

Peer to Peer Blockchain

Ankur Singh, Mahesh Meena, Prashant Kumar
160129, 160375, 160500

Indian Institute of Technology, Kanpur

1 Introduction

Blockchain is stirring a technological revolution that could forever change how we conduct our affairs online. Many expect it to disrupt practically all industries, providing a platform that is secure enough to foster trust and confidence even without a controlling authority to oversee the system.

In 2008, a white paper prepared by a person with the pseudonym Satoshi Nakamoto described the details of a “Peer to Peer Electronic Cash System” that eventually launched as Bitcoin. The system that was presented eliminates any trusted financial institution, such as a central bank. Instead, all the transactions will be recorded and validated by all nodes on a peer-to-peer network.

In a Peer-to-Peer architecture, one doesn’t need a central server to maintain the current state of a blockchain. There isn’t a central authority like a bank that maintains the state. Instead, all the nodes in the Bitcoin network that wish to maintain a copy of the Bitcoin blockchain update their copies of the blockchain to include your transaction. That way, as long as 51 of the nodes in the network “agree” on the state of the blockchain, it maintains its fidelity.

Inspired by the above idea, in this work of ours, we will program a blockchain so that it uses a Peer-to-Peer architecture instead of a central server. For this purpose, we will employ the P2P library written in Go called `go-libp2p`. We will make use of hashing to maintain the integrity of the blockchain.

2 Goals

- Create our blockchain
- Use hashing to maintain integrity of the blockchain
- Use a peer to peer network instead of a central server for our blockchain