Blockchain Demo - Mining in Centralized Network using Proof of Work (TO BE COMPLETED IN JAN 2019)

By Ng Yiu Wai, January 2019

Contents

1. Introduction 1
2. Overview of System 2
3. System Design - Block & Merkle Tree Root........ 3
4. System Design - Block & Proof of Work 4
5. System Design - Blockchain 5
6. System Design - Centralized Network & Data Storage 6
7. Demonstration 7
8. Extra Information - Blockchain should be in a decentralized network 8
9. Reference........ 8

1. Introduction

Bitcoins, the most well-known blockchain network, is described as

> *" A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network.* ***The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power****. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone."*[1]

In this project, I am going to demonstrate below two properties of a proof-of-work blockchain network.

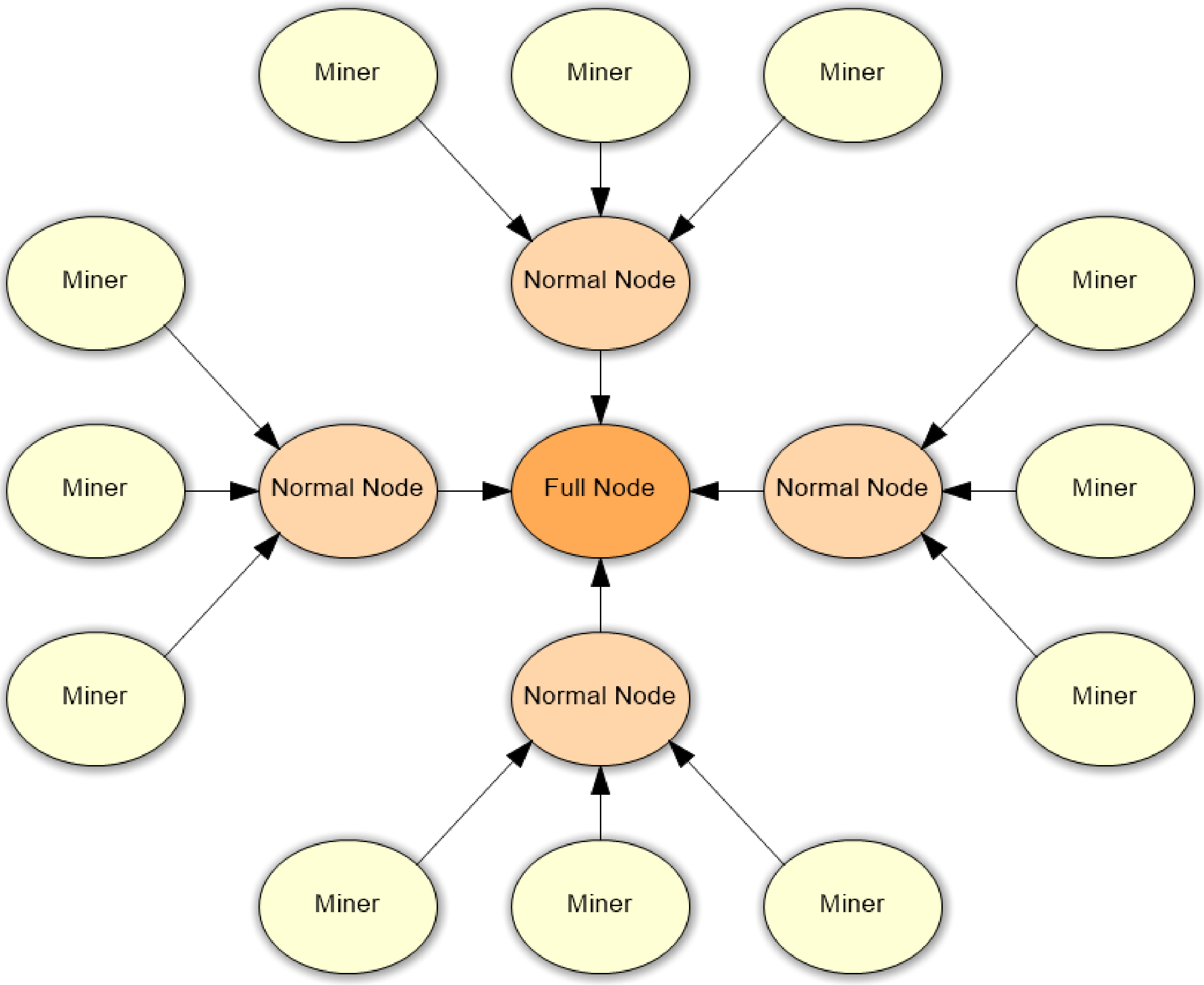
i) building a chain of blocks using hash-based proof-of-work
ii) the miner who has highest CPU power could add new blocks to the blockchain.

Some other properties of bitcoins, e.g. digital signatures, peer-to-peer network, broadcasting on a best effort basis, are ignored.

Bitcoin	This project
◆ Transactions data, which are verified using digital signature, are packed into blocks.	◆ Arbitrary strings data are packed into blocks.
◆ Data are packed into blocks using merkle tree root hash.	◆ Data are packed into blocks using merkle tree root hash.
◆ Each block could be represented by a byte stream under a pre-defined protocol.	◆ Each block could be represented by a byte stream under a pre-defined protocol.
◆ Blocks are chained using hash-based proof-of-work. It is nearly impossible to change data already added into the blockchain.	◆ Blocks are chained using hash-based proof-of-work. It is nearly impossible to change data already into the blockchain.
◆ New blocks are broadcast on a best effort basis in a decentralized network. Usually the miner who has highest CPU power could add new blocks to the blockchain.	◆ New blocks are broadcast in a centralized network. The miner who has highest CPU power could add new blocks to the blockchain.

2. Overview of System

In progress



3. System Design - Block & Merkle Tree Root

To update

4. System Design - Block & Proof of Work

To update

5. System Design - Blockchain

To update

6. System Design - Centralized Network & Data Storage

To update

7. Demonstration

To update

8. Extra Information - Blockchain should be in a decentralized network

To update

9. Reference

1. "Bitcoin: A Peer-to-Peer Electronic Cash System", Satoshi Nakamoto, https://bitcoin.org/bitcoin.pdf

This project is a rebuild of student project I works on for Hong Kong Polytechnic University COMP5311 (Semester 1 Year 2018-2019). Special thanks to Dr Bin Xiao and Mr Haotian Wu.