The Zero Paper

The Zero Team, April 2018

Contents

[1 Introduction 3](#_Toc512717281)

[2 Specifications 3](#_Toc512717282)

[3 Current Features 4](#_Toc512717283)

[3.1 Windows Java Swing Wallet – links & tech details 4](#_Toc512717284)

[3.2 Web Wallet links & Tech details 4](#_Toc512717285)

[3.3 Mobile Android Wallet links & tech details 4](#_Toc512717286)

[4 Future Core Features 4](#_Toc512717287)

[4.1 iOS Wallet 4](#_Toc512717288)

[4.2 Miner 4](#_Toc512717289)

[4.3 Developers Fund 4](#_Toc512717290)

[4.4 Z-DEX (Decentralized exchange) 5](#_Toc512717291)

[4.5 Z-Pay (payment gateway) 5](#_Toc512717292)

[4.5.1 Desktop 5](#_Toc512717293)

[4.5.2 Mobile – Android / iOS 5](#_Toc512717294)

[5 Potential 3rd Party Integrations 6](#_Toc512717295)

[5.1 Ledger Hardware wallet 6](#_Toc512717296)

[5.2 Trezor Hardware wallet 6](#_Toc512717297)

[6 Community & Z-Estival 6](#_Toc512717298)

[6.1 The Zero Community 6](#_Toc512717299)

[6.2 Z-Estival 6](#_Toc512717300)

[7 Roadmap 7](#_Toc512717301)

# Introduction

The Zero Project was created in February 2017 in order to identify and solve many inherent weaknesses in existing cryptographic currencies.

The goal was to create a currency with transactions that required less power consumption than other currencies, that were also processed faster, had less transaction fees, and permitted transactions that were untraceable and anonymous in a mainstream adoption.

Zero uses a decentralized anonymous payment scheme (DAP) that can be integrated with cryptocurrencies using the Bitcoin blockchain structure, and forks thereof.

Zero is presently run by a very strong community, whose aim is to deliver a successful project and product that can be enjoyed and utilised in many applications.

In future, Zero plans to design and implement Z-Dex, a decentralized exchange for primarily the fellow Z-Cash clones / forks that are already (and yet to be) in existence in a unified trading eco-system. Z-Dex will also offer fiat/ Zero trading pair/s for its further core functions (as detailed below).

A payment gateway system known as Z-Pay is also to be implemented as a basis of payment that enables a unique fiat / Zero direct payment system from the Z-Dex exchange for transactions with merchants that do not directly accept Zero. Z-Pay will also acts as standalone payment gateway for real world transactions utilising the overarching Zero currency at merchants that directly accept the currency.

A further proposed function of Z-Pay is to provide an umbrella payment system that caters for 3rd party currencies to adopt for transactions. These transaction will utilise a direct Zero currency pairing with said 3rd party coins for instant, and seamless transactions.

Both Z-Dex exchange and Z-Pay payment gateway system could eventually serve as an ecosystem for other currencies that do not yet have the infrastructure to implement payments and trading.

# Specifications

Zero has a hard-coded option to use shielded transactions (Z), making it impossible for anyone to track ie Zero-Knowledge-‘Succinct Non-interactive Arguments of Knowledge” (zk-SNARKs)

Zero’s transaction times are extremely fast thanks to its infrastructure. Funds are send and received with near instantaneous transactions directly from Zero wallet – Zero wallet applications.

Zero's transaction fees are als 0.0001 ZER, providing the advantage of cost saving, on top of fast transaction timeframes.

Mining operations for Zero require 25-30% less power consumption than other equivalent cryptographic currencies and tokens due to a modified equihash algorithm.

The Zero block size is 4MB, with a higher time complexity X16, and higher memory requirements X16.

Zero has a 4X faster block verification, and smaller solutions of 400 bytes, instead of a typical 1344 bytes.

Zero's total supply is uncapped, with a stable 7200 ZER minted by miners per day, and is also ASIC resistant, meaning that it is unprofitable for larger farming operations with ASIC capabilities.

# Current Features

## Windows Java Swing Wallet – links & tech details

## Web Wallet links & Tech details

## Mobile Android Wallet links & tech details

# Future Core Features

## iOS Wallet

iOS wallet shall commence in 2018, with – further input required from a technical point of view.

## Miner

Need input from a technical and design perspective.

## Developers Fund

In order to fully realize goals for Zero, a development fund will be implemented as a revenue stream to allow for the necessary personnel, equipment, and bounties required to meet the requirements of the roadmap.

The exact detail of the developer fund will be made public in due course.

This funding is key to Zero, not only so the project does not need to rely on the community for donations, but to also ensure the steady, organic growth of Zero in a self-supported manner.

## Z-DEX (Decentralized exchange)

A decentralised exchange that offer P2P (peer to peer) trading of initially other ZCash forked coins (Z-Clones), using Zero as the mainstay trading currency paired with other said currencies.

On top of embracing an initial Z-Clone eco-system, Z-DEX will also provide a fiat / Zero trading pair, not only to offer another form of payment and value other than Bitcoin, but also to integrate into other future functions of Zero.

(much more to add here – can someone with a technical understanding please input?

## Z-Pay (payment gateway)

Z-Pay is intended to be a semi-integrated system and application in conjunction with Z-DEX, where a Z-Pay wallet is used to facilitate payment for both private and everyday transactions (T & Z payments) using Zero as the transactional medium.

The end user will decide which wallet to utilise in terms of private or transparent for their transactions.

The system intended to be implemented in two types of applications:

### Desktop

Z-Pay is to be integrated within e-commerce sites and equivalent outlets similar to existing payment gateways, but in this instance, Zero is utilised as the primary payment in the transaction. This requires the outlet to accept Zero as a payment.

In order to utilise Zero as a form of currency where outlets do not support Zero directly, another feature to be instigated is an instantaneous Zero / fiat conversion from the funds in your Z-Pay wallet for everyday transactions.

This instantaneous transaction is verified through the Z-Dex exchange, based on fiat / ZER trading pairs, and is relevant to the exchange rate of ZER to the applicable category of fiat for that specific point in time of the transaction.

### Mobile – Android / iOS

Z-Pay is also intended to be used as per the desktop application for payment where outlets accept Zero directly, and also where they do not.

With most crypto currencies, an issue of mainstream adoption is encountered due to outlets specifically requiring acceptance of individual coins, and also not having a credit / debit card facility to encourage transactions.

In order to solve the problem of spending Zero without a debit / credit card, Z-Pay will facilitate transactions using NFC (near field contact) that is already applied in current mobile phone technology (ie Android & iOS) that do not require a physical credit or debit card.

The NFC application will be built by Zero, and integrated within outlets that already accept NFC payments to facilitate transactions.

In offering an NFC application for everyday transactions where Zero is not directly accepted by an outlet, Z-Pay will link to Z-DEX to facilitate fiat / ZER conversions in order to settle the transaction instantaneously based on fiat / ZER exchange rates at that point in time.

By offering both a desktop and mobile version of Z-Pay that caters for outlets that accept Zero directly, and also those who do not, Zero becomes much more liquid in a transactional sense, thus enhancing the value of this currency.

In further Z-Pay features, crypto currencies that are also live on Z-DEX will also have the opportunity to utlise Z-Pay as a gateway for their transactions also. This feature needs further integration investigation as of this point in time.

# Potential 3rd Party Integrations

## Ledger Hardware wallet

Blurb / technical input

## Trezor Hardware wallet

Blurb / technical input

# Community & Z-Estival

## The Zero Community

The Zero community is a very strong, loyal, and committed collaboration of dedicated people who only have the interest of Zero’s success at heart.

The Zero team was selected to manage the project from within the community after a recent takeover, and have now set a solid path forged on the foundation of the Zero community to continue the project’s success.

A healthy social media and marketing campaign is confirmed as an ongoing step on the roadmap, and Zero welcomes every new community member along the journey to a successful product.

## Z-Estival

Z-Estival is an idea that envisages a gathering, or festival of the Z-Cash clones / fork team members to celebrate the backgrounds of our blockchains and existence together.

This would be a gathering in the interest of learning, networking, and leisure, and would extend to each of the community members of each Z-Cash clone / fork, with an inaugural meeting yet to be established and determined with other entities.

# Roadmap

1. Release of whitepaper and roadmap;
2. Web wallet UI completion;
3. Mobile wallet official release;
4. Windows desktop miner;
5. Donation, social media, and marketing campaign;
6. Ongoing communication and application for exchanges;
7. Developer fee implemented;
8. Z-DEX architecture commences;
9. Z-Pay architecture commences;
10. Ledger and Trezor investigation;
11. Z-Estival confirmation;
12. Z-Pay NFC establishment;
13. Z-DEX Beta
14. Z-Pay Beta
15. Z-DEX Live
16. Z-Pay Live
17. Ongoing partnerships and 3rd party integrations