What is Blockchain

Blockchain is also a data structure – a decentralized database consisting of fixed length blocks.
- the blocks in a blockchain include a number of transactions.

A whitepaper was released in 2008 by bitcoin founder satoshi nakamoto. Nakamotos whitepaper referred to blockchain as a `chain of blocks` over time, chain of blocks came to be referred as blockchain.

Working of blockchain:

a block consists of two major parts: Header and Body.

Cryptography

Transforming plaintext into ciphertext.

Cryptography provides protection by transforming data into and unreadable form.

Plantext can be converted into ciphertext by using two ways:

* **substitution**: a method that changes or swaps one character for another.

e.g if every letter is shifted right by three letters.

* **Transposition**: A method that changes the order of characters of a word by using some predetermined method.

Symmetric key cryptography

* the same key is used to perform encryption and decryption

* the key is shared betweeen the two parties over a secure channel.

* confidentiality of data is provided.

* Authentication and non-repudiation are not provided.

* Origin of the message cannot be determined.

Asymmetric key cryptography

in asymmetric key cryptography:

* a pair of keys is used.

* a public key is created from a private key.

* it was developed due to problems in symmetric key cryptography.

Cryptographic Hashing

hashing transforms data or a string of characters into a short and fixed length value.

This value is unique and called hash or hash value or message digest

this value is unique

hashing algorithm or cryptographic hash function are used to perform hashing

Hashing Alorithms

* Hashing is an important cryptographic technique that ensures the integrity of data.

* Hashing algorithms are categorized on the basis of their implementations, digest size and other things.

Digital signatures

* digital signature is based on asymmetric key cryptography.

* it provides a high level of security.

* it uses a hash value which is encrypted through the private key of the sender.

* it provides authentication, integrity, and nonrepudiation.

Difference between hashing and encryption

* Hashing is a one-way process.

* Encryption is a two-way or reversible process.

* Hahing will always return a fixed length output regardless of the input size.

* in encryption, the size of the output depends on the size of input.

Consensus Algorithms

Consensus mechanism is implemented in decentralized networks.

Consensus algorithms ensure that nodes agree on a consistent global state of the blockchain.

Some common consensus algorithms in a networks

* Proof of work
* proof of stake
* proof of elapsed time
* crash fault tolerant

programmable Blockchains(smart contracts)

* A programmable blockchain implements smart contracts to execute logic programs.
* Ethereum Is the most popular programmable blockchain.

Smart Contracts

* it includes a set of predefined conditions.

Characteristics:

They are self-verifying in nature.

What is a Dapp

* applications that are executed on a peer-to-peer network of computers are known as \Daaps.

Dapps lack a central authority for decision-making.

To be Dapp

* Applications source code must be open source.
* applications data and records must be stored in a public blockchiain.
* Application must use cryptographic tokens.

IPFS stands for inter-planetary file system.

It is a distributed file ssystem that aims to replace http

What is a DAO

Is an organization which: * functions without any conventional management structure

* manages and sustains itself using smart contracts.

* DAOs are implemented using smart contracts.

DO

* in a decentralized organization, there is no central decision-making authority.

Introduction to cardano

Bitcoin

The main characteristics that define the bitcoin network are :

Distributed , Cryptographically secure, immutable

Ethereum

Ethereum aimed to serve as “the world computer”.

* it interoduced a turing-complet smart-contract language called solidity.

Cardano

Cardano was conceived by charles hoskinson in 2015.

it became functional in 2017 with the launch of the “ byron era” chain.

It is a third generation blockhain technology.

It addresses the shortcomings of bitcoin and ethereum blockchain.

It hosts the ADA cryptocurrency.

What is Cardnao?

Cardano is an open-source, decentralized blockchain, cryptocurrency project

It aims to solve the problems of : scalability, interoperability, sustainability.

Reasons to migrate to cardano

* to eliminate the need for energy-consuming consensus algorithm --- prof-of-work.
* To embrace an advanced blockchain protocol with high security, scalability and decentralization.
* to solve problems of earlier generation blockchains.

Organization behind cardano

* cardano fundation
* input/ouput
* emurgo

Advantages of cardano

it is highly scalable.

It has strong academic foundation

it is a research-first driven approach.

Investors can benefit from the following two aspects of cardano:

* it offers a robust cryptography, known as ADA.
* the project value of cardano as a platform is the sum of all projects built on top of it!

About Cardnao

some of the principles adopted by cardano are listed as follows:

* separation of accounting and computation
* implementation of core components
* development of decentralized funding
* abstracting o transactions
* developing long-term planning
* adopting a standards-driven process

Roadmap and history of cardano

Era of cardano

* byron

* shelley

* goguen

* basho

* voltaire

The working of cardano

Cardnao comprises two layers:

1. Cardano settlement layer(CSL)

2. Compution layer

* The csl layer is used to verify and validate the transactions that use ADA cryptography

* the control layer (side chain) is especially meant for execution of smart contracts with particular assets that are migrated to the control layer.