, a secure and private blockchain, and affordable token prices, BXC is well suited for making everyday transactions.

## Segregated Witness to Optimize Storage

Segregated Withness(SegWig) is the process by which signatures in a Bitcoin transaction are "segregated" from the transactions data. SegWit defines a new structure called a "witness" that is committed to blocks separately from the merkle tree that holds transactions. By removing signature data in this manner, 65% of storage space is freed up so that block capacity for transactions is increased.

## Segwit Blocks




Signatures are relocated away fron the transaction hash in the "Witness"to increase capacity and curb malleability attacks

## THE ADVANTAGES TO FOLLOW SEGWIT?

Block information are divided into trading information and witness information. Trading information means someone transfer amount at a specific time. Witness information means at a specific node and time to verify the reliability of trading information. Bitcoin put two information into the same block directly, so BTC cannot bear more trading information. By using segwit, block only records trading information and each block will record more trading. Bitcoin Classic will increase the unit block to bear more trading, in order to optimize the storage of BXC network.

## Anti-Replay Protection

A replay attack can occur when valid transactions on the BTC blockchain are ‘replayed’ on the Bitcoin Classic network. Attackers could use valid BTC transactions to rob users of BXC even though both chains have forked. To prevent this, the transaction format of BXC has been changed with a new transactions version number rather than BTC’s 1-3 since the fork so that BTC transactions cannot be mistaken as valid.

Additional changes to BXC’s transaction format are planned for the future. This will help Bitcoin Classic be more reliable as it updates.

## Lightning Network

While Bitcoin Classic protocol provides faster transactions, additional scaling solutions are still required for the the protocol to compete with traditional payment methods. To accomplish this, the BXC development team is working to implement Lightning Network, a "second layer" payment protocol first proposed by Joseph Poon and Thaddeus Dryja in
2016. This solution allows users to open “payment channels” by committing an amount of Bitcoin that can then be sent to other participants on the channel without being confirmed on the main chain. Using Lightning Network, Bitcoin Classic can enable users to make instant transactions at a nearly limitless pace for a very low cost.

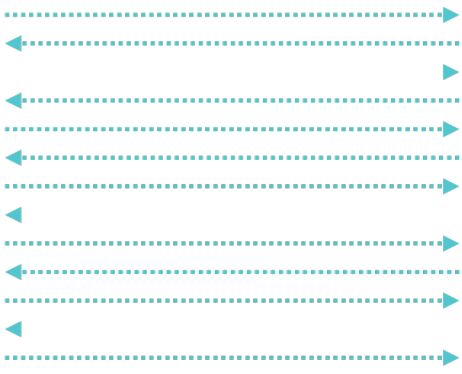
Bitcoin Classic

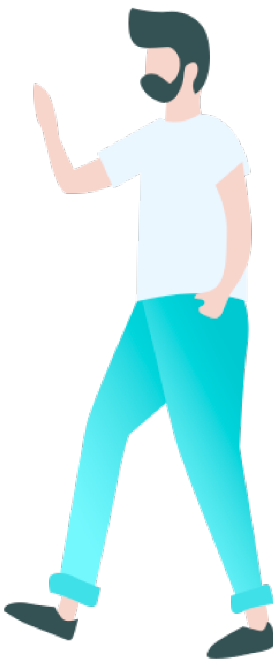
trustless

## Payment Channels on Lightning

Open Channel (on-chain)

Alice and Bob can make a high volume of instant,





Alice

Open Channel (on-chain)

Bob

micropayments off-chain

# FAQ

## Why Blockchain?

Blockchain network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

While the conventional financial system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for nonreversible services. With the possibility of reversal, the need for trust spreads. Receivers must be wary of the senders, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. Bitcoin-like blockchain system is the most secure as long as the other conventional financial systems existing on world keep the same principle they did.

## Why Bitcoin Classic (BXC)?

Bitcoin Classic is committed to keeping fees low. Bitcoin Classic’s objectives are to empower unbanked people to use Bitcoin Classic to build wealth for themselves and their families, to establish Bitcoin Classic as the number one cryptocurrency used in emerging economies, and to make Bitcoin Classic accessible and usable for everyday transactions.

## How to get Bitcoin Classic (BXC) ?

Bitcoin Classic is generated all over the world by anybody running a open-source application called a “BXC Miner". Mining requires a certain amount of work to be performed before they're dutifully rewarder with some BXC. Temporary, there is no (or maybe few) official cooperating crypto exchanges or markets selling BXC. The only way to get BXC is mining.

## How to use Bitcoin Classic (BXC) tokens?

How to use BXC tokens? You can store BXC tokens using the official Bitcoin Classic Wallets. With the peer-to-peer send and receive functions, you can trade BXC to whomever accepts it for products or services. For example, you can sell your house to your friend by telling him your BXC address, and wait for his transaction complete via BXC network's confirmation.

Certified BXC wallets for mobile OS are still under security review of Bitcoin Classic Foundation. The most secure way to store and trade BXC is the official wallets by far.

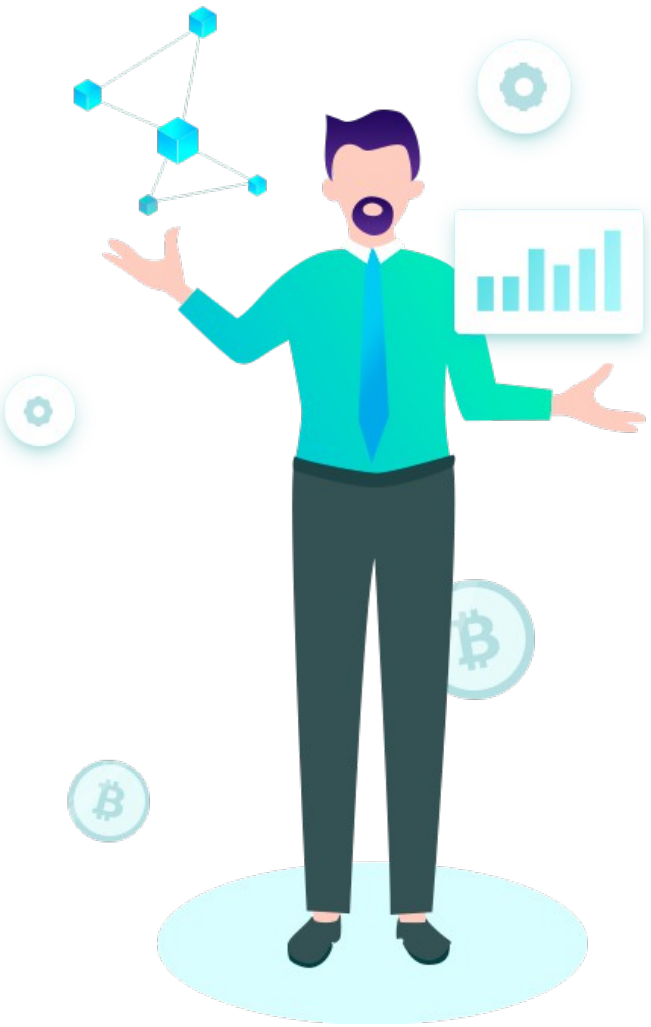
Bitcoin Classic also recommend hardware wallets, it's a strong way to protect your digital assets being attacked. Since BXC shares the base code of the original Bitcoin, some hardware wallets may work well with BXC.

## BXC Issuance and Management

The total amount of BXC to be issued is limited to 210 million. BXC will be distributed as miner rewards, without an ICO or any reserves.

Certified BXC wallets for mobile OS are still under security review of Bitcoin Classic developers and miners. The most secure way to store and trade BXC is the official wallet mentioned above by far.

Bitcoin Classic also recommend hardware wallets, it's a strong way to protect your digital assets being attacked. Since BXC shares the base code of the original Bitcoin, some hardware wallets may work well with BXC.



## SHOULD I BUY Bitcoin Classic?

As the developers of the project, we will not predict price or provide any investment advice. We create BXC as a free dividend for BTC holders. Anyone who holds Bitcoin at the time when Bitcoin Classic was created became owners of Bitcoin Classic. You can receive the full benefits of this project without any additional risk simply by holding Bitcoin, the best form of money the world has ever seen.

## What we see in THE FUTURE

The Bitcoin Classic Project may work in cooperation with many organizations to provide opportunities for global economic systems. With the help of strategic partners and individuals, Bitcoin Classic provides grants to

educational and financial institutions and organizations to encourage international economic freedom. Your participation can help establishing new nodes and support initiatives to prepare individuals navigate through different

languages and countries so they are ready to join the network with global node around. Bitcoin Classic will provide better opportunities to deserving world to a little smarter and more fare economic system.

## Bitcoin Classic BXC

- More information on : www.bitcoinbxc.com
- Blockchain explorer : http://bitcoinbxc.com:3001/
- If you have any questions about the Bitcoin Classic project or BXC tokens, please contact : inboxjackdavis@gmail.com


## ACKNOWLEDGMENTS

BXC is the synthesis of many great ideas and systems. It would be impossible to dare such ambitious goals without standing on the shoulders of such giants. Personal thanks to Satoshi Nakamoto, for his ever brilliant ideas.