Lesson 2 - - Blockchain Intro

In the beginning the first blockchain was a triple-entry ledger system Bitcoin used for administration.   Bitcoin was the first asset recorded using a blockchain ledger. While many cryptocurrencies today are using more advanced blockchain technology, blockchain applications continue to be developed for many other uses than just cryptocurrency.

Here is a more comprehensive definition reflecting how blockchain technology has evolved:

A blockchain consists of permanent accounting records linked together to track something of value, including any and all changes in ownership, status, or location, for two or more parties, who may or may not know each other or trust each other.

Blockchain technology provides the framework for maintaining a persistent, highly-secured, transparent, decentralized, append-only, trusted, shared ledger, used by either the public or permissioned groups, to track exchanges of, or changes to, something of value to each party that is directly involved in the transaction, thereby eliminating the oversight and involvement, and any fees charged, by intermediaries who were needed previously to complete the transaction (e.g. accountants, lawyers, or bankers)

Bitcoin and Ethereum represent the first two generations of blockchain technology, respectively.

As mentioned, Bitcoin used the first blockchain to track ownership of digital currency called bitcoins. Bitcoin also uses operators of network nodes, called "miners," who must agree by consensus when adding new blocks to chain. The consensus mechanism is called Proof of Work (PoW), which requires network nodes to compete with each other by performing extensive computational work. The operator who is the winner of the competition gets paid in bitcoin and is allowed to add the next block of records to the chain. This approach of adding payment, difficulty, and expense to the administration of the ledger is intended to keep hackers or other bad actors from operating network nodes. The payments made to reward network operators explain why cryptocurrencies are mandatory in a public blockchain but are not needed in a permissioned blockchain.

Ethereum came along years later offering a number of improvements over Bitcoin's implementation, along with extensive development capabilities and tools that anyone can use as a development platform to build their own blockchain applications. Ethereum also introduced its own cryptocurrency called Ether (ETH) and replaced the PoW consensus mechanism with a Proof of Stake (PoS) protocol that requires less overall computation. One of its more significant additions was a protocol including custom programs called "smart contracts" that are stored on the ledger and invoked while processing a transaction to enforce rules and conditions in negotiation of legal contracts. To do this, a smart contract can invoke external systems. This is how blockchains become

integrated with existing business application to expand their capabilities. The bottom line is that Ethereum smart contracts enable the exchange of digital assets between parties in a more sophisticated and reliable manner and are the mechanism used to eliminate intermediaries.