BULWARK

CRYPTOCURRENCY

Bulwark Cryptocurrency Whitepaper

Bulwark Core Team:
Levi (Project Director)
Jack (Marketing Director)
Stu (Blockchain Developer)
Dustin (Full-Stack Developer)
Kewagi (Software Engineer)
Patrick (Brand and Design Manager)
Voxterra (Community Manager)

The Bulwark Core Team

May 2018

Version 1.2

We, The Bulwark Core Team, confirm that the work presented in this whitepaper is our own. Where information has been derived from other sources, we confirm that this has been indicated in the attributions.

Abstract

Bulwark (ticker: BWK) is a community-oriented coin born out of an observation of generally unfair practices within the masternode privacy coin space. Our deliberate, fair, launch strategy allows participants the opportunity to join a promising project at inception. We offer a simple value proposition with no grandiose promise: we will deliver a privacy coin that works today and into the future by leveraging best-practices from both DASH and PIVX. No fanciful visions with a limited prospect of delivery, but a working coin on a working platform with support into the future. This does not mean we plan no innovation, but instead that we will deliver results rather than hype. There are too many coins that are fueled by hype - but completely devoid of substance - and we do not want to join the growing cadre of coins driven by the motto of over-promise and under deliver. With no ICO, a soft-launch reward ramp, small premine, and miner-favored block reward allocations, Bulwark adopters will have ground-floor access to a privacy coin offering a blend of masternodes and the best available privacy coin technology alongside a meaningful development roadmap. Masternodes will be available, and functioning, on launch and are a fundamental part of this coin's vision and will stabilize circulation, secure the network, and provide important functionality.

Acknowledgements

Bulwark would not have been possible without the prior works of the respective Bitcoin, Peercoin, Blackcoin, Talkcoin, Dash and PIVX teams. Open source software and its contributors are constantly paving the way toward new and exciting innovations. When information and knowledge are free to build upon, society as a whole benefits. We are grateful to our predecessors for the opportunity to contribute to this growing ecosystem.

Table of Contents

Abbreviations

ASIC	**A**pplication-**S**pecific **I**ntegrated **C**ircuit
CPU	**C**entral **P**rocessing **U**nit
CAD	**C**omputer **A**ided **D**esign
BWK	**B**ulwark **C**ryptocurrency
TOR	**T**he **O**nion **N**etwork
MN	**M**aster**N**ode
BR	**B**lock **R**eward
UI	**U**ser **I**nterface
UX	**U**ser **E**xperience

Chapter 1

Brief Introduction to Cryptocurrency

1.1 Background

In 2009, Satoshi Nakamoto released a paper entitled *Bitcoin: A Peer-to-Peer Electronic Cash System* detailing his vision of commerce. Nakamoto's vision detailed a peer-to-peer currency system backed by a hash based proof-of-work. The network would timestamp transactions by hashing them into an ongoing ledger that could not be changed without redoing the proof-of-work. Nodes would choose the longest chain as proof of events witnessed by the largest pool of hashing power. As long as $\geq 51\%$ of the network hashing power is controlled by nodes not intending to facilitate an attack, the chain they generate will remain the longest. (Nakamoto 2009)

1.2 The Block

Each block on the network is prefaced with an 80 byte header containing a double SHA256 hashed copy of the previous block's header, merkle root (a double SHA256 hashed derivation of all the hashes that occurred in the block), the time stamp at which proof-of-work began, difficulty target this header's hash must be less-than or equal to, and the nonce at which miners reached the difficulty target. As such, any attempts to modify any transaction in any block will result in the rejection of the block by the network's miners. (Bitcoin Core Team 2017)

1.3 The Blockchain

Groups of transactions are formed into blocks and those blocks are placed chronologically into a chain - forming the blockchain. The blockchain creates a moving history of all of the activity within the network and serves as a distributed consensus model where any transaction can be verified at any time (Crosby et al. 2015).

1.4 Proof-Of-Work

Proof-of-work is a system of verification in which miners must devote tangible resources (electricity, hardware costs) to solve an arbitrary probabilistic *word puzzle*. In order for a bad actor to taint the blockchain with a fraudulent transaction, they must complete all proof-of-work up to the present point. (Okupski 2016)

1.5 Proof-Of-Stake

Proof-Of-Stake is a system of verification in which the creator of the next block is picked utilizing variables such as coin count, age of coins, as well as other randomizing factors to assist in centralization prevention. Proof-Of-Stake is far more energy efficient in that it requires no dedicated hardware and negligible amounts of electricity to reward miners.

Chapter 2

Introducing Bulwark

2.1 A solid foundation

Every home needs a solid foundation, and Bulwark is no different. Bulwark is built upon *PIVX*, which itself is built upon the popular *DASH* cryptocurrency. While lineages can all be traced back to the original Satoshi Core, each project has chosen a particular direction with goals and ideals that represent the communities they serve. We will extend, and place emphasis on, the privacy coin features of our predecessor platforms by exploring new technologies, while creating tool sets and opportunities for Bulwark's integration into present day technology platforms.

2.2 A team dedicated to the community

For some projects, communities are an afterthought. Bulwark's number one priority is the community. With giveaways, contests, a lively discussion platform and a zero-tolerance policy toward the harassment of newcomers, Bulwark strives to be the cryptocurrency for all varieties of end-users. Members of our userbase are already contributing useful scripts and guides to further enhance the user experience.

2.3 Fair and balanced

At the time of writing, there have been an influx of cryptocurrencies utilizing a similar foundation. While the underlying technology is solid, oftentimes a deeper examination of their specifications and blockchain parameters reveals less-than-fair practices.

2.4 Fast and functional

With a 90 second block time, masternode consensus and transaction locking, reasonable emissions schedule, and eco-friendly staking, Bulwark aspires to be a truly fast and functional cryptocurrency.

Chapter 3

Our Blockchain Parameters.

3.1 Bulwark Specifications at a Glance

3.1

Table 3.1: At a glance specifications for Bulwark

Specification	Descriptor
Ticker	BWK
Algorithm	NIST5
RPC Port	52541
P2P Port	52543
Block Spacing	90 Seconds
Difficulty Algorithm	Dark Gravity Wave v3.0
Block Size	1MB
Mined/Minted Maturity	67 Blocks (~100 Minutes)
Confirmation	6 Blocks (~9 Minutes)
Circulation (1 Year)	14,505,720 BWK
Circulation (5 Years)	27,668,220 BWK
PoW Period	$nHeight \leq 182{,}700$
PoS Period	$nHeight \geq 182{,}701$
Protocol Support	IPV4, IPV6, TOR
PoS	Blackcoin v3.0 PoS, PIVX SeeSaw rewards.

3.2 SlowStart

Our fair start is provided with the following code snippet (Credit: ZCash).

```
int64_t nSlowSubsidy = 50 * COIN;

if (nHeight < 960 / 2) {          // If block height less than 480,
   nSlowSubsidy /= 960;           // Set nSubsidy to .05208333
   nSlowSubsidy *= nHeight;       // Multiply present height by .05208333
} else if (nHeight < 960 {        // ex: Block 200, BR will be 10.41666600
    nSlowSubsidy /= 960;          // Credits: ZCASH Team
    nSlowSubsidy *= nHeight;
```

3.3 Dark Gravity Wave 3.0

Dark Gravity Wave is employed by Bulwark from the start as a method of retargeting PoW difficulty. It uses a simple moving average that can respond to large nethash increases or drop-offs in just a few blocks. This alleviates the "stuck block effect" often caused by multipools and prevents one person adding a substantial amount of computing power from instantly solving more than a few blocks.

Chapter 4

Block Rewards

4.1 PoW Block Rewards

Subsidy	Block	PoW	MN	Circulation
489720	1	100%	NA	489200
~25(avg)	2-960	100%	NA	513150
50.000	961-28800	80%	20%	1953150
50.000	28801-57600	75%	25%	3393150
50.000	57601-86400	66%	33%	4833150
43.750	86401-172800	50%	50%	8613150
37.500	172801-182700	50%	50%	371212

4.2 PoS Block Rewards

Table 4.2: PoS Period Block Reward Specifications

Subsidy	Block	Budget	PoS/Masternode	Note
37.500	182701-259200	0%	*SeeSaw*	Year 1
31.250	259201-345600	0%	*SeeSaw*	Year 1
25.000	345601-432000	10%	*SeeSaw*	Year 2
21.875	432001-518400	10%	*SeeSaw*	Year 2
18.750	518401-604800	10%	*SeeSaw*	Year 2
15.625	604801-691200	10%	*SeeSaw*	Year 2
10.250	691201-777600	10%	*SeeSaw*	Year 3
10.938	777601-864000	10%	*SeeSaw*	Year 3
9.3750	864001-950400	10%	*SeeSaw*	Year 3
7.8120	950401-1036800	10%	*SeeSaw*	Year 3
6.2500	1036801-1123200	10%	*SeeSaw*	Year 4
5.4690	1123201-1209600	10%	*SeeSaw*	Year 4
4.6880	1209601-1296000	10%	*SeeSaw*	Year 4
3.9060	1296000-1382400	10%	*SeeSaw*	Year 4
3.1250	1382401-1468800	10%	*SeeSaw*	Year 5
2.7340	1468801-1555200	10%	*SeeSaw*	Year 5
2.3440	1555201-1641600	10%	*SeeSaw*	Year 5
1.9530	1641601-1728000	10%	*SeeSaw*	Year 5
1.6250	1728000+	10%	*SeeSaw*	In perpetuity

Chapter 5

NIST5 Hashing

5.1 Why NIST5

Popularized by TalkCoin in 2014, the NIST5 hashing algorithm has seen modest mainstream usage. NIST5 can be mined on a wide array of consumer-grade hardware including CPUs, as well as AMD and Nvidia GPUs. NIST5 is not as ASIC resistant as some other memory hard algorithms, but we believe the trade-off is acceptable to improve system stability and reduce power consumption relative to those memory hard algorithms.

5.2 The Five Finalists (NIST SHA-3 Competition)

The five hashing algorithms that make up NIST5 are the finalists from the NIST Hashing Competition (Chang et al. 2012). They are (in the order that blocks are hashed):

Blake (Aumasson 2010), **Grøstl** (Gauravaram1 et al. 2011), **JH** (Wu 2012), **Keccak** (Bertoni et al. 2012), and **Skein** (Ferguson et al. 2010)

5.3 The new SHA-3 Standard

Keccak eventually passed the final round to be named the new SHA-3 hashing function, while the other four algorithms (despite being considered cryptographically secure) lost a few points from the judges for some minor technicalities. We believe the combination

of the new SHA-3 standard along with the other finalist choices provide a quick, secure, and established hashing algorithm.

5.4 Mining Software Available

At the time of writing, there are several options for miners

Name	Platform	Link
SGMiner-5.0	OpenCL	GitHub
ccminer-2.2.2	CUDA	GitHub
cpuminer-opt	CPU	GitHub

Chapter 6

Feature Set

6.1 Masternodes

Masternodes are, essentially, a decentralized web of computers that serve the Bulwark network. Masternodes perform important network functions and receive part of the block rewards. They serve the Bulwark ecosystem by stabilizing coin supply, processing transactions, and securing the network. Masternodes require 5000 BWK and modest technical knowledge to operate. Any wallet controlling 5000 BWK can set up a masternode.

6.2 Obfuscation / Coin Mixing

Bulwark features Obfuscation, based on CoinJoin but with various improvements over the original, and done via coin mixing in a decentralized fashion facilitated by the network of masternodes. This provides an additional layer of privacy in transactions. While not perfectly anonymous, Obfuscation via node mixing it is far better than the standard Bitcoin transaction. For example, all Bitcoin transactions are transparent. For Bulwark, a nefarious actor would need to control 50% of the operating masternodes to have less than 0.5% chance of de-anonymizing a single transaction that was mixed with 8 rounds of Obfuscation (Kiraly 2017b). This important feature provides a high-level of anonymity for BWK users that elect to obfuscate their transactions.

6.3 SwiftTX

SwiftTX provides masternodes with locking and consensus authority for transactions. When a transaction is submitted to the network, a group of masternodes will validate the transaction. If those masternodes reach consensus on the transaction's validity it will be locked for later introduction into the blockchain, greatly increasing transaction speed compared to conventional systems (like Bitcoin's 10 minute block times with multiple confirmations). SwiftTX makes it possible for multiple transactions to take place before a block on the network is mined with the same inputs. This system is based on Dash's InstantSend. (Kiraly 2017a).

6.4 Sporks

The Bulwark network employs the multi-phased fork mechanism known as "sporking". This will enable the BWK network to implement new features while minimizing the chances of an unintended network fork during rollout. Spork changes are deployable via the network and can be turned on and off as necessary without requiring node software updates (Strophy 2017). This feature is extremely useful and allows the network to react quickly to security vulnerabilities.

6.5 TOR & IPV6 Masternodes

Bulwark allows the user to run their full node or masternode from either an onion address or an IPV6 address. We have been working to add full TOR nodes to both strengthen the TOR network itself, and the Bulwark user experience operating in TOR only mode. A unique feature of TOR masternode support is being able to operate your masternode as a TOR hidden service. TOR nodes enable users with stable internet connections to operate masternodes out of their home network without the privacy implications of revealing their location or the dangers of exposing their home network to the potential for attack or compromise.

6.6 Community Importance and the Governance System

The Bulwark community is the most important factor behind the long-term success of the project, and their ability to meaningfully influence the future of the coin is paramount. As such, at the end of the PoW phase we intend to activate budget superblocks on the network. These superblocks, paid monthly, will enable the community to exert meaningful control over all aspects of Bulwark's development, brand presence, and community affairs. Delaying the activation of this system will give us time to develop the underlying framework necessary for a positive user experience, and maximize block rewards available to miners and masternodes.

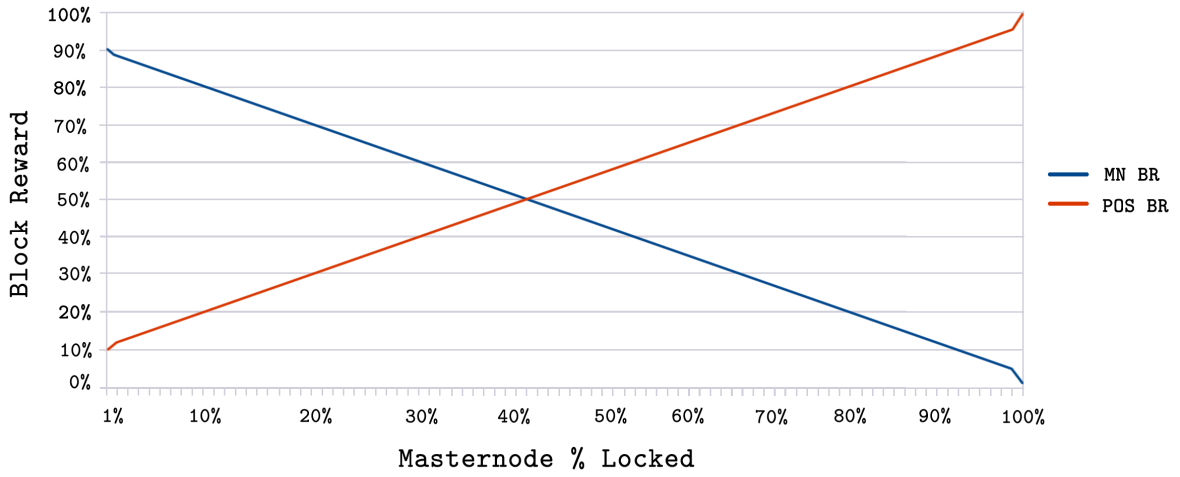
We will utilize a multi-phase process for creating and submitting proposals. Each step will need to be fully completed. Failure to complete the steps outlined will likely result in a proposal not being activated. A basic outline of these steps are as follows:

- Start in our Discord chat, and talk with some of the seasoned users. Gauge interest and if the response is positive, move to the next phase.
- Utilize multiple social media platforms to discuss and get feedback. Remember that Bulwark has a diverse userbase and differing levels of governance participation, reaching a portion of the userbase will often require some footwork. Take note of these discussions and be able to cite them in the formal pre-proposal. The more citations provided, the better.
- Be open to suggestions from the community and developers. Be flexible and willing to incorporate external ideas and suggestions in your proposal.
- Create a formal pre-proposal on the Governance->Pre-Proposal section of our website. Provide citations for all discussions that occurred from the previous step. Treat your pre-proposal as if it is what will be submitted to the blockchain for voting.
- Upon completion of these steps, you will submit your proposal to the blockchain. Be prepared for two fees, one at the time of submission and a ballot fee paid to the developer that activates your proposal on the blockchain. The submission fee is non-refundable, and the balloting fee will only be paid upon approval and activation of your proposal.
- Everyone is free to adjust their proposal to include the reimbursement cost of these two fees. Please make sure in your formal proposal you state that you are adding reimbursement to the stipend requested.
- Be sure to get back in touch with everyone you spoke with so your idea will be voted on. For a proposal to be paid out, 10% of the eligible masternodes must

vote 'yes' on your proposal. This process of getting a 10% consensus can be much harder than it sounds, so be diligent, informative, and respectful in procuring the votes necessary for your proposal to be paid.

6.7 SeeSaw PoS/Masternode Rewards

We have decided to utilize the SeeSaw reward system popularized by PIVX (Jakiman 2017). The SeeSaw reward system begins with a 9:1 block reward ratio (favoring masternodes), and smoothly adjusts the ratio of reward between staking and node operators until around 41.5% of coins in circulation are locked into masternodes, at which time staking rewards reach a slight advantage over masternode rewards on a coin-by-coin basis. The reason we have the SeeSaw slightly favoring staking rewards is because we want to avoid the problems - like significant price volatility and low liquidity - that impact coins with very-high percentages of their circulating supply locked in nodes. This strategy will mitigate user frustration over access to coin supply and maintains the relevance of our robust network. With one of our goals being a well-supported platform for anonymous commerce, transactability is of the utmost importance to those accepting Bulwark and those holding Bulwark.



6.8 Open Source Stance

The Bulwark team is a strong proponent of open source development. All works, present and future, will always be made open source to the community. Cryptocurrency is a massively growing technological endeavor and we strongly believe that proprietary and closed source developments hinder advancement and innovation. Scripts, toolsets, and codebases for all Bulwark projects are free for others to use under the appropriate open source license.

Chapter 7

The Future

7.1 Privacy and Software Enhancements

We are committed to adopting new protocols that will enhance the privacy of our userbase. There are several paths we are evaluating at present and plan to begin internal testing and development of in the first half of 2018. Some of these enhancements include:

- I2P privacy network
- Zerocoin protocol or Stealth addressing (When we are confident in the maturity of the solution)
- Synchronizing our codebase closer with Bitcoin mainline
- Streamlining/Updating QT Wallet

7.2 Bulwark Secure Home Node

We will be working with CAD specialists to design a small, self-contained, home Bulwark node. Users will be able to connect this to their home network and configure using a Web UI. The functions we intend to launch with are as follows:

- For those with stable internet connections, an easy to set up fully onionized masternode (or full node) using TOR hidden services
- Bulwark staking through either virtualization or an add-on device

In keeping with the spirit of decentralization, the 3D printable files and all source code will be available to the community for home assembly.

7.3 Extension of our Branding

We will continue to extend our brand and intend to work with hardware vendors and system integrators which share the same passion and ideals that we do. In five years we want the name 'Bulwark' to be synonymous with not just cryptocurrency but privacy, security, and the respect for a user's freedom. Bulwark's main purpose is to provide freedom of choice through privacy.

7.4 Design and Visual

Through Research and Development, we aim to create a visual design language for Bulwark that sets it apart from its competition in the crypto market. Our design team plans to innovate and experiment with the current UI/UX/Branding to ultimately achieve design excellence by searching for a medium that allows the best user experience, and aesthetics that are innovative and beautiful. This will be done by researching our competitors, keeping on top of current technological trends & standards, and continuously striving to bring new and exciting visuals to the end-users.

7.5 Bulwark Hardware Wallet

The first standalone and open source hardware wallet on which users will be able to safely and securely store Bulwark. Hardware specifications as well as software will be made open source upon launch so any cryptocurrency can fork it to use for their own project. The goal with the Bulwark Hardware Wallet is to allow the community a cheap and cost effective alternative to storing their coins without having to rely on larger companies that provide overpriced solutions on closed source hardware.

Chapter 8

Conclusion

8.1 Summary

Bulwark is a privacy-oriented coin with masternodes, governance, and an evolving ecosystem of tools. The project began with a fair launch and a focus on broad coin distribution. The slow start, block reward split, and hashing algorithm were deliberately selected to create opportunities for significant community participation. Bulwark launched with a variety of important privacy coin features and the development team is hard at work to introduce new features and build upon existing technologies. Bulwark aims to empower choice through privacy and will focus considerable effort to this end.

8.2 Future work

The masternode privacy coin ecosystem has recently been inundated by coins seeking to entice new users through promises of substantial returns on investment, gigantic road maps filled with improbable deliverables, and a general focus on marketing over actual improvement within the space. Bulwark plans to be the opposite: low on hype creation and high on actual creation. Present and future goals for the project will follow the formula of being specific, measurable, attainable, relevant, and time bound.

References

Aumasson, L.M., Jean-Phillipe Henzen, 2010. SHA-3 proposal: BLAKE. Available at: https://131002.net/blake/blake.pdf.

Bertoni, G., Daemen, J., Peeters, M. & Van Assche, G., 2012. The keccak sha-3 submission. Available at: https://keccak.team/files/Keccak-submission-3.pdf.

Bitcoin Core Team, T., 2017. Bitcoin developer reference. Available at: https://bitcoin.org/en/developer-reference#block-headers.

Chang, S.-J., Perlner, R., Burr, W.E., Turan, M.S., et al., 2012. Third-round report of the sha-3 cryptographic hash algorithm competition. Available at: http://nvlpubs.nist.gov/nistpubs/ir/2012/NIST.IR.7896.pdf.

Crosby, M., Nachiappan, Pattanayak, P., Verma, S., et al., 2015. BlockChain technology. Available at: http://scet.berkeley.edu/wp-content/uploads/BlockchainPaper.pdf.

Ferguson, N.L., Schneier, S., Whiting, B., Bellare, D., et al., 2010. The skein hash function family. Available at: http://www.skein-hash.info/sites/default/files/skein1.3.pdf.

Gauravaram1, P., Knudsen, L.R., Matusiewicz, K., Mendel, F., et al., 2011. Grøstl – a sha-3 candidate. Available at: http://www.groestl.info/Groestl.pdf.

Jakiman, 2017. PIVX purple paper. Available at: https://pivx.org/wp-content/uploads/2017/03/PIVX-purple-paper-Technincal-Notes.pdf.

Kiraly, B., 2017a. InstantSend. Available at: https://dashpay.atlassian.net/wiki/spaces/DOC/pages/1146928/InstantSend.

Kiraly, B., 2017b. PrivateSend. Available at: https://dashpay.atlassian.net/wiki/spaces/DOC/pages/1146924/PrivateSend.

Nakamoto, S., 2009. Bitcoin: A peer-to-peer electronic cash system. Available at: https://bitcoin.org/bitcoin.pdf.

Okupski, K., 2016. Bitcoin developer reference., pp.3–4. Available at: https://lopp.net/pdf/Bitcoin_Developer_Reference.pdf.

Strophy, 2017. Understanding sporks. Available at: https://dashpay.atlassian.net/wiki/spaces/DOC/

pages/128319489/Understanding+Sporks.

Wu, H., 2012. The hash function jh. Available at: http://www3.ntu.edu.sg/home/wuhj/research/jh/jh_round3.pdf.