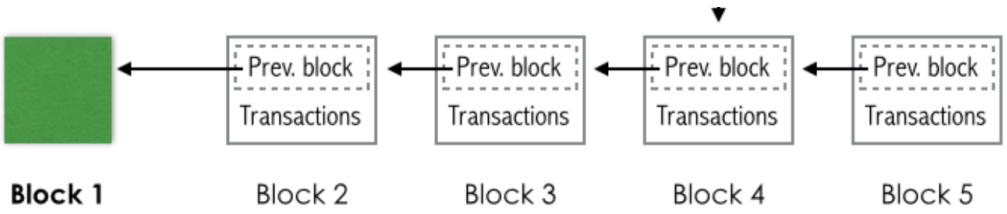
Understanding Blockchains

Arpit Mathur (@arpit)

Trust is a basic requisite for commerce. We trust banks with our money, trusting that we'll be able to access it when we need it. Services like Amazon, Uber and AirBnB do not provide any products directly but we pay them trusting that the services they guarantee will be delivered appropriately. Blockchains have a potential to disrupt the current state of affairs by providing trust at a technical infrastructural level instead of at an institutional level. Data and agreements recorded on the Blockchain are permanent and rules for interacting with the Blockchains are simple and well defined thereby increasing efficiency and reducing cost. Additionally, since the system is entirely digital, the agreements can involve not only people but connected devices as well. For example, a smart-lock can conditionally lock or unlock a door based on a financial transaction on a Blockchain.

A Blockchain is a datastore similar to a database. However, unlike typical databases which run on individual servers, Blockchains are a distributed system that is managed by a network of computers. Each node on the network maintains a copy of the blockchain making it extremely fault tolerant.

The data in a Blockchain is held in a series of **Blocks**. Each Block references the hash of the previous Block, thereby forming a chain that goes back all the way to the birth of the project. Changing any historical data in a Block would invalidate its hash and thus break the chain. This makes historical data on Blockchains unmodifiable because of the computational cost of redoing all the links. This also makes Blockchains append-only, which means that the entire history of transactions is always available to audit and verify. This makes them very valuable in domains where transparency and chain of ownership is important.



Each Block also contains a list of **Transactions** that were announced on the network during the period the Block was being created. Transactions can hold any kind of data but is usually represents a change of state. In Bitcoin this is the ownership of a coin, but it can also represent change in ownership of properties, stocks, digital rights etc.

Blockchains use various **Consensus Algorithms** to decide on who gets to write the next block. The Bitcoin Blockchain for example uses an algorithm called **Proof of Work**. Roughly every 10 minutes, it announces a cryptographic puzzle to its network. Nodes connected to the network compete with each other to solve the puzzle and the winner not only gets to write to the Blockchain but is also rewarded a certain amount of Bitcoin (currently 12.5 BTC). The act of trying to solve the puzzle is called mining and each node is called a **Miner**. On the other hand, private Blockchains like JPMorgan's Quorum use a voting based system to choose the node that gets to write to the chain.

Various different Blockchains available today offer different opportunities. The Bitcoin Blockchain lets you conduct financial transactions while Ethereum is trying to build a global computing platform for running decentralized applications coded as Smart Contracts. These apps leverage the transparency of the Blockchain to declare their intent and the integrity of the Blockchain to guarantee their execution. There is also a rise of industry-specific Blockchains like Quorum for Banks MediaChain which was recently acquired by Spotify as well as completely private chains used within a company for internal efficiencies.