# Blockchain

* Video 1
* Blockchain is chain of blocks that contains information
* Originally intended to timstamp digital documents so it's not possible to tamper with them
* Satoshi Nakamoto adapted it in 2009 to create digital cryptocurrency Bitcoin
* Blockchain is a **distributed ledger for recording transactions.**
* Each block contains Data, Hash of block and hash of prev block
* Data inside block depends on which type of blockchain it is.
* Hash is unique is fingerprint
* Changin something inside block will change its hash too
* The first block is genesis block
* Chaging any block’s hash in between of chain will break chains validity. But someone can once again easily calculate hash for all subsequent blocks again and make that chain valid
* Here it comes the story of PRoof of work
* Proof of work is mechanism that slows down creation of new block
* Blockchain used peer to peer network
* When someone joins he gets full copy of blockchain
* Someone creates new block, that block is sent to everyone on the network
* EAch node then verifies block to make sure it hasn’t been tampered with
* IF everything checks out each node adds this block to their own blockchain
* SO to successfully tamper with a blockchain you’ll need to tamper with all blocks on chaing, redo the proof of work for each block and take control of more than50% of the peer to peer network.
* **Smart contracts**: This contracts are simple programs that are stored on blockchain and can be used to automatically exchange coins based on certain conditions
* How does bitcoin actually work
* - It is a fully digital cryptocurrency with no government to mandate or no bank to authorize transaction
* - Ledger – trust + cryptography = cryptocurrency
* Digital signatures – Idea behind this is it should be infeasible to forge signatures
* Way it works it – Everyone creates a public key and a private key
* A digital signature is much stronger concept compared to physical signatures because it changes for different messages (Public key)
* Look at this as a function sign(message, privatekey) = Publickey
* Idea was to build a signature that much strong it should be infeasible to know signature if you don’t know secret key
* There should be no better strategy than guessing and checking, this is 2^256 possible signatures we are talking about
* Which ledger is correct – Solution offered by bitcoin – Trust ledger with most computational work put into it
* SHA256 – Our proof of work
* A transactions is valid only if it has sign on it and block is valid only if it has proof of work
* Bitcoin each block is limited to 2400 transactions
* **Smart contracts**
* A tiny computer program that is stored inside a blockchain
* With smart contracts we can remove need of third parties
* Sockets in operating system
* Used for communication in client server system
* A socket is defined as an endpoint for communication
* A pair of processes communicating over a network employ a pair of sockets – one for each process.
* A socket it identified by IP address concatenated with a port number
* The server waits for incoming client requests by listening to a specified port. Once a request is recieved, the server accepts a connection from the client socket to complete the connection.
* All ports below 1024 are considered well known; we can use them to implement standard services
* Servers implementing specific services listen to well known ports ( a telnet sever listnes to port 23, ftp – 21, a web or htpp – 80)
* Host <-> web server
* Port number some arbitary greater than 1024 <-> upto 1024
* Different processes – different socket – different port numbers
* Socket by gatesmashers
* Socket (domain, type, protocol)
* {server}
* bind() - Associating socket adress (IP + port number = 32bit + 16bit = 48bit)
* Listen() - Passive mode waiting by server, pending requests are stored in queue
* Accept() - Connection established
* {client}
* Connect() - server socket address
* Listen establishes connections after connect
* Close()
* OSI model