GBBC Global Blockchain Business Council

Open Learning Forum

PISA: Arbitration Outsourcing for State Channels

Patrick McCorry; Surya Bakshi; Iddo Bentov; Sarah Meiklejohn; and Andrew Miller
University College London; University of Illinois at Urbana Champaign; Cornell University; and IC3
Date Published: 5/22/2018

Executive Summary written by GBBC

Introduction

Scalability is one of the most significant challenges facing existing blockchains and cryptocurrencies. As the chain extends with new blocks of transactions, it requires more and more bandwidth and storage to process transactions. State channels can improve scalability of blockchains by allowing "a group of distrustful parties to optimistically execute an application-defined program amongst themselves, while the blockchain serves as a backstop in case of dispute or abort." Essentially, state channels allow users to transact off the blockchain while storing the most recent "state" on the blockchain to resolve potential disputes. State channels reduce congestion on the blockchain and allow parties to avoid transaction fees.

Problem

The nature of state channels requires parties to remain online to deal with any fraudulent dispute claims or attempted execution forks. When a questionable dispute is initiated, parties have a "fixed time period to submit a newer signed state to resolve the dispute." Nefarious actors may also attempt to manipulate the authorized states with an execution fork.

PISA

PISA attempts to solve the problems associated with state channels by creating a "custodian." The custodian is a third party that ensures the security of a state channel; they are appointed and paid by a party that wishes to go offline for a period of time. Custodians advertise their services and store a security deposit that will paid out to the party if the state channel is not defended.

When the party identifies an appropriate custodian, they distribute a hash of the channel's state to the custodian, which allows the custodian to defend the network against a fraudulent dispute or execution fork. Importantly, the custodian can only access the hash of a channel's state, meaning that state privacy is maintained. The custodian would then provide a signed receipt that indicates how long they will be monitoring and defending the channel.

Conclusion

State channels are a promising solution to the problem of blockchain scalability, though they come with some challenges of their own. First and foremost is the requirement that a party stay online to monitor the state channel and guard against malicious actors. PISA presents a solution to this problem by adding a third party that is financially motivated to uphold the state channel's integrity while a party is offline.