**INTRODUCTION**

It is obvious you’ve heard the term Blockchain Technology or Blockchain for short but how do you really understand this concept? Most people also buy and sell or trade Bitcoin, Ethereum and other cryptocurrencies but don’t understand the behind the scenes of whatever that happens. Blockchain is a relatively new technology that is gaining popularity and change how businesses, finance, government, health, media and other industries operate.

Through out this course, we learn and understand the blockchain technology, Bitcoin, Ethereum, Smart Contracts, Mining, Decentralized Apps (DApps), Tokens etc.

We’ll start the course by understanding blockchain technology and other concepts will follow.

NB: This course is not to make you a blockchain master but to help you understand the blockchain technology, what it is and what it’s not.

I won’t discuss how to trade or buy and sell Bitcoin, Ethereum or any other cryptocurrency here.

This course is to make you a **BLOCKCHAIN LITERATE.**

THANK YOU FOR EMBARKING ON THIS JOURNEY WITH ME!!!

**PART 1: BLOCKCHAIN**

This chapter is an introduction to blockchain technology, the fundamentals and theories behind it, the various concepts that have been combined to build the **Blockchain.**

In the year 2008, when Bitcoin was invented the world was introduced to a new concept which revolutionized the whole society. It was something that aims to impact upon every industry. This new concept was **Blockchain**, the underlying technology that powers Bitcoin.

Bitcoin was the first technology that was successfully built on the blockchain.

In 2008, a paper entitled Bitcoin: A Peer-to-Peer Electronic Cash System, was written by an unknown person or group called Satoshi Nakamoto.

This paper can be viewed on the bitcoin.org website via the link: <https://bitcoin.org/bitcoin.pdf>.

No one knows the actual identity of Satoshi Nakamoto.

**WHAT IS BLOCKCHAIN?**

BLOCKCHAIN is a peer-to-peer, decentralized, distributed ledger that is secure by cryptography, immutable and updated only via consensus among peers.

This means that the blockchain is just like a database that is held my individuals, which has no central controller and data can only be added to it if only there’s a total agreement between all individuals who are part of the blockchain network.

Create, Read, Update, Delete (CRUD) operations on traditional databases cannot be performed on the blockchain. That is, you cannot update or change any data on the blockchain after it has been appended.

To change something on the blockchain is very difficult and sometimes almost impossible to do.

NB: We will learn how data on the Bitcoin or Ethereum blockchain can be changed later through **soft and hard fork.**

**COMPONENTS OF A BLOCKCHAIN**

1. Address: Addresses are unique identifiers used in a blockchain transaction to denote sender and recipients.
2. Transaction: It is a fundamental unit of a blockchain. A transaction represents a transfer of value from one value (usually cryptocurrencies like Bitcoin or Ether) from one address to another.
3. Block: It contains multiple transactions and other elements such as previous block hash of a block header, timestamp and nonce (number once).

Other elements of a block include:

* 1. A reference to a previous block except the genesis block.

NB: Genesis Block is the first block in the blockchain that is hardcoded at the time the blockchain was first started or constructed.

* 1. Nonce is a number that is generated and used only once. It is value that is used to authenticate a block through Proof of Work (PoW) consensus algorithms.
  2. A timestamp is the creation time of the block.
  3. Merkle root is a hash of all the nodes of a merkle tree. Merkle trees are used to allow efficient verification of transactions.

1. Peer-to-Peer Network: This is a network where all nodes can communicate with each other and send and receive messages.
2. The Scripting or Programming language: Scripts perform various operations on a transaction in order to facilitate various functions. In Bitcoin, transactions are predefined in a language called Script, which consists of commands to allow nodes to transfer bitcoins from one address to another.

NB: Bitcoin’s Script language cannot be used in the development of other programs on the blockchain because it is not **Turing Complete.**

A Turing Complete Language means that it can perform any computation. It is named after Alan Turing, who developed the idea of a Turing machine that can run any algorithm however complex.

Ethereum’s Solidity Language is Turing Complex, that is it can be used to build other programs called **smart contracts** on the Ethereum blockchain.

1. Virtual Machine: It allows smart contracts to run on a blockchain such Ethereum Virtual Machine (EVM).
2. Smart Contracts: These are programs or code snippets that run on top of the blockchain and contains the business logic to be executed when certain conditions are met.
3. Node: A node has different functionalities on a blockchain.
   1. It can propose and validate transactions and perform mining to facilitate consensus and secure the blockchain.
   2. Nodes can perform simple transaction verifications etc.

**HOW BLOCKCHAIN WORKS**

Nodes are either miners who create new blocks and mint cryptocurrencies. They can also validate and digitally sign the transactions. A critical decision that every blockchain network has to make is to figure out which node will append or add the next block to the blockchain. This decision is made using a consensus mechanism. Consensus mechanism will be explained later.

Now how does a blockchain validate transactions and creates and adds blocks to grow the blockchain?

1. Transaction is initiated or started: First a node starts a transaction by creating it and digitally signing it with its private key. Usually, this is a transfer of value between users on the blockchain network. Maybe the transfer of Bitcoin from Person A to Person B.
2. Transaction is validated and broadcast: A transaction is disseminated through a protocol to other nodes or peers on the blockchain to validate it.
3. Find new block: When the transaction is validated by nodes or miners it is included in the block and the process of mining starts.
4. New block found: Once a miner solves a mathematical puzzle ( implementation of consensus mechanism), the block is considered found or mined. Usually, miner who solves the mathematical puzzle is rewarded a certain number of coins as an incentive for their effort and resources spent in the mining process.
5. Add new block to the blockchain: The newly created block is validated transactions or smart contracts within it are executed and it is propagated to other peers or nodes. Peers also validate and execute the block. It now becomes part f the blockchain (ledger) and the next block links itself cryptographically back to this block. This link is called a hash pointer.

BENEFITS OR FEATURES OF BLOCKCHAIN

1. Decentralization: There is no need for a trusted third party to validate transaction, instead a consensus mechanism is used by nodes to validate and agree on transactions.
2. Transparency and Trust: Blockchains are shared and everyone can see what is on the blockchain network. Blockchain is known as a trustless network.
3. Immutability: Once data has been added to the blockchain it is difficult to change.
4. Highly Secure: All transactions on a blockchain are cryptographically secured and thus provide network integrity.
5. Highly available
6. Cost saving
7. Platform for smart contracts

LIMITATIONS OF BLOCKCHAIN

1. Scalability
2. Adoption
3. Regulation
4. Relatively immature technology

TYPES OF BLOCKCHAIN

Basically, these are the types of blockchain:

**Public blockchains:** Public blockchains, such as Bitcoin, are large distributed networks that are run through a native cryptocurrency. A *cryptocurrency* is a unique bit of data that that can be traded between two parties. Public

blockchains are open for anyone to participate at any level and have opensource code that their community maintains.

**Permissioned blockchains:** Permissioned blockchains, such as Ripple, control roles that individuals can play within the network. They’re still large and distributed systems that use a native token. Their core code may or may not be open source.

**Private blockchains:** Private blockchains also known as distributed ledger technology (DLT) tend to be smaller and do not utilize a token or cryptocurrency. Their membership is closely controlled. These types of blockchains are favored by consortiums that have trusted members and trade confidential information.

NB: There may be other types which have not been discussed here but the ones stated above are the common types.

CONSENSUS MECHANISM

Consensus is the backbone of a blockchain, as it provides the decentralization of control through an optional process known as mining.

Consensus is a process of achieving agreement between distrusting nodes on the final state of data. To achieve consensus different algorithms are used.

Consensus mechanism is a set of stages that are taken by most or all nodes in a blockchain to agree on a proposed state or value.

TYPES OF CONSENSUS MECHANISM

These are the common types of consensus mechanisms:

1. Proof of Work (PoW): It relies on proof that adequate computational resources have been spent before proposing a value for acceptance by the network.
2. Proof of Stake (PoS): This algorithm works on the idea that a node has adequate stake in the system that is the node has invested enough in the system so that any malicious attempt by the user would outweigh performing an attack on the network.
3. Delegated Proof of Stake (DPoS): It is an innovation over standard PoS whereby each node that has a stake in the system can delegate the validation of a transaction to other nodes by voting.

Other less consensus mechanisms are:

1. Proof of Elapsed Time (PoET)
2. Proof of Deposit (PoD)
3. Proof of Importance (PoI)
4. Practical Byzantine Fault Tolerance (PBFT)
5. Proof of Activity (PoA)
6. Proof of Capacity (PoC)
7. Proof of Storage
8. Proof of Authority

WHAT IS DECENTRALIZTION?

Decentralization in blockchain simply means that no single central authority is in control of the network.

CRYPTOGRAPHY

Cryptography is the science of making information secure in the presence of adversaries.