**Cryptocurrency – Bitcoin**

There are a large number of cryptocurrencies: ethereum, ethermine, Monero, Zcash, aion, Pascal, Dash, Litecoin and Bitcoin being the most popular and widely used/supported cryptocurrencies around the world. All cryptocurrencies work in a similar way, and are built off of the Bitcoin protocol. Bitcoin being the first ever cryptocurrency was built by an anonymous programmer who goes by the name “satoshi nakamoto” on Github.

Bitcoin was designed 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”, satoshi implied that banks where flawed, they are vulnerable to attack, and rather than putting your trust into a bank to guard your money, he proposed an idea that would allow you to put that trust into hashing (what is hashing? hashing is a one way process that takes data, then uses bitwise operators to manipulate the data: e.g. changing the order of bits, removing/adding new data, etc. to create an output value that is impossible to trace back to the inputs).

As quoted from bitcoin whitepaper: “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 method of taking timestamps, unique wallet address of sender/receiver, transaction amount, hash of the previous hash in the chain and hashing them is the block chain. Anytime anyone makes a transaction (e.g. sending virtual money from one user to another), there transaction is appended to the block chain and becomes a permanent record.

Every single person that uses the cryptocurrency has a copy of the block chain, this makes it nearly impossible to hack/cheat money, as your copy of the chain has to match everyone else’s inorder for you to append transactions. Cryptocurrencies are foolproof by design, apart from one small problem: what if you had multiple chains being used in the same network, the legit chain and one fake one created by an attacker. There can only be one chain so how does your bitcoin software know which chain to append to and which to ignore? Satoshi said: “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 longest chain is the one which is used. So the only way to cheat bitcoin would be to have a super computer more powerful than the combined processing power of every bitcoin miner in the world, in order for you to create a longer chain because you would have to redo all of the chains proof of work.

why do miners exist? Satoshi realised that in order for bitcoin to be secure, he need lots of powerful computer to be running and doing proof of work, obviously no one would contribute there processing power unless there was some reward involved. So just like a job, miners are rewarded a small amount of money for each hash they produce. The rewards are randomly given to users on the network and only given once a “block” is mined (currently a block is around 2,440,643 \* 2^32 hashes in size). Currently miners have a chance of earning money about every 10 mins.

What is a pool? A pool is a group of miners working together. Mining a single block on your own is very time consuming and just not possible for most miners. So pools where created, a single leader will distribute workload to every miner in the pool. Once the required number of hashes is reached (e.g. the block is mined), the leader will breakup and distribute the reward (money) to each miners accordingly to the amount of work they have contributed. By working together and breaking up workloads, miners can be rewarded quicker.

Sources:

Official bitcoin whitepaper (it’s like an RFC): <https://bitcoin.org/bitcoin.pdf>