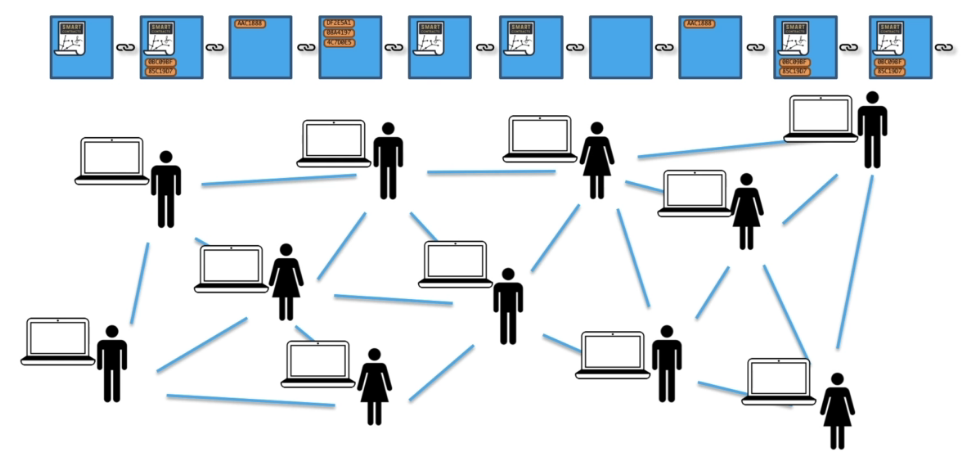
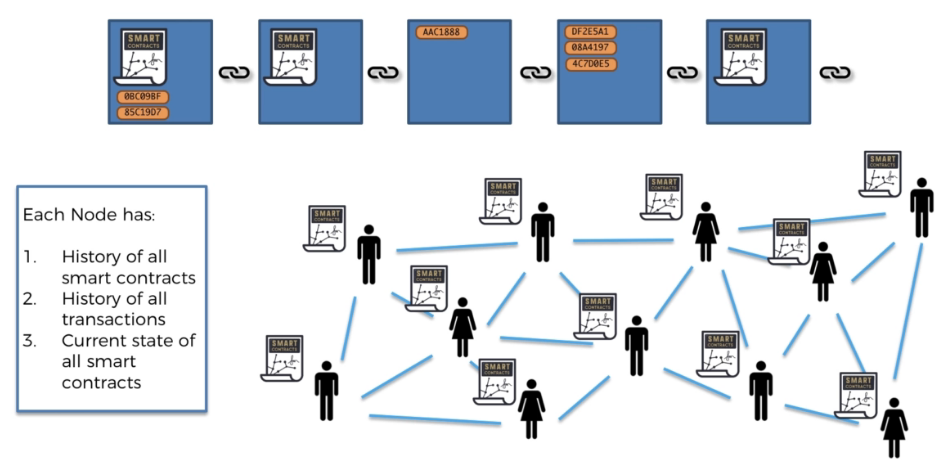
***What is Ethereum?***

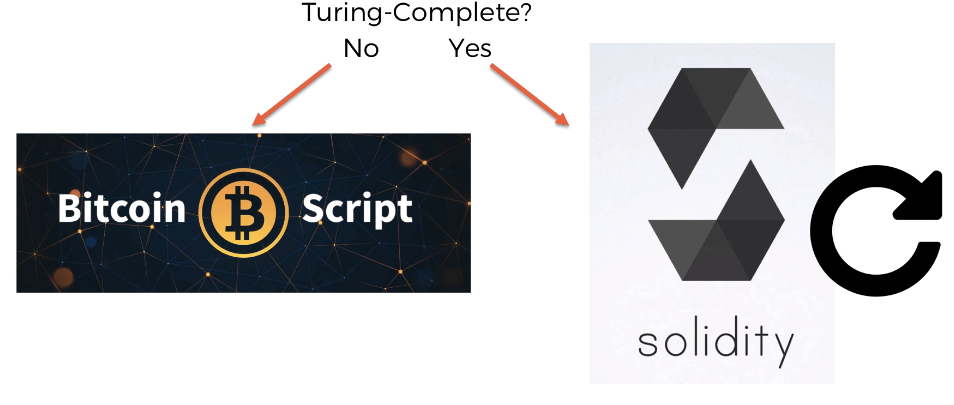
Ethereum tries to create an application that runs on decentralized network. Means that every one of us will execute the program, not as Facebook where everything relies on 1 single server.





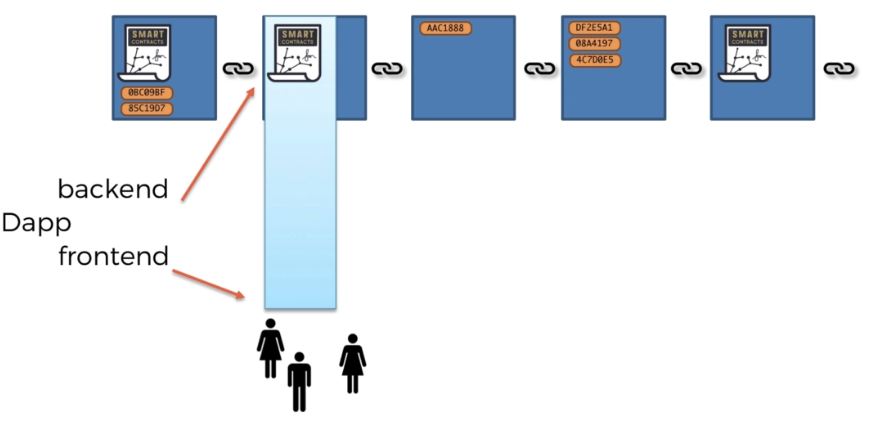
***What is Smart Contract?***

Difference between Bitcoin Script and Solidity is that Solidity is Turing-Complete while Bitcoin Script is not. The reason is because Solidity has loops.



***Decentralized Applications (DApps)***

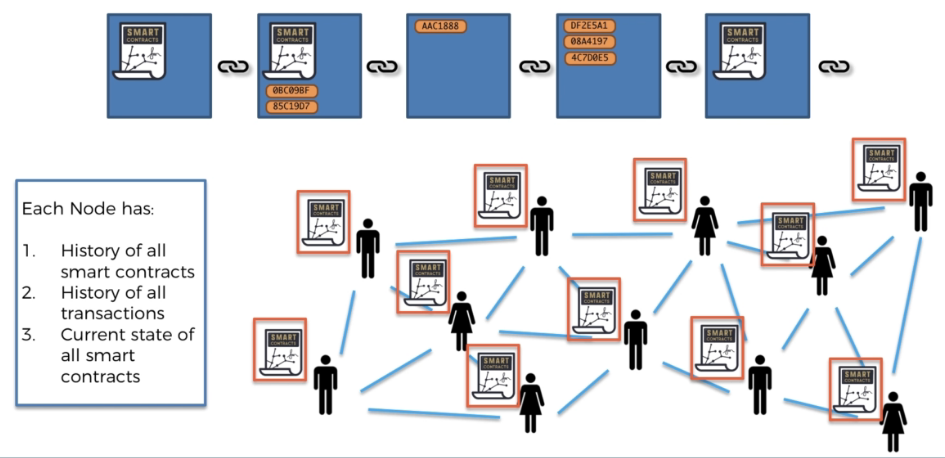
A Dapp contains an interface for people to interact with something on the blockchain. So smart contract is like an API (application programming interface).



***Ethereum Virtual Machine & Gas***

Two security threats to blockchain:

* Viruses and access to private files
* Infinite loops



Solution to threat 1:

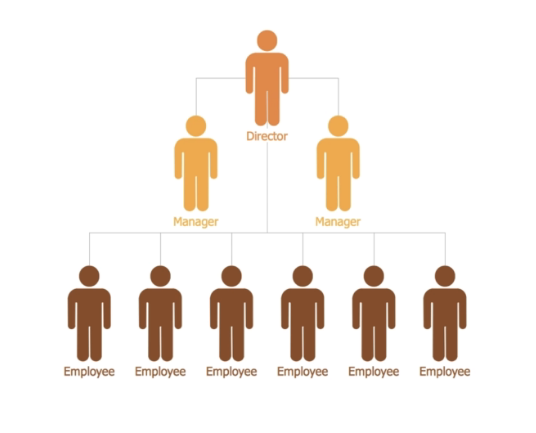
* EVM (Ethereum Virtual Machine) is a virtual machine that is running on your computer and therefore completely encapsulates everything that runs there.

Solution to threat 2:

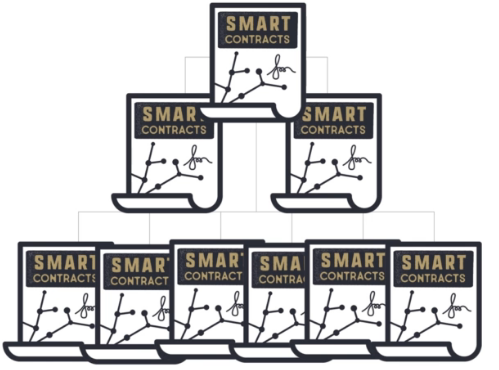
* For any computation that’s run on the blockchain, the developers of smart contract to pay. It encourages people to write efficient code, because the cleaner your code, the lower gas you pay.

***Decentralized Autonomous Organizations (DAOs)***

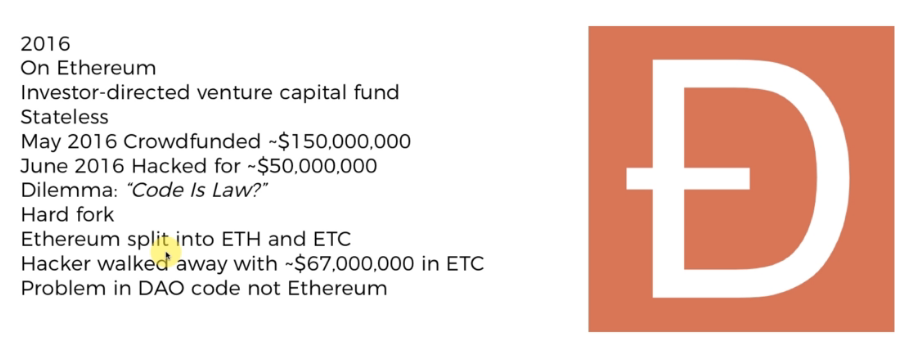
All of these people do certain things to make the company operate. They follow certain PROCEDURES.



How about we can create an organization where people don’t have to be doing this. This is all done automatically. That brings in the notion of smart contract. => We have an organization that is running itself. => That is what DAO about.



***The DAO Attack***

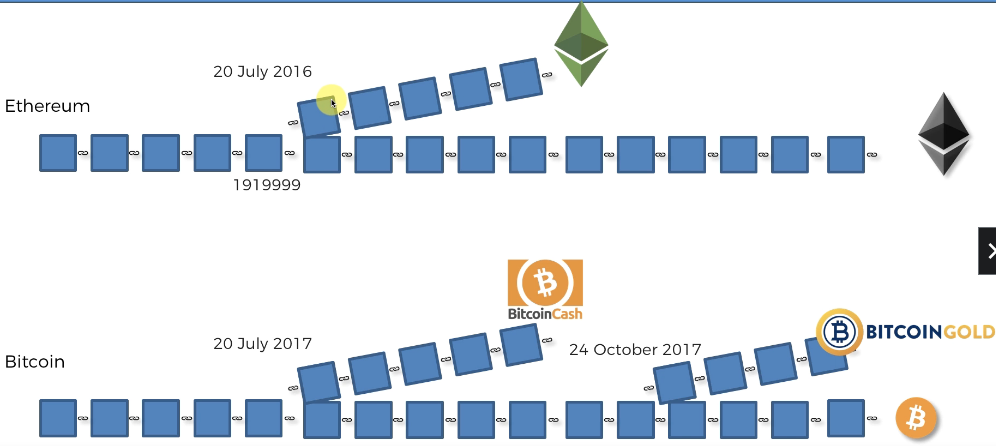


***Soft and Hard Forks (Part 1)***

For the DAO attack, most of the people agree on the hard fork to return the amount of money to the owner. However, some of the people still want to retain the concept of blockchain (cannot change), so they hard fork to Ethereum Classic.

For Bitcoin, 20 July 2017, they hard fork to BitcoinCash because some people don’t agree on the segregated witness concept (signature transfer in different message system). On 24 October 2017, some miners don’t like A6, they want to move back to GPU miner so they hard fork again to BitcoinGold.

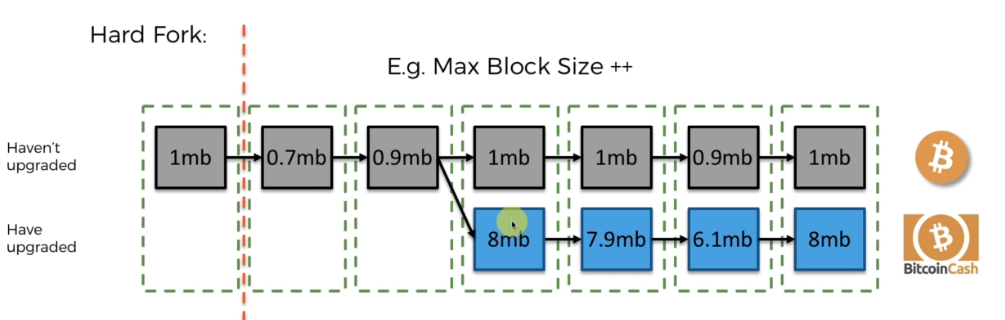
If you hold $100 at the beginning, then after the fork you will have $100 in Ethereum Classic AND $100 in Ethereum because the history is shared.



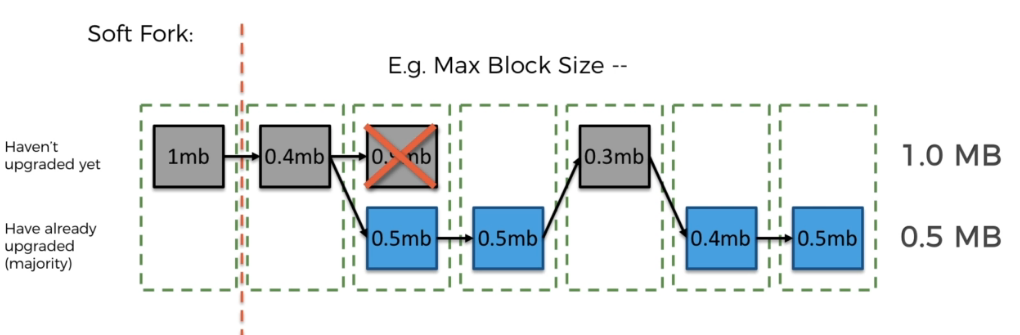
***Soft and Hard Forks (Part 2)***

Hard Forks = Loosen Rules (not backwards compatible)

Soft Forks = Tighten Rules (backwards compatible, all miners will be forced to upgrade eventually)



*Hard fork:* Before updated, everyone is on the same chain, and as soon as there is a situation where something in the new rules which are broader, looser and it doesn’t fit in with the old network, there would be a split.



*Soft fork:* Before updated, everyone is on the same chain. So when we have a chain split, but we have the majority of miners in the 0.5MB chain, they are likely to mine a new block (0.5mb), then the old block of the 1MB chain will get rejected (longer chain wins). Eventually, the 1.0MB will get rejected more because they are minority => they will be forced to move to the new group.

***Initial Coin Offerings (ICOs)***

For ICO, the company will sell coins that will be later used on their products whereas IPO will have share of company.

