CSC 724 Project Presentation: Anonymity in BFT protocols using Zero Knowledge Proofs

Varun Madathil (vrmadath)
Vaibhav Singh (vsingh7)
ChuWen Chen (cchen31)
Motivation

What? - BFT protocols where each node does not know the identity of the other nodes.

Why? - Applications like e-voting, privacy preserving blockchains

How? - Cryptographic techniques like zero knowledge proofs (zk-SNARKs)
Introduction

- **BFT protocol** - Agreement protocol where there are no restrictions, and no assumptions about the kind of behavior a node can have.
- **Zero knowledge proof** - Allows you to prove that you know some secret without revealing the secret. In our case this will be the identity of the party participating.

**REACH CONSENSUS ANONYMOUSLY!!**
Project Milestones

There are three planned milestones each led by one team member:

1. Coming up with an anonymous BA protocol - **Varun**
2. Implementing the protocol on a few nodes - **Vaibhav**
3. Deploying on a distributed network - **Wayne**
Anonymous Byzantine Agreement

- Using SNARKs, each node creates a proof that shows that the identity of the node is valid.
- The node then sends this proof along with the message it wants to send.
- All parties verify that the message is received from a valid node by verifying the zero knowledge proof.
- Our BFT protocol will assume $< \frac{1}{3}$ corruption and a weakly synchronous network. Eg - PBFT, [FM85]
Standalone implementation of protocol

- Proof of Concept Testnet
- ZK libraries - libsnark, Bellman, snarkjs
- RPC libraries - gRPC, Apache Thrift, XML-RPC
- Consensus over a (few) nodes
- Messages received with assumed bounded delay (weak synchrony)
- Serves as validation of BA protocol (not the distributed system)
- Evaluate measurements of anonymity over these nodes
Deploying on a Distributed Network

Topology of the network: Fully connected

How do machines communicate? By applying gRPC (Remote Procedure Calls).

What are the machines we are going to use? Local machines (separate hardwares) / on-cloud VMs
References


THANK YOU

Questions?