Vertical Cryptocurrency Whitepaper

Authors:
Neithender
Anonymity
Yo
Zero
Undead
Suds

The Vertical Core Team
April 2018

The Vertical team confirms that the ideas and information presented in this whitepaper are our own. Information derived from outside sources has been appropriately attributed.

Contents

Brief Overview

Vertical (VTL) believes that privacy should be simple, fast, and accessible to everyone. That's why we are introducing this project to the marketplace. Vertical is a mineable coin with the Zerocoin protocol implemented from day one. Too many projects market with amazing future features and rarely deliver. Vertical's promise is simple and straightforward: our goal is to become a widely accepted privacy coin by staying focused on organic growth and community development. In keeping with this focus, Vertical also offers masternode technology immediately and masternode rewards.

Acknowledgements

The Vertical Team is grateful to Satoshi Nakamoto, the Bitcoin Core Developers, and the Zcoin development team for their work and plans to contribute to the open source cryptocurrency community via the Vertical project. Thanks to Zawy for his work on LWMA difficulty algorithm.

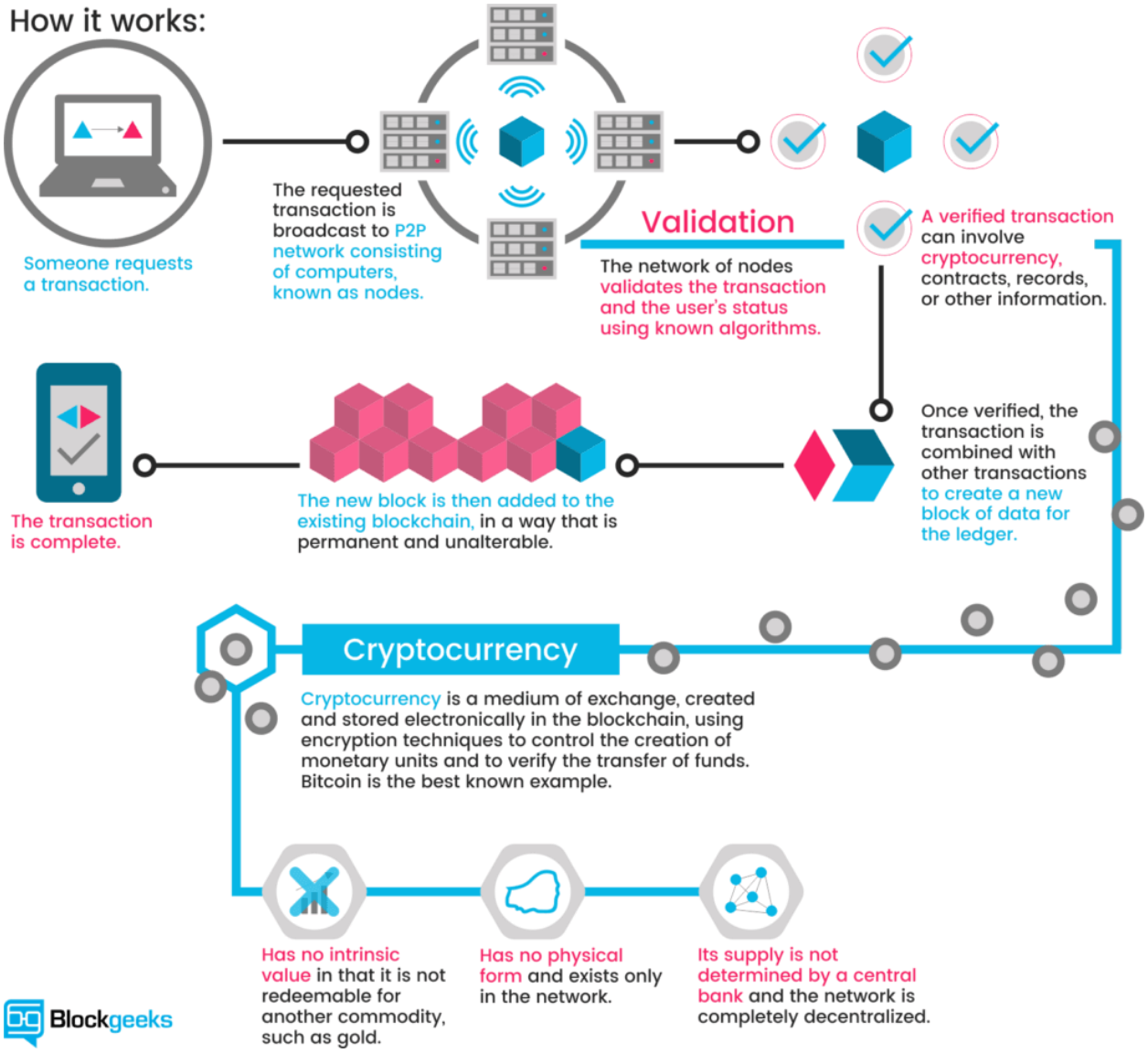
What is Cryptocurrency

Introduction

Cryptocurrencies are a speculative digital asset class that consist of thousands of different coins backed by "cryptography, networking and open-source software." (Greenberg, 2011). Cryptocurrencies may represent business concepts, physical objects, ideologies and they can serve as units of value. Many currencies rely upon the blockchain technology that Satoshi Nakamoto introduced in the seminal paper, *Bitcoin: A Peer-to-Peer Electronic Cash System* which brought about much of the modern cryptocurrency era.

Blocks and Blockchains

Many modern cryptocurrencies rely upon the blockchain structure to, "record a public history of transactions that quickly becomes computationally impractical for an attacker to change" (Nakamoto, 2008). Individual transactions, which represent the transfer of digital signatures from one owner to another, are validated by the network and bundled together. As individual transactions are aggregated into groups of transactions or "blocks" they are then appended onto a progressive chain of bundled transactions, called the blockchain. Each block in the blockchain is secured by complex cryptographic functions completed by users securing the network in what is called proof-of-work mining. This infographic, from Blockgeeks, may help illustrate blockchain technology for some readers:



Source: https://blockgeeks.com/wp-content/uploads/2016/11/image-1-1024x936.png

The Need for Privacy

Blockchains are extremely useful tools to create publicly verifiable ledgers of coin transfers and transactions. Fully-transparent ledgers can be analyzed by any party which may lead to security or legal risks for network participants. For instance, if a user sent Bitcoin into the Silk Road in 2012 and then later used that same address to send Bitcoin into an exchange, it would be possible for authorities to link the Silk Road transaction back to that specific user via the blockchain. The same goes for a user who elected to contribute to Wikileaks via Bitcoin, that transaction would be publicly searchable forever.

What is Vertical?

The Coin

Vertical is a cryptocurrency that is focused on privacy and utility. The coin is a fast, private and secure payment option with a decentralized supply. Vertical is forked from Zcoin and brings a number of meaningful features with it. Vertical employs the Zerocoin protocol that was implemented by the Zcash team and employs the zNode masternode technology first released by the Zcoin team. Vertical is a proof-of-work and masternode hybrid coin, meaning that individuals can earn coins by operating masternodes or mining to support the network.

Why Vertical?

We acknowledge that there are many "privacy" coins that offer masternodes in the marketplace. It seems like a few pop up within the cryptocurrency sphere every week. Many of them feature massive premines, favor ASICs, or are vulnerable to network abuse via purchased hash power. Dozens offer "private" transactions through obfuscation and tout instant transactions that exchanges don't seem to honor. They promise the Zerocoin Protocol as a roadmap item but rarely deliver.

Vertical is different. Vertical launches with Zerocoin enabled. Vertical's block time and number of confirmations required makes for quick transactions. The Lyra2z algorithm provides for strong ASIC resistance and buying Lyra2z hashpower on the secondary market is not as easy as other algorithm candidates we looked at.

Vertical is for Everyone

Vertical is designed in a way that encourages broad, fair, distribution. We have worked hard to engineer a project that will provide the most people the most access to our coin. This is for a simple reason: we need everyone to utilize Vertical if we are going to achieve our goal of becoming a mainstream, transactable, privacy coin. Many of our roadmap items are related to expanding the Vertical footprint from an economic and access perspective. We need a large community of engaged miners, traders, masternode operators, and (ultimately) businesses to decentralize supply and encourage actual use of the coin.

The Vertical Blockchain

Coin Specifications

Block Size	2 MB
Proof-of-Work Algorithm	Lyra2z
Block Time	2 minutes
PoW Block Reward	32 VTL
Coin Maturity:	50
Difficulty Retargeting	The LWMA Algorithm
Maximum Supply	35 million (243,800 Premine)
SegWit	Yes
Masternodes	Enabled (vNodes)

*When 35 million VTL have been minted, the blockchain will go into indefinite PoW of 1 VTL per block reward. Then after a certain period of time we will decide on a full 100% Masternode ecosystem or hybrid of Masternode and PoS.

Masternode Details

Vertical features the innovative Masternode system initially developed by Darkcoin. We employ this system in order to stabilize supply, incentivize holding, and to provide a rate of return for the coin from an economic perspective. Masternode details are as follows:

Masternode Collateral	3750
Masternode Payment Start	~Day 2, Block 720
Masternode Subsidy	25% of Block Reward 8 VTL

The LWMA Difficulty Algorithm

VRT employs the LWMA difficulty algorithm to react to changes in hashing power. The purpose of a difficulty algorithm is to maintain block times regardless of hash power over a period of time so that the network has a steady rate that coins are released. The LWMA difficulty algorithm does this by giving more weight to the most recent solve times and is designed for small coin protection against timestamp manipulation and hash attacks. This will help mitigate problems when there are changes in hashpower by changing the difficulty every set number of blocks.

The Lyra2z Hashing Algorithm

VTL features the Lyra2z hashing function for Proof-of-Work calculations. We selected Lyra2z because it is ASIC resistant and relatively underutilized within the cryptocurrency space. The Lyra2z algorithm will help VTL to decentralize supply due to relative scarcity of purchasable hashing power. Lyra2z is relatively energy efficient and is supported by AMD and Nvidia, which will broaden access to the coin and helps our goal of decentralizing supply.

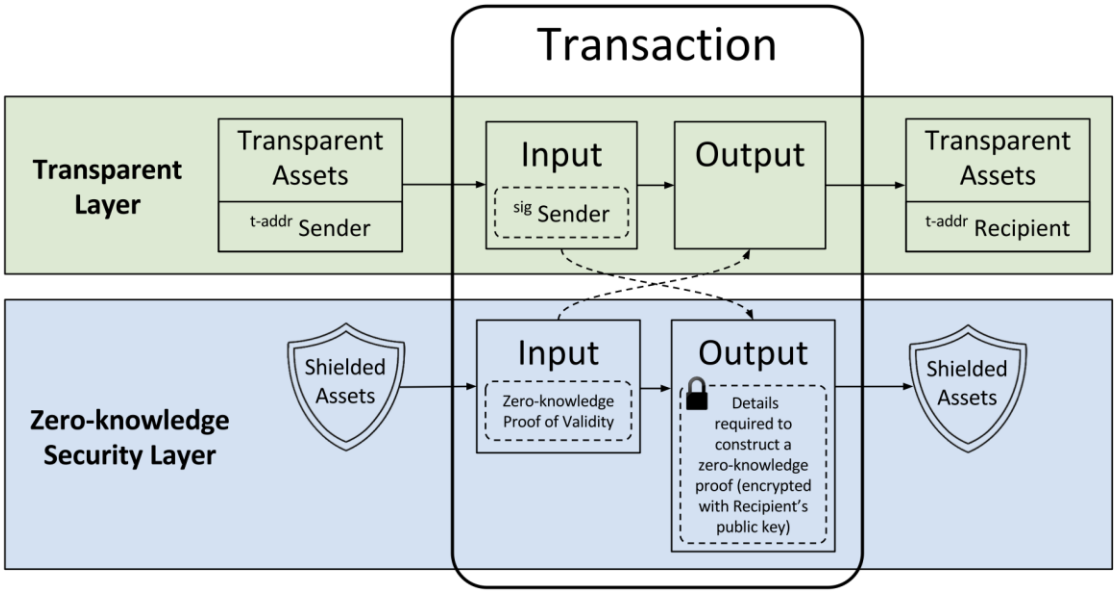
Vertical Features

The "Zerocoin" Protocol

Many users describe the protocol used in Zcash as "Zerocoin", even though there are material differences. For the sake of simplicity, we refer to the Zerocash trusted setup as "Zerocoin" in this document. The Zerocoin Protocol is a privacy solution first described in 2013 by Ian Miers, Christina Garman, Matthew Green and Aviel Rubin in their whitepaper, *Zerocoin: Anonymous Distributed E-Cash from Bitcoin.* This seminal work began a larger movement toward privacy coins and even precedes Saberhagen's October, 2013 publication on the CryptoNote v 2.0 system that Monero employs. Following in the Zerocoin and CryptoNote v2.0 Footsteps, Eli Ben-Sasson, et. al. (2014) described the Zerocash system which ultimately spawned Zcash, the trusted setup, and all Zcash forks (including: Zcoin, Zclassic, Komodo, ZEN, ZOI, Vertical, and many others).

The Zerocoin protocol employs zk-SNARKS, which describes a way to prove private key / coin control to other users without providing them with any additional information. Ben-Sasson, et. al. (2014) describes a scenario where Alice wants to verify ownership of coins to Bob. With Bitcoin, she could sign a message using her private key to the coins to prove ownership, however, this would provide Bob with knowledge (he would know which coins Alice controlled, and could track them). With zk-SNARKS, Alice could prove ownership of ANY 30 coins to Bob, thus providing him with no additional information.

Practically, this means that Vertical users will be able to enjoy private transactions. The Zerocoin protocol relies on minting and pouring coins for privacy. Minting is the conversion of a VRT coin into a zVTL. Pouring is the conversion of a zVTL into a VTL. zVTL can be transacted in complete privacy, where VTL transactions are not private. The following illustration may help explain how VTL inputs interact with zVTL for privacy purposes. Everything that happens within the Zero-knowledge Security Layer is shielded from outsider observation.



Source: https://z.cash/images/zcash-transaction.png

Masternodes

Masternodes are network validators that help to secure cryptocurrency systems. They are the validators for Zerocoin transactions and enable “normal nodes to have low requirements” (Zcoin, 2017). Vertical nodes are incentivized and provide validation services for private transactions, but have no visibility to those transactions other than providing mathematical proof that a zVTL mint took place for a given transaction.

Masternodes also serve economic functions for any cryptocurrency ecosystem. Fundamentally, Masternodes reduce circulating supply by providing users an incentive to temporarily lock their coins. Providing a rate of return for coin holding and reducing a coin’s circulating supply means that price is more responsive to demand and demand may increase due to the coin’s rate of return. This phenomenon is very common in Masternode coins and often results in price equilibrium as users attempt to accumulate larger quantities of the coin to operate more masternodes for passive returns.

The Vertical Roadmap

Market Adoption

Vertical is a coin that will rely on broad market adoption and penetration for success. This is not a unique requirement for Vertical and - in fact- every cryptocurrency has a similar requirement. Projects that have durable footprints and long-term viability rely upon market adoption. The Vertical team is going to invest considerable time and effort into driving broad decentralization of Vertical's supply and adoption of the coin into regular use. Cryptocurrency is still in its infancy and simple, fast, private, and accessible coins are the future of the space.

Commerce Integration

Adoption is one part of the broader picture when considering the long-term viability of a project. Adoption also means users will expect that their coins will have purchasing power. This is why the Vertical team will focus heavily on integration into existing commerce platforms as well. After our initial exchange listings and organic price discovery, the Vertical team will begin reaching out to e-Commerce integrators (like WooCommerce and Coinpayments.net) to expand the economic reach of the Vertical project,

Merkle Tree Proof (MTP) Proof-of-Work System

The Lyra2z algorithm is a useful solution to coin distribution in the short term, but it is still susceptible to attack from hashpower aggregators and ASIC development should a third party decide to undertake either effort. MTP PoW is an ideal solution to confront the threat of centralization and Vertical is on the front-lines of this fight. MTP is largely focused on the notion of "egalitarian computing" (Biryukov & Khovratovich, 2016) as a way to combine "arbitrary computation with a memory-hard function to enhance security against off-line adversaries equipped with powerful tools" like ASICs. MTP works by establishing "the same price/cost for a single computation unit on all platforms" (Zcoin.io, 2016).

MTP may require computational effort and be memory demanding to create solutions, but those solutions are easily verifiable with lightweight hardware. Due to the significant workload that MTP hashing requires, Biryukov & Khovratovich also suggest that Botnets operating MTP hashing would likely be detected by end users who noticed their computers were running slower.

The end-goal of the Merkle Tree Proof algorithm is a broad and healthy distribution of VTL across many users. MTP furthers this goal by allowing ordinary users to be computationally competitive regardless of the size or specialization of their mining hardware. Contrast this with coins, like Bitcoin, where ordinary users have - essentially - no contribution to make to securing the network due to massive ASIC farms.

MTP integration will be a major step forward for Vertical and we are excited to be one of the few cryptocurrency projects focused on bringing egalitarian computing forward as a primary focus.

Block Reward Adjustments

Vertical is focused on a broad, decentralized, supply that will support our goals of becoming a durable and functional cryptocurrency. Over time this means we may need to adjust block rewards and the reward split between our masternode operators and miners. At current, the split is 25% to masternodes and 75% to miners. Once MTP is implemented, there may be some need to re-adjust the block reward scheme to ensure our focus on decentralized supply is being realized throughout our coin's economy.

Closing Remarks

Vertical - ready for today!

Vertical is a functional privacy coin with masternodes to encourage economic participation. The coin features important privacy functionality on day one and is resistant to purchased hashpower. Vertical is a long-term project with the goal of becoming a broadly distributed transaction coin. We are excited to invite you to join us on our mission of delivering private, fast and secure transactions to the world!

References

Ben-Sasson, E., Chiesa, A., Garman, C. Green, M., Miers, I., Tromer, E., Virza, M.. (2014). Zerocash: Decentralized Anonymous Payments from Bitcoin (Extended Version). Retrieved 2/2/2018 from http://zerocash-project.org/media/pdf/zerocash-extended-20140518.pdf

Biryukov, A., & Khovratovich, D.. (2016). Egalitarian Computing. Retrieved on 2/3/2018 from https://zcoin.io/wp-content/uploads/2016/11/mtpwhitepaper.pdf

Bohannon, J. (2016). Why criminals can't hide behing Bitcoin. Retrieved 2/1/2018 from http://www.sciencemag.org/news/2016/03/wh y-criminals-cant-hide-behind-bitcoin

Gavigan, J. (2017). A high-level skeleton diagram of a Zcash transaction. Retrieved on 2/3/2018 from https://z.cash/images/zcash-trans action.png

Greenberg, A. (2011). Crypto Currency. Retrieved on 2/1/2018 from https://web.archive.org/web/20140831001109/http://www.forbes.com/forbes/2011/0509/technology-psilocybin-bitcoins-gavin-andresen-crypto-currency.html

Miers, I. Garman, C. Green, M. Rubin, A. (2013). Zerocoin: Anonymous Distributed E-Cash from Bitcoin. Retrieved on 2/2/2018 from http://spar.isi.jhu.edu/~mgreen/ZerocoinOakland.pdf

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Retrieved 2/1/2018 from http://nakamotoinstitute.org/bitcoin/

Rosic, A. (2017.) What is Cryptocurrency: Everything You Need to Know [Ultimate Guide]. Retrieved 2/1/2018 from https://blockgeeks .com/wp-content/uploads/2016/11/ima ge-1-102 4x936.png

Saberhagen, N. (2013). CryptoNote v 2.0. Retrieved 2/2/2018 from https://github.com/monero-project/research-lab/blob/master/whitepaper/whitepaper.pdf

Yap, R. (2017) Zcoin Development Update: Znodes and Scaling Zerocoin. Retrieved 2/3/2018 from https://zcoin.io/zcoin-development- update-znodes-and-scaling-zerocoin/

Yap, R. (2016). What is MTP (Merkle Tree Proof) and why is it important to Zcoin. Retrieved 2/3/2018 from https://zcoin.io/what-is-mt p-merkle-tree-proof-and-why-it-is-important-to-zcoin/