Distributed Trust and Blockchains		Date:	*30th September 2019*
Instructor: *Sujit Prakash Gujar*		Scribes:	Rishabh Singhal, K A Meghashree

Lecture 8: Bitcoin Mining

1 Recap

1.1 Joining Bitcoin Network

- Can join as a miner/full node or a client to receive payments
- Advantages and disadvantages of being a Thin/SPV clients
- Gossip protocol is used to join a bitcoin network. Contact a seed node, know about other nodes, contact them, choose peers and become a member of the network.
- Roles of being a bitcoin node.
  - Maintain Peer-to-Peer network
  - Maintain decentralization
  - Verify proof-of-work
  - Ensure no double spending
  - Maintain Consensus in network
  - Execute output script
- UTXO set is used to keep track of output transactions that have not been used.

1.2 Role of a Bitcoin Full Node

- Check if transactions inputs are in UTXO.
- Ensure it is not a double spend attack.
- Execute output script of input transaction along with script signature.
  - If true add it to transaction protocol.
  - If true in previous step , broadcast transaction.
  - If a transaction is repeated, do not broadcast it again (to avoid flooding).

2 The Task of Bitcoin Miners

To be a Bitcoin miner, you have to join the Bitcoin network and connect to other nodes. Once you're connected, there are six tasks to perform:

1. Listen for transactions
2. Maintain block chain and listen for new blocks
3. Assemble a candidate block
4. Find a nonce that makes your block valid
5. Hope your block is accepted
6. If all other miners do accept your block, then you profit

3 How to Solve Crypto Puzzle ?

For solving the crypto puzzle, one have to find a nonce which satisfies a given condition (to achieve a given target).

3.1 Different Strategies for Generating Nonce

For generating and checking nonces, there are two methods one is *random* and other is *sequential*. Here the generated nonces have equally likely chances of being a solution, assuming very less bias of current hash functions.

- A random nonce is produced by stringing arbitrary numbers together while a sequential nonce is produced incrementally.
- Using the sequential nonce method guarantees that values are not repeated, cannot be replayed and do not take up unnecessary space.
- However for random nonces, we need to keep a record for the tried nonces.

3.2 Nonce is a 32-bit Field

Nonce is a 32-bit field, hence one can check only 2^{32} possible combinations (or trials) but the current difficulty level of crypto puzzle requires more number of expected trials to find a suitable nonce i.e. $\sim 2^{72}$. So, even after checking 2^{32} different nonces once is not able to find the required nonce which satisfies the problem, these methods can be employed :-

- Changing the order of the transactions which in turn will change the merkle root, and try again.
- In coin-base transactions, the coin-base field (100 bytes) can be arbitrarily changed by altering any bit.

4 Bitcoin Mining Resources

As bitcoin puzzles i.e. calculating nonces achieving a certain target is a very repetitive task, computer hardware that does repetitive things quickly works best for mining. Computers can have faster or slower processors, more or less RAM, bigger and smaller hard drives, and so on. It is also true that some types of processor are better at mining than others.

4.1 Central Processing Unit (CPU)

Early when the difficulty of bitcoin puzzle was low, bitcoin clients versions allowed users to use their CPUs to mine. But as the hashrate of the network grew to such a degree, the amount of bitcoins produced became lower than the power to operate CPU.

- Miners simply searched over nonces in a linear fashion, computed SHA 256 in software and checked if the result was a valid block.

```
TARGET = (65535 << 208) / DIFFICULTY;
coinbase_nonce = 0;
while(1)
{
    header = makeBlockHeader(transactions,coinbase_nonce);
    for(header_nonce = 0;header_nonce < (1 << 32);header_nonce++)
    {
        if(SHA256(SHA256(makeBlock(header,header_nonce))) < TARGET)
        break; //block found
    }
    coinbase_nonce++;
}
```

Figure 1: CPU mining pseudocode

- It can calculate $\leq 2^{32}$ hashes per second which is very low when compared to the number of hashes required to mine 1 block (according to current difficulty) i.e. $\sim 2^{72}$.
- Millions of years will be required to mine one block hence not suitable.

4.2 Graphics Processing Unit (GPU)

Due to parallelism, GPU mining is drastically faster and more efficient than CPU mining. But still, when compared to current level of difficulty not suitable.

- Lots of parallelism
- 1.5 times speed up with 70% accuracy, net effect 5% increase
- $4 - 5$ times speed up as compared to CPU
- But still, racks of GPUs ($\geq$ 100) takes more than 1000 years to mine a block, hence not suitable.

4.3 Field Programmable Gate Array (FPGA)

An FPGA is simply a highly programmable processor. FPGAs tend to be more expensive than CPUs and GPUs but they are also quite efficient in their use of electricity. Miners who are looking to operate where electricity is more expensive can invest more money up front to buy an FPGA miner and then pay less in ongoing electricity costs.

- Customizable
- Way faster than GPUs
- Better cooling and energy efficient as compared to GPUS

4.4 Application Specific Integrated Circuit (ASIC)

It is a microchip designed and manufactured for a very specific purpose. For the amount of power they consume, they are vastly faster than all previous technologies.

- Especially designed chips for mining Bitcoins.
- At least 10x improvement over FPGA.
- One of the fastest development of ASICs for mining has happened ever in the history of ASICs.

References

[1] Chapter 5: Bitcoin and Cryptocurrency Technologies - Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, Steven Goldfeder

[2] `https://en.bitcoin.it/wiki/Mining`