BitcoinWSpectum

White-Paper

BWS Team

Executive Summary

BWS is a Bitcoin-based community-centric crypto currency with a focus on decentralization, privacy, and real-world use. It utilizes an energy efficient Proof of Stake protocol and a second-tier Masternode network for inclusive community-based governance along with a block chain based self-funding treasury system ensuring its sustainability. BWS is continuously striving to achieve a better governance system, instantaneous private transactions, and fungibility in order to remain next generation crypto currency.

In layman's term, BWS is basically a form of online digital money that can be easily transferred all around the world in a blink of an eye with nearly non-existent transaction fees. You can convert your money into BWS at various exchanges and just hold to earn rewards similar to interest, trade on an exchange to buy other digital currencies or buy goods or services online and offline where it is accepted. It is not owned or governed by any single person or organization and its network is secured by thousands of nodes all around the world by its users.

The goal of BWS is to be an advanced digital currency that is fast, secure, decentralized & private.

Contents

Executive Summary	2
Coins Specifications	4
Why BWS?	7
CRYPTOCURRENCY TRANSACTION PRIVACY	8
OUR SOLUTION : ZEROCOIN PROTOCOL (zBWS)	11
UNIQUE FACTOR	12
BWS/zBWS TECHNICAL ADVANTAGES	13
REAL LIFE BENEFITS OF USING zBWS	13
HOW ANONYMITY IS ACHIEVED	14
Unique Features	16
Spend Security Level	18
Handling of Change	18
zBWS Data Integrity	19
Conclusion	21

Core Specifications

Consensus Algorithm: PoS + zPoS Hybrid

Block size: 8 MB

Total Supply: 103,316,000 (On June 30, 2018)

Max Supply: 910,000,000 (On May 05, 2210 i.e after 192 Years)

Block Time: 60 Seconds (Re-targeting every block)

Masternode minimum confirmations: 15

Transactions per second: 8MB block size can effortlessly accommodate 80,000 transactions per minute (assuming each transaction is 1KB in size).

Mine-able: No

Masternode Support: Yes, 50,000 BWS per masternode

Staking Parameters

Stake-able: Yes (Earn block reward from coin ownership)

Minimum Stake age: 6 hours

Min coins required for staking: 15 BWS

Coin Emission Rate

Block reward: 8 BWS per block (split 70% for masternodes (5.6 BWS) + 30% (2.4 BWS) for stakers)

Coin Supply Control

Dynamic Coin Supply: ALL transaction fees & zBWS minting fees are burnt.

PoS Stake Eligibility (BWS)

Maturity Confirms: 101 confirms

Wallet Status: Requires core wallet to remain online and unlocked for staking.

zPoS Stake Eligibility (zBWS)

Maturity Confirms: 200 confirms

Wallet Status: Requires core wallet to remain online and unlocked for staking.

Maximum Coin Supply:

At June 2018: 103,236,490 BWS

By June 2020: 111,646,090 BWS (After Two Years)

By June 2025: 132,670,090 BWS (After Seven Years)

By June 2030: 153,694,090 BWS (After Twelve Years)

By June 2038: 187,332,490 BWS (After Twenty Years)

(Theoretical maximum. Will actually be lower due to fee burning + partial budget generation.)

Transaction Send Eligibility

Minimum Confirm (BWS) : 10 confirmations

Minimum Confirm (zBWS): 20 confirmations + 1 new mint of the same denomination in the network

SwiftX Eligibility

Confirmations: 1 for locking and 6 to spend.

Collateral held time: 15 minutes.

Privacy Feature

Privacy Technology: Custom Zerocoin Protocol based on libzerocoin (we call this zBWS)

Key Features: Custom accumulator check-pointing system

Accumulator Modulus: RSA-2048

zBWS Denominators: 1, 5, 10, 50, 100, 500, 1000, 5000

Mint time: >= 0.5 seconds

Spend time: >= 2.5 seconds

Proof of Work (PoW) Phase Period

May 25th 2018 to June 16 2018 (FINISHED)

Proof of Stake (PoS) Phase Period

May 25th 2018 from block 23001 onward (CURRENT)

Block Distribution

MN Share in block reward: 70% (5.6 BWS)

POS share in block reward: 30% (2.4 BWS)

Inflation

As each BWS block produces 8 coins it means that 4,204,800 coins will be added annually which comes at about 4.2% of total supply, which is ideal because it doesn't add much towards inflation.

Why BWS?

Masternodes

These are incentivized nodes that receive rewards based on their availability and their ability to offer network services in a decentralized and trust-less manner. Running a masternode requires 50,000 BWS collateral for as long as you choose to run the masternode and allows the owner to vote on budget and development proposals. These nodes are the backbone of the present and future services offer on the BWS network, and as such are rewarded at a slightly higher level as compared to just staking when the number of them is at a predetermined level defined in the seesaw mechanism.

Code Base: PoS 3.0 Bitcoin Core 0.10.x

BWS is one of the only few proof of stake cryptocurrency to be based on the version 0.10 or higher Bitcoin codebase, and the PoS structure utilised does away with coin age, meaning in order to get the most out of your staking you must keep your wallet open at all times, resulting in more constantly available nodes, strengthening the network. No more users opening their wallet once or twice a month for a few minutes and getting rewarded equally with those that have 24/7 up-time with their wallet.

Zerocoin

Zerocoin which has been implemented by BWS, is a protocol that does what Bitcoin can not. Zerocoin provides full privacy to the users of BWS. The BWS implementation of the Zerocoin protocol converts publicly view-able BWS into anonymous BWS (dubbed by the BWS team as Zerocoin BWS or zBWS for short). When a user wishes to spend (that is send from a to b) zBWS, the zBWS appear in the receivers wallet as regular BWS without history of where that BWS originated from.

SwiftX

Instant Transactions: SwiftX transactions are confirmed and spendable within seconds, guaranteed by the network of masternodes, with no need to wait for multiple confirmations in order to be confident in the validity of the transaction.

CRYPTOCURRENCY TRANSACTION PRIVACY

Most common crypto currencies such as Bitcoin has a well known public ledger system where all transactions are visible and traceable through its block explorer. This results in anyone and everyone having the ability to see all associated transactions and balances but more importantly its associated addresses as well. This means that the history of its

previous address owner is now visible through your own address once the coins have traversed through the blockchain and end up in your own wallet address.

An address may seem like it is fully anonymous but if you made a transaction with an address that is generated by the exchanges and/or other merchant services, you have essentially linked your anonymous address with an address that may lead to your identity. In most scenarios, such transparency may not be an issue. But it could become a serious problem if the coin that you hold was once associated with an undesirable history or if your address was being targeted by potential thieves.

For example, coin you received was from an address owned by a person or organization that has been conducting illegal activities and was being monitored and tracked by governing authorities. This now means that you may be questioned on your relationship to the previous owner of those coins that you now possess even though you received them legitimately and without knowledge. This could also mean that the coins with such history may be deemed less valuable than those coins without resulting in reduced fungibility.

OUR SOLUTION : ZEROCOIN PROTOCOL (zBWS)

To overcome this issue, beginning with the v3.0.0 core wallet update released on October 7th 2017, BWS has implemented a well known highly-vetted protocol called Zerocoin with many custom enhancements allowing blockchain-level transaction anonymity in the way of unlinkability.

We call this zBWS, where BWS is a unit of BWS and z prefix is for Zerocoin. What zBWS provides is a protocol-level coin mixing service using zero knowledge proofs to sever the link between the sender and the receiver with 100% anonymity and untraceability. This means that each coin that gets sent using zBWS is now 100% fungible as it has no determinable history attached to them.

The use of zBWS also means your balance can be masked to avoid being targeted by potential thieves. This is a very unique feature that nearly no other cryptocurrency currently in the market possesses.

BWS zBWS accumulators are encrypted using RSA-2048[1] challenge generated keys which negates the need for a developer trusted setup and means that no individual knows the factors. This means that everyone's privacy is ensured through the use of zBWS.

UNIQUE FACTOR

As of writing (SEP 2017) BWS is the only Proof of Stake cryptocurrency to have implemented the full set of Zerocoin protocol ideologies and practices. While based on the original libzerocoin public repository that was created by academic cryptographers, the majority of the BWS zBWS code is custom, making zBWS very unique also.

Original Zerocoin Whitepaper: https://isi.jhu.edu/~mgreen/ZerocoinOakland.pdf

Unlike most other cryptocurrencies that currently utilize a zerocoin-based protocol, BWS zBWS utilizes a very efficient accumulator checkpointing system which allows the zBWS spend process to utilize checkpoints that contains all mints that were made prior to the zBWS mint being spent, as well as a user selected amount of zBWS mints beyond the checkpoint. This allows for a large pool of coins in the accumulator while still having much smaller computation requirements. BWS's zBWS implementation yields minimal resource consumption and makes zBWS transactions one of the fastest private transfers in the market today.

BWS zBWS TECHNICAL ADVANTAGES

- Smaller spend transaction sizes by an average of 25% over any other current implementation in a production environment (further optimization in the works).
- Fast verification and network sync performance.
- Direct spend of zBWS to a BWS address. Multiple Zerocoin denomination spends is possible in a single transaction
- Ability to spend exact amounts and issue the remaining change to either a BWS address or more zBWS.

REAL LIFE BENEFITS OF USING zBWS

- zBWS can hide your coin balance from prying eyes protecting you from being targeted. So your zBWS balance isn't linked to any particular address.
- zBWS can hide the transaction history of the coins being sent.
- Source & target addresses aren't visible making it private, safe & fungible.
- zBWS anonymous transactions are very fast.
- It takes as little as 0.5 seconds to mint and 2.5 seconds to spend zBWS.
- Automatic conversion to zBWS is enabled by default but transparent transfer option is still available. It means that you can always send a fully transparent transaction when required.

HOW ANONYMITY IS ACHIEVED

Mint (convert) your BWS into zBWS denominations. (Wallet auto-mints some by default)

Spend (send) your zBWS as BWS to any internal or external BWS wallet address

Essentially the zerocoin protoco pools (thus combines) all the zBWS that people have converted (minted) from their BWS balance into set denominations and uses them to send when a spend is initiated. Keep in mind that the pooling does not mean that everyone's zBWS is stored in a centralized location. Rather, the public ledger (decentralized blockchain) keeps track of how many zBWSs are created.

When you want to send (spent) some zBWS amount to a BWS address, your wallet sends a zero-knowledge proof to the blockchain that allows the zBWS to be converted back to BWS and sent to the target address all in a single step.

Since zBWS spending creates brand new coins if a spender can provide zero-knowledge proof that she has coins in the accumulated pool (accumulator), the coin's transaction history from its previously associated addresses become unlinked and thus results in an untraceable transaction.

Finally, a simple analogy. Think of zBWS as casino chips. You give your 100 dollar bill (i.e. BWS) to the cashier and you get some 1x$10, 2x$20, 1x$50 dollar chips (i.e. zBWS). This means that you no longer own that particular 100 dollar bill you exchanged and instead have "proof" that you still own $100. Now when you need

50 dollars of it back as fiat (BWS), you give your chips (zBWS) back to the cashier and the cashier delivers a brand new uncirculated 50 dollar bill to a recipient of your choosing.

Unique Features

People often ask why they should choose BWS above other crypto currency, here is a short list of features that make BWS stand out from the crowd.

- BWS is an anonymous Peer-To-Peer currency.
- BWS is working towards Private Instant Verified Transactions as its default transaction.
- BWS is Community Driven
- BWS uses Blackcoin's improved Proof of Stake 3.0 protocol instead of Proof of Work. So it is more efficient in keeping the network secure than PoW.
- BWS has incredibly low transaction fees that are typically a fraction of a penny due to the PoS efficiency. This means it is perfect for micro-transaction business pricing models that previously existed using Bitcoin.
- BWS had no ICO.
- BWS is based on Bitcoin 0.10.x core with some v0.13.2 updates and Dash / BWS core v0.12.1, which means it is more up to date than most other PoS digital currencies that commonly use a lower Bitcoin core version.
- BWS has a very large and growing active community on multiple social networking sites such as BCT, Discord, Reddit, Twitter, Telegram, Facebook etc.
- BWS has a highly active, accessible and responsive development team.

- BWS is available to trade on multiple exchanges including Crypto Bridge and South Exchange with plans to be added to larger exchanges.
- BWS has monthly reward inflation level of approx. 4.2% pa.
- BWS has had consistently higher profitability percentage compared to other digital currencies utilizing masternodes such as DASH since launch and even now.

Spend Security Level

When spending zBWS denominations, a user is prompted to enter a Security Level choosing from 1-100. In an indirect way, the Security Level parameter allows the user to choose how many coins to obfuscate their transaction with.

A Security Level of 1, for example, would take all of the minted coins in the blockchain before your mint was added to the blockchain, and would then add any coins that were minted within the next 10 blocks as well. A Security Level of 2 would do the same thing, except add the next 20 blocks worth of mints. A Security Level of 100 will add the maximum amount of mints up to the current end of the blockchain.

The higher the Security Level, the more computation and time it will take to spend. Although it takes longer, a level of 100 is recommended for transactions that need maximum anonymity.

Handling of Change

As zBWS is made up of fixed denominations, there will be times when the amount needed to be spent cannot be made up by existing denominations. For example, if you have a single 1000 zBWS denomination but you want to send 985 BWS to an address, there will be a difference of 15 BWS that will be received back as change. This change can compromise the privacy of the transaction as it can lead back to your existing address if you mistakenly mix your change back in with your other BWS addresses.

In order to prevent this, there are 2 methods that can be used. First option is the use of the built-in feature that automatically converts the change back into zBWS. This will spend the zBWS into the required amount of BWS to the target address, then mint the remaining change of BWS back into zBWS. This is the most convenient method. However, the amount of change that is not convertible to a denomination (the lowest denomination available is 1) will be converted to a fee.

The second option is to issue change to a standard BWS address, which leaves you up to handling the segregation of that BWS from your day-to-day BWS balance. This option can lead to mistakes and is not recommended if anonymity is important for the transaction.

zBWS Data Integrity

Every minted zBWS denomination is associated with a unique serial number that is stored in the local wallet.dat and not on the blockchain. This means that when a new zBWS denomination is minted, the wallet.dat should be backed up as the previous backup will not have the serial numbers for the newly minted zBWS denominations.

The serial number and other essential zBWS data are committed to the database (wallet.dat) before the transaction is completed and broadcasted to the network. This minimizes the risk of losing your freshly minted zBWS denominations during an

unexpected event during the minting of zBWS, such as a PC crash or internet connectivity issues.

Due to its local database design, it is imperative that your wallet is backed up after every new zBWS mint to ensure that your denomination serial numbers are up to date.

Conclusion

This White Paper introduces various concepts unique to BWS that will improve upon the design of Bitcoin, resulting in an enhanced platform that is secure in its ability to maintain maximum privacy and optimal functionality for each user through immediate message propagation throughout the network and with the hope of delivering less token price volatility. This is all accomplished by utilizing an incentivized two-tier model, rather than the existing single-tier model currently used in other Cryptocurrencies whose function more closely resembles that of Bitcoin. With BWS utilizing this alternative network design, it becomes possible to deliver various types of services that include, but are not limited to, the decentralized mixing of coins, instant asset transactions, and decentralized information transfer services that take full advantage of masternodes and encryption to encryption protocols.