CSci 8271
Security and Privacy in Computing
Day 14: zkBridge

Stephen McCamant
University of Minnesota

Merkle trees and proofs

- Merkle tree: parent node includes hash of children
- Good hash function → root determines whole tree
- Can prove value of leaf with log-sized evidence

Multi-chain ecosystem

- Different blockchains/cryptocurrencies vary with features, pros and cons
- Perhaps the long-term state is multiple popular chains
  - Compare: programming languages, banks, credit card networks
- Some designs (e.g., Cosmos) facilitate inter-chain transactions
- Popular older chains (Bitcoin, Ethereum) do not

Ethereum and smart contracts

- A smart contract is a program that runs on a blockchain and can operate on money
- Ethereum is the most popular blockchain with rich smart contracts
- Based on a specialized virtual machine programming model
  - Expensive (pay-per-instruction "gas") because the execution is widely replicated

Bridging from Cosmos to Ethereum

- Bridges based on trusted committees show demand, but security risk
- This paper: build a bridge to convey Cosmos state to Ethereum, with cryptographic proof checking
- Untrusted parties create proofs of Cosmos light updates, Ethereum smart contract verifies
- (Opposite direction also desirable, not discussed here.)

Proofs for this application

- Succinct (constant proof size)
- Cheap on-chain proving using Ethereum-supported cryptography
- Low-latency proof construction (close to real time)
- Provers have industrial-strength parallel execution available ($8k/month cluster)

Post-paper updates

- zkBridge is being commercialized by a pre-Series-A startup
  - Founded in Berkeley by the paper lead authors
- Also bridging to/from Bitcoin, to direction needs third parties
- To bridge from current Ethereum you might really want a heavy client, further pushing scalability