Kasper Borgbjerg
kasperib@uio.no

Bitcoin

From the get-go, let's start of by touching upon bitcoin and some of its history to continue with some of the more technical complexity of it and its architecture as a blockchain technology in an easy language.
Bitcoin, the creation of Satoshi Nakamoto is a decentralized network and currency that is based on blockchain technology. Bitcoin was first launched in 2009 with its whitepaper launched just a handful of moths before in 2008. Satoshi Nakamoto, who is this person or persons? The identity of Nakamoto has been hidden forever, and it is still up till this day unknown who this person or group is. The identity Nakamoto was the first "miner" on the blockchain network and mined the genesis block (very first block of a blockchain) and was active on forums and different blockchain sites in the aftermath of bitcoins launch, in order to spread the word.

Many people from the public and media saw the launch of this technology as a reaction (possible cure?) to the financial crisis that broke out in the US in 2008. Why is this? Well, Bitcoin is a digital cryptographic currency that is based on a blockchain technology. The keywords here are cryptographic currency and blockchain technology – these two terms combined give bitcoin its characteristics of being a decentralized, permissionless and a trustless network. The bitcoin network is just a network of replicated state machines that continuously communicate with each other to ensure that the communication that is exchanged, the transactions, are valid and secure.

The blockchain technology has its name from how the underlying technology works, a chain of blocks that in total constitute the truth of the network. Every block in the network contains 1mb of transactions, that is data of who are taking with each other. Every block has a cryptographic hash pointer to the last block in the network, e.g., they are chained together. And is secured in that way. Every node that is running the network, has a ledger that contains the whole blockchain.

The security of the network is based on the consensus mechanism that governs the network, a proof-of-work consensus mechanism. The nodes that perform this consensus on the blocks are called miners. Miners are verifying transaction on the network and puts these into the last block on the chain. When a block is full of transactions, new one must be created in order for the chain to continue. Miners participate in a cryptographic raffle where each miner must compute an algorithmic equation, sha256 hash function, aiming after getting a number that is below a target set. The miner who first computes the target number is the one who is allowed to put the new block on the chain and is rewarded with a certain number of bitcoins. Since the algorithmic equation are extremely energy demanding in terms of power and hardware, this is actually one mechanism to how bitcoins holds in value in fiat price, although bitcoin is not pegged to the global electricity price.