GBBC Global Blockchain Business Council

Open Learning Forum

Proof-of-Stake Sidechains

Peter Gaži; Aggelos Kiayias; and Dionysis Zindros
University of Edinburgh; National and Kapodistrian University of Athens; and IOHK
Date Published: 12/18/2018

Executive Summary written by GBBC

Introduction

The three most pressing technical questions regarding blockchain technology are its (1) interoperability; (2) scalability; and (3) upgradability. Using the following processes, it is possible to design an efficient and effective proof-of-work sidechain that does not sacrifice security.

Firewall Property

An effective firewall is critical to the success of a sidechain, as it guards against negative consequences of the potential failure of a sidechain. The firewall prevents transfers from the sidechain to the mainchain unless it can be proven that the sidechain is secure.

Merged Staking

To guard against attacks to a nascent sidechain, mainchain stakeholders must be able to create sidechain blocks without moving their stake from the mainchain. This is known as merged staking and it is crucial to sidechain security in its beginning phase.

Cross-Chain Certification

The transfer of assets between the mainchain and sidechain is made possible by cross-chain certification. This is a process in which mainchain stakeholders receive information from the sidechain by monitoring an authenticated sample of sidechain stakeholders. This subset of sidechain stakeholders must be able to accurately broadcast the state of the sidechain as determined by the stakeholder majority. The subset is responsible for signing transfers from the sidechain to the mainchain.

Ad-Hoc Threshold Multisignatures

Ad-hoc threshold multisignatures (ATMS) is a cryptographic process by which signatures of a subset of sidechain stakeholders are packaged together to create sidechain certificates. Using a variety of methods, it is possible to reduce the size of the sidechain certificates to a non-burdensome level.

Conclusion

Proof-of-stake sidechains have numerous benefits when compared to mainchains. First, they enable the transfer of assets between different blockchains without transforming the asset. Second, stakeholders can reduce the number of transactions performed on the mainchain by shifting certain transactions to a sidechain. Finally, sidechains provide for greater flexibility and innovation, as it is possible to create a sidechain with a specific goal (speed, security, etc.) in mind without the need for a fork. If enough stakeholders see the value in a sidechain, it can usurp the mainchain while maintaining the same assets.