A Zilliqa Decentralized Exchange

Karim Helmy
Carnegie Mellon University
khelmy@andrew.cmu.edu

October 26, 2018

Abstract

We propose a project to build a decentralized exchange for fungible tokens on the Zilliqa platform. The core smart contracts for the exchange will require use of both Scilla, and the front-end will be built in JavaScript. The project will draw inspiration from Uniswap, an active decentralized exchange on the Ethereum platform.

Contents

Proposal

Decentralized Exchanges

Traditional, centralized exchanges keep custody over their users' funds to facilitate trading. While this eliminates the requirement that users trust their counterparty, it requires them to trust the exchange, as any funds left on the exchange by the user are prone to seizure. Users of numerous exchanges have lost custodied funds due to theft, hacking, or exit scams,[1] most notably in the incidents surrounding Mt. Gox.[2]

In response to the danger of using a centralized exchange, there is a growing movement to develop decentralized exchanges, which do not retain control of user funds.

To minimize counterparty risk, decentralized exchanges rely on atomic swaps, which are smart contracts structured such that the ability of each party in a transaction to access the asset offered by their counterparty is dependent on the transfer of their own asset to either the contract or their counterparty. This mechanism ensures that defection from the agreed-upon terms of exchange voids the entire transaction.

There currently exist several decentralized exchanges for ERC20 tokens, including 0x[1], AirSwap[3], and Uniswap[4]. This project draws inspiration from Uniswap in building the first decentralized exchange for fungible tokens on Zilliqa.

The deployment of a decentralized exchange could be hugely beneficial for increasing token liquidity within the Zilliqa ecosystem. As the core requires a complex suite of contracts, the deployment of a decentralized exchange to Zilliqa represents a major use Scilla programming language, and shows developers of other decentralized applications that Scilla is ready for use.

Implementation

The core Zilliqa contracts for this project will be implemented in Scilla. The project will require analysis of the Uniswap contracts, which are written in Vyper. The frontend application will be developed in JavaScript with React.

Team

Karim Helmy will be conducting this project with supervision from a member of the Zilliqa team. Karim is a senior Statistics and Machine Learning major at Carnegie Mellon University. He sits on the executive board of the CMU Blockchain Group, managing corporate relations, and has previously worked on Valex, a platform for trustless cross-chain cryptoasset exchange.

[1] https://magoo.github.io/Blockchain-Graveyard/

[2] https:/wired.com/2014/03/bitcoin-exchange/

[1] https://0xproject.com/

[3] https://airswap.io/

[4] https://uniswap.io/

Timeline

The proposal for this project follows a ten-week structure similar to the ten-week Hackternship structure used by the Ethereum Foundation for their grants.[5] The project will commence in January of 2019. We request a grant of 8,000 USD to conduct the project.

Date	Milestone
Weeks 1 and 2	Study Uniswap Vyper contracts, analyzing with goal of implementation in Scilla.
Weeks 3 and 4	Implement Scilla contracts.
Week 5	Write test suites for Scilla contracts.
Weeks 6 and 7	Build frontend application.
Week 8	Deploy and test project on Kaya TestRPC.
Week 9	Deploy and test project on Zilliqa Testnet.
Week 10	Deploy project to Zilliqa Mainnet.

[5] https://blog.ethereum.org/2018/03/07/announcing-beneficiaries-ethereum-foundation-grants/