CSC 591 Cryptography November 5, 2018

Lecture 14 - Bitcoin

Lecturer: Alessandra Scafuro *Scribe: Fatema Olia*

What is Bitcoin?

Bitcoin is a form of digital currency called *cryptocurrency* which is not maintained by any central agency such as a bank. It is distributed over a decentralized peer-to-peer network called the *blockchain* in which no single node has control over any aspect of the network. The blockchain is considered a trustless network since every transaction on it is published in a *ledger* and every node present on the network maintains a copy of the ledger and so there is no need for any node to "trust" another node.
Bitcoin was invented by a person or group of people under the pseudonym Satoshi Nakamoto in 2008. Since then the number of cryptocurrencies has been growing with over 1900 cryptocurrencies in circulation today.

Ingredients

From the cryptography point of view, the Bitcoin blockchain depends on the following main ingredients:

1. **Digital Signatures:**
   Every transaction on the blockchain must be signed by the node that publishes it. Thus, the digital signature scheme implemented on the blockchain has the following properties:
   - Unforgeability
   - Unforgivability
   - Public Verifiability
2. **Hash Functions:**
   The transactions on the blockchain are hashed and stored in order to prevent the nodes from tampering with the contents of the transactions. Thus, the hash functions implemented on the blockchain have the following properties:
   - Collision Resistance
   - Completely Random/Unpredictable Outputs

Bitcoin Ledger:

An important aspect of the Bitcoin blockchain is the ledger. It keeps a record of all the transactions published on the blockchain. The ledger is an "append-only" file which means that new transactions can be added to it but older ones cannot be edited or deleted and so

every transaction ever published to the blockchain is present in the ledger. Any node on the blockchain can traverse through the ledger and view every transaction all the way to the first transaction on the Bitcoin blockchain.
The most important task of the nodes on the blockchain is to maintain identical copies of the ledger. Thus, before any transaction is added to the ledger, the nodes must follow a consensus protocol to ensure that every node agrees upon the same chain of transactions.

Need for Bitcoin (Philosophical Aspects)

Before the introduction of cryptocurrencies, if people wished to perform transactions or store their currency they would have to depend on institutions such as Banks. Thus, all parties involved would have to "trust" the Bank to securely and accurately complete transactions and keep record of every individual's wealth and proof of transactions. This means that the Bank is the central node on this network and if the Bank is compromised then so is the entire network and all the data could be tampered or lost. As a result Banks could be considered unreliable.
To overcome these shortcomings, Bitcoin introduced a form of currency with in which:

- There is no single trusted entity.
- Every node contains an identical copy of the Bitcoin ledger through consensus.
- All transactions are stored on the Bitcoin ledger.
- Every node on the network can read the ledger, i.e. there is complete transparency with respect to the transactions on the network.

Working of Bitcoin (Technological Aspects)

In a general sense, each node on the blockchain can generate transactions to transfer Bitcoin to other nodes. Each node must sign their transaction with a digital signature. Some nodes on the blockchain are *miners* who collect the transactions and group them together form *blocks*. These blocks are then added to the blockchain in an order that is determined by consensus of the nodes. Once a block is added to the blockchain then a transaction is considered completed and it cannot be undone.

We can elaborate on the working of the Bitcoin blockchain as follows:

Generating and Signing Transactions

Each node on the blockchain is identified by an address. This address has two parts: private and public. The public address is what a node is publicly identified by on the network and it is shared with everyone. The private address is used by the node to access the account, and generate and sign transactions. To generate a Bitcoin transaction, a sender requires the public address of the receiver and must sign the transaction with their private address. Whenever a node generates a transaction they must sign it to prove that they have initiated

the transaction. Digital signatures make transactions on the blockchain unforgeable and verifiable. The Bitcoin blockchain utilises the Elliptic Curve Digital Signature Algorithm (ECSDA) to implement digital signatures. It consist of:

- Private Key: This is the private part of the address. It is 256 bit integer.
- Public Key: This is the public part of the address. It is calculated from the private key and is also used to determine if a signature is genuine. Compressed public keys are 33 bytes and the older uncompressed keys are 65 bytes.
- Signature: It is a hash generated of the transaction to be signed. The public key is used to determine if the hash was generated using the original transaction and the private key.

Block Generation

Once the transactions have been generated they need to be added to the blockchain. There are certain nodes on the blockchain called *miners* that complete this task. The miners gather the transactions submitted, validate them, and combine them to form a block. The number of transactions in a block on the Bitcoin blockchain is such that the block size is usually below 1MB. Once these blocks are generated, they are added to the blockchain.

Mining

Since the Bitcoin blockchain is an extremely expansive network there are a large number of blocks generated at any given point in time. To maintain an identical blockchain in each ledger it is necessary for the nodes on the network to come to a consensus about the order in which the blocks are added to the blockchain. This is done by the miners through a process called *mining*. For a block to be added to the blockchain, a miner must first show proof of work.

Proof of Work: Once a miner generates a block then the miner must solve a puzzle. This puzzle is a hard mathematical problem that will take significant time and processing power to solve. Once a miner solves this problem, it is considered to be the proof of work done by the miner and the block is considered mined. In the Bitcoin blockchain, the problem is as follows:
Consider B as the block to be mined and H to be the hashing function to be used. The miner needs to find x such that, $H(B, x) = 0^k || *^{n-k}$
Where, the first half is k zeros concatenated with any $(n - k)$ values.
This hash basically generates an n bit value of which the first k are only zeros.
$Pr[\text{finding } x] = \frac{1}{2^k}$
k is considered to be the difficulty parameter. The value of k and the size of the block depends on the network delay.
The has function H used in Bitcoin is SHA256 since It is optimization free, progress free and parameterisable

Once the block has been mined, the miner adds it to the blockchain and passes along

this information. Accordingly, the nodes around add this block and forward the information. In this way everyone maintains a single copy of the blockchain.
However, it is still possible that different blocks have been added by nodes before this information was received. This results in a fork in the blockchain and different nodes end up working on different paths of the fork. To resolve this, the longer chain is preserved and blocks on the shorter one are orphaned and their transactions are lost. Thus, a transaction on the blockchain is considered valid only after it is at least 6 blocks deep in the chain.

Incentives: In order for the miner to honestly mine blocks they receive certain incentives. Nodes engaging in transactions can add a coinbase transaction at the top of their block as incentive for miners to mine their transactions. Also, miners earn Bitcoin for every block they mine.

Security

The Bitcoin blockchain is considered extremely secure since the transactions cannot be tampered with once they are added to the blockchain. This is due to the hashing algorithms involved when generating blocks. When a new block is generated, a hash of the last block in the blockchain is computed and it is appended to the end of the block along with the value of x generated during mining. This makes it secure because if even one value on any block in the chain is tampered then the hashes at the end of every block that proceeds it will not tally. Since the ledger is completely transparent, all the nodes would detect the tampering.

Vulnerability: Double Spending Attack

Although the Bitcoin blockchain is considered extremely secure, a possible attack called the *Double Spending Attack* has been theorized. In this attack, the dishonest party publishes a transaction in a block and adds it to the last block on the chain. Then the dishonest party generates another chain from the same last block which is longer than the current chain and publishes it. Since the longest chain wins the original transaction would be orphaned. However, the receiver of that transaction might have considered it valid.
For example consider a sender A sending Bitcoin to a receiver B. This transaction is published by A and after it is 6 blocks deep it is considered valid by B. However, A could simultaneously mine a longer chain and publish that without the block containing the transaction from A to B. Then all the nodes would consider this chain to be valid since it is longer and the original transaction would be orphaned. So eventually B would not receive the Bitcoins from A even though they might have assumed they have.

This attack however is not feasible. If the dishonest party controls less than 50% of computing power on the blockchain then the probability of block replacement decreases exponentially fast as blocks are added to the chain. Since it is unlikely that the honest parties would have less than 51% of the computing power, the chain being worked on by the honest parties will always be longer than the substitution chain being generated by the adversary.