ZERIUM

THE WORLD'S SMARTEST
BLOCKCHAIN APPLICATIONS

DUAL BLOCKCHAIN ENVIROMENT
FOR DECENTRALIZED APPLICATIONS

Carlos Reglero
CReglero@Zerium.org

Hugo Teijiz
HTeijiz@Zerium.org

v 1.0.1
DEC 18. 2017

Decentralised peer-to-peer scalable crypto-currency, binary blockchain ecosystem,
secure transaction ledger and smart contract ecosystem

ABSTRACT

—//—

Zerium introduces a blockchain architecture designed to facilitate scaling of decentralized applications (DApps) and Smart contracts in an intuitive environment. The Zerium blockchain is an open-source operating system-like construct upon which applications can be built. The Blockchain can host accounts, authentication, databases, asynchronous communication and scheduling of applications across hundreds of CPU cores or clusters around the globe. The result is an architecture that scales to millions of transactions per second, diminishes user fees, and allows opportunities for development of no-cost Decentralized Applications.

Note

TABLE OF CONTENTS

ZERIUM

—//—

Zerium is a cryptocurrency that supports a stable architecture inside a blockchain designed to facilitate scaling of decentralized applications (DApps) and Smart contracts in an intuitive environment. The Zerium blockchain is an open-source operating system-like construct upon which applications can be built. Zerium is built using an updated version of the ethash mining algorithm (involves finding a nonce input to the algorithm so that the result is below a certain threshold depending on the difficulty) and will gradually be expanded to include PoST (Proof-of-Stake-Time). ZRM has a decreased block generation time, reduced difficulty and improved transaction times, by doing this we assure the inclusion of CPU mining expanding the number of nodes available, promoting decentralization and securing an efficient defense against attacks to the network.

The network itself requires minimal structure as messages are broadcasted on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof and evidence of what happened while they were gone, untieing each miner of the processed transaction regardless of the amount, class or type of use of the hashed block. The Smart contracts are developed natively inside the cryptocurrency acting as cryptographic containment that incorporates value and only unlocks it if certain conditions are met, with vastly more power than that offered by Bitcoin scripting because of the added powers of value-awareness, blockchain-awareness, and state.

ZRM is adapted to support a binary blockchain system (2 blockchains synced with a shared address and key to increase security against attacks to the network, financial stability, and versatility of the smart contracts), the second blockchain under development includes zero-knowledge proof (SK-SNARKS) to increase efficiency and anonymity on transactions.

ZRM'S DUAL-BLOCKCHAIN PROTOCOL AND HARD-CODED UPGRADE PROTOCOL

Zerium secondary blockchain has a protocol that enables the change of hard-coded limits, including natural elements of the original design such as block frequency, and a minimum of number of confirmations per block, we maintain an evolving algorithm in charge of modifying the established parameters according to hard-coded milestones that are only applied if certain conditions are presented.

It analyzes the growth of the cryptocurrency and increases limits in block size and adjust the maximum amount of money supply without creating inflation. This provides a baseline to change and modify both natural and artificial constraints within the blockchain environment.

ZERIUM APPLICATION ENVIRONMENT (ZAE)

Zerium's architecture allows to easily write and deploy decentralized applications using blockchain technology in many developer-friendly languages, without the added cost (and in some cases extensive cost) of the GAS used for deployment. We work around this by implementing Staking technology (PoST) to grant access to different levels and tools from the developing kit in ZAE.

IO SMART WALLET

IO is an implemented technology that is directly embedded in the main blockchain of Zerium. It integrates all necessary tools to create, distribute and manage decentralized Blockchain applications without tokenization (directly on Zerium) or by deploying their own sidechain in Zerium's blockchain (if a side chain is required then a custom token must be implemented) this adds flexibility to developers to customize their applications entirely. It behaves as a multi-token wallet with a future implementation as a multi-crypto payment gateway. It will add a total balance amongst several cryptocurrencies and tokens and executes a sell command whenever the user wishes to pay via BTC payment gateway without having to manually sell individual transactions of each amount to pay for a balance (I.E. Item costs 1 BTC. The user has 0.02 BTC, 20 Eth (0.87 BTC), 6.7 XMR (0.11 BTC), the wallet upon reaching a payment gateway will clear all amounts into BTC, ZRM, ETH or XMR and then executes the payment).

DAPPS NAMES AND ACCOUNT HANDLING

ZEA allows accounts to be named with a human-readable name-value of 2 to 32 characters. The name-value must be chosen upon creation of the contract and is unchangeable throughout the duration of the DApp or Smart contract. All accounts must be funded with the minimum account balance at the time they are created to cover the cost of storing account data (the only fee applicable). Account names also support namespaces (I.E @domain & User@domain)

ZAE (ZERIUM APPLICATION ENVIRONMENT) SPECIFICATIONS

A ZAE account contains the following fields:

- The Account Name (Human readable) and address (within the ZRM network)
- The nonce (counter used to make sure each transaction is only processed once)
- The account's current ZRM balance
- The account's contract code, if present (depends)
- The account's storage

ZAE accounts are feeless, however for access to specific tools a determined amount must be staked (PoST) in order to access said tools, this is used as a barrier to prevent abusive usage of the platform.

ZRM EMISSION

Zerium emission is an open process which employs computing powers of all network members. Any user can join the Zerium network and take part in the emission process (thus, becoming a miner).

Mining in the network is rewarded with cryptographic money, which is securely paid to users who employ their computing power in order to process transactions.

All transactions are carried out every 60 seconds. Miners ensure that the transactions are processed correctly and provide cryptographic protection of transactions and personal data.

ZRM'S ACQUISITION IN PREICO & ICO

The ZRM is already being premined and the initial purchase can be made through Bitcoin (BTC), Ethereum (ETH), Litecoin (LTN), Monero (XMR) during the preICO. During the ICO we will allow FIAT currencies (USD & EUR). Investment information is the following:

- The primary currencies will have an individual exchange rate that can be corroborated on the website
- Investments in other currencies will be accepted upon review. For more information contact: Investments@zerium.org

The token sale will be capped ("Soft Cap") upon receip of the different currencies equivalent to 1 Million Swiss Franc (CHF). This amount is subjet to change depending on initial investments

and adaption amount is subject to change depending among different regions as well as mining operation and other factors. The total required amount to raise to complete the project is the equivalent of CHF 300.000 (Three hundred thousand Swiss Francs). Upon reaching the global a new redistribution of founds will be issued and more developed in the first semester of 2018 (Q1 & Q2). As of December 2017 stage 1 of the Zerium Blockchain is already functional.

DEFLATION

ZRM will gradually get more expensive over time. The number of ZRMs emitted every 60 seconds is correlated to the number of workers providing computational power, upon reaching a currency cap of 10 million ZRMs the reward will slightly decrease on periods of time in relation to an increase in the difficulty of the algorithms and miners providing more computational power. As a result the ZRM gains value and exchange rate increases.
This emission protects the currency from economic shocks and increases stability over time.

GEOGRAPHIC REGION

Fiat currencies are assigned to specific territories while Zerium is bound to the Internet and therefore is international by its nature.
Zerium has formed its own network that consists of users who use ZRM for mutual settlements and contracts. The ZRM network is open-source creating an added value allowing the improvement and creation of smart contracts carried through the blockchain.

SAFETY AND RELIABILITY

The reliability of the Zerium is defined by the total computational power of all the computers that take part in transactions processing. The greater the processing power, the more reliable the network. Being so, it guarantees a zero downtime for financial operations.
In so doing all money stored in your wallet is already protected during the transaction processing and the safety doesn't depend on network reliability. Your money is safe wherever you are.

MARKET INTEGRATION IN A GLOBALIZED ECONOMY

The Zerium expansion in local markets grant a clean low-cost solution for money transferring and savings possibility, as it does not depends on any government legislation or decisions to manage the growth of the coin, it is truly in the hands of the coin-holder to decide the future of the cryptocurrency and its value.

Integrating Zerium in globalized exchanges of other altcoins, the user can change with little technical expertise the ZRMs into any local or online currency, serving as an instant method to send funds to friends and family all over the world in a risk-free and low-to-no-cost environment.

ZAE & IO Smart Wallet allow for extensive adaptability and customization of decentralized applications, coinciding with a reduced cost compared to other DAPP environments, it is foreseeable a wide implementation from users of Zerium for Smart contracts and decentralized applications creation and deployment.

ZERIUM INITIAL FUNDING

FUNDING BREAKDOWN

Funds invested during the initial seed investment will be used solely for the development of the **Zerium network.** The following distribution of funds is preliminary and can be subjected to change.

15% OPERATIONAL

This covers the necessary costs incurred for a functional system. This includes hosting and infrastructure costs, staffing, outsourcing, management and other related expenses.

25% MARKETING AND SALES

Marketing costs will be used for partnerships development and direct consumer marketing.

5% LEGAL AND COMPLIANCE

There are legal costs associated with the introduction of the coin in different global markets. The legal costs might vary from region to region.

ZERIUM INITIAL FUNDING

55% CORE DEVELOPMENT

Core development involves the final development and improvement of the roof-Of-Stake-Time IO, ZAE and secondary blockchain system.

UPCOMING DEVELOPMENT AND TECHNICAL FEATURES

- Password Login Screen for IO Smart Wallet
- Two-Factor Authentication (2FA) for IO and Tiny wallet
- New Dapps dashboard in IO Smart Wallet
- Proof-of-Stake-Time
- Wallet Auto-Update
- FIAT Purchasing In Wallet
- Decentralized Exchange and CryptoSmart payment in IO the ability to spend ANY coin within
- New Wallet UI Template and add-ons with repository integration
- Synced website for zerium.org with a blockchain explorer
- Tiny Android Wallet
- IO Android Wallet
- Tiny IOS Wallet
- IO IOS Wallet
- ZRMixer - (coin mixing service for full transaction privacy in the wallet - IO Add-on)
- ZRM.txt (Send ZRM with Text messages)
- Tiny Miner client Windows & Mac OS X
- Mino Smart multi crypto-mining software.

REFERENCES

—#—

1. Nakamoto, S. 31 October 2008. "Bitcoin: A Peer-to-Peer Electronic Cash System". Also known as the
Bitcoin whitepaper. http://nakamotoinstitute.org/bitcoin/.
http://bitcoin.org/bitcoin.pdf. https://github.com/saivann/bitcoinwhitepaper. Accessed 7 July 2017.

2. Ethereum whitepaper. https://github.com/ethereum

3. Zerocash whitepaper. http://zerocash-project.org/paper

4. ADSNARK: Nearly Practical and Privacy-Preserving
Proofs on Authenticated Data. https://eprint.iacr.org/2014/617.pdf

5. PoST. http://resources.vericoin.info/post-white-paper/

6. Altquick (acquisition of altcoins with FIAT currency.
https://info.shapeshift.io/blog/2015/07/07/AltQuick-integrates-shapeshiftAPI

DONATIONS AND MORE INFORMATION

For more information on how to help this project grow and for investment opportunities please contact

Investments@Zerium.org