

# Bluecoin 2.0

## “The BluePrint”



Bluecoiner  
bluecoiner@yandex.com

## 1. Introduction

Bluecoin is a hybrid Proof-of-Work/Proof-of-Stake-Velocity (PoW/PoSV) cryptocurrency that has been actively developed, used, and traded since 2014. Since the introduction of Bluecoin, there have been important advancements in the field of cryptocurrency development. These advancements include multisignature addresses to better add security to managing BlueCoins, cold-staking protocols to protect tokens held in stake accounts, so-called “Layer 2” scaling solutions such as the Lightning Network, and the introduction of novel extensibility techniques such as Segregated Witness.

In July 2016, Bluecoin core developers began working to upgrade the protocol to add better security for end-users. After much deliberation, it was decided that the most secure way to perform the upgrade to Bluecoin 2.0 was through a Proof-of-Burn upgrade to a new blockchain. Details of the Proof-of-Burn upgrade procedure are described later in this paper.

The new Bluecoin 2.0 client will be based on the Bitcoin Core 0.13.0 codebase, with several important changes including the activation of Segregated Witness and the preservation of Bluecoin's PoW/PoSV hybrid consensus algorithm. This move to the Bitcoin Core codebase brings over two years of advanced cryptocurrency research to Bluecoin, bringing the protocol and client up-to-date with the state of the art developments in cryptocurrency and setting the stage for virtually unlimited transaction scalability via sidechains and Layer 2 extensions. Other notable changes coming to Bluecoin 2.0 include the modification of the Bluecoin Proof-of-Work algorithm from Dark Gravity Well to Auxiliary-Proof-of-Work (AuxPoW) using the Scrypt algorithm, the introduction of cold-staking to protect coin balances while they are staking, a new inflation algorithm to better align the incentives for AuxPoW miners and the user base, and finally off-line bluetooth transactions which will allow users to make payments without having access to the Internet.

The publishing of this paper and the corresponding code that implements the features described herein marks the beginning of a new era for Bluecoin development. We consider Bluecoin to be an active cryptoeconomic research project that tests proposed advancements in real-world adversarial game theoretic conditions with real money on the line, and we look forward to learning from the results of this experimentation. It is our hope that our research and findings will continue to influence the future

of cryptocurrency development and help usher in the next generation of peer-to-peer blockchain advancements that will revolutionize stagnant industries and bring greater economic freedom to the world.

## 2. Bluecoin 2.0 Codebase

With an opportunity to start fresh, the Bluecoin development team has chosen to base the codebase of the Bluecoin 2.0 reference client on Bitcoin Core 0.13.0, the most recent release of the Bitcoin Core client at the time of this writing. With over two years of advancements implemented in their codebase since the first release of the Bluecoin reference client, there are too many changes to list here, however, there are some notable scalability and privacy enhancements worth mentioning to provide a glimpse of what is to come for Bluecoin 2.0:

- **Multisignature addresses and transactions** – multisignature transactions require signatures from multiple private keys before they are considered valid by the rest of the network. This provides better security for funds held in multisignature addresses.
- **Headers-first synchronization** – drastically increases the speed of the initial full node synchronization stage by first asking peers for all block headers, then downloading the block data after the headers have been validated.
- **Block pruning** – allows full nodes to delete the raw block and undo data once it's been validated and build the transaction databases. This can be useful for users that want to preserve hard drive space.
- **CLTV** – adds a new opcode that allows a transaction output to be made unspendable until some point in the future. This opcode can be used to create more robust payment channels.
- **Faster signature verification** – use of the libsecp256k1 library results in signature verification that is 7x faster than the previous OpenSSL library.
- **Automatic Tor usage** – if Tor is running on the same machine as the Bluecoin 2.0 client, the client will attempt to route all Bluecoin traffic over the Tor network.
- **Compact block relay** – reduces the amount of bandwidth used by transaction relay nodes, eliminates bandwidth spikes when nodes receive a new block, and speeds propagation of blocks across the network.
- **Segregated Witness** – fixes transaction malleability issues, increases the security of multisignature accounts, reduces UTXO growth, and increases transaction capacity. Segregated Witness paves the way for additional features via sidechains and easier advanced scripting upgrades, as well as scalability increases via Layer 2 extensions such as the Lightning Network.

## 3. BlueCoin 2.0 Consensus

The consensus algorithm used in Bluecoin 2.0 is an Auxiliary-Proof-of-Work/ Proof-of-Stake-Velocity (AuxPoW/PoSV) hybrid consensus algorithm. While Bluecoin 1.0 used a variation of the Dark Gravity Well algorithm for its implementation of Proof-of-Work, Bluecoin 2.0 uses an AuxPoW Script algorithm that enables merge-mining with Litecoin and other AuxPoW Script networks. This will help protect the Bluecoin network from 51% attacks.

## 3.1 Aligning Incentives

As part of the reactivation of PoW mining, Bluecoin 2.0 is adjusting the inflation algorithm from the current 5% annual inflation rate to 3% annual inflation, with 2% annual inflation going to the AuxPoW miners and 1% annual inflation going to the PoSV miners. The extra coinbase rewards for AuxPoW miners are to compensate for the fact that AuxPoW mining requires an investment in specialized hardware and ongoing operational expenses that can be orders of magnitude more expensive than the cost to setup and maintain a PoSV mining node. Bluecoin developers will continue to monitor the performance of the network to ensure that these incentive parameters provide the intended security benefits.

## 3.2 Cold Staking

In traditional Proof-of-Stake protocols, it is necessary to store a private key on a computer that is connected to the internet so that the private key can sign and broadcast new blocks of transactions. The same private key used to sign new blocks must also control a balance of tokens (“stake”) to produce new valid blocks (“staking”). Since the private key used to sign staking messages is the same private key used control transfers of the stake, hackers have a significant financial incentive to find and compromise staking nodes in order to steal the stake. Some Proof-of-Stake clients require a password to be entered before online stake can be moved to another address, but this does not protect against keyloggers. What is needed is a protocol that separates block signing and transaction signing authority.

Bluecoin 2.0 adds a mechanism for “cold staking” whereby validators can delegate block signing authority from a transaction account to a validation account and keep the private keys controlling the transaction account offline in cold storage.

### 3.2.1 The Cold Staking Process

Cold staking in Bluecoin is a six-step process:

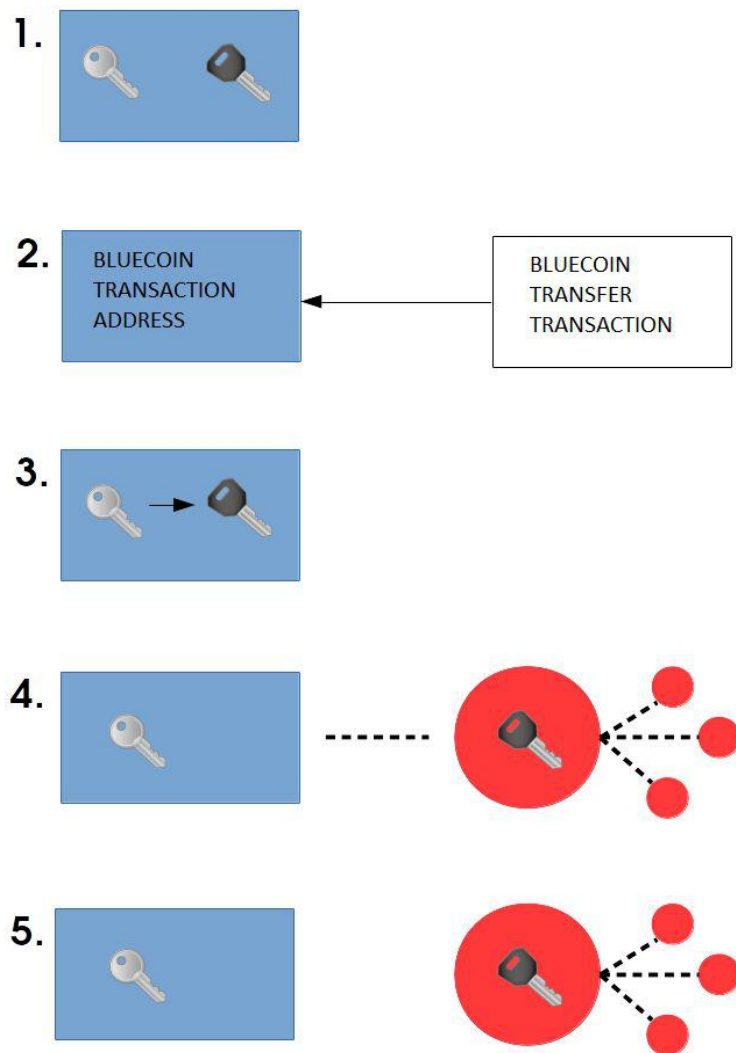
1. On a permanently offline computer, two accounts are created. One is a transaction account that is used to create a transaction address. The private key of the transaction account can sign *transfer transactions* that move coins controlled by the transaction address. The private transaction key should be kept offline in cold storage at all times. The other account is a minting account that is used to sign new blocks. The minting account will be kept on an online computer so that it can readily sign and broadcast new blocks to the network.
2. Send stake to the transaction address to prepare the address for the cold staking procedure.
3. On the offline computer, sign a *delegation transaction* that delegates validation authority from the transaction account to the minting account.
4. Transfer the minting account, the transaction address, and the delegation transaction to a hot wallet on an online computer and import the transaction address into the hot wallet as a watch-only address. This address can be used to receive block rewards and increase the minting power of the minting account and broadcast the delegation transaction to the network. Once the delegation transaction is

confirmed by the network, the minting account can begin signing new candidate blocks.

5. Begin signing new blocks with the private minting key to compete for block rewards.

*Note: All of the keys in this scheme are vulnerable to quantum attacks since the public keys must be broadcast to the blockchain so that blocks and transaction signatures can be verified by the network. This is a flaw with all Proof of Stake systems, and the author is not aware of a solution to this problem.*

## **Figure 1. The five-step cold staking process.**



## 4. Offline Bluetooth Transactions

Bluecoin 2.0 will enable Bluetooth based offline transactions, allowing senders (customers) to transmit bluecoins to their designated receiver (merchants) without requiring an Internet connection. This feature is especially useful in the developing world where cellular coverage is unreliable and roaming costs are prohibitive. Bluecoin 2.0 will use a single pairing interaction; by scanning the receivers payment request, a bluetooth channel is established which subsequently is used to communicate the signed transaction back to the receiver.

### 4.1 Bluetooth Transaction Process

Offline Bluetooth transactions are a 4-step process in BlueCoin:

1. Bluecoin payment server establishes a new Bluetooth socket connection directly to the given MAC address in the &request= parameter of the bluecoin: URI.
2. Receiver sends back a signed payment request. The submit URL in the payment request is another Bluetooth mac address.
3. The client parses the string, verifies the signature, and displays the sender a confirmation on their device. The sender confirms and transmits the PaymentACK back through the open Bluetooth socket.
4. The payment server accepts the message and the payment is complete.

*Note: Transactions executed in Bluetooth mode may be vulnerable to spoofing & double-spend attacks. Merchants must ensure that incoming payments are validated on the bluecoin network before finalizing the transaction. The larger the amount, the longer the validation waiting period should be.*

## 5. BlueCoin 2.0 Burn Upgrade

Due to the radical changes introduced in Bluecoin 2.0, including a transition to a completely new codebase based on Bitcoin Core 0.13.0, the Bluecoin development team have determined that the most fair way for the network to upgrade is to use a 60 day Proof-of-Burn (PoB) procedure to move value from the old Bluecoin blockchain into the new Bluecoin 2.0 blockchain.

**WARNING: DO NOT SEND BLUECOINS FROM AN EXCHANGE OR HOSTED WALLET ADDRESS TO THE PROOF-OF-BURN ADDRESS. YOU MUST FIRST WITHDRAW ALL OF YOUR COINS TO YOUR BLUECOIN DESKTOP WALLET AND THEN SEND THE COINS TO THE BURN ADDRESS.**

The details of this PoB procedure are as follows:

1. The Bluecoin development team will announce a start date for the Proof-of-Burn procedure on the Bluecoin website at <https://bluecoin.org> and on the official Bluecoin ANN thread on the BitcoinTalk forum. The PoB period will last until sixty calendar days after the announced start date, after which it will no longer be possible to transfer bluecoins from the Bluecoin 1.0 blockchain to the Bluecoin 2.0 blockchain.
2. Download and install the Bluecoin 2.0 desktop wallet from <https://bluecoin.org/download>
3. Open your Bluecoin 1.0 desktop wallet and send all of your bluecoins to the Proof-of-Burn address at BXXXXXXXXXXXXXXXXXXXXX.
4. Go to the Bluecoin data directory on your computer and save a backup of your wallet.dat file.
5. Copy and paste your Bluecoin wallet.dat file into the data directory of your Bluecoin 2.0 wallet.
6. After the PoB period is complete, the Bluecoin development team will announce the date of the launch of the Bluecoin 2.0 genesis block. On the day that the genesis block of the Bluecoin 2.0 blockchain launches, open up your Bluecoin 2.0 wallet. You will have the same number of coins in this wallet as you sent to the Bluecoin Proof-of-Burn address, and you will be able to transfer these coins to any other address on the Bluecoin 2.0 network.

Once the genesis block of the Bluecoin 2.0 blockchain is launched, miners and minters will be able to begin competing to find blocks and earn their portion of the 3% annual inflation of bluecoin. The Bluecoin 1.0 blockchain will continue to exist as long as it has users and minters but the Bluecoin development team will no longer be supporting any of the software compatible with the legacy blockchain.

# Glossary of Terms

Account: a public/private keypair.

Mining: creating new blocks through Auxiliary-Proof-of-Work.

Minting: creating new blocks through Proof-of-Stake-Velocity.

Minting account: an account that has been delegated minting power by a transaction account. The private key of a minting account is used to sign new blocks.

Stake: bluecoins held by a transaction account for the purpose of adding minting power to the delegated minting account.

Transaction account: an account used to send and receive bluecoins. The private key of a transaction account is used to sign delegation and transfer transactions.

## References

1. Various, "Bitcoin release notes," 2014 – 2016. [Online]. Available: <https://github.com/bitcoin/bitcoin/tree/master/doc/release-notes>
2. L. Ren, "Proof of Stake Velocity: Building the Social Currency of the Digital Age," 2014. [Online]. Available: <https://www.reddcoin.com/papers/PoSV.pdf>
3. Various, "Merged mining specification," 2011 – 2015. [Online]. Available: [https://en.bitcoin.it/wiki/Merged\\_mining\\_specification](https://en.bitcoin.it/wiki/Merged_mining_specification)
4. J. Poon, T. Dryja, "The Bitcoin Lightning Network: Scalable Off-chain Instant Payments – DRAFT Version 0.5.9.2," 2016. [Online]. Available: <https://lightning.network/lightning-network-paper.pdf>
5. A. Back, M. Corallo, L. Dashjr, M. Friedenbach, G. Maxwell, A. Miller, A. Poelstra, J. Timón, P. Wuille, "Enabling Blockchain Innovations with Pegged Sidechains," 2014. [Online]. Available: <https://www.blockstream.com/sidechains.pdf>
6. Andy Schroder, "The Original Bitcoin Fluid Dispenser," 2007-2016. Available: <http://andyschroder.com/BitcoinFluidDispenser/TheOriginal/>