bitcoin cz

mintpaper

disclaimer

The information provided in Bitcoin CZ mintpaper and accompanying material is for informational purposes only. It should not be considered legal or financial advice. You should consult with an attorney or other professional to determine what may be best for your individual needs.

Bitcoin CZ does not make any guarantee or other promise as to any results that may be obtained from using our content. It is not recommended to make any investment decision without first consulting his or her own financial advisor and conducting his or her own research and due diligence. To the maximum extent permitted by law, Bitcoin CZ disclaims any and all liability in the event any information, commentary, analysis, opinions, advice and/or recommendations prove to be inaccurate, incomplete or unreliable, or result in any investment or other losses.

Content contained on or made available through the website (https://bitcoincz.org/) is not intended to and does not constitute legal advice or investment advice and no attorney-client relationship is formed. Your use of the information on the website or materials linked from the Web is at your own risk.

For more information contact legal@bitcoincz.org

contents

specifications......................................5
introduction.......................................6
overview..7
details...13
purpose...19
products...22
monetization......................................24
roadmap... 27
references..29

coin specifications

Bitcoin CZ / BCZ

Block reward: 3.1 BCZ
Max supply: 3,999,999
MN collateral: 5,000 BCZ
PoS requirement:100 BCZ

Website: https://bitcoincz.org
Github: https://github.com/BitcoinCZ
Block explorer: https://chainz.cryptoid.info/bcz
Bitcointalk: https://bitcointalk.org/index.php?topic=5140548

Discord: https://discord.gg/MarVC2B
Twitter: https://twitter.com/bitcoincz_org
Telegram: https://t.me/BitcoinCZ_ann
Telegram chat: https://t.me/Ecosystemz

Exchanges: crex24.com, sistemkoin.com

introduction

Cryptocurrencies use a combination cryptography and blockchain technologies to attempt to decouple financial transactions from the central banks and governments by committing all transaction to an immutable, public ledger.

In contrast to the daily spending medium of the people, by the people, and for the people–instead of fiat–that cryptocurrency endeavors to be, slow block times have proven that earlier projects are not scalable to become the daily buying and spending solution that is needed in order to achieve wide-scale social and commercial adoption. Moreover, many cryptocurrencies have become highly centralized, and decisions about on-going development are decided by a few powerful mining pools as opposed to a decentralized solution.

Finally, cryptocurrency has been unable to achieve market penetration due to a lack of accessibility to the average consumer because prior iterations lack the infrastructure and applications to meet the changing demands and expectations of a typical person. These are the issues that Bitcoin CZ seeks to address.

"Writing a description for this thing for general audiences is bloody hard. There's nothing to relate it to."

- Satoshi Nakamoto

overview

Bitcoin CZ's primary goal is create to accessible, high-end technology with a low barrier to entry while simultaneously delivering a product that is more useable, more reliable, more versatile, and more smoothly integrated and assembled than even the market leaders. BCZ has been designed build upon the strengths of the Unspent Transaction Output (UTXO) model. The recordation of all transactions on an immutable ledger successfully removes the need for trusted third parties.

The challenges that the initial versions of cryptocurrencies have encountered demonstrate that the next generation of cryptocurrency will need to be structured in such a way as to be decentralized and resistant to the control by large mining pools, scalable by having low block times so as to facilitate actual transactions and commerce on a significant scale, and provide effective anonymity rather than pseudo-anonymity.

Bitcoin CZ's technical design and initial distribution have been thoughtfully and purposively designed in order to prevent accumulation of determinative power, or centralization, amongst a limited group of coin holders.

Throughout an initial phase of Proof of Work (PoW) for block generation to the current phase of Proof of Stake, PoS, the blockchain is intentionally designed to have new blocks be disbursed widely with the maximum spread amongst of miners, originally, or stake holders, currently. Broad eligibility to find or forge blocks so that the rewards are widely distributed prevents concentration into the wallets of a powerful few.

coin distribution information

initial supply	new supply	mainnet launch
9044973.77839209	2228593.49154938	April 26, 2019
burnt supply	max supply	coinburn date
6816380.28684271	3999999.00000000	June 01, 2019

The Bitcoin CZ development team has transitioned the blockchain propagation from Proof of Work (PoW) to Proof of Stake (PoS). PoS presents numerous advantages over the traditional PoW means of blockchain propagation, and many projects are discussing and promising to make the change. BCZ uses PoS exclusively at this time.

Algorithm

It is a technically difficult transition, and the majority of projects are scheduling a transition for 2021 or beyond. Consistent with prior technical achievements by the lead community developers, such as patching several privacy protocol flaws in other projects, developing and deploying NEXXT for PoW propagation, and inventing KNIFE technology, the Bitcoin CZ developers have successfully integrated PoS technology into Bitcoin CZ.

Rather than scheduling the transition for a distant time in the future that would likely suffer delay, as many scheduled events do, the developers have quietly and simply effectuated the change. Delivering the best available technology and solutions is a priority of the current core developers. In this way, Bitcoin CZ remains a leader in the blockchain space by promptly moving to an energy efficient means of blockchain propagation that serves Bitcoin CZ's mission of ensuring decentralization while also providing robust disincentivation for malicious attacks.

Algorithms can be seamlessly implemented and adjusted by the lead community developers in order to reach a proper balance to ensure the optimal decentralized state as opposed to periodic mining difficulty adjustments that permit attacks and coups. Furthermore, the initial distribution was conducted in order to avoid any particular address from having a disproportionately large quantity of coins from the outset that would have otherwise put others at a significant disadvantage.

Bitcoin CZ has been scrupulously crafted to fit into a system of products that facilitates widespread adoption for financial transactions and commercial applications. By having a faster block time, transactions can process quickly and reliably which will accelerate users’, buyers,’ sellers’, and vendors’ willingness to embrace and use Bitcoin CZ. Bitcoin CZ’s implementation allows it to establish and maintain itself as a means of low cost on-chain transactions, which is effectively establishing an alternative to the traditional high fee per transaction structures as credit cards.

The first of the family of supporting products that has been introduced is PayBOXX. PayBOXX is a decentralized payment channel for fast and smooth transactions using BCZ. PayBOXX is easily accessible for internet connected devices via desktop web browsers in addition to having mobile access. In order to protect user privacy, no user information is stored by PayBOXX.

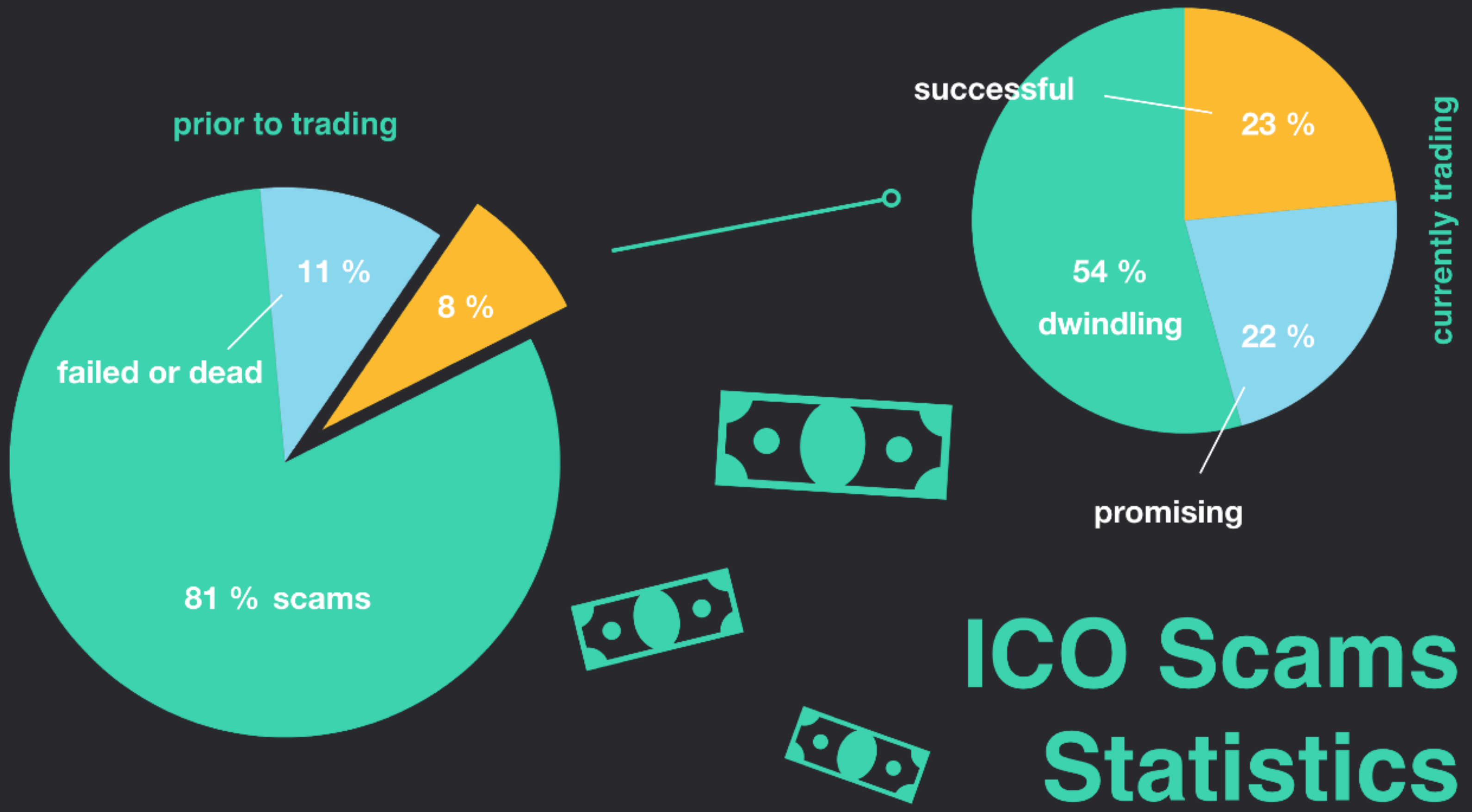
PayBOXX does not store information in cookies, does not record IP addresses, does not follow HTTP Referrers, does not compile information from user agents, and does not use tracking scripts. PayBOXX is safe, private, and easy-to-use.

Privacy

Privacy solutions continue to evolve. The lead community developers have begun the process of infusing BCZ with Sigma (Σ) privacy protocol (core v. 6.0.1.2), which provides a privacy solution that does not require a trusted setup. Projected public launch of ΣBCZ is Q4 2019. Furthermore, the lead community developers are progressing through the technical challenges of private staking in order to provide the community with the option to earn staking rewards from coins protected with Sigma privacy, which will be an industry first. Projected public launch of ΣBCZ staking is Q1 2020.

In stark contrast to the rest of the blockchain space, the lead community developers' and contributors' finances are at least equal if not greater risk than the holders' finances are. Should the project fail, there are no adverse consequences for other development teams because they either received funds directly up front or they have ample pre-mine that they can sell on the open market. Conversely, the Bitcoin CZ developers had no ICO and no pre-mine. The Bitcoin CZ community seeks to take the path of highest integrity.

Unlike all other modern business models in cryptocurrency today, only the Bitcoin CZ developers have more to risk than any of the holders. This facet of the development team alone gives an investor confidence in the credibility and dedication on the part of the development team. The developers only win like everyone else: when the holders win by Bitcoin CZ's positive performance. This is a level of integrity that instantly distinguishes Bitcoin CZ from every other blockchain technology on the market today. Eventually, we are looking for a larger community of responsible developers who would be motivated by the ability to contribute their applications and services to the community ecosystem.



ICO Scams Statistics

Background

All blockchain is software, and software requires periodic revisions, changes, and updates. When the patched blockchain is no longer interoperable with earlier blockchain, the outcome is called a hardfork and may result in two separate blockchains. When the update is sufficiently adopted by the earlier blockchain, the outcome is a softfork and results in a continuation of a single blockchain because the update is integrated into the main blockchain by consensus. Prior projects have used the process of a hardfork to effect philosophical changes and new approaches to the existing chain. Earlier projects would create new projects from a single chain, for instance when BitcoinCash hardforked from Bitcoin. Subsequently, Bitcoin Satoshi's Vision hardforked from Bitcoin Cash. These were all single step forks.

KNIFE

Hardforks require a complete combination of all the involved blockchains, which creates a very large blockchain history in order to complete the ledger. This also necessarily includes outdated, non-functional, and redundant parts of the code. While working on other projects, the lead community developers discovered a custom UTXO tool that they named KNIFE. With KNIFE, many different blockchains can be joined as one new coin without the inclusion of unnecessary and irrelevant complications that a forking process necessitates.

Rather than combining entire blockchains, frames can be used resulting in a lighter output chain without a huge coin supply. A lightweight blockchain is critical for mass adoption with low cost on-chain transactions. This allows for a precise process for exact inclusions and specific exclusions for maximum efficiency and effectiveness while simultaneously minimizing the size, or weight, of the blockchain. The ability to control the final initial allotment of coins is one of the means by which decentralization is assured, as discussed above.

Unlike other processes, KNIFE technology provides a unique vehicle for connections between blockchains. Specifically, blockchain inter-operability is an emergent property of the technology. Multiple coins on different blockchains can be joined to create one new coin via multiple blockchain injection. Unlike Bitcoin forks that cannot interact after forking and unlike Ethereum tokens that all run on Ethereum, KNIFE allows for coins to have their own, separate main network yet still interact with one another. Resultant from KNIFE's process of cutting frames out of the target blockchains, many coins can be combined into one yet still result in a final new coin with a manageable chain size and without an excessive coin supply. KNIFE then effectively allows some degree of flexibility in demographic selection or targeting.

Since UTXO are KNIFE injected rather than merge forking entire blockchains together, the process is both stable and eliminates the need for replay protection. This property of KNIFE coins can effectively function as a replay filter.

SPORK

Furthermore, Bitcoin CZ is equipped with SPORK technology that allows for changes to the blockchain code without introducing concerns about a hard fork and separation of the blockchain into multiple, independent chains. The included SPORK technology allows for network-level adjustments to ensure the health of the blockchain without need for all users to update wallets.

BCZ launched with masternodes ensure the health and stability of the network through off-loading some functions as well as storing complete copies of the blockchain in order to maintain the integrity of the ledger, which thwarts malicious attacks or attempts to exploit the chain. Nodes are computers that host a full copy of Bitcoin CZ's blockchain and help to verify the validity of transactions. Masternodes are a special type of node that earn part of Bitcoin CZ's block reward—currently at 1 BCZ of the 3.1 BCZ block reward—in return for hosting a reliable and powerful node that helps to support the network. Masternodes require a collateral of 5,000 BCZ to ensure

MN

masternodes holders have a stake in the cryptocurrency and are incentivized to keep it working honestly, updated often, and have a high uptime. Collateral may be redeemed at any time the holder wishes to deactivate the masternode.

BCZ's masternodes will be useful, effective, and multifaceted. With SPORK, Bitcoin CZ will be the first blockchain technology to offer multi-adaptive masternodes that are able to adjust as needed based upon network conditions. Moreover, sporks can be deployed to expeditiously address critical security issues, rectify malfunctions in the blockchain propagation, or augment functionality, and all of these actions can be accomplished without requiring users to install new wallets, which enhances the user experience through seamless maintenance.

Additionally, BCZ is projected to launch a tiered masternode system in Q4 of 2019. Tiered masternodes allow for smaller holders and larger holders alike to enjoy the rewards of masternodes while also supporting the health of the network. Larger nodes will provide larger rewards to acknowledge the confidence in the future of BCZ that is captured in a holder locking up significant amounts of funding for collateralization of a masternode. By holders locking up BCZ as collateral for masternodes, they also thereby increase the scarcity of BCZ on the open market, which may provide upward price pressure. Different tiers of masternodes may also provide different functions that then enhance and expand the features and abilities of the growing BCZ network.

Stake

Following from BCZ's foundational principle of decentralization, the PoS reward system has been meticulously engineered in order to promote equal staking for all. In order to achieve this, BCZ desktop wallet automatically optimizes transactions into blocks greater than 100 BCZ but less than 200 BCZ. The wallet will automatically combine transactions of less than 100 BCZ into a transaction greater than 100 BCZ. The wallet will also automatically split transactions greater than 200 BCZ down to multiple transactions less than 200 BCZ.

These dual mechanisms promote the equality and fairness of decentralization that no other cryptocurrency has achieved. Furthermore, the minimum amount required to earn a stake is 100 BCZ, which allows a broad range of holder to have comparative access to rewards, unlike most cryptocurrencies wherein only the wealthy and powerful can earn rewards.

BCZ embraces the necessity of ease-of-use for widespread adoption. To that end, some of the tools that are currently available include SwiftX and MultiSend. SwiftX is powerful feature that facilitates adoption by merchants, vendors, and purchasers because up to a 1000 BCZ can be sent instantly with only one confirmation. This is kind of rapid exchange that will finally be able to put electronic, peer-to-peer (p2p) transactions on parity with fiat ones as a means to displacing fiat as the default medium of trade.

MultiSend is an innovative means of helping users to maximize their passive returns with BCZ. Both masternodes and PoS provide rewards to holders. With MultiSend, the rewards can then be transferred to a specific address upon maturity in order to increase future earnings by increasing the size of one's stake, which increases the chances of future reward. Thus, rather than having to manually combine rewards into a transaction or wait for the wallet to periodically do so, the MultiSend setting can be used to help increase chances of reward for staking as soon as the received reward has matured.

Ten years of blockchain history indicate that one coin—one blockchain—cannot do it all. It does not appear to be possible for payments, services, contracts, anonymity functions, data storage, and decentralized applications (dApps) to all reside on a single blockchain technically, let alone practically. In order to be able to maximize the potential for cryptocurrency and blockchain, there needs to be both specialization and interconnectivity amongst blockchains. While each needs to be able to fulfill the role and mission for which it was developed, blockchains also need to be able to effectively interact with one another in order to be connect economics and daily life in a manner that will facilitate widespread adoption.

Interoperability and acceptance of an ecosystem of interacting, yet independent blockchains, is the best solution to meet all the demands which blockchain is capable of satisfying in the marketplace and in society. To that end, Bitcoin CZ's place in the ecosystem of blockchains is as a lightweight currency to allow for fast, smooth transactions both inside the ecosystem and to the larger outside market and world. Bitcoin CZ is poised to offer accessible interoperability and extra-operability by leveraging current set infrastructures with innovative new tools as well.

CZ

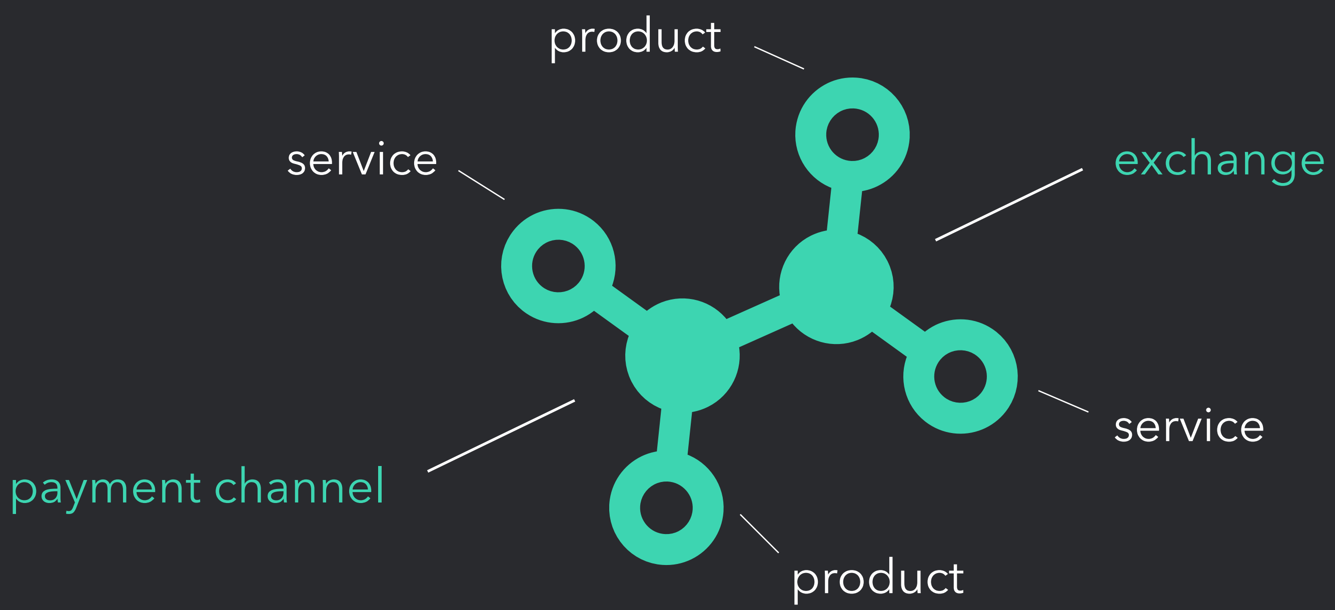
Consistent with the development team's philosophical, principled, and pragmatic approach, the team recognized the stance that CZ of Binance took regarding Bitcoin Satoshi's Vision, which was actively pursuing questionable means and ends. Additionally, CZ has made significant contributions to the cryptocurrency space through his leadership at Binance by a consistent pursuit to grow cryptocurrency projects and make them more accessible to the larger world. He has created a convenient and efficient ecosystem of comfortable and accessible products, which is moving blockchain forward as an industry. In order to acknowledge his actions for the larger cryptocurrency community, Bitcoin CZ was named in tribute to him.

The Bitcoin CZ community has collectively decided that it would like to support technological initiatives and educational development amongst users. In order to achieve this, the Bitcoin CZ Foundation has been established to recognize, encourage, and award efforts by non-traditional innovators, such as youth, elderly, and others who make contributions from blockchain from without the traditional field of developers. The Bitcoin CZ Foundation initiative is consistent with the greater Bitcoin CZ focus on decentralization of power and accessibility to the greater population.

purpose

The Bitcoin CZ Foundation acts to ensure adoption of blockchain development and programming skills by a larger audience as a means of helping to prevent centralization of the critical development skills from being confined to a limited number of enlightened individuals.

Similarly to CZ Binance, this community is seeking a network of interconnected services and applications based on the blockchain. Bitcoin CZ vision is bringing blockchain opportunities to the real life: our community believes that every use case is a step forward for the industry. Therefore, our current mission is to create as much quality services and applications as we can think of, at the same time making them a sustainable network from the social, economical, and environmental perspective. The progress of a certain application development is regularly updated and can be either monitored on the website or in the products section of this documentation.



products

PAYBOXX (Alpha 100%)

Web browser payment channel for comfortable shopping with various cryptocurrencies. Alpha version is available at https://payboxx.io.

ELECTRUMXX (95%)

A digital utility for creating unlimited variations of lightweight applications and data sync. This is the base of most applications and use cases within the ecosystem.

DEXX (25%)

Comfortable trading platform that does not store any funds allowing users to fully control them.

GAMEBOXX (65%)

A gaming platform where people could use their BCZ for PvP gaming and developers could earn profit for their games by sharing a commission.

GameBOXX
A gaming platform for PvP and Solo competing in your favorite classics!
Games developers are welcome to join the platform and share the commission!
Place BCZ bets, win big, and have fun with your mates!

products

PIXX (90%)

Specific version of wallet for Raspberry Pi developed in order to make Bitcoin CZ more accessible.

MIXX (15%)

Cryptocurrency mixer that solves fungibility problem by disconnecting funds from history. A privacy protocol is to be utilized in order to prevent any funds tracking.

LOXX (5%)

Multifunctional mobile wallet intended to become a comfortable and intuitive tool for a daily usage.

PIXX: BCZ Raspberry Pi Wallet

Meet **PIXX**:

PoS Mining
Masternodes
Energy efficient
Auto-Mint

Opportunity for 24/7 staking and node running without 3rd party.

A desktop wallet for Raspberry Pi users - most decentralized option to run **BCZ**.

Tons of opportunities. Full control of your funds.

Let's make crypto a world standard together!

monetization

Bitcoin CZ provides financial transparency. The team has developed a financially viable model that meets Bitcoin CZ's fiscal requirements, provides funding for development and expansion, and delivers value to the Bitcoin CZ community and larger, global community.

Bitcoin CZ currently offers revenue generating services and is developing a number of additional services.

Currently, Bitcoin CZ generates revenue when transactions are made on the blockchain as well as through the PayBOXX product, which both collects its own fee and also induces a fee from being transacted on the blockchain.

With revenues from these in addition to the fees that will be collected from other products, such as MIXX and DEXX, the developers will use 33% of the revenue to purchase Bitcoin CZ. This will provide a two-step process of added value for Bitcoin CZ holders.

First and most immediately, the team's purchasing of Bitcoin CZ will be an additional market pressure to drive price upwards, thereby increasing the value of a holder's assets. Secondly, the Bitcoin CZ team will then periodically distribute all of the purchased Bitcoin CZ to holders on a proportional basis to each's holding on the distribution date, which will be randomly scheduled in order to avoid accumulation followed by post-distribution market selling.

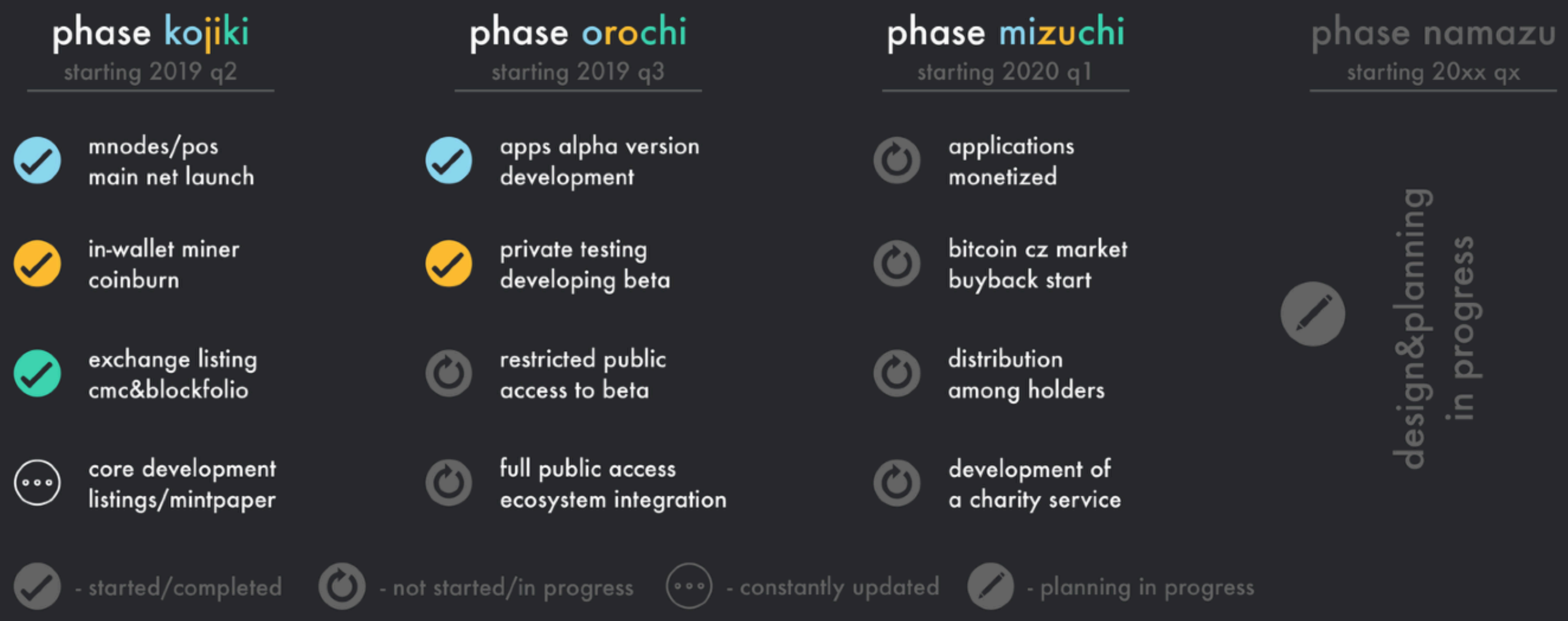
The Bitcoin CZ team will use the revenue to also return value to the greater global community at large through a charitable donation channel. 1% of the collected revenues from product and services will be given to a charitable cause that is nominated by the community of coin holders. In this way, Bitcoin CZ will help the larger world in a way preferred by the community.

Finally, 66% of the revenues from Bitcoin CZ will be used to maintain and expand the operation of the blockchain. The expenses paid include, and are not limited to, server space, advertising and marketing, ancillary services, and various listings. All revenues for the community fund, or c-fund, go to the costs, maintenance, and development of Bitcoin CZ.

The community vote will take a place if there is any need in reviewing the allocation of profit created by any services or products. In order to guarantee transparency in fund management, BCZ lead developers are designing a set of tools that would eliminate domination by any particular individual. In other words, the process of distribution is intended to be automatized and provide every user with an access to the transaction history of BCZ distribution or chosen charitable organizations.

roadmap

The community development has been separated into several steps based on the philosophy of the project at a certain age. Phase Kojiki is responsible for the basics of any currency - core development, initial listings, and informational resources. Meanwhile, phase Orochi is focused on creating apps and services based on the core tech developed during phase Kojiki. Next, phase Mizuchi will benefit from the achievements of the community during the phase Orochi. Phase Namazu will follow right after the first monetization takes place. It is important to understand that there is only a start date to a certain phase - once the phase has started, the work in that direction does not stop at a certain point. Thus, the lead community developers are seeking to grow the team to meet the growing demands that will accompany success and growth.



phase kojiki
starting 2019 q2

- ✓ mnodes/pos main net launch
- ✓ in-wallet miner coinburn
- ✓ exchange listing cmc&blockfolio
- ••• core development listings/mintpaper

phase orochi
starting 2019 q3

- ✓ apps alpha version development
- ✓ private testing developing beta
- ⟳ restricted public access to beta
- ⟳ full public access ecosystem integration

phase mizuchi
starting 2020 q1

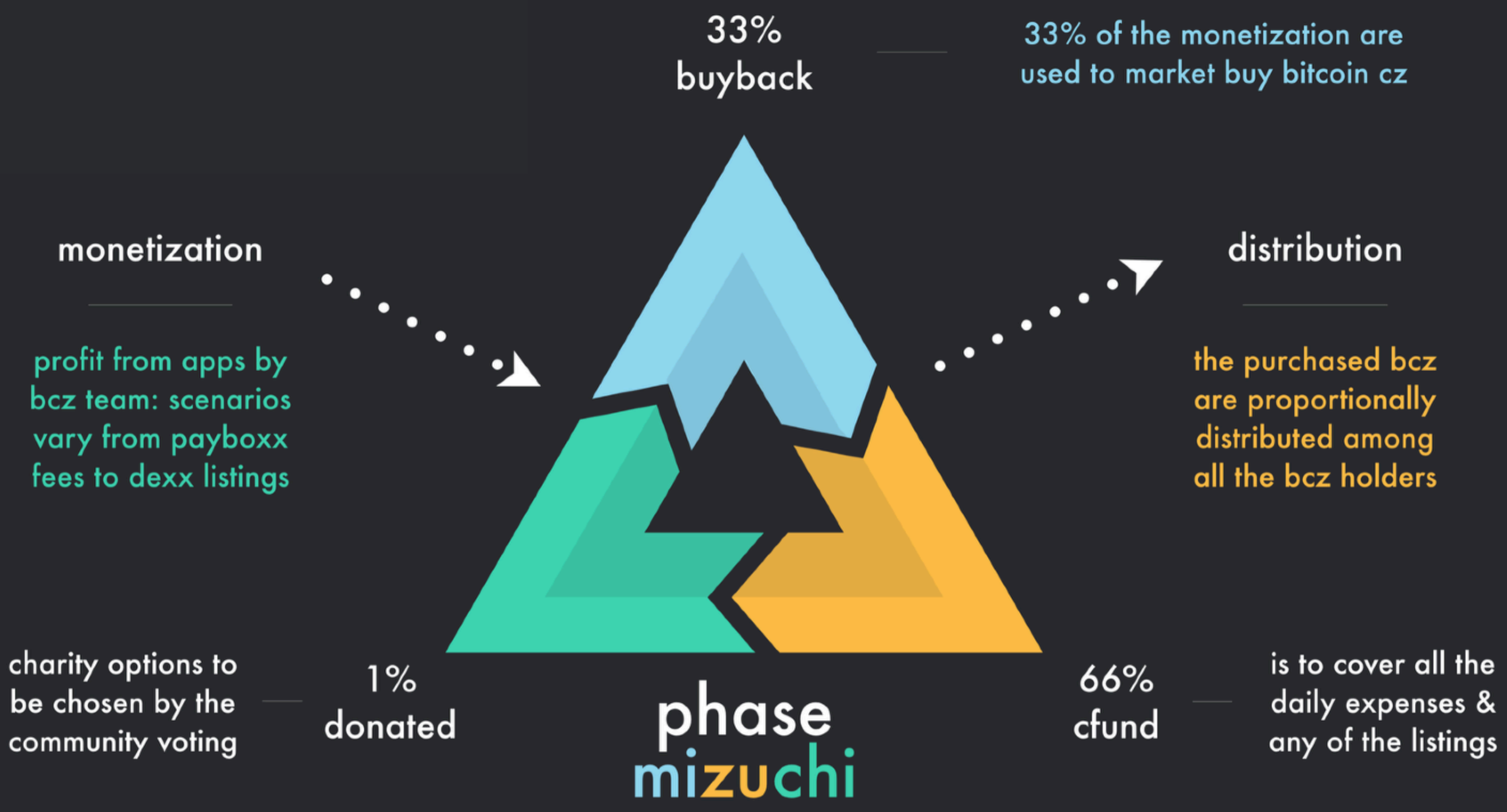
- ⟳ applications monetized
- ⟳ bitcoin cz market buyback start
- ⟳ distribution among holders
- ⟳ development of a charity service

phase namazu
starting 20xx qx

- ✎ design&planning in progress

✓ - started/completed ⟳ - not started/in progress ••• - constantly updated ✎ - planning in progress roadmap

The whole monetization process is a big part of our roadmap and has been detailed in the previous section. A visual summary is presented below in order to deliver the sequence of financial operations in a clear way. Holding BCZ through any distributions does not guarantee a precise payout and could not be considered a security of any kind.


33%
buyback
33% of the monetization are used to market buy bitcoin cz
monetization
profit from apps by bcz team: scenarios vary from payboxx fees to dexx listings
distribution
the purchased bcz are proportionally distributed among all the bcz holders
charity options to be chosen by the community voting
1%
donated
phase
mizuchi
66%
cfund
is to cover all the daily expenses & any of the listings

references

These references contain more information about core mechanisms utilized in BCZ and concepts discussed in this documentation:

2nd Global Cryptoasset Benchmarking Study

Bitcoin: A Peer-to-Peer Electronic Cash System

Bitcoin scalability problem

Dash: A Payments-Focused Cryptocurrency

Decentralization in Bitcoin and Ethereum Networks

Eth2.0 Implementers Call #19 [2019/6/13]

General Data Protection Regulation (GDPR): What you need to know to stay compliant

One-out-of-many proofs: Or how to leak a secret and spend a coin

Own Initiative Report on Initial Coin Offerings and Crypto-Assets

Proof of Stake versus Proof of Work

Understanding Bitcoin traceability

references

List of scientific publications:

Bulletproofs: Short Proofs for Confidential Transactions and More, https://crypto.stanford.edu/bulletproofs/, https://eprint.iacr.org/2017/1066.pdf

Duffield, E., Diaz, D., Dash Whitepaper, Section 2 Masternode Network, https://github.com/dashpay/dash/wiki/Whitepaper

G. O. Karame, E. Androulaki, and S. Capkun, "Two bitcoins at the price of one? double-spending attacks on fast payments in bitcoin," Cryptology ePrint Archive, Report 2012/248, 2012, http://eprint.iacr.org/.

J. Camenisch and M.Michels, "Proving in zero-knowledge that a number n is the product of two safe primes," in EUROCRYPT '99, vol. 1592 of LNCS, 1999, pp. 107–122.

J. Camenisch, "Group signature schemes and payment systems based on the discrete logarithm problem," Ph.D. dissertation, ETH Zu¨rich, 1998.

P. Vasin, BlackCoin's Proof-of-Stake Protocol v2, https://blackcoin.co/blackcoin-pos-protocol-v2-whitepaper.pdf

R. Cramer, I. Damgard, and B. Schoenmakers, "Proofs of partial knowledge and simplified design of witness hiding protocols," in CRYPTO '94, vol. 839 of LNCS, 1994, pp. 174–187.

S. King, S. Nadal, PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake, 2012

S. Barber, X. Boyen, E. Shi, and E. Uzun, "Bitter to better – how to make bitcoin a better currency," in Financial Cryptography 2012, vol. 7397 of LNCS, 2012, pp. 399–414.

Zero-knowledge proofs, https://en.wikipedia.org/wiki/Zero- knowledge_proof#Abstract_examples

Special thanks to DevØØ9, DC,
2Infinity for the technical
achievements of BCZ

Special thanks to Beaner, J.W.
Cnfused, Dr for writing this
documentation

? how much
is the fish