D.O.O. Transfer Logical Solution Group
XVI Zgrada Solidarnosti Local BR7, Budva
MB/PIB: 03276635

BCE White Paper

[version 1.01, May 2020]

D.O.O. Transfer Logical Solution Group
XVI Zgrada Solidarnosti Local BR7, Budva
MB/PIB: 03276635

ABSTRACT

Currently, the cryptocurrency market is awash with tokens from parties of varying intent, motivation, and affiliation. The myriad of tokens and projects—some novel and ambitious uses of blockchain, others in essence clones with catchy names—serves as a deterrent to widespread adoption of crypto as a legitimate, borderless alternative to fiat currency. This document serves as a comprehensive resource on the Private Instant Verified Transaction (BCE) cryptocurrency, a currency whose defining purpose is to provide users with a secure, private, and stable means of transacting over the web.

BCE integrates features inspired by Bitcoin's pioneering distributed ledger consensus technology; speed and governance accessions from Dash, such as SwiftX (from InstantSend) and a Masternode network; and incentivises Zerocoin protocol anonymity through zPoS. BCE also incorporates its own features, such as a Proof of Stake consensus algorithm, and a dynamic coin supply restrained by the burning of transaction fees.

Note that this paper, while an extensive introduction and explanation of BCE, does not contain mathematical or cryptographical breakdowns or explanations. These can be found separately on the BCE project's GitHub.

INTODUCTION

The advent of the blockchain era occurred in 2009 with its implementation in Bitcoin by the entity known as Satoshi Nakamoto. Following Bitcoin's success, many competing cryptocurrencies—known as altcoins—have arisen.

The potential of blockchain to revolutionise not only the way transactions are made, but the way business is conducted across many strata, has seen an explosion of interest in the technology. Currently, the cryptocurrency market is awash with tokens from parties of varying intent, motivation, and affiliation. The myriad of tokens and projects—some novel and ambitious uses of blockchain, others in essence clones with catchy names—serves as a deterrent to widespread adoption of crypto as a legitimate, borderless alternative to fiat currency.

Bitcoin, despite its constant innovation, has so far failed to be widely accepted and adopted as a currency, and remains widely viewed as a store of value rather than means of conducting everyday business. As the world approaches a decade since the launch of Bitcoin, a definitive identity for cryptocurrencies has yet to emerge. This lack of identity has caused the public to view the crypto marketplace as a stock market 2.0.

Its volatility and saturation intimidate potential adopters, who regard it not as an alternative to fiat currencies, but as a risky investment opportunity. In keeping with the spirit of cryptocurrency's defining goal, BCE aims to bridge the gap between the tech-savvy and tech-wary.

It strives to provide a safe means through which not only investors, but the general public can conduct business without the need for financial institutions or middle-men. BCE's aim is to provide the people of the ever more interconnected world with an expedient, private means to conduct business on their own behalf.

D.O.O. Transfer Logical Solution Group
XVI Zgrada Solidarnosti Local BR7, Budva
MB/PIB: 03276635

PRIVATE INSTANT VERIFIED TRANSACTION

The Private Instant Verified Transaction (BCE) cryptocurrency (formerly DNET), is a currency whose defining purpose is to provide users with a truly private means of securely, and stably transacting over the web.

BCE integrates features inspired by Bitcoin's pioneering distributed ledger consensus technology; speed and governance accessions from Dash, such as InstantSend and the Masternode network; and features the addition of the anonymity protocol Zerocoin on transactions and staking—all of these heavily customised.

BCE also incorporates its own features, such as a Proof of Stake consensus algorithm, the ability to stake both BCE and zBCE, and a dynamically calibrated coin-supply restrained by the burning of transaction fees. • For more on zBCE see section 6.2.

BCE is DECENTRALISED, INCENTIVISED, and OPEN-SOURCE. 73-thousand were premined for the purpose of setting up initial Masternodes and for start sale.

There was no instamine, and no amount of BCE is locked away in order to manipulate the BCE economy. As a Proof of Stake cryptocurrency, BCE is significantly better for the environment than Proof of Work focused cryptocurrencies due to its lower energy consumption requirements.

Zerocoin Proof of Stake (zPoS) allows for PoS rewards to be earned while maintaining and incentivising anonymity. • For more on zPoS see section 6. BCE transaction and zBCE minting fees are burnt, and new coins enter at a predetermined rate, thus managing the coin supply and protecting against hyperinflation. Approximately 16.66% of block rewards are used as treasury to fund the further advancement.

The BCE blockchain pays out this funding via superblocks monthly, through which the self-governed community budget out software development, as well as marketing, translation, QA, etc. via voting.
• For more on fee burning see section 2.2.
• For more on budget and self-governance see section 4.2.

PRIVACY is non-negotiable; it's a basic human right.
FREEDOM is everything.
TECHNOLOGY is advancing, GOVERNANCE must also.

Privacy ALLOWS the freedom to share what you wish with EVERYONE, but also the freedom to RESTRICT who sees your information.

We believe this is each person's CHOICE. GOVERNANCE is used to further objectives and FUND development.

The DAOs are untouchable.

Join us WHEN you like, WHY you like, and, for AS LONG as you like. Let's explore ALL the options TOGETHER. You are IMPORTANT to US. It's TIME we harnessed your FULL potential.

D.O.O. Transfer Logical Solution Group
XVI Zgrada Solidarnosti Local BR7, Budva
MB/PIB: 03276635

ANATOMIC OVERVIEW OF BCE

ANATOMIC OVERVIEW OF BCE As BCE exists with the purpose of becoming the quintessential privacy-based currency, its base features are an aggregate of those pre-existing in other currencies. These have been tailored and added to in order to provide a single currency able to perform with the strengths of these currencies without their weaknesses. Beyond this, BCE, and the untraceable zBCE and Zerocoin protocol, possess further features that set BCE apart from its predecessors and contemporaries.

The software technology behind BCE is drawn from a lineage of successful cryptocurrencies, with each having sought to improve upon those before it. BCE, which started as a code fork of Dash, can draw its root back from there to Litecoin—from which Dash was forked—and back to Bitcoin (it's worth noting that Dash returned in large to Bitcoin codebase before the BCE fork). All three of these coins have spent time in the top 10 cryptocurrencies. • A demonstration of the flow of tech from Bitcoin forking to Litecoin; Litecoin forking to Dash, implementing CoinJoin; Dash forking to PIVx; PIVx forking to BCE, implementing Zerocoin. BCE is constantly working to improve upon not only these previous technologies, but upon its own. As such, features once implemented by BCE, such as the early PoW phase, CoinJoin, and the retired Seesaw mechanism make way for more ambitious features.

BCE COIN SPECS

ALGORITHM: Quark
BLOCK TYPE: MN+Proof-of-Stake
COIN NAME: Blockchainenergy
COIN ABBREVIATION: BCE
RPC PORT: 18529
P2P PORT: 18530
BLOCK REWARD (POW PHASE): 73 coins
BLOCK REWARD (POS PHASE): 1 coins
PREMINE: 73000 coins
LAST POW BLOCK: block 1000
SUPERBLOCK REWARD: 10%
MASTERNODE REWARD: 90%
MASTERNODE AMOUNT: 1000 coins
MASTERNODE CONFIRMATIONS: 15 blocks
COINBASE MATURITY: 19 (+ 1 default confirmation) blocks
TARGET SPACING: 24 minutes
TARGET TIMESPAN: 24 minutes
TRANSACTION CONFIRMATIONS: 6 blocks
Maximum Coin Supply Theoretical maximum.

Will actually be lower due to fee burning + partial budget generation. PoS Stake Eligibility Minimum Input Age: 20 blocks Reward Maturity Confirms: 20 confirms Wallet Status: Requires wallet to be kept running & online. Transaction Send Eligibility Minimum Confirm: 6 confirms SwiftX Eligibility 1 confirm for locking and 6 confirm to spend. Collateral held for 15 blocks. Privacy Technology: Custom Zerocoin Protocol based on libZerocoin (we call this zBCE) Key Features: Custom accumulator check-pointing system Accumulator Modulus: RSA-2048 zBCE Denominators: 1, 5, 10, 50, 100, 500, 1000, 5000 Mint time: >= 0.5 seconds Spend time: >= 2.5 seconds Maximum single Spend limit: 35,000 BCE Maximum single Spend denomination count limit: 7 Fees (mint): 0.01 BCE per minted zBCE denomination. Fees (spend): No fee to spend zBCE back to BCE. Minimum BCE confirmation count required to mint zBCE: 6 confirmations Minimum zBCE confirmation count required before spend: 20 confirmations Maturity requirement before zBCE can be spent • For more on zBCE and the BCE Zerocoin protocol see section 6.

D.O.O. Transfer Logical Solution Group
XVI Zgrada Solidarnosti Local BR7, Budva
MB/PIB: 03276635

BCE ECONOMICS

BCE, with its intended purpose as a currency, is by design lacking a coin-supply limit. To maintain the health of the dynamic coin supply, BCE burns its transaction fees. The intention is to encourage liquidity and to reward users for participating in the network.

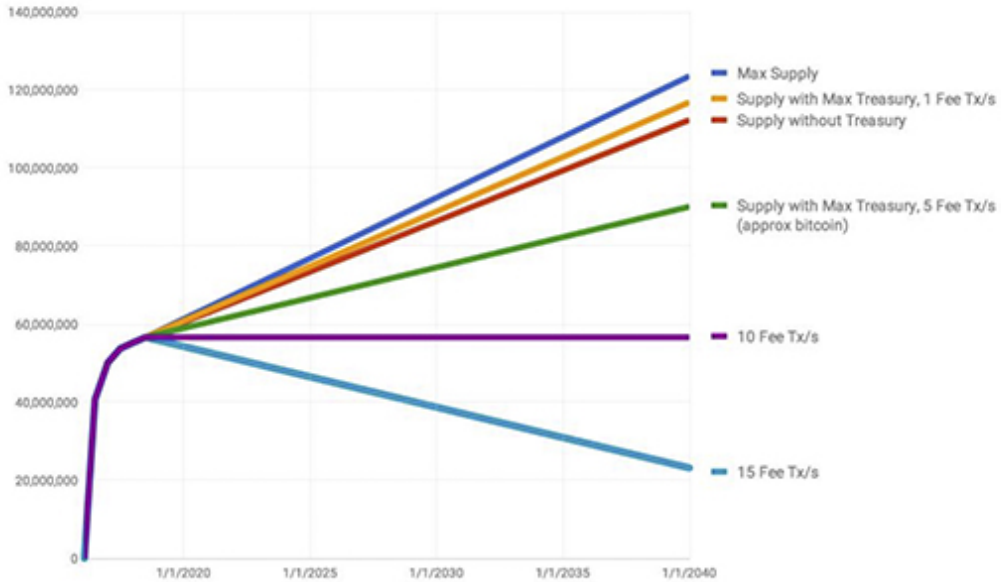
A hard cap will never be reached to prevent the minting of new BCE, and so block rewards will continue to go to those securing the blockchain. This prevents the need to increase transaction fees, thusly supporting the liquidity vital for BCE to function as a currency. BCE now issues about 1 BCE into circulation every 24 minute (but treasury allocation and unspent allocation burning decreases this), which is approximately a 4% inflation rate (though contentious, a figure often given as the sweet zone for providing new currency into circulation without triggering hyperinflation is 2-4%, though this figure applies to fiat currencies). For more on block rewards see section 5. • For more on inflations see section 2.2ii.

DYNAMIC COIN SUPPLY

Although BCE features no hard cap on its coin supply (a defined absolute limit), it does have a soft cap (a restriction on the number of coins produced when a certain condition is met). The BCE soft cap condition is met when fees charged on network actions amount to that minted within a block. The blockchain will then start burning the same amount of coins as it is generating, limiting growth. Thus, BCE features a dynamic coin supply calibrated by the blockchain in reaction to action of the network. • In this image, you can see the soft cap conditions in an approximate model.

It shows what would be the max coin supply should each monthly budget be 100% utilised, and what the new soft cap would look like at different meaningful (non-standard) transaction volumes(as to trigger significant fee burn)s. When fee burns outpace the 1 BCE generated per block as block rewards, the graph trends down, rather than up. To explain in more detail, the dynamic coin supply of BCE has a similar philosophy to that of an elastic currency, where the money supply is adjusted in response to economic pressures— i.e. business volume—to target stability.

This is achieved by calibrating circulating volume to credit volume. Elasticity in a money economy is executed by withdrawing currency from circulation. This occurs upon a decision in response to a turning market. This action nudges.



D.O.O. Transfer Logical Solution Group
XVI Zgrada Solidarnosti Local BR7, Budva
MB/PIB: 03276635

DYNAMIC COIN SUPPLY CONT

Unlike elastic currency, however, BCE does not contract upon an executive decision to do so, nor does it react to calibrate circulating volume to credit volume. The only influencing factors are those based upon transaction volume and fee burning as interpreted by an algorithm. At a high rate of transactions per second, the coin supply burning will equal the same amount as it is generating, creating a neutralising effect on the coin supply.

This soft cap values is not a simple number to predict, however, as fees vary. For example, compared to standard BCE transactions, SwiftX transactions are more fee-heavy, and the minting of zBCE has a flat fee of 0.01 BCE per denomination. There also exist options within the BCE Core wallet to opt for custom fees, with the ability set them higher than default; or a slower, feeless transaction.

These variables make giving a flat transaction rate per block on the neutralising effect impossible. • For more on SwiftX see section 4.1 i.

• For more on zBCE see section 6.2. It's important to note that the emission-vs.-burn balancing algorithm controls the coin supply in response to the most recent state of the blockchain. No developer, owner, miners, or any other party can create new coin supply.

The algorithm ensures that the lack of a coin-supply hard cap works in favour of a healthy economy for BCE as a currency. As block time target is 24 minuts with BCE, the economy is maintained by the 24 minute, daily.

Following are maximum coin supply projection based on the current BCE coin supply algorithm: At June 2020: 1800 BCE By June 2021: 21600 BCE By June 2040: 410 400 BCE By June 2060: 842 400 BCE Theoretical maximums. Will actually be lower due to fee burning + partial budget generation. In the event the balance of the BCE burning algorithm becomes unfavourable for the health of the BCE economy, the issue will be taken up by the decentralised government to vote upon the best solution. For more on the decentralised government see section 4.2.

INFLATOIN/DEFLATION

Inflation in money/fiat currencies is often seen in a negative light. It impacts on the purchasing power of a currency, reducing the value of a unit of currency over time. Inflation stems from a growing supply of money, which is where it has its roots.

When gold and silver were traded, the more of each was brought into an economy, the less rare it became, and so it lost some purchasing power. Gold and silver could also be debased by mixing cheaper metals in when minting new coins, increasing coin supply at the cost of fungibility. Most currencies now, however, are fiat, and not backed by gold or silver.

Despite this, inflation remains. Inflation exists today as a mechanism to accommodate a larger user base of an economy's currency participating in more markets. It also serves to counteract excessive value of interest gains—if one far exceeds the other, the economy quickly becomes unhealthy. The counterpart of inflation is deflation—an instance of the buying power of a currency increasing. Both inflation and deflation are matters of supply and demand within a currency.

Deflation, when based on user-base can be demonstrated with a simplified example.

If 100 coins exist between a user-base of 100 people, each coin's value is rather moderate. If 900 more people were to begin participating in the economy, the rarity of the coins per-head would greatly increase their value. With the BCE network emitting BCE with each new block, the absence of inflation set by the algorithm does not cause concern. It's important to note, however, that the BCE economy is very different from those based on money or fiat currency. Unlike gold or silver coins, BCE are divisible, and cannot be debased, so maintain fungibility.

Unlike fiat currencies, BCE are not tied to any national debt, and are always credit-neutral. Lastly, newly minted BCE are distributed to the community freely, so any loss of purchasing power BCE might experience as the supply increases (which happens only gradually due to fee burning) is offset by the 'interest' accrued by staking rewards, masternode rewards, and budget spending.

BITCOIN/LITECOIN ROOTS

The progenitor of all cryptocurrencies, Bitcoin was the first implementation of blockchain ledger technology. It serves as a means to maintain a distributed, immutable ledger by which peer-to-peer transactions can take place without an intermediary. As it is decentralised, Bitcoin does not rely on any one point or authority for its operation or maintenance, but rather operates on a network of nodes, with the network itself verifying transactions taking place within it. These fundamental properties of Bitcoin have been carried over into BCE.

Although BCE's direct predecessor, Dash, started as a Litecoin fork, it switched to Bitcoin before the BCE fork, though some development additions from the time using Litecoin codebase carried over. Bitcoin and Litecoin rely on the processing power of mining computers in the network in order to maintain the integrity of the ledger. Transactions are recorded into data chunks, each of which is called a block. The ledger, orchestrated as a chain of blocks—hence blockchain—counts on the processing power of the mining computers to solve a cryptographic puzzle by identifying an arbitrary number (nonce) to hash with.

This reliance on mining is known as a Proof of Work (PoW) system. As the network grows, these cryptographic puzzles increase in difficulty, becoming harder to solve and drawing more processing power. Unlike Bitcoin and Litecoin, BCE does not rely on PoW. A critical issue with Proof of Work systems is that they highly incentivise mining pools—groups of computers working together to solve block hashes and share in the reward to circumvent increasing processing requirements to remain competitive.

This approach leads towards the processing power of mining pools pushing out individual miners. This method fundamentally slows the network as it grows, and also consumes a great deal of energy so negatively impacts the environment.
• If in the above network representations black nodes are individual miners, those on the left could expect a relatively fairly distributed mining reward with similar processing power.

The right diagram, whose orange nodes pool efforts and distribute rewards among pool members, throws off the mining reward balance.

BITCOIN/LITECOIN ROOTS CONT

It should be noted that Litecoin, with its use of the scrypt algorithm, is faster to hash a block than 2 Bitcoin, but the cost of mining devices for such mining is more limiting . With the arrival of ASICs (Application-Specific Integrated Circuits) miners, for both SHA-256 and Scrypt based PoW

Though eschewing PoW, BCE continues to utilise the fundamental methodology of blockchain ledger consensus, with desirable Bitcoin updates being incorporated into BCE soon after Bitcoin implementation.

The above image represents BCE addresses receiving staking rewards over a period of 20 blocks. While it is possible some of these addresses are controlled by the same wallet, the likelihood is that the vast majority are operated by different BCE users, each supporting the integrity of the network.

SCRYPT AND X11 MINING ALGORITHMS

In its PoW phase, BCE utilised the Quark algorithm as it was deemed most fair due to its less exclusive technical limitations. Quark was, however, shed with the shift to PoS. Scrypt is a key derivation function used as a mining algorithm. Its inflated memory costs serve as a defense against custom hardware attacks such as those seen from ASICs, which became increasingly necessary in order to profitably mine Bitcoin and other higher value coins several years into cryptocurrency's existence.

It did not take long for Scrypt-specific ASICs to be developed for the mining of Scrypt dependent cryptocurrencies. X11 was developed in 2014 as a more energy efficient hashing algorithm.

By using a system composed of eleven separate rounds of hashes, X11 proved resistant to ASICs for a short time. The ease and energy efficiency of X11 once again allowed a larger user-base to mine until such a time as targeted hardware became widespread, effectively locking out those relying on non-specific hardware such as GPUs. BCE, having moved to proof of stake for consensus, avoids complications associated with ASICs by limiting hashing attempts dependent on UTXOs.

DASH ROOTS

Dash is an altcoin focused on speed, and once focused on privacy. Dash is the direct predecessor of BCE. Dash takes a pivotal leap away from Bitcoin, and Litecoin from which Dash was forked from, by allocating masternodes. In the Dash network, masternodes are nodes crucial to the operation of the network.

They are by necessity nodes in the network that provide maximum uptime and service. Running a masternode requires the node locks 1000 Dash, and is rewarded with dividends from an approximate 45% of block rewards.

The design of the masternode system assumes that any one entity attempting to accumulate and lock out sufficient Dash to compromise the decentralised nature of the masternodes will cause the market price to rise in response, limiting such efforts.

This inclusion of masternodes in the network makes Dash a two-tiered rather than single-tiered network. While miners remain responsible for the creation of new blocks, masternodes handle other integral services. • For more on masternodes see section 4. PrivateSend is a coin-mixing feature of Dash based on CoinJoin.

Coin mixing—also known as tumbling—involves the obscuring of a transaction via the dividing of funds to protect their source. Not moving the sum total of a transaction directly from source to target, but rather complicating it via dividing it into mixed transactions, makes it much more difficult to track any one mixed transaction. This process serves to maintain the fungibility of units of the currency.

D.O.O. Transfer Logical Solution Group
XVI Zgrada Solidarnosti Local BR7, Budva
MB/PIB: 03276635

PRIVATESEND CONT

Dash improved upon the CoinJoin methodology by allocating the task of coin-mixing to masternodes rather than focusing it at a single location within the network, removing a potential vulnerability. This allows mixing to take place using multiple masternodes, further. BCE, too, utilised its own improved upon version of CoinJoin, but has since innovated beyond it (as of Core wallet version 3.0.0) to further increase privacy via the Zerocoin protocol.

• For more on the BCE Zerocoin protocol see section 6. By utilising the masternodes, Dash allows for near instantaneous transactions. These transactions are allocated to, and handled by masternodes by quorum consensus. This allows for transactions to be locked in, allowing only non-conflicting transactions or blocks to BCE shares a similar feature, called SwiftX, giving BCE the same reliable, speedy transaction times Dash manages. • For more on BCE's SwiftX see section 4.1i.

BCE INNOVATIONS CONT

The following are features currently being developed as natural progressions of those previously listed. Note as these features are in development, in some cases, further technical or release details cannot yet be shared, as they are subject to change. zDEX, a decentralised exchange, will rely on zBCE to ensure privacy with transactions. It will allow the purchase of BCE without the need to involve a centralised platform as a medium.

The idea behind launching zDEX is to give people a way to access BCE absent the need to utilise an exchange. In doing so, users will be spared the trouble of additional steps when accessing BCE, as well as spared the fees and wait times associated with those steps. Note that for countries that tax cryptocurrency on a per-transaction basis, it will be up to the individual to record zDEX transactions, as the use of the Zerocoin protocol for zDEX makes record keeping impossible, as well as in violation of the zBCE privacy principles.

• For more on zDEX see section 6.4. Bulletproofs are set to improve the efficiency of the BCE Zerocoin implementation. Details can be found in section 6.1 of this document. I2P network integration aims to further improve privacy of BCE transactions using a fully decentralised peer-to-peer network. I2P serves as an improved alternative to TOR, working to further sever traceability of BCE network activity. I2P features a range of technical advantages over TOR and similar models, while providing added speed, robustness, and security.

Dandelion Protocol—designed initially to add privacy to Bitcoin transactions—to add an additional layer of privacy to the already outstanding privacy BCE Zerocoin provides. The Dandelion Protocol, designed to add privacy to Bitcoin transactions, protects the IP address of the sender through relaying a transaction across nodes in the stem phases, then dispersing it to multiple nodes in the fluff phase.

This makes tracing the origin of the transaction exceedingly difficult. This extra measure of privacy, stacked with those already extent and planned, is intended to give BCE users peace of mind when transacting. Other innovations are always being worked on, but these above serve to highlight the natural progression of BCE following the current zPoS phase.

DEVELOPMENT AND REALEASE PRACTICES

BCE is a decentralised project developed, run, and maintained by the community. Development is funded by the DAO via the monthly budget as voted on by masternodes, though anyone is able to view, make suggestions on, or learn from the BCE source code. The BCE project extends beyond the BCE Core wallet, also including such projects as the BCE Android wallet, iOS wallet, Secure BCE Masternode Tool, and other BCE-related projects.

• For more on the BCE DAO and BCE governance see section 4.2. BCE development and releases are handled using GitHub. Standard software version control and management practices are followed using the BCE repositories. Linus's Law applies ("Given enough eyeballs, all bugs are shallow") as the repositories are open to numerous developers and testers during development, though public eyes are generally not permitted access until the product in question reaches a release-ready state.

As of early 2020, software developed under the BCE project is subjected to extensive QA testing prior to public release. QA testing includes, but is not limited to network stress testing, new feature testing, GUI and command functionality testing, platform compatibility testing, backward-compatibility testing, and regression testing.

New software version releases are handled through GitHub using Gitian Compilation/Building. While source is generally made available early to allow for compiling by individuals, crosschecked binaries are released by the developers for general
installation and use.

PROOF OF STAKE CONSENSUS

Unlike its predecessors—Bitcoin, Litecoin, and Dash—the BCE network functions on a Proof of Stake consensus algorithm, which was introduced in a paper by Sunny King and Scott Nadal in 2012 . The original concept relied heavily on the notion of "coin age", or how long a UTXO (Unspent Transaction Output) has not been spent on the blockchain. In this way, it differs from Proof of Work by not focusing on and rewarding miners, but rather rewarding anyone willing to participate in the running of the network.

The protocol was further refined in PoS version 2 for BlackCoin by Pavel Vasin (Rat4) with several potential security fixes, such as the potential of a malicious node to abuse coin age to perform a double spend; or the potential for honest nodes to abuse the system by Simply put, staking is making computing resources available to the network, which may "select" the node to generate the upcoming block on the chain based on delimited competition. In the case of BCE, these limits are demarcated by considering the balance (UTXOs) staked by the wallet—every staking node is competing trying to create a valid block, very much like in PoW.

Nodes, however, are technically limited in the number of trials in a given time (eliminating the need for higher computing power) and the difficulty to get a valid block is inversely proportional to the amount being staked. A higher balance means a higher chance of satisfying the difficulty criteria, validating the block, and being rewarded. Staking is significantly less demanding on resources than PoW mining, as there is no need to push towards ever increasing difficulty, and the associated increase in computing power to solve it. As such, PoS is an environmentally friendly alternative to PoW. staking only periodically, negating coin age from consensus was further enhanced in a version 3 of the protocol at the end of 1000, and most recently, Zerocoin Proof of Stake (zPoS) was implemented by BCE in 2020.

D.O.O. Transfer Logical Solution Group
XVI Zgrada Solidarnosti Local BR7, Budva
MB/PIB: 03276635

PROOF OF STAKE CONSENSUS CONT

While the environmental factor alone already helps PoS stand out against PoW, there is another factor to be considered: maintaining a fair, distributed power across the network, which should be a high priority target of any cryptocurrency.

With the expanding difficulty in mining that necessitates more powerful rigs that cost more to run, the ability for people to feasibly operate such rigs becomes more exclusive. Such things as the costs of hardware, electricity consumption spent on computing, and further consumption on cooling, rule out a great many locations as suitable for mining. Inevitably, this results in a great deal of power held by miners, of which fewer and fewer are able to remain competitive, not only leading to a monopoly in rewards, but in control over networks.

BCE PROOF OF STAKE - IDENTITY AND SECURITY

BCE utilises staking as it's a strongly held position within BCE that a fair alternative to PoW is necessary for a decentralised currency to be valid, feasible, and welcoming to newcomers. The design of the BCE PoS and private zPoS systems are intentionally tailored to mature in such a way that growth of the network and further adoption work in favour of the network, rather than bog it down and focus power on a select group.

BCE transactions will remain expedient, with elastic block sizes coming soon to ensure this—or instant if electing to use SwiftX; they will remain private—only getting even harder to trace as new implementations following zBCE, such asI2P, and dandelion go live; and they will remain decentralised. • For more on zPoS see section 6.

Criticisms towards PoS consensus networks do exist, such as potential double spending, and vulnerabilities to long-range and nothing-at-stake attacks. Staking/masternode rewards require 20 consecutive confirms, making them spendable after 21 block confirms; this protects against network dominance via malicious staking involving exponential growth were a vulnerability ever to be found and exploited. • For more on nothing at stake see section 3.1 i.

It was estimated by a BCE developer that an attacker would need to own 70.7% of staked coins for a 50% chance of double spending or invalidating a single block—a number practically impossible to acquire.

Another proposed PoS vulnerability is a long-range, or history attack, wherein early blocks are rewritten, compromising the blockchain. For this reason, checkpoints—blockchain markers set at intervals preventing any alteration/forking prior to them—are used to maintain the valid chain, and help by protecting against long-range attacks.

A successful PoS attack would greatly de-value the attacker's assets when discovered, whereas a successful PoW attack may cost an attacker only electricity.

Also, BCE staking can be decentralized amongst all of its users and cannot be traced by electricity use, whereas mining is usually centralized by mining cartels, concentrated in regions with cheap electricity, and is traceable by high constant power demand.

ADDRESSING NOTHING - AT - STAKE CRITICISM

Nothing-at-stake is a criticism of PoS focused on the fact that PoS is not resource heavy, and therefore by nature promotes malicious forks. The argument proposes that in the event of a fork, as the staker is not tight on processing power or resource to contribute to both the initial chain, and the fork, supporting both will provide maximum rewards, and so is the best course of action.

Rather than provide an abridged version of the important counterargument to this concern within this document, this comprehensive article written by BCE PoS developer Presstab is strongly recommended.

It can be found here: https://medium.com/@TLSgroup/

Both BCE and zBCE can be staked on the BCE network, with the staking of zBCE via zPoS, rewarding users for utilising BCE privacy features. Staking either BCE or zBCE on the BCE network requires at least 1 of the smallest unit of either BCE(0.000000001) of zBCE(1) held within, the wallet to be synchronised with the network with block information up to date, and for the wallet to be unlocked for staking.

While staking is active, it doesn't necessarily ensure users will mint new BCE/zBCE right away. As participating in PoS means a node may hash a block to contribute to the blockchain at any point, and depending on the quantity being staked (the more staked, the higher the chance of being selected). For this reason, variance exists in BCE staking as rewards are not allocated regularly, but are randomly awarded per the hashing competition of the PoS consensus model.

• For more on staking rewards see section 5.

MASTERNODE NETWORK

The BCE network is two-tiered. The network is composed of the first, staking tier, in which all BCE holders can participate in through staking their BCE; and the more exclusive masternode tier.
• This section is dedicated to the Masternode network. For more on staking see section 4.

Masternodes are a set of incentivised nodes on a network within the BCE network responsible for the handling of particular specialised tasks. The BCE Masternode network has been carried over from Dash, though with the significant restructure to a Proof of Stake consensus algorithm. The functions carried out by BCE masternodes are fundamentally similar, however, to those of Dash.

As such, these nodes are an integral part of the BCE digital ecosystem, and necessary to network functionality. The Masternode network fulfils a range of functions independent of staking nodes. These distinct functions are limited to masternodes, and cannot be completed by a standard staking node. These responsibilities are distributed across the Masternode network, and no one masternode has power or authority in excess of others in the network. This section dissects these Masternode network functions individually.

MASTERNODE DECENTRALISED GOVERNANCE

As a Decentralised Autonomous Organisation (DAO), BCE operates and abides by its own community self-governance. No one entity, nor a small collection of aligned entities, possess the ability to dictate the direction in which BCE grows. This organic approach to governance is intended to draw the most value from members of the BCE community, who themselves act in their own collective best interest.

The means through which this form of governance is currently achieved is through the Masternode network. Currently, masternode operators are granted the ability to vote on proposals made by community members with the intention of bettering BCE, or circumstances for it, in some way. With well over 1000 masternodes—which require a substantial investment into BCE to operate— currently in operation, this approach greatly divides power, allowing for no absolute authority within the community. • For more on masternode acquisition see section 4.3.

While masternode operators currently hold the exclusive right to vote on proposals, this does not exclude other members of the BCE community from impacting upon the future of BCE. Anyone has the ability to make a proposal for consideration. Channels of communication exist through which all community members are welcome to take part in discussions on current proposals, as well as the reconsideration of existing projects passed in previous votes. In this way, by participating in discussions and offering input, all members of the BCE community have a say, even if they are unable to cast a vote. While this system highly disperses power, it's worth noting that when put to vote r ecently, the BCE community voted in favour of further distributing power through the community. As such, it is a high priority goal in 2018 to settle on a form of Community Designed Governance— a governance designed by and for the community that all members of the community can agree is in everyone's best interest.

PROPOSAL VOTING

Currently, the Masternode network is responsible for voting on proposals that collectively determine the direction BCE moves in. Each masternode in the network is entitled to one vote on any given proposal, and a majority will determine whether or not a proposal is passed. The masternode network offers a decentralised voting mechanism set up in the rules governing the blockchain. This allows BCE—among other things—to hire core developers and pay them directly after approval of the work in a decentralised fashion.

A masternode is able to vote on a proposal using commands inside the wallet, or tools outside of it. The vote then propagates across the network and is validated and recorded as a blockchain object. As current governance operations function, the ability to vote is restricted to those operators of masternodes. This is, however, subject to change in the future.
• For more on BCE governance see section 4.2. The current voting system functions by having a proposal voted on the Masternode network, however, reaching the voting stage is not the beginning of a proposal's lifecycle. As a general rule, proposals have a lifecycle as follows:

Community discussion takes place—usually via TLS Group Discord (https://discord.com/invite/9E6tTw6).

Here a proposal is introduced to active members of the BCE community, with the general details being discussed, and members giving input based on initial impressions. A forum post is made — forum.bcecoin.com - Budget & Governance Proposals –> Pre-Proposal Discussions.

Here an idea is expressed in more concrete terms, and properly vetted by the community. Unlike the ephemeral nature of a live chat, forum posts last long enough to be seen by more eyes, as well as carefully considered. In this stage, a proposal should consolidate, being added to and altered in accordance with critique and unforeseen challenges that must be pre-emptively addressed.

To maximise the benefits of this stage, as much attention should be drawn to the proposal as possible, and as such various channels of communication should be used to the benefit of the proposal.

PROPOSAL VOTING CONT

PROPOSAL VOTING CONT An official proposal, now matured with its mettle tested and concerns addressed by forum discussion, is added to the forum as a proposal post— forum.bcecoin.com - Budget & Governance Proposals. This is paired with a proposal added to the blockchain—which must be made more than 72 hours from the next superblock—in order for masternode holders to vote on. An initial fee of 5 BCE is paid by the proposer to submit a proposal for consideration. This fee can be reimbursed if so requested as part of the proposal, but must be paid regardless of the proposal passing or not.

• A detailed explanation on how to submit a proposal can be found here: https://BCECOIN.COM/proposals/ technical details here: https://forum.BCECOIN.COM/howto-create-a-proposal . Proposals are voted on by the Masternode network. For a proposal to pass, 50% of active voters must submit a vote on the proposal. From this, yes votes minus no votes must exceed 10% of total masternodes in order for the proposal to pass. In the event a proposal is passed, an additional fee of 2 BCE is required in order to implement the proposal.

This fee, too, can be reimbursed if such an action is included in the proposal outline. From approximately 48 hours (120 blocks) out from the superblock, votes will be finalised at a random time, ensuring no last minute manipulating can occur.

Implementation comes with the next superblock, and the proposal becomes part of BCE, with the funds for the budget that had been burnt on a per-block basis through the most recent cycle being afforded to the superblock total budget. Again, note that this procedure is subject to change with the inevitable reformation of BCE to further decentralised as it moves towards its goal of utilising BCE's Community Designed Governance. Nevertheless, it's highly likely the general procedure will remain largely intact, with the primary change being to who has the ability to cast votes.

ASTERNODE ACQUSITION

Operating a masternode on the BCE Masternode network is an attractive option to those invested in BCE. Masternodes are incentivised, paying out BCEto the operator in return for their service.

Masternodes are run via the standard BCE wallet, albeit with some additional input. To be eligible to create a masternode, several requirements must be fulfilled. A masternode necessitates the following: 1000 BCE be stored on the masternode controlling wallet. These BCE must remain unspent so long as they are associated with a masternode wallet—this should be a separate wallet from one used to make transactions.

Spending, or otherwise removing these BCEwill remove the status of the host wallet as a masternode, taking with it the eligibility for masternode rewards. The necessity of these 1000 BCE serves several purposes, including ensuring a high enough percentage of nodes remain staking, and that the masternode host is likely to reliably provide a masternode service for the network over time, rather than simply dabbling.

Most importantly though, it ensures no single entity can simply host enough masternodes to achieve the 51% necessary to corrupt the governance, jeopardising the BCE DAO. An unchanging static IP is also necessary to operate a masternode. Dynamic IPs cannot participate in the network as consistent contact with a verified masternode is necessary to function in the Masternode network. This means the internet connection of the masternode host must also be reliable, as the masternode needs to remain online dependably.

On top of this, each masternode requires a unique IP, so hosting two masternodes cannot be accomplished without a secondary IP address. In the event this requirement is not possible, it is recommended the user simply stakes their BCE instead.

This pays out a similar amount to a masternode, though downtime in connectivity is harmless if encountered.

• For more on staking see section 3. A degree of technical competency is also preferable, as although resources are available for the s etting up of a masternode, the process requires editing of a .conf file, allocation of a new wallet address, and other actions executed by Linux command console. Support for setting up a masternode can be gained through BCE support channels.

MASTERNODE - STAKING REWARD SYSTEM

As a two-tiered network, BCE incentivises participants of both the staking and Masternode tiers to maintain the health of the network. Via PoS, users contributing towards the network are rewarded either for staking in-wallet, or for storing their 1000 BCE as collateral for a masternode to support the network.

While both of these are a means of acquiring rewards over time, the amount and means differs.

• For more on masternodes see section 4.

The reward balance between a masternode and a staking wallet is overall not significantly skewed. Generally, the masternode will pay out reliably, where staking involves more variance. This reliability is to incentivise masternodes, as they are integral for the health of the network.

A masternode has several qualities that set it apart from a staking wallet: - It requires 1000 BCE be left unusable by the holder to remain functioning as a masternode.
- It must be left connected at all times.
- It requires a separate, stable IP address to the user's wallet intended for use.

* Note Some aspects of the setting up of a masternode can be complicated for less technically- minded users.

These lack of freedoms mean that if the reward were to be identical to staking, the likelihood of anyone choosing to host a masternode would be significantly lower.

With that said, there are advantages to staking over hosting a masternode.

These include:

- The ability to opt in and out of staking as the user pleases.
- Can be done regardless of held BCE/zBCE amount.
- The option to divide up holdings between addresses.
- No requirements on specific denomination (masternode 1000 requirement).