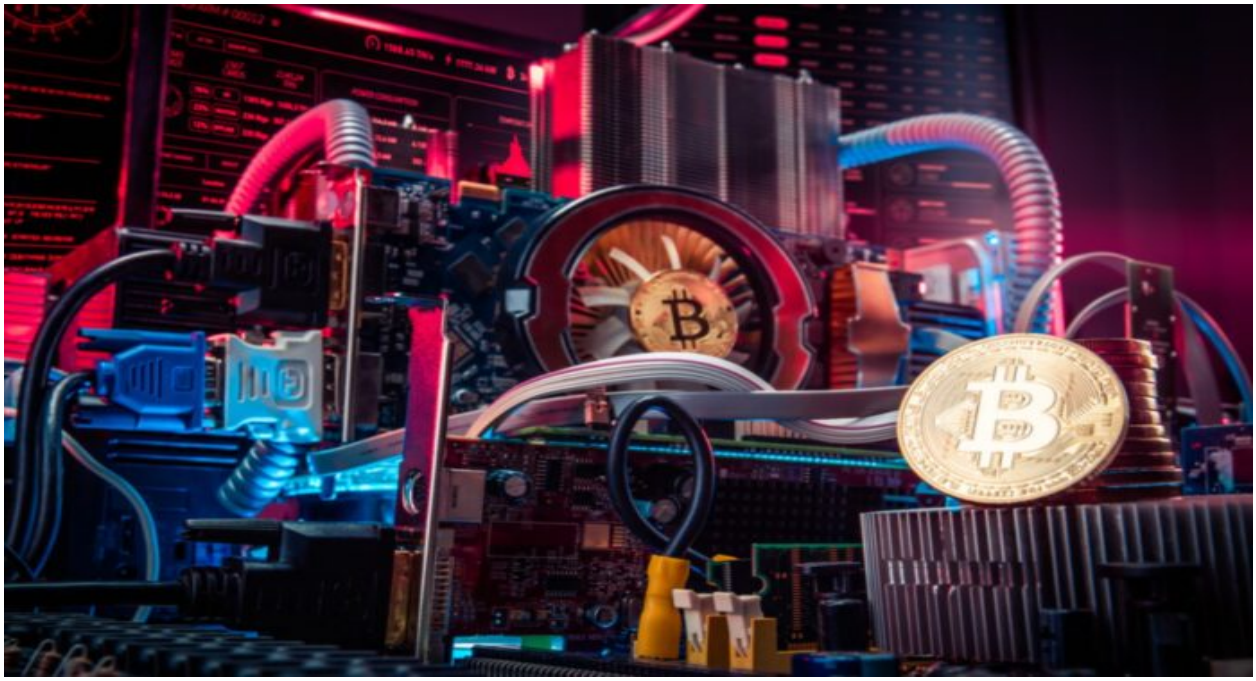
Symbiosis Institute of Computer Studies and Research

Subject : Blockchain

Topic : Crypto Mining Case Study Assignment



Name : Amal Sunil Pillai

Prn: 19030121009

Class: Div A

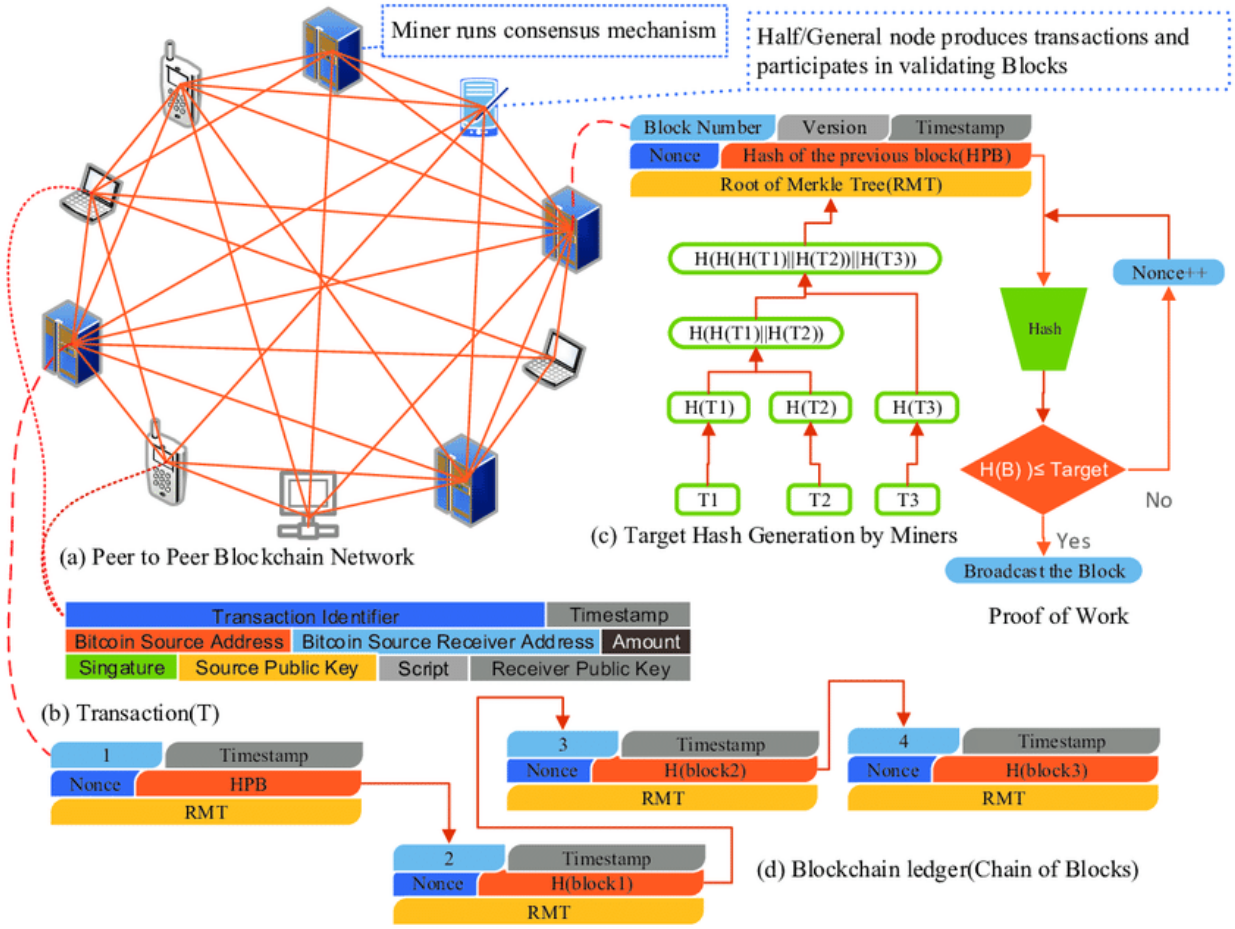
Semester : V

What is crypto mining?

Cryptocurrency mining is the process of mining the transactions in a blockchain network into a block, the miner or the people successful in mining the block is rewarded with some amount crypto for updating the blockchain network state, i.e. in simple words, adding a new block into the blockchain network by solving a computational problem is called cryptocurrency mining.

There's plenty of different types of blockchain networks and cryptocurrencies but for a detailed explanation and understanding I'll be considering the Bitcoin cryptocurrency and it's blockchain network. Bitcoin is the first and the most popular(from the value point of view) cryptocurrency in the world, every other cryptocurrency and blockchain network in the world derives its principles from the Bitcoin blockchain network, every other blockchain can be seen as a fork of Bitcoin.

The cryptocurrency blockchain network is a decentralized network, i.e. there's no central bank, no central database, or no central authority that manages the network. In blockchain we have a decentralized network with a cryptocurrency community consisting of the users(that own and transact their crypto currencies), miners(mine the transaction into block to update the state of the blockchain) and nodes(nodes is a general term that can be thought of as a computer or a database that keeps track of the blockchain history), everything in blockchain network can be thought of as a node, for example the users could be a light node or a full node, light nodes don't store the entire copy/history of the blockchain, they only keep the information that is required for the verification of the transactions(the header of the blocks in the blockchain network) that's in relation to the set of private/public keys of that node, whereas a full node keeps the entire blockchain history with it, therefore a miner is required to be a full node as its required to store the entire blockchain for the mining and verification process in the Bitcoin blockchain.



The Bitcoin blockchain in detail :

The Bitcoin blockchain architecture :

- The data inside of a block will have the transaction details (eg: from, to and the transaction amount etc.).
- Each block will have a block header and the body which contains the transactions, the block header contains :
    - Timestamp
    - Version number
    - Merkle root (the result of a tree like hash function done on the transactions)
    - Difficulty target
    - Nonce
    - Hash of the previous block

Understanding what makes the blockchain immutable:

One of the most important property of blockchain is that it's immutable, as any change made in the information contained in a block will change it's hash therefore we'll have to regenerate the hash of all the previous blocks to make it seem legit, but the number of blocks we have in blockchain is huge so changing will result in having to change all of those, basically mine each block(solve the puzzle) and add them to the blockchain which is not so difficult as there's supercomputers, ew can connect thousands of devices with us and change the hash of each block. To prevent the above scenario and make it more secure we use the concept of POW(proof of work). Everytime we change something in a blockchain or add a new block it has to be validated, without validation we cannot add a block i.e. some processing must be done to add a block. In case of Bitcoin POW says it will take at least 10 mins for anyone to add a block into the blockchain(on average) i.e. theoretically if we change 1 block and we have 5 blocks after that, it'll take 50 mins to change the entire chain, on top of that the blockchain will be stored of multiple machines. This is how blockchain gets its immutability.

Consensus in blockchain:

Suppose we have 5 mining nodes, all these nodes will have a copy of the blockchain and all the copies will be of the same state. Let's say some transactions happened and we got a new block and this block needed to be added in the block chain(in case of Bitcoin blockchain the number of transactions including the blockheader has to be below the size of 1 MB). Node 5 adds the block to the blockchain, then with the help of protocols we can just replicate this in all the nodes, but the question is what if Node 5 is a malicious node? How will we make sure that all the nodes come to the consensus and they'll have the same copy of it.
This is where in blockchain we have to follow some consensus algorithm. In the blockchain world we have so many consensus algos using which we can agree on one particular state of a blockchain, if the new block is added in a blockchain who will add it can be defined with the help of consensus.

Bitcoin uses POW to achieve the consensus. All nodes will spend some computing power doing some calculations and whoever wins in it will add the block in the blockchain(It's the miners that spent some computing power to add the block so we can trust them).
Some other consensus algos include :

- POET (Proof of elapsed time) created by intel.

- POD (Proof of deposit)
- POC (Proof of capacity)

Some important terms :

- Bitcoin address (Ownership of public and private key)
- Bitcoin wallet :
    - Is basically a software that stores all these public/private keys and lets users generate the keys etc. In the case of Bitcoin as it follows the UTXO(Unspent transaction outputs) model the wallets have the responsibility to compute the balance associated with a private key and to choose the right combination of UTXOs that must be used for a transaction etc. But from the users point of view it's just a software that helps you manage the keys, transactions that are associated with the user etc. Another important point I would like to point out is that any device that has a wallet is considered as an SPV(Simplified Payment Verification) node, in simple terms it's just a light node as I have discussed earlier, they don't store the copy of the entire blockchain but just the block headers.

- Coinbase : Called 'Coinbase' transaction, it's the first transaction in each block, inserted by the 'miner' of that block in order to reward her/himself the bitcoin incentive for mining the block(which is the sum of the freshly generated bitcoins and all the transaction fees in the block). The freshly generated bitcoins is how bitcoin generates new bitcoins into the blockchain network, i.e. it's through mining new coins are introduced in the blockchain and the bitcoin system increases the money supply(as of today it's 6.25 BTC).

- Crypto Exchanges : With example of bitcoin, a bitcoin exchange is a digital marketplace where traders can buy and sell bitcoins using different fiat currencies or altcoins, i.e. the crypto exchanges is just a online platform that acts as an intermediary between buys and sells of a cryptocurrency.

The mining process:

Transactions happen and if they're not mined into blocks, will remain as an 'Unconfirmed transaction'. I.e. everytime there's a transaction it's verified by each node(verification in the sense that it's not double spent etc) and it broadcasted to every node, every node or the miner nodes have a transaction pool(also called mempool) that contains this 'Unconfirmed transactions', when a block is mined(add the transaction into the block and then add the block to the blockchain) it becomes a confirmed transaction.

Once the block is mined(i.e. A miner on hashing the block header and finding the right nonce get's the specified number of leading zeros in the blocks hash) the miner will publish this block to all the nodes for validation, once the block is validate by the nodes it'll add the block on top of the blockchain stack(local blockchain copy).

The bitcoin network on average produces a new block every 10 mins, this is by it's design of the difficulty target. This difficulty target is set to auto-adjust depending upon how many mining nodes are at competing to mine a block, i.e. if in certain time the network has a lot of computing power or many number of miners, the difficulty target will increase making it even more difficult to find the nonce value to find the valid hash. "Nonce" is termed as number once, it's the only value we can change in the blockchain while mining the block to find the valid hash.

The target is a 256 bit number, the hash of the block has to be less than or equal to that of the target binary number to be considered has a valid hash value which is then considered as a mined block.