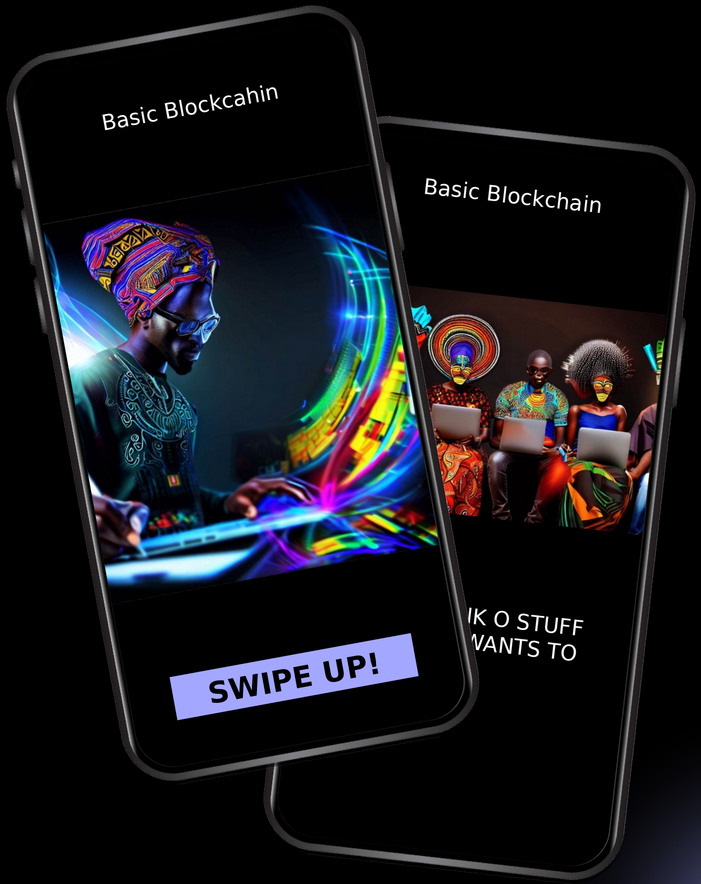
Basic Blockcahin

Decentralized system



Why do we need decentralized systems?

If a central entity crashes or misuses information, the whole system is compromised.

Decentralization distributes decision making power across entities instead of a single authority.

Network Definition

Is a system of linked nodes or computers that share resources such as storage, processing units, and communication channel bandwidth.

Network Types

Centralized, decentralized, and distributed.

BitTorrent is a great example of a distributed protocol for file-sharing .

The Original Bitcoin Whitepaper

In 2008, Satoshi Nakamoto published the original Bitcoin white-paper: “Bitcoin:A Peer-to-Peer Electronic Cash System.

What is block-chain

It allows users to send and receive digital assets securely and transparently without needing a central authority or intermediary, by having a copy of all transactions distributed across the network using consensus mechanism, storing data in blocks, where each block is tied to the previous, resulting in a chain of block or block-chain.

Hash Function

It takes an input and returns a fixed-size output called a hash digest and the original input can’t
be derived from the hash.

Any change to the original input will be reflected in completely
different hash output.

Careers in Block-chain

Smart contract Developer …

Block-chain Generations

1) First Block-chain Generation
Bitcoin

2) Second Block-chain Generation
Ethereum Introduced Dapps and new types of Tokens.

3) Third Block-chain Generation
Third-generation block-chains, like Cardano, work to address scalability, interoperability, and sustainability.

Blockchain Types

1) Public,permissionless
2) Public, permissioned
3) Private, permissionless
4) Private, permissioned

Evolution of the Internet

Web 1.0, 2.0, and 3.0

Cryptography

There are two types of algorithms for encrypting messages:

symmetric encryption and asymmetric encryption.

In symmetric, the same key is used to encrypt and decrypt the data, making it fast and simple but less secure. Asymmetric, also known as public key cryptography,
uses two keys: a public key and private key.

Digital Signatures

Can be used to authenticate the identity of the sender of a transaction and verify that a transaction has not been tampered with or altered in any way.

Wallets in a block-chain network

1) Custodial and
2) Noncustodial Wallets

To store and handle private keys securely there are two main options:

1) Hot and
2) cold storage

Transaction Models

Two major accounting ledgers exist in block-chain space:

UTXO-based blockchains(Bitcoin for instance). And

Account(Ethereum, and others).

Cardano Blockchain.

Cardano is a blockchain platform known for its focus on sustainability, scalability, and security.

It was created by Charles Hoskinson, one of the co-founders of Ethereum, and developed by the company Input Output Hong Kong (IOHK).

“If the Mountain won’t go to Mohammed, then Mohammed must come to the Mountain”

—Someone Ancient

Some key aspects of Cardano:

Proof-of-Stake (PoS) Consensus:

Cardano uses a PoS consensus mechanism, specifically the Ouroboros protocol. PoS is considered more energy-efficient and environmentally friendly compared to the Proof-of-Work (PoW) mechanism used by cryptocurrencies like Bitcoin.

Some key aspects of Cardano:

Staking and Governance:

ADA holders can participate in staking, where they can delegate their ADA to a pool to help secure the network and earn rewards.

Cardano also has a treasury system called Project Catalyst, which allows the community to propose and vote on projects to be funded.

Some key aspects of Cardano:

Smart Contracts:

Cardano's development includes the introduction of a smart contract platform called Plutus.

It is designed to be secure and flexible, allowing developers to create decentralized applications (DApps) and execute smart contracts on the Cardano blockchain.

Some key aspects of Cardano:

Decentralization:

Cardano aims to be a decentralized and community-driven platform, with the goal of minimizing the concentration of power and control.

Some key aspects of Cardano:

Interoperability:

Cardano is designed to be interoperable with other blockchains and legacy financial systems. It aims to provide a bridge for assets and information to flow between different networks and ecosystems.

Some key aspects of Cardano:

Layered Architecture:

Cardano is designed with a layered architecture, separating its settlement layer from its computation layer. The settlement layer is used for transferring ADA, the platform's native cryptocurrency, while the computation layer is intended for smart contracts and other applications.

Cardano

Cardano combines Bitcoins’s utxo model with the ability to handle smart contracts into an extended unspent transaction output(EUTXO) accounting model.

The adoption of eutxo facilitates the implementation of smart contracts into the cardano chain.

Plutus Core

The implementation of Eutxo includes two key elements that differentiates it from an account model: script and data
scripts require a definite, well-specified scripting language, and it is also important to define the
type of data attached to outputs and used as redeemers.
Redeemer data is a simple data type that can be easily defined in haskell.

Plutus Core

Plutus core, Cardano scripting language, provides these two elements. It is a simple and functional language similar to haskell. Indeeed, a large subset of haskell can be used to write plutus core scripts.

Developers do not write any plutus core code. A haskell compiler plug-in generates all plutus core scripts.

UTXO + Contract script + Data

How does the EUTXO model extend UTXO?

it generalizes the concept of address by using the lock-and key analogy. Instead of restricting locks to public keys and keys to signatures, address in the eutxo model can contain arbitrary logic in the form of scripts.

The second difference between utxo and eutxo is that ouptus can carry almost arbitrary data in addition to an address and value. This makes scripts much more powerful by allowing them to carry state.

EUTXO as a springboard to scale Cardano in 2022

* Reference inputs(CIP-0031)- plutus scripts can inspect transaction inputs without needing to spend them. This means that it is not necessary to create utxos simply to inspect the information held by an input.

EUTXO as a springboard to scale Cardano in 2022

* Plutus Datums(CIP-0032)- Datums can be attached directly to outputs instead of datum hashes.
This simplifies how datums are used, as a user can see the actual datum rather than having to supply
the datum that matches the given hash

EUTXO as a springboard to scale Cardano in 202

* Script sharing (CIP-0033) – Plutus Script references can be associated with transaction outputs, meaning that they can be recorded on-chain for subsequent reuse. It will not be necessary to supply a copy of the script with each transaction, hugely reducing friction for developers.

Cardano Wallets:

Daedalus:
Yoroi:
Nami:
Eternal:
Hardware Wallets:

Cardano Staking

Cardano allows users to stake their ADA to participate in the network's PoS consensus mechanism.

Staking is a process where ADA holders lock up their coins to support the network's security and, in return, earn staking rewards.

Governance:

The Cardano community participates in the governance of the network through initiatives like Project Catalyst, which enables community members to propose and vote on projects to be funded by the treasury.

Sustainability:

Cardano emphasizes long-term sustainability, with a focus on research, development, and gradual improvements to the platform.

> “If the Mountain won’t go to Mohammed, then Mohammed must come to the Mountain”
>
> —Someone Ancient

Thanks