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.
Consensus algorithms are the way those decisions are reached, it provides a way for d/t components in a system to achieve agreement on a single data value without the need for a central 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.”
Bitcoin introduced the proof-of-work consensus algorithm.
Bit Gold : was one of the earliest attempts at creating a decentralized virtual currency, proposed by blockchain pioneer Nick Szabo in 1998.

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.

Block-chain technology provides an opportunity to decentralized many applications across industries like insurance, banking, logistics, supply chain management, agriculture, and more.

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.

Use cases:
DB, signature, block creation in block-chain …

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.

Smart Contracts: A key innovation of Ethereum is the smart contract.
- Is a program stored on a blockchain, Deployed smart contracts cannot be deleted by default, and interactions with them are irreversible.
- Ethereum implemented Solidity programming language to develop smart contracts.Follows “if this, then that” logic.

Native Assets and Non-fungible Tokens:
Some blockchains, like Ethereum, allow for the creation of other tokens through smart contracts, and have value based on user demand.

Another type of token in blockchain is the non-fungible token or NFT. An NFT is a digital asset that represents ownership of a unique item, like an artwork.

Decentralized Finance(DeFi):
DeFi aims to replicate financial services in a more open and transparent way than traditional finance using smart contracts.

Decentralized Autonomous Organization (DAO):
The idea of managing and running an organization where decision-making and rule-making are transparent, executed by code, and not controlled by any central authority.

3) Third Block-chain Generation:

Third-generation block-chains, like Cardano, work to address scalability, interoperability, and sustainability.

Cardano Native Token:
In cardano creating other kinds of token has the same security properties as ada.
The security properties are not derived from a smart contract as in Ethereum.

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

Public Key Encryption

Encryption Algorithm and Decryption Algorithm

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. What one key can encrypt, the other can decrypt.

Hash Functions

Hash functions are used throughout block-chain. For example:

- Linking blocks in a chain by hashing each transaction with the previous block’s hash.
- In mining, to solve a proof-of-work puzzle, validate transactions, and add them to the block-chain.
- They are used in digital signatures, which verify the authenticity and integrity of data.

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.

How does this work? The sender uses their own private key to sign the message creating a unique digital signature. This signature can be verified by anyone with access to the sender’s public key.

Two algorithms are needed in a digital signature scheme: the signing algorithm(to create a signature) and the verifying algorithm(to verify the signature).

Wallets in a block-chain network

Producing digital signatures and managing secret credentials can be tedious.

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

Utxo-based and Account-based models:

Two major accounting ledgers exist in block-chain space: UTXO-based blockchains(Bitcoin for instance). And Account(Ethereum, and others).

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.

What is a Blockchain accounting model?

Block-chain use transactions as records to track provenance and ownership. These transactions contain a lot of information(where the coins come from, where they're going, and whatever change is leftover from these transactions).

UTXO Model:

In a utxo model, the movement of assets is recorded in the form of a directed acyclic graph where the nodes are transactions and the edges are transaction outputs, where each additional transaction consumes some ot the utxos and adds new ones. The users wallets keep track of a list of unspent outputs associated with all addresses owned by the user, and calculate the users balance. In other words, the balance held in a given wallet address is the sum of all unspent UTXOs from previous transactions.

You cannot split a utxo into smaller bits. Utxos are used whole and changes is given back to your wallets addresses in the form of a small utxo.

To sum up:

- a utxo is the output of previous transaction, which can be spent in the future.

- utxo chains have no accounts. Instead, coins are stored as a list of utoxs, and transactions are created by consuming existing utxos and producing new onees in their place

- Balance is the sum of utxos controlled by given address.

- UTXOs resemble cash in that they use changes, and are indivisible (utxos are used whole)

Account Model:

In this model, assets are represented as balances within users accounts and the balances are stored as a global state of accounts, kept by each node, and updated with every transaction.

Account chains operate in a similar fashion to traditional bank accounts.

The wallets balance increases when coins are deposited, and decreases when coins are transferred elsewhere.

To sum up:

- This accounting model resembles how a bank operates.

- Users have accounts that hold their coin balances.

- It is possible to spent partial balances.

- The concept of change does not apply.

The EUTXO Model

EUTXO (Extended Unspent Transaction Output) is an enhanced model for blockchain transactions that allows for the execution of complex smart contracts and scripts, with Cardano utilizing it for its secure and programmable transaction capabilities.

Transaction output:

A transaction output includes an address (that you can think of as a lock) and a value. In keeping with this analogy, the signature that belongs to the address is the key to unlock the output. Once unlocked, an output can be used as input.

New transactions spend outputs of previous transactions. Each utxo can only be consumed once, and as a whole. Each output can be spent by exactly one input, and one input only.

Transaction input:

A transaction input is ouput of a previous transaction. Transaction inputs include a pointer and a cryptographic signature that acts as the unlocking key. The pointer refers back to a previous transaction output, and the key unloks is ouput. When an ouput is unlocked by an input, the blockchain marks the unlocked output as spent. New ouputs created by a given transaction can then be pointed to by new inputs, and so the chain continues. These new outputs) which have not yet been unlocked, I.e, spent) are the utxos. Unspent ouputs are simply that, ouputs that have not yet been spent.

EUTXO is a transaction mechanism combining:

- smart contract: these lock-up utxos, ada, native assets, and NFTs.

* are programmes stored on the blockchain that run when preexisting conditions are met. They can be thought of as locks that hold utxos, ada on the cardano block-chain.

- Redeemers: user-supplied data provided to unlock locked assets and spend them.

* The data passed from the user to the smart contract. In a simple utxo a redeemer could be a signature which provides proof of ownership of utxo and access to the contents.

- Datum: data such as a high score, user information or other information relevant to your app.

* A piece of information that can be associated with a UTXO. It is used to carry script state information such as its owner or the timing details (which define when the utxo can be spent)

- Context: information like metadata about the transaction being validated.

* The context is essentially a summary of the pending transaction and includes information about witnesses, certificates as well as how value is flowing as it allows access to transactions inputs and outputs.

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).

Here are some key aspects of Cardano:

1. **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. Cardano's PoS model also enables the platform to scale efficiently.
2. **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.
3. **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.
4. **Formal Verification:** Cardano places a strong emphasis on formal methods and peer-reviewed research. It aims to create a more secure and reliable blockchain by using mathematical proofs and verification techniques to ensure the correctness of its protocols and code.
5. **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.
6. **Sustainability:** Cardano is committed to sustainability, with a focus on the long-term development and maintenance of the platform. This approach involves ongoing research and updates to adapt to changing needs and technologies.
7. **Decentralization:** Cardano aims to be a decentralized and community-driven platform, with the goal of minimizing the concentration of power and control.
8. **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.

Cardano has gone through several phases of development, including Byron (the initial phase), Shelley (introducing staking and decentralization), and Goguen (smart contract functionality). It continues to evolve, with ongoing development and upgrades.

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.

The eutxo model offers uniqe advantage over other accounting models. For example, the success or failure of transaction validation depends only on the transaction itself and its inputs, and not on anything else on the block-chain. As a consequence, the validity of a transaction can be checked off-chain, before the transaction is sent to the blockchain. A transaction can still fail if some other transaction concurrently consumes an input that the transaction is expecting, but if all inputs are still present, the transaction is guaranteed to succeed. This is in stark contrast to Ethereum, where transactions can fail mid-execution.

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, 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 (datum)

How does the EUTXO model extend UTXO?

EUTXO extends the basics utxo model in two directions:

1) 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. For example, when a node validates a transaction, the node determines whether or not the transaction is allowed to use certain ouputs address and will execute the script if the transaction can use output as an input.

2) 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

Input ouput global inc, is leveraging the power of eutxo to optimeze tha smartcontracts built on cardano in three ways:

* **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.

* **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.

* **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:

Cardano wallets are software or hardware applications that allow users to store, send, and receive ADA. There are various Cardano wallet options, including:

- **Daedalus:** Daedalus is the official Cardano wallet developed by IOHK. It's a full-node wallet, which means it downloads and maintains a copy of the entire Cardano blockchain. This wallet is known for its security and features.
- **Yoroi:** Yoroi is a light wallet developed by Emurgo. It doesn't require users to download the entire blockchain, making it quicker to set up. Yoroi is available as a browser extension and mobile app.
- **Nami Wallet:** is another Cardano wallet option. It is a popular browser extension wallet for managing ADA.
- **Eternal Wallet:** is a relatively new wallet option in the Cardano ecosystem.
- **Hardware Wallets:** These are considered very secure options for storing cryptocurrencies because they store private keys offline.

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.

To stake ADA:

- Choose a stake pool: ADA holders can delegate their ADA to a stake pool of their choice. A stake pool is a group of validators that work together to produce new blocks and secure the network.
- Delegate ADA: Delegators (ADA holders) can delegate their ADA to a stake pool by designating the pool as their delegate. This can usually be done through Cardano wallet interfaces.

- Earn rewards: By staking with a pool, you can earn rewards in the form of additional ADA. Rewards are distributed based on the amount of ADA you delegate and the pool's performance.

Staking is an integral part of Cardano's PoS system, and it helps secure the network while allowing ADA holders to earn a passive income.

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.