**Bitcoin - A Popular Blockchain Deployment**

With the invention of the peer-to-peer (P2P) cash system known as Bitcoin in 2008, we have an example of a global decentralized payment network with a distributed and publicly-owned infrastructure, operating as a 'permissionless' system.

One can send and receive bitcoins anywhere in the world in a completely P2P manner, *without having to intermediate through a trusted third party, such as a bank*.

And so, why were Bitcoin and Ethereum created? What problems do they solve?

* So, Bitcoin was first launched in January of 2009, as a response to the global financial crisis at the time.
* Part of the motivation for the system was to be able to transfer value over the internet, without an intermediary.
* So, one of the biggest inventions and problems that it solved was that of the 'double spend' problem.
* So, Bitcoin, in fact, is programmable money.

Ethereum, on the other hand, was created as a response to Bitcoin.

While Bitcoin is focused upon transferring monetary value between parties, it has a very limited programming language.

The core invention of Ethereum is it's EVM, or Ethereum Virtual Machine.

The EVM runs on the Ethereum network, and it runs a Turing-complete software.

"Ethereum is an open blockchain platform that lets anyone build and use ***decentralized applications*** that run on blockchain technology".

However, Ethereum may be defined as an open source platform that enables developers to build and deploy both smart contracts and decentralized applications, also known as Dapps.

As of October 2017, Ethereum had a [market cap](https://coinmarketcap.com/currencies/ethereum/) of over $28 billion, making ether the second most valuable cryptocurrency after Bitcoin.

**Peer-to-Peer Network Architecture**

**Peer-to-peer** (P2P) networks consist of computer systems which are directly connected to each other via the Internet, without a central server.

P2P networks are generally considered to be more secure than centralized networks, as they do not have a single *point of attack*, as in the case of a server-based network, where the security of the entire network can be compromised if the central server is successfully attacked.

Permissionless P2P systems do not require a set amount of peers to be online and are generally slower.

Permissioned P2P networks have to guarantee uptime and require a high level of quality of service on the communication links.

What is a Peer-to-Peer network, and how do peers come to agreement about what is on the blockchain?

Consensus is a process whereby the peers synchronize the data on the blockchain.

There are a number of consensus mechanisms or algorithms.

1. Proof of Work.
2. Proof of Stake.
3. Proof of Elapsed Time

* Bitcoin uses Proof of Work,
* While Ethereum uses Proof of Work currently, but is moving towards Proof of Stake.
* The Hyperledger Sawtooth uses Proof of Elapsed Time.

**Consensus Algorithms**

**Consensus** in the network refers to the process of achieving agreement among the network participants as to the correct state of data on the system.

Consensus leads to all nodes sharing the exact same data.

A **consensus algorithm**, hence, does two things:

1. it ensures that the data on the ledger is the same for all the nodes in the network, and,
2. in turn, prevents malicious actors from manipulating the data.

The consensus algorithm varies with different blockchain implementations.

While the Bitcoin blockchain uses Proof of Work as the consensus algorithm, other blockchains and distributed ledgers are deploying a variety of consensus algorithms, like

* the Proof of Stake,
* Proof of Burn,
* Proof of Capacity,
* Proof of Elapsed Time, and many others, depending on their unique requirements.

**Proof of Work (PoW)**

The Proof of Work consensus algorithm involves solving a computational challenging puzzle in order to create new blocks in the Bitcoin blockchain.

The process is known as 'mining', and the nodes in the network that engage in mining are known as 'miners'.

The incentive for mining transactions lies in economic payoffs, where competing miners are rewarded with 12.5 bitcoins and a small transaction fee.

"Proof-of-work (PoW) is the outcome of a successful mining process and, although the proof is hard to create, [it] is easy to verify."

For better understanding, please consider the following example

"(...) guessing a combination to a lock is a proof to a challenge. It is very hard to produce this since you will need to guess many different combinations; but once produced, it is easy to validate. Just enter the combination and see if the lock opens".

Multiple criticisms exist for the PoW consensus algorithm.

* PoW requires a huge amount of energy to be expended
* PoW has a high latency of transaction validation
* In terms of the network security, PoW is susceptible to the '51% attack', which refers to an attack on a blockchain by a group of miners controlling more than 50% of the network's computing power.

**Proof of Stake (PoS)**

The Proof of Stake algorithm is a generalization of the Proof of Work algorithm.

In PoS, the nodes are known as the 'validators' and, rather than mining the blockchain, they validate the transactions to earn a transaction fee.

There is no mining to be done, as all coins exist from day one.

Nodes are randomly selected to validate blocks, and the probability of this random selection depends on the amount of stake held.

The PoS algorithm saves expensive computational resources that are spent in mining under a PoW consensus regime.

**Proof of Elapsed Time (PoET)**

Hyperledger's Sawtooth implementation is an example of PoET at work.

Instead of competing to solve the cryptographic challenge and mine the next block, as in the Bitcoin blockchain, the PoET consensus algorithm is a hybrid of a random lottery and first-come-first-serve basis.

In PoET, each validator is given a random wait time.

"The validator with the shortest wait time for a particular transaction block is elected the leader."

This "leader" gets to create the next block on the chain.

**Proof of Authority (PoA)**

Proof-of-Authority (PoA) is a consensus algorithm which can be used for permissioned ledgers. It uses a set of 'authorities', which are designated nodes that are allowed to create new blocks and secure the ledger. Ledgers using PoA require sign-off by a majority of authorities in order for a block to be created.

Dapps

Ethereum applications are developed on the decentralized consensus-based network itself, third-party censorship is virtually impossible. Malicious actors cannot secretly tamper with the application by changing the code and compromise all application users (or nodes that are actively interacting with it). These *Decentralized Applications* have come to be known as **Dapps**.

The Ethereum network is a distributed global public network, which means it is not run on central servers in a certain geographical location. Instead, the computing power that runs the network is contributed by nodes that are spread across the globe. In other words, Dapps have 'zero downtime' - they never go down and, in general, cannot be switched off.

Since they are cryptographically secured, Dapps are referred to as 'secure applications'. Some of the [high profile Dapps](http://www.ethdocs.org/en/latest/introduction/web3.html) built on the Ethereum platform include:

* **Augur**, which is a Decentralized Prediction Market. Learn more at <https://augur.net/>.
* **Digix**, which tokenizes gold on Ethereum. Learn more at: <https://digix.global/>.
* **Maker**, which is a Decentralized Autonomous Organization (DAO). Learn more at: <https://makerdao.com/>.