"The community project for miners, gamers and traders"

zBucks Whitepaper v.1

## Abstract

zBucks embodies an anonymous, innovative and decentralised cryptic network allowing users to participate in numerous services provided by the zBucks community while providing a range of applications specifically designed for miners, gamers and traders.

**July 2018**

# Contents

Section 1

# Motivation

"Blockchain technology" remains listed in the top ten disruptive technologies that influence change in the way enterprises and society do business. Individuals and organizations across a wide range of sectors are already experimenting with blockchain technology to establish networks, improve transparency, increase efficiencies and reduce costs. Industrial applications will expand, encompassing the obvious financial uses as well as innovative solutions for energy, trade, marketing, healthcare, security, communication and many more.
The disruptive technology has not been without its own critics and in some ways has been introduced poorly to society which has created opportunities for sceptics to criticize the ultimate objectives of the technology. The hype and excitement around cryptocurrencies exists but even more is the ignorance and lack of understanding by the majority of people.
zBucks will pronounce differently to society.

*"If you are not willing to risk the unusual, you will have to settle for the ordinary" Jim Rohn*

zBucks exists primarily as a cryptocurrency, a simple peer to peer digital cash system. Us, like many others, are working towards bridging the economic gap between the wealthy and those less fortunate regardless of where in the world you may reside. This industry is pioneering, thought-provoking and somewhat vastly unpredictable - but this is to be expected – nonetheless the Economists, Bankers, Investment Brokers and Media resent the value placed along with the technology. Without value at its core the technology is meaningless.
We firmly believe the youth of today and generations of tomorrow will embrace, improve upon and implement cryptocurrencies in their daily lives and in our opinion, they'll be better off for it. Investing in their children's education and their own retirement if sensibly planned, ought to be rewarded.

Section 2

# Introduction

zBucks is a decentralized cryptocurrency embedded with privacy and alternative applications. Commonly, users who are entering the crypto space are miners, gamers and traders. zBucks will bridge the gap between these three groups to create a growing community.
We plan to achieve this through zNodes. A gamer employing our zNode will get Paid-to-Play, which will facilitate in decentralizing our network. There are currently hundreds of millions of active gamers in the world, spending billions of dollars per year. This population will be incentivized to run a zNode while playing games, not only in aid of growing and assisting our decentralized network, but earning them a piece of the currency in return. Furthermore, our Trade Manager will amass data, along with graph tools, currency calculations, conversions, world map timestamps and social media information for multifaceted fundamental analysis.

Lastly, the zBucks Mining Manager will contain each distinct mining algorithm with a growing list of mining pools, for operators to effortlessly start mining. The development team carries the priority of smoothing and bettering the experience of everyday Cryptocurrency users and consumers. We align with a transparent and decentralized system which favors no mining or node operator by virtual of size. The market forces that currently drive the world's economics based on the race to the bottom and market size create discrepancies that ignore the needs of the minority.

Section 3

# Applications

## Paid to Play zNodes

Our plan is to grow and implement the largest decentralised network globally, by strongly supporting our miners while introducing and incentivizing the international gaming community with our Paid-to-Play model. zBucks (ZBK) intends to take a different approach to Masternodes for second layer solutions by utilising zNodes bootstrapped to gaming profiles.
Gamers can download and activate the zNode software and earn ZBK while playing based on their hours. These zNodes will need to be activated and fully operational before launching any game or application ensuring the security and expansion of the network.

## Operating zNodes

zNode operators are required to stake a set amount of zBucks while gaming to ensure they obtain and control a fully operational node. In simpler terms, the user will have a full copy of the blockchain open while gaming. This verifies the transaction, preventing access to blockchain technology via censorship that gives zBucks blockchain network resilience. The primary requirement to run a zNode on the zBucks network hasn't been announced yet. However, this is known as the collateral, and if spent will interrupt operation of the zNode. The second requirement is the actual software running the zBucks zNode, which is currently being developed by the team.

## Technical Specifications

With most Masternode cryptocurrencies, the hardware requirements often seems a bit expensive - the operator would usually end up having to pay more for the VPS than what his/her return would be. Most gamers are geared with high end computing hardware, however, we still plan to make the technology lightweight and less resource intensive for uninterrupted gameplay. Nonetheless, there are distinctive hardware specifications required.

## Trade Manager

The zBucks Trade Manager Application is designed to help users manage and trade cryptocurrencies. It makes possible the ability to create mock trades and associate them with an array of user created strategies. These tools will have various technical indicators intended at improving your trading skills. The dashboard will provide your historical data as well as the analysis tools to manage your portfolio.

Key features:

- Aggregating live market data.
- Calculating indicators.
- Executing live orders.
- Simulating order execution.
- Calculating profit and risk metrics.
- Graphing the results in a web interface.
- Managing and importing historical market data.
- Simulating live markets using historical market data.
- Providing summaries of historical trades via a dashboard.
- Analysis tools for historical trades.

## Mining Manager

zBucks plans to implement an exclusive mining manager in the crypto sphere, with unique features such as a multi-algorithm and multi-platform programs, which will support NVIDIA, AMD, and CPU platforms. The zBucks Mining Manager is designed to allow miners to setup and go without having to worry about doing extensive research on what is the most profitable mining algorithm to use. Miners can compare block rewards against live coin data over specific times of the day, based on the average hash rate of a particular cryptocurrency. The intended design is for essential yet effective management.

**Pool Support**

We will include a section for mining pools within our Mining manager to ensure that all the applications a miner needs will be easily accessible from within our application. There will be a request system in which pool creators can add their pools to the manager for easy access amongst all miners.

**Remote Access**

Miners are not always monitoring their rigs. We believe mining setups and rigs require a lot of attention. In the zBucks mining manager we will include a remote feature that allows the user to gain remote access to ensure their rig is always functional, having the ability to change algorithms and mining pools externally.

| | |
|---|---|
| **JCE cryptonote** | CryptoDredge |
| **CCminer (any)** | Claymore XMR |
| **Ewbf** | Claymore Neoscrypt |
| **Nheqminer** | PhoenixMiner: Ethash |
| **sgminer (any)** | XMRig all |
| **Gatelessgate** | XMRstak all |
| **Z-Enemy** | Dstm Zcash: Equihash |
| **Bminer (Ethash, Dual, Equihash)** | CastXMR |
| **CPUminer-opt** | Nevermore-brian |
| **cpuminer-opt** | Claymore Equihash |
| **CPUminer** | Claymore Eth |

Table 1: Algorithms supported by the mining manager.

Section 4

# Design Overview

## Coin information

zBucks is passionately fashioned upon the CryptoNote algorithm and Monero foundation to allow for anonymous transactions. When mining zBucks blocks on the blockchain we use the CryptoNight-Heavy as the proof-of-work algorithm. zBucks can be mined efficiently with processor (CPU) power and (GPU) power. The proof-of-work mechanism to create zBucks Coins emphasizes the egalitarian philosophy of the product. We plan to stick to this model along with utilizing it's core philosophy with use of incentivized nodes targeted at gamers.

| zBucks Symbol | ZBK |
|---|---|
| zBucks Total Supply | 100 Million |
| zBucks Block Reward | 120 Seconds |
| Emission Speed Factor | 21 ($10^{-21}$) plus 0.5% annual compound growth |
| Hash algorithm | CryptoNight-Heavy |
| Elliptical curve | Curve25519 ECDH |
| P2P Port | 50501 |
| RPC Port | 50502 |
| Founders Reward | 5% |
| Miners Reward | 70% |
| zNode Operators | 25% |

Table 2: Basic coin information.

Division of each proof-of-work block reward and transaction fees between miners and other stakeholders:

- Miners will receive 70% of block rewards.
- Node operators will receive 25% of block rewards.
- Treasury will receive 5% of block rewards.

## CryptoNote

The CryptoNote algorithm is released under an open source license and has been adopted and incorporated into zBucks as it forms the basis for a solid, well tested cryptocurrency application making use of anonymous transactions, ring signatures, double spending protection, adaptive network limits, and egalitarian proof-of-work. It is the same technology used by some of the best currencies out there like Monero and Bytecoin.

## Ring Signatures

Ring signatures are a cryptographic digital signature used to prove that a transaction has occurred between parties without compromising the identity of the receiver or the sender. It is a sophisticated structure demanding several different public keys for verification. Conceptually, we have a group of individuals each with their own secret and public key. The statement proved by ring signatures is that the signer of a given message is a member of the group. The main distinction with the ordinary digital signature schemes is that the signer needs a single secret key, but a verifier cannot establish the exact identity of the signer. Therefore, if you encounter a ring signature with the public keys of Alice, Bob and Carol, you can only claim that one of these individuals was the signer, but the actual signer is not distinguishable among the group.

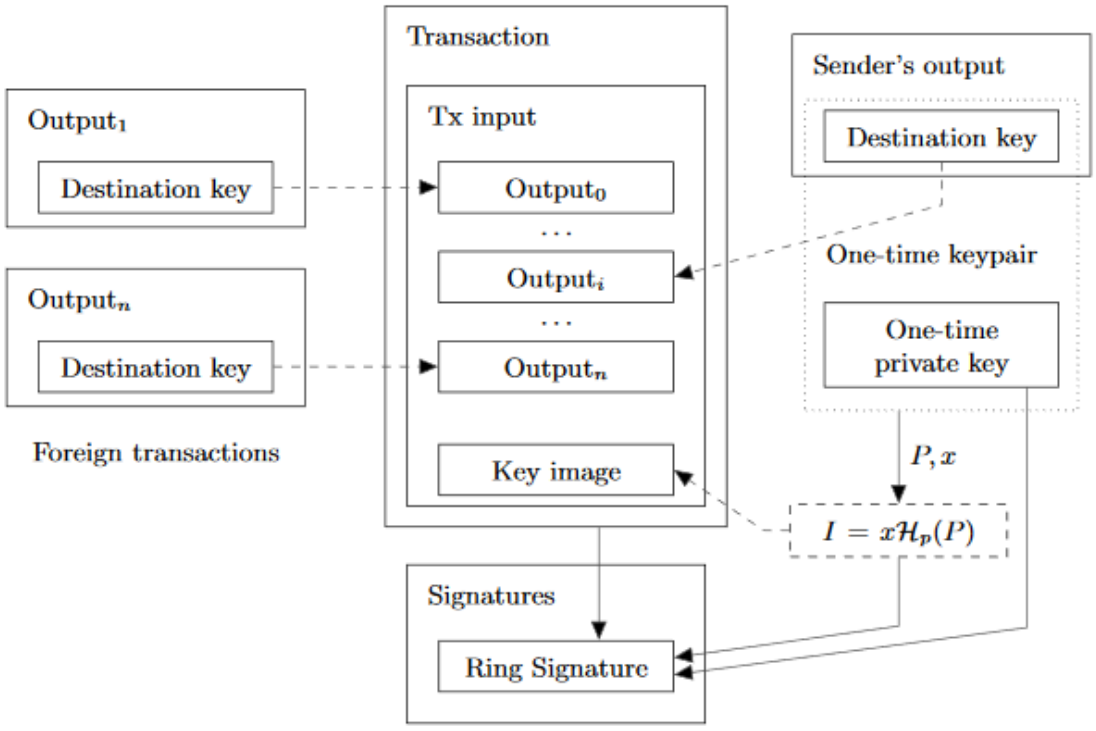


Table 3: zbucks uses a modified method for choosing ring signature mixins, to further obfuscate output distributions

## Stealth addresses

A stealth address is specialized technology used to protect the privacy of receivers of cryptocurrencies. They require the sender to create random, one-time address for every transaction on behalf of the recipient so that different payments made to the same payee are un-linkable. This technology originated from CryptoNote technology and has been implemented by Bitcoin and Altcoins over the years. For Bitcoin and Altcoins, stealth addresses must be explicitly supported by the sender's and recipient's wallets, but such support is implicit to CryptoNote wallets. zBucks has incorporated this technology as one of its key features ensuring the receivers privacy above all else.

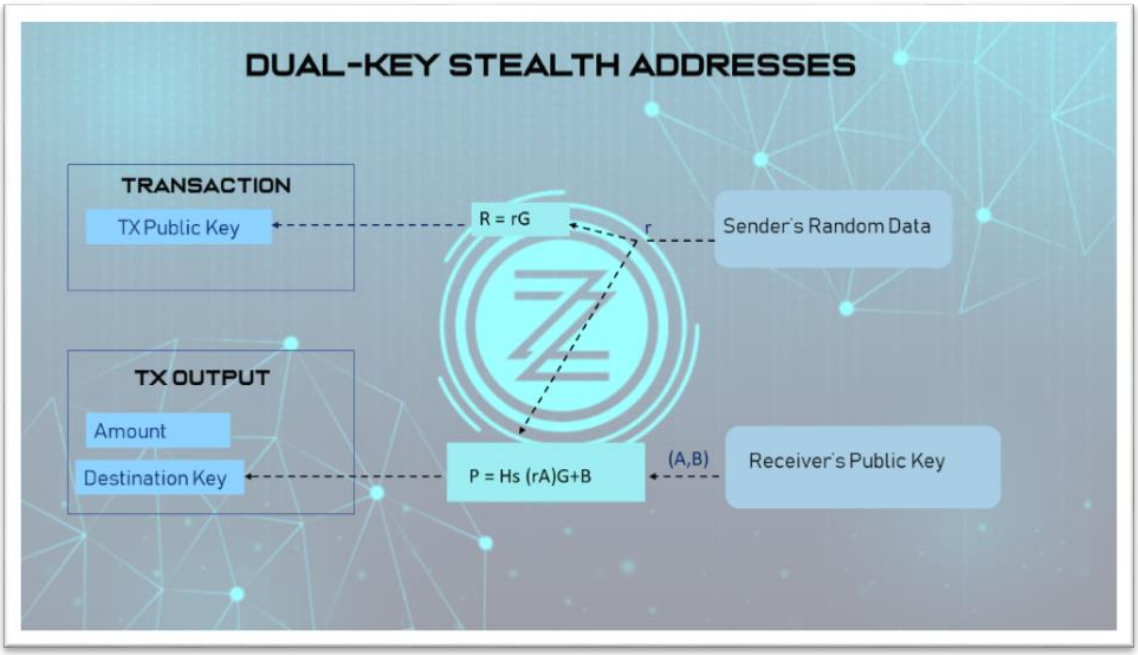


Table 4: Dual-key stealth addresses demonstrating private transactions.

## ASIC resistant hashing algorithm

An application-specific integrated circuit (abbreviated as ASIC) is an integrated circuit (IC) customized for a particular use, rather than intended for general-purpose use. In Bitcoin mining hardware, ASICs were the next step of development after CPUs, GPUs and FPGAs.

We see an increase in centralization and fail in privacy in the Bitcoin blockchain. The stereotypical mining rig is a string of Graphics Processing Units or GPUs, but ASIC units have almost entirely replaced the traditional rigs. Application-specific integrated circuit units are hardware systems created for one purpose only. In mining rigs, their hardware is specifically for mining cryptocurrency. This creates an incredibly powerful miner when compared with previous generations. Banks of these ASIC mining rigs allow companies to accrue massive amounts of specific cryptocurrencies.

This is damaging to the decentralization of the targeted blockchain. Bitmain's Antminer factories have had a detrimental effect on Bitcoin's decentralization. Further, their ability to kill mining rigs on a whim gives them an incredible amount of control over currencies once known for a lack of control. zBucks plans to stay ASIC resistant to reduce centralization by incentivizing mining with accessible hardware.

## Smooth Emission Curve

Many cryptocurrency coin reward structures include "Halvenings." In Bitcoin, these occur every four years, resulting in the block reward being split in half from its current value. When a halvening occurs, the network often sees a short, temporary drop in hashing power leaving the network vulnerable to a hostile take-over by a party that could bring a large amount of hashing power online and perform a 51% attack. To avert this, zBucks has incorporated the CryptoNote model, where a smooth emissions curve is followed. The block reward decreases slightly after a new block is created, precluding abrupt reductions and hash rate fluctuations.

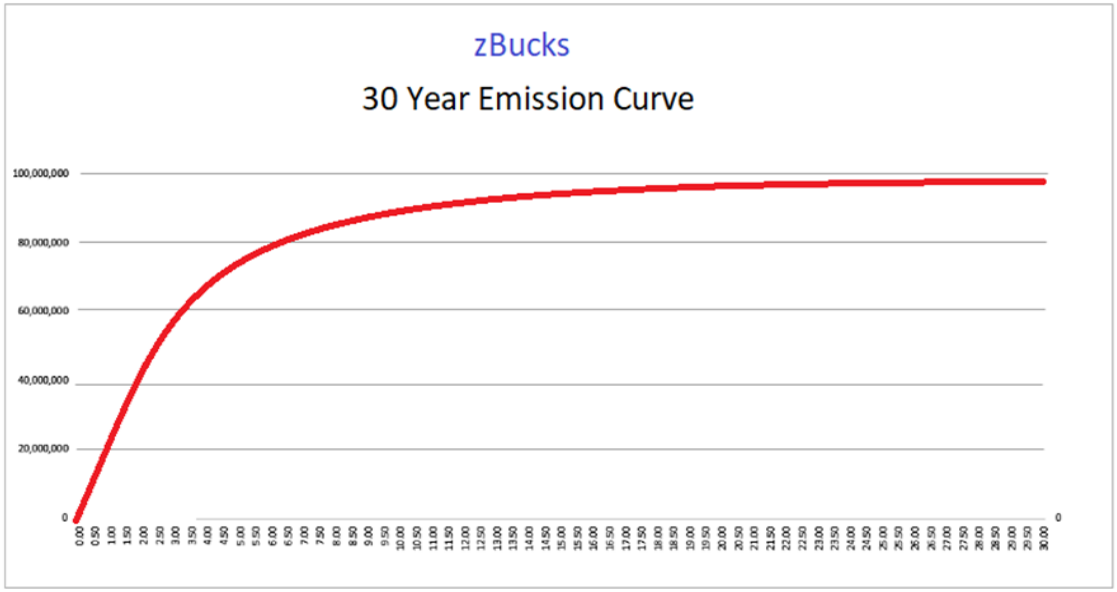


Table 5: Emission curve demonstrating supply vs time.

Section 5

# Roadmap


Table 6: zbucks timeline for completed and developing projects in 2018.

Section 6

# Treasury reward

zBuck's monetary base will consist of 100 million zBucks currency units (ZBK or ) which will be mined over time. Five percent of that reward will be distributed to the stakeholders in the zBucks Company — founders, investors, employees, and advisors for the "Founders Reward". The treasury block reward will go to a fixed address held by the zBucks team. In the header of every block, miners must include the transaction ID, and transaction key of the transaction that rewards the treasury pool. With this information, nodes and third parties can verify this candidate block pays the governance address. Additionally, the treasury address will have its view key published publicly so that third parties can audit incoming flows.

## Development team

The zBucks core team is dynamic, enthusiastic and highly skilled. The team has over twenty years combined experience in information technology and remain leaders in innovation in the cryptocurrency sector, with members residing in South Africa, England, and Sweden.

Section 7

# Conclusion

Our whitepaper is intended to provide a laid-back space to read about the vision that the zBucks team will be working passionately towards. zBucks is not an ICO, there is no pre-sale of ZBK, privately or otherwise, and no method for the zBucks team to accept funds. We are focused on creating a stable development platform and expanding our dedicated universal team so that we, as comradeship, can grow, learn, and thrive together. There is no power for change greater than a community discovering what it cares about, so come join us, learn alongside us, the world's invited.

Section 8

# Bibliography

MRL-0001: A Note on Chain Reactions in Traceability in CryptoNote 2.0
https://lab.getmonero.org/pubs/MRL-0001.pdf

MRL-0002: Counterfeiting via Merkle Tree Exploits within Virtual Currencies Employing the CryptoNote Protocol
https://lab.getmonero.org/pubs/MRL-0002.pdf

MRL-0003: Monero is Not That Mysterious
https://lab.getmonero.org/pubs/MRL-0003.pdf

MRL-0004: Improving Obfuscation in the CryptoNote Protocol
https://lab.getmonero.org/pubs/MRL-0004.pdf

MRL-0005: Ring Signature Confidential Transactions
https://lab.getmonero.org/pubs/MRL-0005.pdf