BLOCKCHAIN

What is Blockchain?

Blockchain is about enabling peer to peer transaction in a decentralized network. Establishing trust among unknown peers. Recording the transaction in an immutable distributed ledger.

Blockchain enables peer to peer transfer of digital assets without any intermediaries. It was a technology originally created to support the famous cryptocurrency, Bitcoin.

Backbone of Blockchain:

- Validation
- Verification
- Immutable Recording or Immutable Ledger
- Consensus

Types of Blockchain:

- Only Cryptocurrency. Ex- Bitcoin
- Currency + Business Logic. Ex- Ethereum
- Only Business Logic. Ex- The Linux Foundation's Hyperledger

Blockchain Categories:

- Public
  Bitcoin is a fantastic example of a public blockchain class.

- Private
  In a private blockchain, access to the blockchain is limited to selected participants for example, those participants within an organization. This restriction helps in simplifying the normal operations such as block creation and contingence model.

- Permissioned (Consortium Blockchain)
  It is meant for a consortium of collaborating parties to transact on a blockchain for ease of governance, provenance, and accountability for example, a consortium of all automobile companies or healthcare organizations.
  Permissioned blockchain has the benefits of a public blockchain with allowing only users with permission to collaborate and transact.

Private and permissioned blockchain allow for controlled access to the blockchain enabling many diverse business models.

Areas of Blockchain:

- Finance
- Healthcare
- Government
- Manufacturing
- Distribution

Wide range of Applications:

- Goods Transfer. Ex- Supply Chain
- Digital Media Transfer. Ex- Sale of Art
- Remote Services Delivery. Ex- Travel & Tourism
- Platform for decentralized business logic. Ex- Moving computing to data sources.
- Distributed intelligence. Ex- Education credentialing.

Additional applications of Blockchain:

- Distributed resources. Ex- Power generation and distribution.
- Crowd funding. Ex- Start-up fund raising.
- Crowd operations. Ex- Electronic voting.
- Identity management. Ex- One ID for all your life's functions.
- And government public records and open governing

Blockchain Structure:

Transaction is the basic element of the Bitcoin Blockchain. Transactions are validated and broadcast. Many transactions form a block. Many blocks form a chain through a digital data link. Blocks go through a consensus process, to select the next block that will be added to the chain. Chosen block is verified, and added to the current chain.

Validation and consensus process are carried out by special peer nodes called miners. These are powerful computers executing software defined by the blockchain protocol.

Operations of Blockchain:

- Validation of Transactions
- Gathering transaction for a block
- Broadcasting valid transactions & blocks
- Consensus on next block creation
- Chaining the blocks

The process involves validation of more than 20 criteria, including size, syntax, etc. Some of these criteria are: Referenced Input Unspent Transaction Output, UTXOs are valid, recall, UTXO is well-defined earlier in lesson two, reference output UTXOs are correct, reference input amount and output amount matched sufficiently, invalid transactions are rejected and will not be broadcast. All the valid transactions are added to a pool of transactions. Miners select a set of transaction from this pool to create a block. This creates a challenge. If every miner adds the block to the chain, there will be many branches to the chain, resulting in inconsistent state. Recall, the blockchain is a single consistent linked chain of flux. We need a system to overcome this challenge, the solution. Miners compete to solving a puzzle to determine who earn the right to create the next block. In the case of bitcoin blockchain, this puzzle is a computation of puzzle and the central processing unit or CPU intensive. Once a miner solves the puzzle, the announcement is broadcast to the network and the block is also broadcast to the network. Then, another participant verifies the new block. Participants reach a consensus to add a new block to the chain. This new block is added to their local copy of the blockchain. Thus, a new set of transactions are recorded and confirmed. The algorithm for consensus is called **proof-of -work protocol**, since it involves work a computational power to solve the puzzle and to claim the right to form the next block.

Unspent Transaction Output (UTXO):

A fundamental concept of a bitcoin network is an Unspent Transaction Output, also known as UTXO. UTXO's are referenced as inputs in a transaction. UTXO's those are also outputs generated by a transaction.

Role of UTXO:

The transaction uses the amount specified by one or more UTXOs and transmits it to one or more newly created output UTXOs, according to the request initiated by the sender.

Structure of UTXO:

- It includes a unique identifier of the transaction that created this UTXO.
- An index or the position of the UTXO in the transaction output list.
- A value or the amount it is good for.
- And an optional script, the condition under which the output can be spent.