GBBC Global Blockchain Business Council

Open Learning Forum

Proof-of-Work Sidechains

Aggelos Kiayias and Dionysis Zindros
University of Edinburgh; National and Kapodistrian University of Athens; and IOHK
Date Published: 10/30/2018

Executive Summary written by GBBC

Introduction

As the use of blockchains has increased, so have questions regarding the technology's interoperability, scalability, and upgradability. Sidechains have been proposed as a partial or full solution to each of these problems. They have to potential to enable transactions between different blockchains, increasing interoperability. This paper presents the first decentralized sidechain construction designed to work with proof-of-work blockchains. The proof-of-work sidechains proposed in the paper allow for both remote ICOs and two-way pegs.

Remote ICO

A remote ICO allows a user to pay in a certain currency/token on one blockchain in exchange for tokens on a different blockchain. This would enable a user who holds Bitcoin and wants to take part in an ICO on the Ethereum blockchain to pay in Bitcoin rather than trade Bitcoin for Ether before buying in.

Two-Way Peg

The two-way peg allows users to transfer assets back and forth between blockchains without altering the nature of the asset. This can be done without an intermediary or exchange.

Non-Interactive Proofs of Proof-of-Work (NIPoPoWs)

NIPoPoWs is the cryptographic process that makes the proof-of-work sidechain possible. This protocol involves a "prover" and a "verifier"; the prover is attempting to show that a certain event took place in the blockchain. This is done by providing a polylogarthmic proof, a proof that "does not grow linearly with the size of the blockchain." The verifier must compare multiple proofs against one another to extract "a reliable truth value corresponding to the same value it would deduce if it were to be running a full node on the blockchain itself."

Requirements

The "source" blockchain (from where the asset is being moved) must support NIPoPoWs, which is possible without a fork on major blockchains like Bitcoin and Ethereum. The "target" blockchain (to which the asset is being moved) must be able to support advanced smart contracts; Ethereum is one such blockchain.

Conclusion

The paper claims this is the first construction of proof-of-work sidechains that is truly decentralized and resistant to fraud, such as double spending. NIPoPoWs enable proof-of-work sidechains to conduct both remote ICOs and two-way pegs. Importantly, sidechains allow developers to create new features for large blockchains without jeopardizing the security of the blockchain.