Teechain: Reducing Storage Costs on the Blockchain With Offline Payment Channels

Joshua Lind  
Imperial College London  
joshua.lind11@imperial.ac.uk

Oded Naor  
Technion and IC3  
odenaor@technion.ac.il

Ittay Eyal  
Technion and IC3  
ittay@technion.ac.il

Florian Kelbert  
Imperial College London  
f.kelbert@imperial.ac.uk

Peter Pietzuch  
Imperial College London  
prp@imperial.ac.uk

Emin Gün Sirer  
Cornell University and IC3  
egs@systems.cs.cornell.edu

CCS CONCEPTS
- Security and privacy → Hardware-based security protocols; Tamper-proof and tamper-resistant designs; Distributed systems security; Security protocols;

KEYWORDS
Blockchain, Cryptocurrencies, Scalability, Payment Channels, Trusted Execution Environments

Blockchain protocols such as Bitcoin [4] exchange payments in a secure and decentralized manner, but their performance is limited due to their need to achieve consensus across a network [1], and each node in the network needs to process the entire blockchain, which introduces major storage limitations.

Cryptographic payment channels [2, 5] have been proposed as a second tier on top of the blockchain, allowing efficient direct payments between parties, and the removal of many payments from the blockchain to only the participating parties of the channel. Existing payment channel protocols, however, have two limitations: (i) their security relies on synchronous access to the underlying blockchain, which an attacker may prevent; and (ii) they suffer from long channel establishment times when placing collateral deposits on the blockchain.

We describe Teechain (TEE + Chain), a payment network that supports secure and scalable payments for blockchain-based cryptocurrencies using hardware trusted execution [3]. Teechain creates chains of payment channels using multiple TEEs. Teechain is the first payment network that assumes asynchronous blockchain access and does not require bounded time write-access to the blockchain. It also permits payment channels to be established near instantly by dynamically assigning deposits. To overcome TEE crash failures, Teechain uses a novel replication protocol between TEEs that may be of independent interest.

We experimentally evaluate our Teechain implementation and show that it achieves orders of magnitude improvement in performance compared to existing solutions; with replicated Teechain nodes in a trans-Atlantic deployment, we measure a throughput of between 33k–135k transactions per second with 0.3 second latency, in comparison to the current state of the art which achieves 1,000 transactions per second.

In addition, we define and prove the correctness of the Teechain protocol, i.e., we show that a user has the ability to unilaterally receive all his money from open channels on the blockchain, and that other users cannot interfere with that ability.

REFERENCES