BlueCoin Whitepaper

Abstract

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

Archived copy · cryp2nova.com

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.

BlueCoin Website
BlueCoin Whitepaper

Social

CRYP2NOVA

Archived copy · cryp2nova.com