



BitcoinZ + zkSNARKs
In Decentralization We Trust



(BitcoinZ Seal)

BitcoinZ - Community Paper

A Community Gift To The World

Fairness Core = fair start + PoW + decentralized + 21 billion = at least 1 for all



BitcoinZ + zkSNARKs
In Decentralization We Trust

(BitcoinZ Logo + Mantra)



BitcoinZ + zkSNARKs
In Decentralization We Trust

Coin: BitcoinZ

Ticker: BTCZ

Algorithm: Equihash

Type: Proof of Work (PoW)

Current Block Reward: 12,500 BTCZ

[Community Team](#)

Background

BitcoinZ was officially launched by an anonymous developer on September 9th, 2017 at Block #1 with [BlockHash 0007844681f84249ad7829f9673ea4b6d26a139c741c5847926aff944337d908](#).

They deemed BitcoinZ a community gift to the world, emphasizing that it is, and will continue, as a community creation. The following timeline of events occurred to memorialize and publically announce the launch:

- GitHub announcement at Block #71 with no public pools. [Link](#)
- Announced in Zclassic Slack in #general at Block #284 with 15KSol/s network hash
- BitcoinTalk Announcement ('ANN') on September 10th, 2017. [Link](#)

Within four (4) weeks of launch, the block height broke 15,000 and had a network hash of 4-5MSol/s.

The founding principles are:

- One-hundred percent decentralized development
- Zclassic spirit, Zcash core, Bitcoin fundamentals
- Always immutable, hardforks only for improvements, changing history is banned
- Fair proposal system
- Everyone is equal and every coin is made by the community and for the community
- Everyone should be able to mine (ASIC resistant)



BitcoinZ + zkSNARKs In Decentralization We Trust

- We fight for freedom and personal liberty
- No pre-mine, no ICO, no dev taxes

To enshrine this vision of liberty, fairness, and the fight for freedom, a message was encoded in the genesis block timestamp of BitcoinZ dedicated to The Purest Son of Liberty - Thaddeus Kosciuszko, whose 200th death anniversary is October 15th. [See here](#)

Code of Conduct

As the BitcoinZ Community continues to grow, we need to advise of certain behaviors that will not be tolerated in the community. The BitcoinZ community will disassociate itself with any entities, associations, groups, or other collection of persons who:

- Insult others about characteristics that are naturally a part of being human, such as, but not limited to: race, national origin, color, sex, sexual orientation, ethnicity, religious beliefs, language spoken, social status, cultural traits.
- Engaging in or promoting activities reasonably expected or known to be illegal, harmful, or fraudulent to the community and/or the public.
- Using the BitcoinZ or BTCZ community name or likeness to facilitate fraud, scams, or other harmful behaviors.
- Intentionally or negligently conducts themselves in any way that damages, or falsifies the image of the BitcoinZ community.
- Conducts themselves or engages in disruptive behavior across BitcoinZ or other communication channels. (chats, social media, forums, message boards, chat on Exchanges, Youtube chats, etc.)

We cannot force good behavior, but we strongly encourage everyone to be respectful to each other. This is a historic global decentralized movement. As we continue to grow, we expect that anyone who chooses to join the community can do so without fear of experiencing insulting, threatening, or harmful behavior. “In Decentralization We Trust”.



BitcoinZ + zkSNARKs In Decentralization We Trust

Tech / Coin Supply Policy

BitcoinZ is a bitcoin compatible [cryptocurrency](#) based on the zcash core. It utilizes the Equihash algorithm with t-addresses and zk-snarks anonymous z-addresses.

The combination of these technologies enables BitcoinZ to operate as a proven cryptocurrency with the ability to offer graphics processor unit (GPU) mining to anyone in the world with access to off the shelf graphics cards, also known as commodity hardware. Additionally, it enables the portability and compatibility with BitcoinZ and other cryptocurrency blockchains.

Since BitcoinZ has adopted the zcash core, it inherits a 'halving interval', adjusted for BitcoinZ's total supply. The halving interval is set for block 840,000 and is estimated to occur in approximately 4 years from the Sept 9th, 2017 launch. The interval is set in line 44 of chainparams.cpp here: [Github](#)

The approximate calculation can be completed by the following steps:

- a.) Blocks Per Day = Seconds In A 24hr Day / Block Time = $1,440 / 2.5 = 576$
- b.) Blocks Per Year = Blocks Per Day x Days In Year = $576 \times 365 = 210,240$
- c.) Halving Interval In Years = Halving Block Interval / Blocks Per Year = $840,000 / 210,240 = 3.99$

So in approximately 3.99 years, the block reward will go from 12,500 to 6,250, in accordance with the consensus code Halving Interval set at the 840,000th block.

At this point, BTCZ will have reached approximately half of its total supply, or approximately 10,500,000,000. (10.5 billion)



BitcoinZ + zkSNARKs
In Decentralization We Trust

Community Sites (as of Jan 01, 2018)

I. BitcoinTalk Announcement ('ANN')

<https://bitcointalk.org/index.php?topic=2166510.0>

II. Frequently Asked Questions (FAQ) & Guides

FAQ: https://docs.google.com/document/d/12y7alZZ1Oj_JS5U43jTwWL9u-CVJAG21FhukSby6uk4

Guides (Mining, Pools, Wallets, etc.): <http://bitcoinzguiding.ovh/>

TOR Node Guide: <https://btcz.rocks/documents/tutorial-tor-node.pdf>

III. Exchanges

Stocks.Exchange: <https://stocks.exchange/trade/BTCZ/BTC>

TradeSatoshi: https://tradesatoshi.com/Exchange?market=BTCZ_BTC

C-Cex: <https://c-cex.com/?p=btcz-btc>

IV. Social Media / Chats / Forum

Discord - <https://discordapp.com/invite/u3dkbFs>

Facebook Page - <https://www.facebook.com/BTCZCommunity/>

Facebook Group - <https://www.facebook.com/groups/bitcoinz.community/>

Reddit - <https://www.reddit.com/r/BTCZCommunity/>

Rocket Chat - <https://bitcoinzcommunity.com/>

Slack - <http://slack.bitcoinz.global>

Telegram - <https://t.me/joinchat/CDzlaRGMvBm4P2Z76sNclQ>



BitcoinZ + zkSNARKs

In Decentralization We Trust

Twitter - <https://twitter.com/BitcoinZTeam>

WhatsApp Brazil Community: <https://chat.whatsapp.com/LV2frpF0LfPIBEICGRvoWe>

V. Explorers

<https://explorer.bitcoinz.global>

<https://explorer.btcz.rocks>

<https://explorer.bitcoinz.site>

<https://btczexplorer.blockhub.info>

<https://bitcoinz.ph>

VI. GitHub

<https://github.com/bitcoinz-pod/bitcoinz>

<https://github.com/bitcoinz-sites>

<https://github.com/bitcoinz-wallets>

<https://github.com/cryptorex/bitcoinz-explorer>

<https://github.com/anthony19114/>

VII. Wallets

Android (Google Play Store): <https://play.google.com/store/apps/details?id=com.btczcom.btcz>

Cold Wallet: <https://github.com/bitcoinz-pod/zgenerate/releases>

Linux CLI: <https://github.com/bitcoinz-pod/bitcoinz/releases>

Linux GUI: <https://github.com/bitcoinz-wallets/bitcoinz-copay-wallet/releases>

MacOS GUI: <https://github.com/bitcoinz-wallets/bitcoinz-copay-wallet/releases>

Mini Cold Wallet: <https://github.com/bitcoinz-pod/bitcoinz-mini/releases>

Web Wallet: <https://www.mybitcoinzwallet.com> OR <https://mybtczwallet.org>

Web Wallet Source: <https://github.com/anthony19114/mybitcoinzwallet>

Windows CLI: <https://github.com/bitcoinz-pod/bitcoinz-win/releases>

Windows GUI: <https://github.com/bitcoinz-pod/bitcoinz-windows-wallet/releases>



BitcoinZ + zkSNARKs

In Decentralization We Trust

VIII. Sites / Services

Donation Tracking: <https://btcz.fund>

Project Tracking & Proposal Submittal: <https://info.btcz.rocks>

Web: <https://btcz.rocks> OR <https://www.bitcoinz.global> OR <https://www.bitcoinz.site>

CoinMarketCap: <https://coinmarketcap.com/currencies/bitcoinz>

WhatToMine: <https://whattomine.com/coins/207-btcz-equihash>

CryptoCompare: <https://www.cryptocompare.com/coins/btcz>

Crypto-Coinz: <https://www.crypto-coinz.net/crypto-currency-statistics/>

Proposals, Community Map, Voting, Community Chest Withdrawals

I. Proposal Criteria

Like a road map, the Community Map is a decentralized approach to implementing use cases for the BitcoinZ community project. The proposals shall abide by the criteria in the figure below. The circular representation is meant to indicate the criteria are perpetual and exist as one - no other component criteria outweighs the other.

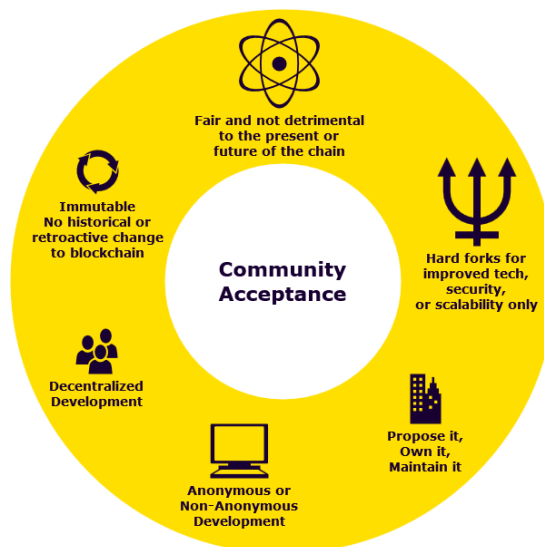


Figure 1 - Proposal Criteria for Community Acceptance



BitcoinZ + zkSNARKs In Decentralization We Trust

II. Core Community Map

The Core Community Map outlines components that do not require a proposal process to implement, but shall abide by the Proposal Criteria for Community Acceptance. However, modification of the Core Community Map components must follow the proposal process outlined in Part III. Zcash core adoptions are not required to pass proposal criteria scrutiny, but their adoption must not cause historical or retroactive changes to the BTCZ blockchain.

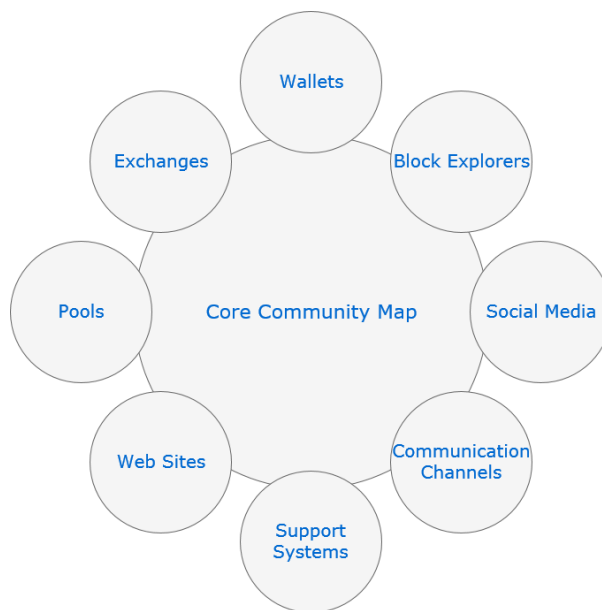


Figure 2 - Core Community Map (See 'Community Questions' below for definitions)

III. Proposal Systems / Voting (Tier 1, Tier2, Tier 3)

A. Core Use Cases (Tier 1)

Keeping true to our belief in community development, and our “fairness core” philosophy, a proposal to add functionality outside the Core Community Map components, such as use cases for the BitcoinZ blockchain, must garner community acceptance by meeting the Proposal Criteria for Community Acceptance (Figure 1). A core use case or, Tier 1 use case, is one that



BitcoinZ + zkSNARKs In Decentralization We Trust

utilizes the BitcoinZ blockchain to deliver a service, other than the transfer of value. Additionally, the proposal must be posted as an Issue on the official [GitHub](#) for BitcoinZ as a BitcoinZ Improvement Proposal (BTCZIP) and a 7 day Request For Comment (RFC) must follow.

After the expiration of 7 days from the Github BTCZIP Request for Comment phase, a vote for community acceptance must be initiated. The vote for a Tier 1 use case must last 7 days and is intended to allow time for the proposal to be analyzed and subjected to the Proposal Criteria on Community Acceptance (Figure 1), to ensure its full compliance.

The voting platform utilized for this process must be one which can reasonably be expected to produce an accurate result, for example one that cannot reasonably be manipulated to achieve a specific result. While respecting the aforementioned, there should not be any additional restriction on the choice of voting platform. A vote of acceptance shall require 55% of the vote above any alternative proposals on the voting ballot.

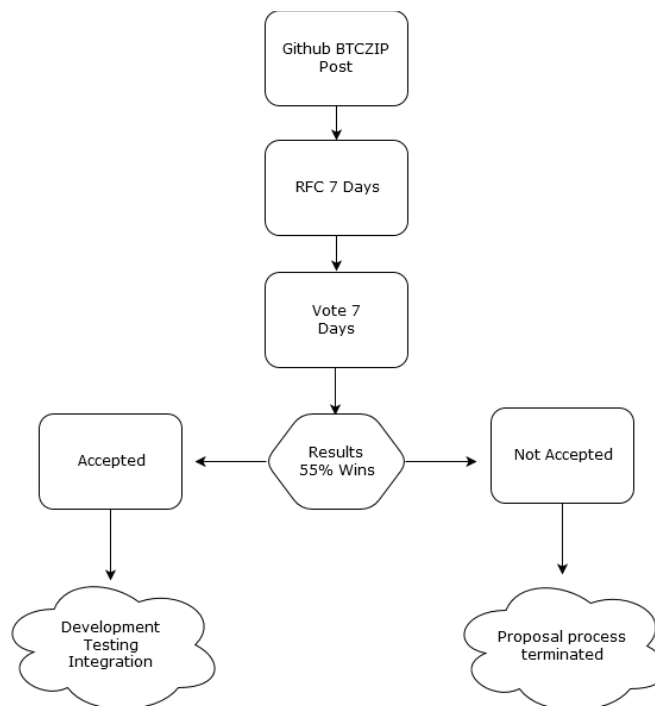


Figure 3 - Voting Proposal Process



BitcoinZ + zkSNARKs In Decentralization We Trust

Example of Tier 1 Proposal voting process:

- Improvement proposal is posted on official [GitHub](#) in the 'Issues' tab, using the next available BTCZIP-# (ex. BTCZIP-1, BTCZIP-2, BTCZIP-3, etc.).
- The community is encouraged to comment (Request for Comment) on the proposal in the comments section of the posted proposal. This must continue for 45 days from the date of the BTCZIP-# Issue post.
- After 45 days from the date of the BTCZIP-# Issue post, the community must vote on acceptance of the proposal.
- Voting should last 14 days from the date the voting was first posted. The voting platform can be any the proposer chooses, but should be a fair system. One that, for example, eliminates duplicates via IP checking, cookies, or whatever else exists in our abundant technology world and that has been proven to produce reasonably fair results.
- After voting has ended – the next steps are predicated by the results (55% wins) – 1) Development / Testing / Integration by the proposal team or 2) Proposal process terminated, proposal fails, and is effectively denied.

True Story: The project had a vote for a secondary logo, and the proposer used strawpoll.com to initiate a vote, another used Google forms. These are examples, but this Community Paper purposely does not directly endorse a particular platform as to not confine any proposer to a voting platform, in the interest of fairness and freedom of the BitcoinZ community.



BitcoinZ + zkSNARKs
In Decentralization We Trust

B. Other Use Cases (Tier 2)

A Tier 2 use case, or 'other use case' is one that utilizes the BitcoinZ blockchain's value transfer, i.e. the BTCZ coin value. The most relevant use cases that fall under Tier 2 are costs associated with (but not limited to):

- *Marketing*
- *PR & Media*
- *Campaigns*
- *Contests*
- *Sponsorships*
- *Infrastructure*
- *Exchanges*

Although the list is not exhaustive, other categories can be considered that are directly connected to the progression of BitcoinZ.

A Tier 2 proposal must be submitted on the BitcoinZ Info Bulletin by visiting <https://info.btcz.rocks> and clicking the 'Submit New Proposal' button. Extensive details are encouraged, as the proposal will be posted on the 'Proposal' board and voting for a period of 7 days from the date of posting will commence.

The voting platform utilized for this process must be one which can reasonably be expected to produce an accurate result, for example one that cannot reasonably be manipulated to achieve a specific result. While respecting the aforementioned, there should not be any additional restriction on the choice of voting platform. A vote of acceptance for a Tier 2 use case shall require 70% of the vote above any alternative proposals on the voting ballot.



BitcoinZ + zkSNARKs In Decentralization We Trust

Example of Tier 2 Proposal voting process:

- Tier 2 proposal is submitted on the BitcoinZ Info Bulletin by visiting <https://info.btcz.rocks> and clicking the 'Submit New Proposal' button.
- If additional details are required, a member from the BitcoinZ community team will reach out to you to gather the details.
- A proposal is written by a member from the BitcoinZ community team that includes details received/gathered and the budget amount sought.
- The proposal, along with a voting link, is posted on the Proposal board at <https://info.btcz.rocks>
- The proposal is announced via BitcoinZ communication channels and a vote commences for 7 days from the date of posting of the proposal to the Proposal board.
- If vote passes (70% in favor), the allocated funds are transferred in full, or in phases, depending on the circumstances and persons involved.

C. Exigent Circumstances / Re-allocation of voted funds (Tier 3)

There may be a need to allocate funding for certain emergency situations, or where a bill for a component of our infrastructure is required. These situations will be decided by the BitcoinZ team members and funds will be withdrawn if, and only if, they are for a necessary and reasonable amount, and not excessive.

Additionally, if voted funds are not exhausted or expired from use, we may re-allocate the unused, but approved fund amount, for a substantially similar proposal or campaign.



BitcoinZ + zkSNARKs In Decentralization We Trust

Decentralized Techniques

In furtherance of the fairness core formula, methods to continue the decentralized nature are strongly encouraged. Innovative methods of decentralization should always be researched to keep the integrity and principal vision of “a coin for all”.

The following Core Decentralization Techniques / Specifications have successfully been injected into the BitcoinZ community coin. There are no limits to discovery of new techniques, in accordance with the Proposal Criteria of Community Acceptance (Figure 1).

- A. 21 billion coins as total supply to enable every person on the planet to own at least one (1) BTCZ
- B. Equihash PoW algorithm to enable mining with commodity hardware, thereby reducing the barrier to entry for mining.
- C. Decentralized development by volunteers with no geographical boundaries. Everyone can, and is encouraged to participate and contribute to the project, to further progress BitcoinZ as a gift to the world.
- D. Fair start of the coin by posting in public forum, offering the opportunity to all. No pre-mine, no development fund, all coins to be mined by the community.

Community Questions

Q. How can I help keep the decentralized vision?

A. There are endless opportunities to support the community vision of decentralization, including, but not limited to:



BitcoinZ + zkSNARKs In Decentralization We Trust

1.) Submitting requests to exchanges for listing using official channels, social media, email, forum posts, etc. Exchanges rely on demand for a market to profit, let your interest be heard.

2.) Develop wallets for different platforms or operating systems, or contribute to official Github repositories in furtherance of existing developments. Submit requests to multi-wallet mobile device services.

3.) Maintain a block explorer, or two. The BitcoinZ network will always need a window into the movement of fair wealth across the chain. The pulse of BitcoinZ thrives and depends on the visibility and integrity of the blockchain, keep the pulse healthy.

4.) Power of social media is probably self explanatory. However, here are some ideas. Start a Facebook group, make a sub-Reddit, create a Steem-it post, create a YouTube video, reach out to YouTubers. The possibilities are endless in this area. These efforts create everlasting positive impacts.

5.) Communication channels, whether it's Facebook, Slack, Telegram, Discord, Rocket.Chat, or any other collaborative environment. Request a BitcoinZ channel to be listed in an already existing communication channel. Community coin means communication should be easily accessible by everyone and everywhere in the cryptocurrency ecosystem.

6.) Support systems are running wallet nodes, [dns seeders for node discovery](#), or peer reviewed and open sourced web wallet nodes. Are you a programmer? Contribute at your leisure. If you can't program, no problem, are you versed in linux command line or understand the way windows wallets work? Write a guide! Learning, teaching, and the sharing of knowledge from within, creates an indestructible community foundation. People learn and contribute differently, have different skills-sets, and ideas. This gives the project a diverse scope and perspective - with endless possibilities.



BitcoinZ + zkSNARKs In Decentralization We Trust

7.) There is no central website, in fact we encourage many sites to be created. Each community member possesses a different perspective, let it be known. Discrepancies can always be addressed with the community. The power of decentralization comes with the power to destroy fear, uncertainty, and doubt.

8.) Mining pools are the heart of the growth for BitcoinZ, as many pools as possible are encouraged to spread hashing power and create redundancy of the BitcoinZ blockchain. Don't own a pool? Like to learn? Start one. Community decentralization is to team up and improve together. You could also always submit to an existing pool and request BitcoinZ be added.

Technical Definitions

BitcoinZ Daemon / Wallet - program that runs on a Linux, Windows, macOS, or mobile device that communicates with the BTCZ blockchain, allowing sending and receiving BTCZ coins. The program contains your BTCZ addresses and can also export your address's 'private key' allowing import into another BitcoinZ daemon or wallet.

Block Height - the number of blocks preceding a particular block on a block chain. For example, the genesis block has a height of zero because zero blocks preceded it. [Read More](#)

Blockchain Explorer - a program or web site that lets users search and navigate a block chain. Uses include checking address balances, tracking coin transactions, getting the number of blocks.

[Read More](#)

DNS Seeder - a crawler for the BitcoinZ network, which exposes a list of reliable nodes via a built-in DNS server. The nodes list is used by wallets to connect to the network and synchronize the blockchain.

[How-To](#)

GitHub - GitHub is a web-based Git or version control repository and Internet hosting service. It is mostly used for code. It offers all of the distributed version control and source code



BitcoinZ + zkSNARKs In Decentralization We Trust

management (SCM) functionality of Git as well as adding its own features. The BitcoinZ core source code is on GitHub.

[Read More](#)

Mining Pools - the pooling of resources by miners, who share their processing power over a network, to split the reward equally, according to the amount of work they contributed to solving a block. A "share" is awarded to members of the mining pool who present a valid proof-of-work that their miner solved.

[Read More](#)

Proof of Work (PoW) - a proof of work is a piece of data which is difficult (costly, time-consuming) to produce but easy for others to verify and which satisfies certain requirements. Producing a proof of work can be a random process with low probability so that a lot of trial and error is required on average before a valid proof of work is generated. BitcoinZ uses Equihash as its PoW algorithm.

[Read More](#)

Virtual Private Server - a virtual machine sold as a service by an Internet hosting service. A VPS runs its own copy of an operating system (OS), and customers may have superuser-level access to that operating system instance, so they can install almost any software that runs on that OS. It shares hardware resources with other users running their own instance of OS. You can run wallets 24/7 on a remote system such as a VPS.

[Read More](#)

zk-SNARKs – Zero-knowledge Succinct Non-Interactive Argument of Knowledge. They allow one party to prove to another that a statement is true, without revealing any information beyond the validity of the statement itself. In BitcoinZ, these are the transactions that occur when using z-addresses.

[Read More](#)