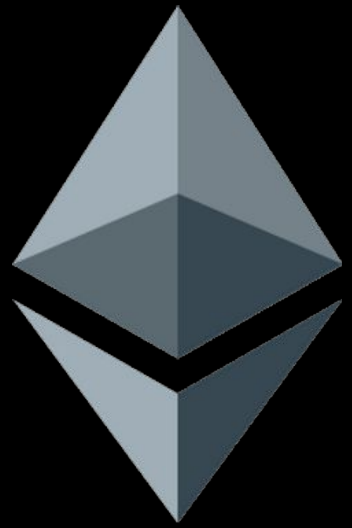


Building your own Blockchain

(one block at a time)

ABDUL WASAY | ANKUSH PATHAK

MIT Kothrud, 08 / 10 / 2018

Distributed Ledger Technology

- Are cloud based systems decentralized?

  Not really. There is decentralization in terms of hardware but application level centralization still exists.

- We are currently witnessing a transition from traditional centralized systems and processing to decentralized architectures.

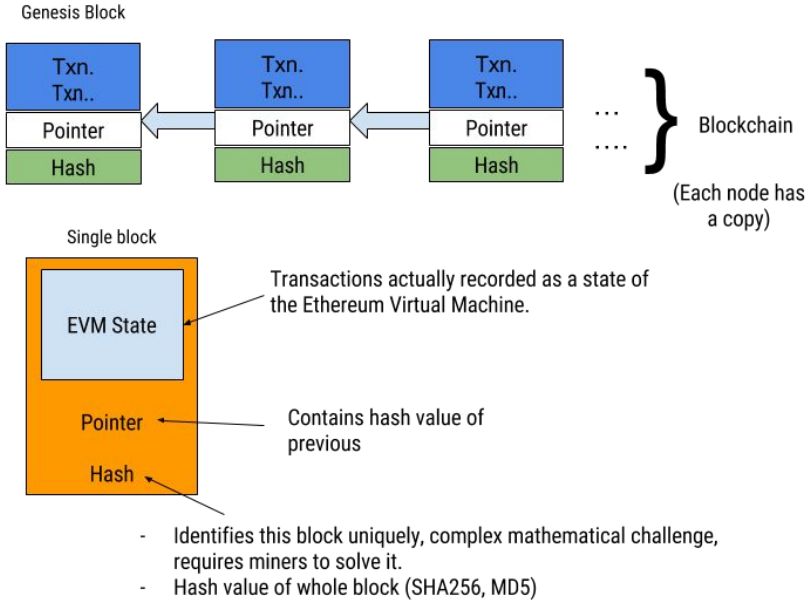
"Decentralized systems give explicit control of digital assets to end-users and remove the need to trust any third-party servers and infrastructure".

-Muneeb Ali, The next wave of computing

(https://medium.com/@muneeb/the-next-wave-of-computing-743295b4bc73)

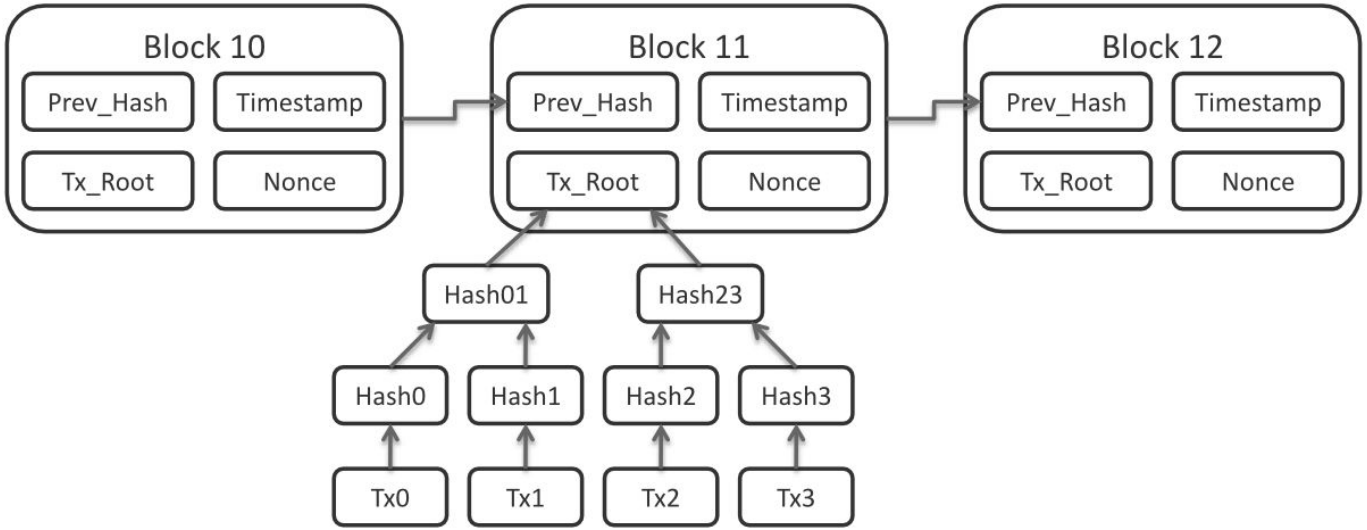
The Blockchain

- **Blockchain** is a subset of distributed ledger technologies, which constructs a chronological chain of blocks, hence the name 'block-chain'.
- A **block** refers to a set of transactions that are bundled together and added to the chain at the same time.

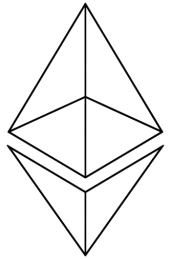


Merkle Tree (or Binary Hash Tree)

- A Merkle tree summarizes all transactions in a block thus acting as an anti tamper mechanism ensuring that the data in the large dataset has not been changed.



Ethereum

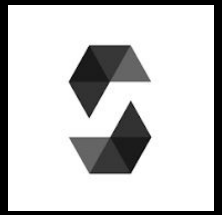


- Founded by Vitalik Buterin.
- Intended to be a robust platform allowing developers to build blockchain applications or dapps .
- White paper titled “ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER” released in 2013.
- Broke into the mainstream in early 2017 when the price of Ether jumped by 1000 percent over the course of a few months.

Strengths over the Bitcoin blockchain

VS

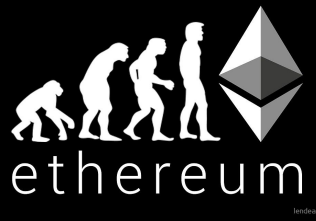
- **Addresses limitations of the scripting language implemented in Bitcoin**
  - Lack of Turing-completeness: loops for example are missing.
  - Value-blindness: no fine grained control over the amount that can be withdrawn.
  - Lack of state: binary behavior of tokens; inability to build multi stage contracts or scripts.
  - Blockchain blindness: blind to nonce, timestamp and previous block hash.
- **The philosophy:**
  - Simplicity: Be simple even at the cost of some data storage or time inefficiency
  - Universality: Complete control over the Ethereum blockchain through the scripting language
  - Modularity: Innovations are implemented as separate, feature rich libraries
  - Non discrimination and non censorship: No restriction on specific categories of usage



Terminologies

(what does all that jargon mean anyway?)

Consensus algorithms in Ethereum



Frontier

July 2015

Homestead

March 2016

Metropolis

Byzantium (Oct 2017)

Constantinpole (Oct 2018)

Serenity

TBD

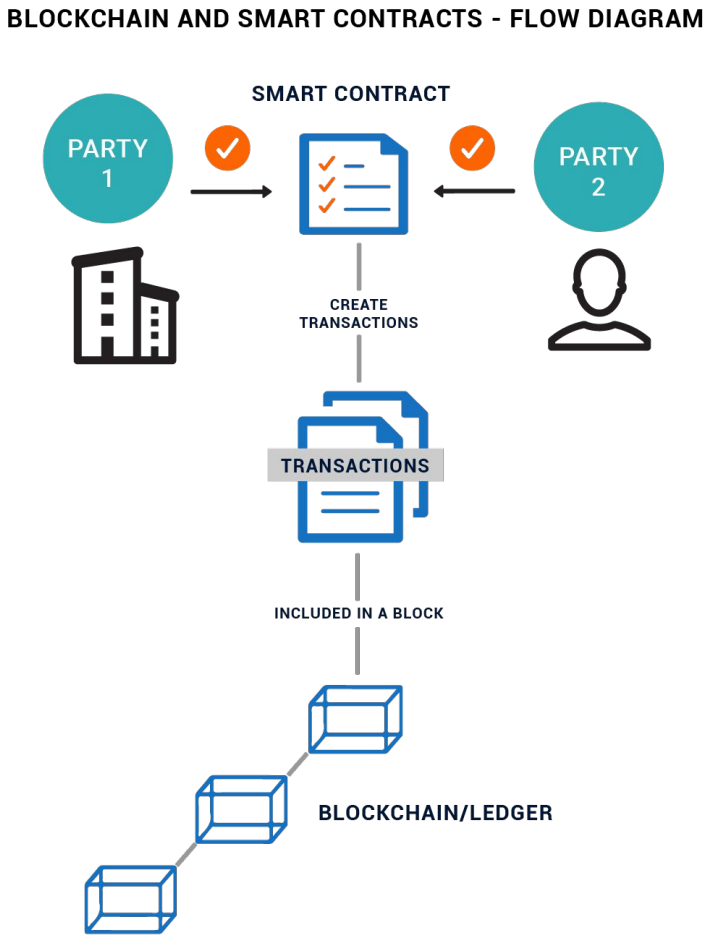
Switching to the Casper protocol

Proof of work

Proof of stake

Smart Contracts

- They define how and what kind of operations will be allowed on the ledger.
- Can be thought of as simple computer programs that execute predefined actions when certain conditions within the system are met.



- **Ethereum Virtual Machine:**

  Designed to serve as a runtime environment for smart contracts based on Ethereum. Every node in the network runs their own implementation of the EVM.

- **Solidity:**

  A statically typed, contract based high level programming language. All Ethereum smart contracts are written in Solidity.

Gas

- Gas is the metering unit for the Ethereum “World Computer”
- It is the execution fee paid for every operation processed by Ethereum nodes.
- Every operation has a Gas cost (Eg: ADD: 3 Gas, MUL: 5 Gas)
- The fee to be paid is measured by Gas price. The formula is:

```
(startGas - remainingGas) x gas price
```

An example*

	Gas consumed by operation	Gas remaining
Start of transaction		150
STORE 31	45	105
ADD 2 numbers	10	95
STORE sum	45	50
End of transaction	The number 31 and the sum is stored and written to the blockchain.	

Assuming Gas price is set to 0.02μETH

The originator pays the miner a fee
= (150 - 50) × 0.02μETH
= 2μETH
= 0.000002 ETH.

*all values are hypothetical


ether

Hands on

let's Connect!

abdul_wasay@persistent.com

wasaya@acm.org

ankush_pathak@persistent.com

ankushvpathak@acm.org