b-hash Cryptocurrency Whitepaper

The b-hash Core Team

May 2018

The b-hash team confirms that the ideas and information presented in this whitepaper are their own and that outside sources have been appropriately attributed.

Brief Overview

b-hash (HASH) believes that cryptocurrencies are the future of storing and transferring value. That's why we are introducing b-hash to the cryptocurrency community. b-hash is a privacy oriented project that features instant and private transactions. The coin can be generated via proof of work mining or by operating masternodes, and the blockchain is secured by the complex XEVAN algorithm.

Acknowledgements

The b-hash team thanks Satoshi Nakamoto and the Bitcoin Core, Dash, and the PIVX Development teams for their contributions to the open source community. The b-hash team intends to contribute to the open source cryptocurrency community via this project.

Table of Contents

What is Cryptocurrency

Introduction

Cryptocurrency is the description given to speculative assets like Bitcoin, Ethereum, and b-hash. Currencies may be electronic representations of physical things but - more likely - function as stores of value and units of transfer within the electronic economy. Modern cryptocurrencies rely upon some form of distributed ledger technology, like the blockchain Satoshi described in *Bitcoin: A Peer-to-Peer Electronic Cash System*, in order to validate transactions and prevent malicious actors from manipulating the data stored within the ledger. Generally, cryptocurrencies are created through a combination of "cryptography, networking, and open-source software." (Greenberg, 2011).

The Block and the Chain

A blockchain is a series of blocks, which represent transactions that were validated within a specific time frame, that are linked together with a cryptographic hashing function. "As records are created, they are confirmed by a distributed network of computers and paired up with the previous entry in the chain thereby creating a chain of blocks, or a blockchain." (Martindale, 2018) Within the b-hash chain, block times are targeted at 3 minutes apart and they are chained together with the XEVAN hashing algorithm. This provides the b-hash network with an adequate opportunity to obtain network consensus between blocks and should help avoid chain splits and other outcomes of hash-based chain attacks.

Privacy Matters

Blockchains are very good at creating publicly verifiable, immutable, distributed ledgers. Not everyone wants to maintain total public transparency to all of their spending or economic activity. Doing so may create latent legal or security challenges down the road and because of the risks associated with computing in general, privacy is an important component of any successful project. For example, if a user utilized Bitcoin in 2011 to conduct some illicit activity and then later utilized that same Bitcoin address in 2018, the evidence of their long-ago misdeeds would be directly tied to their recent transaction. b-hash addresses the need for privacy by allowing users to obfuscate their transactions via coin mixing, effectively hiding where transactions originate and terminate.

What is b-hash

The Coin

b-hash is a cryptocurrency that is focused on privacy and solving the cryptocurrency to fiat gateway problem. b-hash features instant transactions, fungibility, masternode technology, and provides a secure payment option with a decentralized supply. b-hash is forked from PIVX and brings a number of meaningful features with it. b-hash is a proof-of-work and masternode hybrid coin, meaning that individuals can earn coins by operating masternodes or mining to support the network. Both of those activities are important to the b-hash network and users participating in either are actively strengthening the b-hash chain improving the security of our ecosystem.

Why b-hash?

The genesis of b-hash is rooted in our desire to contribute a fairly-distributed, functionally well-rounded, and market-appropriate project to the cryptocurrency ecosystem. We believe that, by focusing on bridging the cryptocurrency to fiat gateway problem, we have the opportunity to meaningfully improve the long-term use case of cryptocurrencies by addressing a current market need. We appreciate that there are many projects like b-hash that have launched with similar goals and that many of them fail to meet their goals. That's why we started with a simple, yet ambitious, focus and are working hard to meet our objectives. b-hash's low-hype launch created the opportunity for broad coin distribution and decentralization while also affording early adopters the chance to join a project at an early stage and benefit from subsequent potential growth.

Unlike most coins, which fail to produce a working product and make grandeur claims of solving the issues plagued in typical transactions, the b-hash team is focused on an organic evolution by exploring options for our goals. We believe in working towards an end goal of a fair, secure, and decentralized cryptocurrency and wish to avoid any claims that a definitive solution has been discovered. Far too often, projects oversell and fail to have any plan of “going-to-market”. Many on our team are veterans in the field and have witnessed repeated umbrella terms and overly-ambitious approaches to adoption; this is not what b-hash attempts to do. Instead, we want to focus on the long-term, which means a gradual scaling process and natural adoption. We will make timely decisions that is most appropriate for our project and only focus on presenting the truth.

b-hash for everybody

One of the major problems that cryptocurrencies face is supply centralization. The b-hash team had a deliberate launch strategy aimed at decentralizing coin supply in order to strengthen the network. The project will also rely upon a large community to achieve many of its goals. Expanding the b-hash footprint means bringing b-hash to more users as a transaction settlement solution. Our roadmap is focused on expanding b-hash’s economic footprint, and relying upon a large community of engaged users, miners, and node operators to validate the need and relevance of b-hash as a potential solution to the crypto to fiat gateway problem.

The b-hash Blockchain

Coin Specifications

Block Size	2 MB
Proof-of-Work Algorithm	XEVAN
Block Time	3 minutes
PoW Block Reward	20 HASH
PoW Period	Indefinite
Coin Maturity:	100 blocks
Confirmation	6 blocks
Difficulty Retargeting	DGWv3
Maximum Supply	24,831,360
Masternodes	Enabled
Masternode Collateral	2000 HASH
Protocol Support	IPV4, IPV6, TOR

Masternode Details

The b-hash network employs masternodes to stabilize coin supply, promote coin holding, and support and strengthen the function of the network itself. Masternodes receive a share of the block reward, making them an effective way to store and produce b-hash.

Masternode details are as follows:

Masternode Collateral	2000
Masternode Payment Start	Day 7, Block 3361
Masternode Subsidy	50% of Block Reward 10 HASH

DGWv3 Difficulty Algorithm

The DGWv3 difficulty algorithm allows the HASH blockchain to promptly and effectively respond to large swings in hashing power. The algorithm is designed to maintain a consistent block time (3 minutes) during times when the network hash power is fluctuating significantly. Difficulty algorithms are one means of defending against hash attacks and b-hash's use of DGWv3 and the nicehash-resistant XEVAN hashing algorithm are two defenses that the b-hash network has against malicious actors.

XEVAN Hashing Algorithm

b-hash features the XEVAN hashing function for Proof-of-Work calculations. XEVAN is undervalued within current cryptocurrency projects and is strongly ASIC resistant. Cloud-based hashing services like NiceHash provide a reliable vector for classic hash-based attacks and we selected the XEVAN algorithm specifically because it is not available to purchase via NiceHash. There are viable AMD and NVidia GPU mining solutions which will broaden coin distribution and mining rewards, driving coin supply decentralization.

b-hash Features

Instant Send

Instantaneous transactions are a valuable feature for any cryptocurrency project to offer. b-hash offers instantaneous transactions via masternode validation through a protocol known as InstantSend. InstantSend allows a user to generate a transaction and request that masternodes validate the transaction before it can be appended to the blockchain. This important feature allows b-hash users to instantly transact in the coin without having to wait for the standard 6 confirmations required for a normal transaction.

Obfuscation

Beyond instantaneous transactions, b-hash also offers strong privacy functionality with obfuscation. Obfuscation is a means of mixing transactions of common sizes (1000, 100, 10, 1, etc...) between multiple wallets, which effectively anonomizes the movement of b-hash between user wallets. This method was originally described by Gregory Maxwell (2013) in his presentation of CoinJoin and is a provably strong privacy method that is resistant to scrying, even in situations where attackers control substantial portions of the masternode network.

Masternodes

Masternodes validate transactions and operate as nodes for the b-hash network. They also enable b-hash's instant and private transactions. These important functions make masternodes an integral part of b-hash's network and they are rewarded for their service. Masternodes receive 50% of the block reward, meaning they are an effective way of generating b-hash outside of proof of work mining. This important feature allows average cryptocurrency users the opportunity to generate coins without investing into a large and energy intensive mining farm. Masternodes also reduce circulating supply by encouraging users to use coins as collateral for a node that provides a predictable rate of return.

Near-term goals

The focus of the b-hash project is to bridge the fiat payment gateway and have a fully utilized coin across the internet that is compliant with privacy regulation: a feat that has not been achieved by any currency.

The b-hash team believes in an alternative approach to the current state of crypto: setting yearly goals that are manageable and attainable for the project, which can be altered and focused based on the current market, regulatory, community, and technological environment.

To be specific:

- b-hash will always be aligned with market conditions and the team will steer the project in the direction they feel is best for long-term adoption. The b-hash team has a wide array of experienced and successful crypto-traders and industry experts, which we feel will help keep the project relevant;

- b-hash will be be aware and responsive to the regulatory environment. Most projects fail to recognize that their "game-plan" will need to change as regulations and other pressures develop over time. In short, the team will ensure b-hash is adamant of adapting to these issues and compliant with privacy standards;

- b-hash will always focus on the community first. This means the team and project are committed to open, transparent, and widely decentralized applications and use cases for all ideas. We will also listen and respond to community suggestions. Although we may not agree or take action on these suggestions, we will always provide a well-educated and thoughtful response, as needed;

- b-hash will always focus on the technological advancements in the space and align the project with the most cutting-edge, efficient, and secure tech that is available. We do not believe there is a completely sustainable solution, currently, so we are focusing on building the infrastructure first before deploying the use-case across applications and platforms.

We are cryptocurrency believers at our core and believe in the disruptive empowerment and mass adoption that will occur with this new form of technology. However, we also do not believe a single solution, technology, or approach has been solidified. As such, we want to be an adaptive project. One that embraces disruption, change, and uncertainty and focus on the long-term evolution of the coin and our project. This means we will set broad goals and commit to updating the community as the project evolves. Much like the early day of bitcoin, no one knew what to expect. Only through the consistent effort, faith, and community support did bitcoin evolve into the powerhouse it is today. We wish to emulate this approach and focus on transparency and realistic solutions as cryptocurrency and blockchain evolves.

In sum, our edge is that we will always be honest, open, and realistic on what we can achieve. Many projects will fail because of their inability to scale and maintain relevance over time. Post-ICO, most projects do not have any relevance or fizzle away in relevance. We decided against that approach and are looking for broad participation and, just like bitcoin, hope to reward early-adopters with their support over time.

Goal 1: Year Long Market Adoption/Scaling

We are focused on long-term success. Year one will be focused on organic word-of-mouth adoption and gradual scaling. We will focus on testing the chain and adding improvements as more and more people engage with the network.

b-hash's long term success, like any cryptocurrency, relies upon broad market adoption and integration into existing ecosystems. b-hash is designed with the features necessary to facilitate broad adoption and our team is hard at work marketing and encouraging use of the b-hash network. We appreciate your help in expanding our reach and recognize that operating a stable, long-term project relies on an engaged market and community.

Our approach will be organic, conservative, and realistic. We will never give false promises in respect to our project's abilities and will set attainable goals. Despite what other projects tout, adoption does not occur instantaneously or over night. The best approach is one that is planned and organic. b-hash intends to raise awareness and encourage participation in a decentralized manner—this means wide distribution and decentralization. We firmly believe this will occur over time and without the hype-marketing tactics of most coin.

Goal 2: Commerce Integration

We are currently focused on integrating enterprise payment processing infrastructure and peer to peer (P2P) transaction protocols.

As a cryptocurrency designed for broad adoption, b-hash is also focused on integrating into existing e-commerce systems. We will reach out to integrators for inclusion into existing cryptocurrency payment channels as a way to increase b-hash's footprint. We will target numerous operators, such as WooCommerce and CoinGate and also explore the appropriate model and scale for an an efficient P2P ecosystem for secure, instant, and private transactions (we hope to align with the current GDPR goals).

At present, we are solidifying and exploring commerce partnerships for a testing grounds.

Goal 3: Midnight Protocol

Privacy is a critical part of any free society and b-hash aims to strengthen the privacy of all cryptocurrency users by developing the Midnight protocol™. The Midnight Protocol™ will focus on existing privacy regulatory frameworks, the most important being the General Data Protection Regulation (GDPR), one of the most extensive data and privacy regulations, to ensure the coin and platforms aligns with policy goals and regulatory standards to ensure long term sustainability.

In short, we will focus on managing and implementing the project's key privacy function so that users can feel that their privacy rights are protected, at least, as prescribed by legislation. We believe this offers an extensive competitive advantage towards the adoption of b-hash amongst others that have similar goals.

To further add layers of privacy and control to the user, b-hash will seek to explore developing the Midnight Protocol™ by routing through

I2P and TOR. We believe that TOR is inherently more risky considering the National Security Agency's oversight, but we will determine the best routing service, if appropriate. We are also exploring other proprietary options, but do not wish to divulge all information as not to suggest or misrepresent our goals.

In addition, the b-hash team will explore implementing specific encryption layers to appropriate information and applications to ensure the security and anonymity of the user is private. We wish to fully encrypt data on all platforms that interact with b-hash from B2B or P2P.

References

Greenberg, A. (2011). Crypto Currency. Retrieved on 4/21/2018 from https://web.archive.org/web/20140831001109/http://www.forbes.com/forbes/2011/0509/technology-psilocybin-bitcoins-gavin-andresen-crypto-currency.html

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Retrieved 4/21/2018 from http://nakamotoinstitute.org/bitcoin/

Maxwell, G. (2013). CoinJoin: Bitcoin privacy for the real world. Retrieved 4/21/2018 from https://bitcointalk.org/?topic=279249

Martindale, J. (2018). What is Blockchain? Retrieved 4/21/2018 from https://www.digitaltrends.com/computing/what-is-a-blockchain/