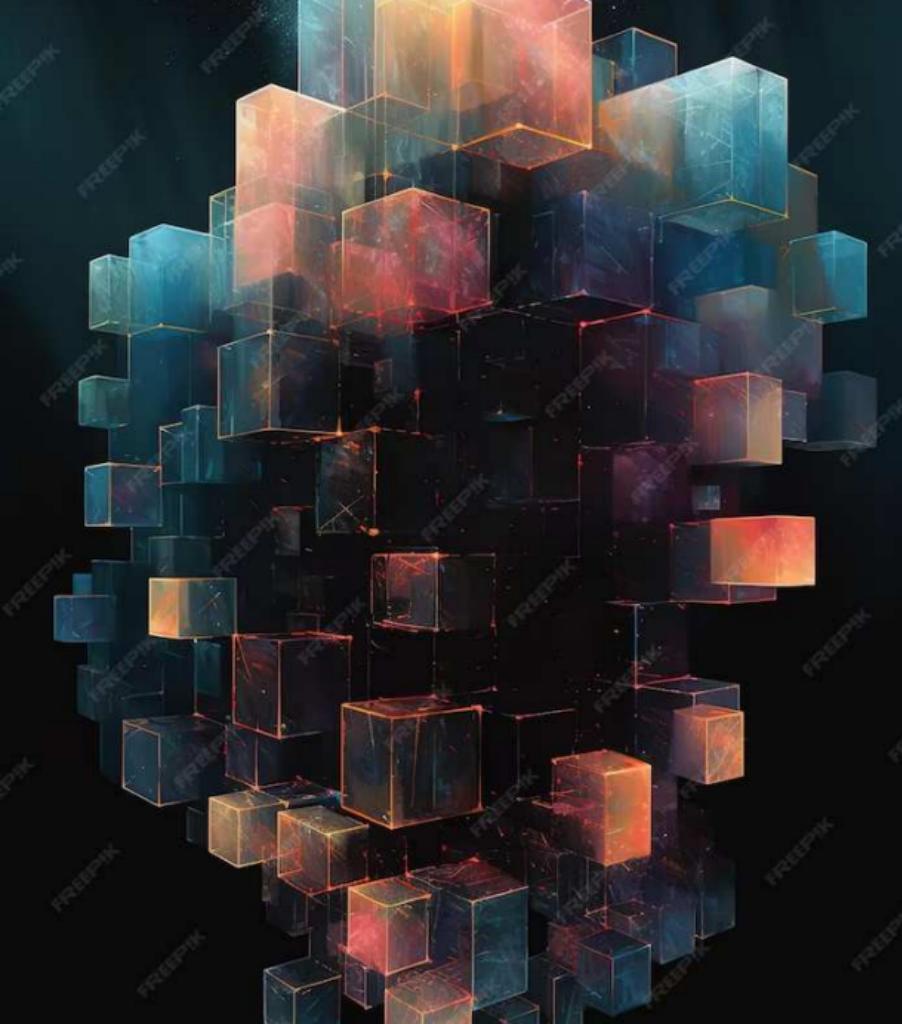


An In-depth Exploration of the Cardano Blockchain



Introduction

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:

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.



Here are some key aspects of Cardano(Cont...)

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



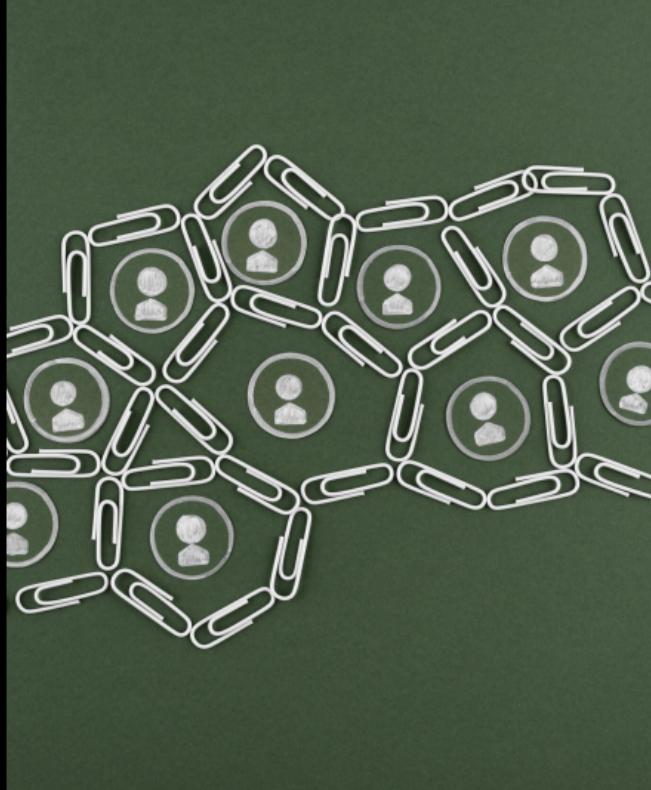
Here are some key aspects of Cardano(Cont...)

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.



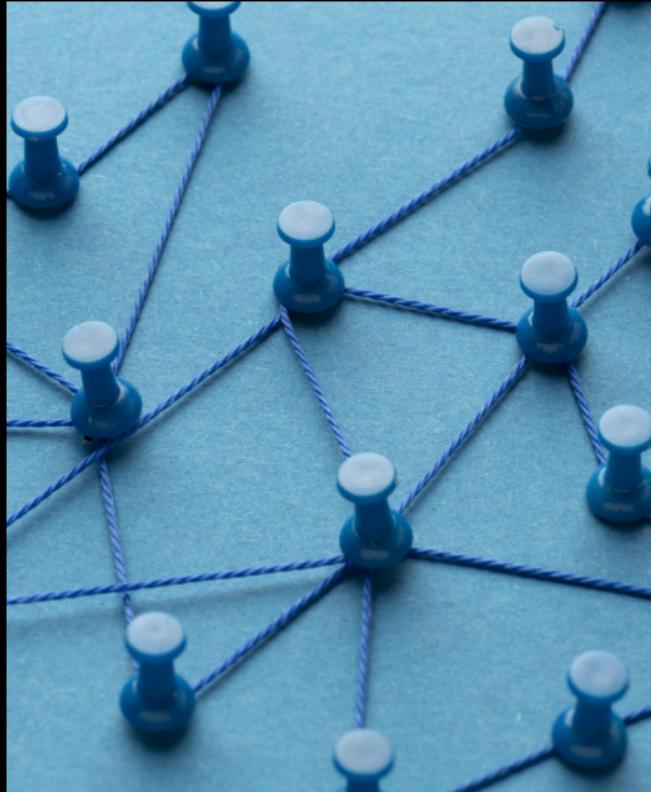
Here are some key aspects of Cardano(Cont...)

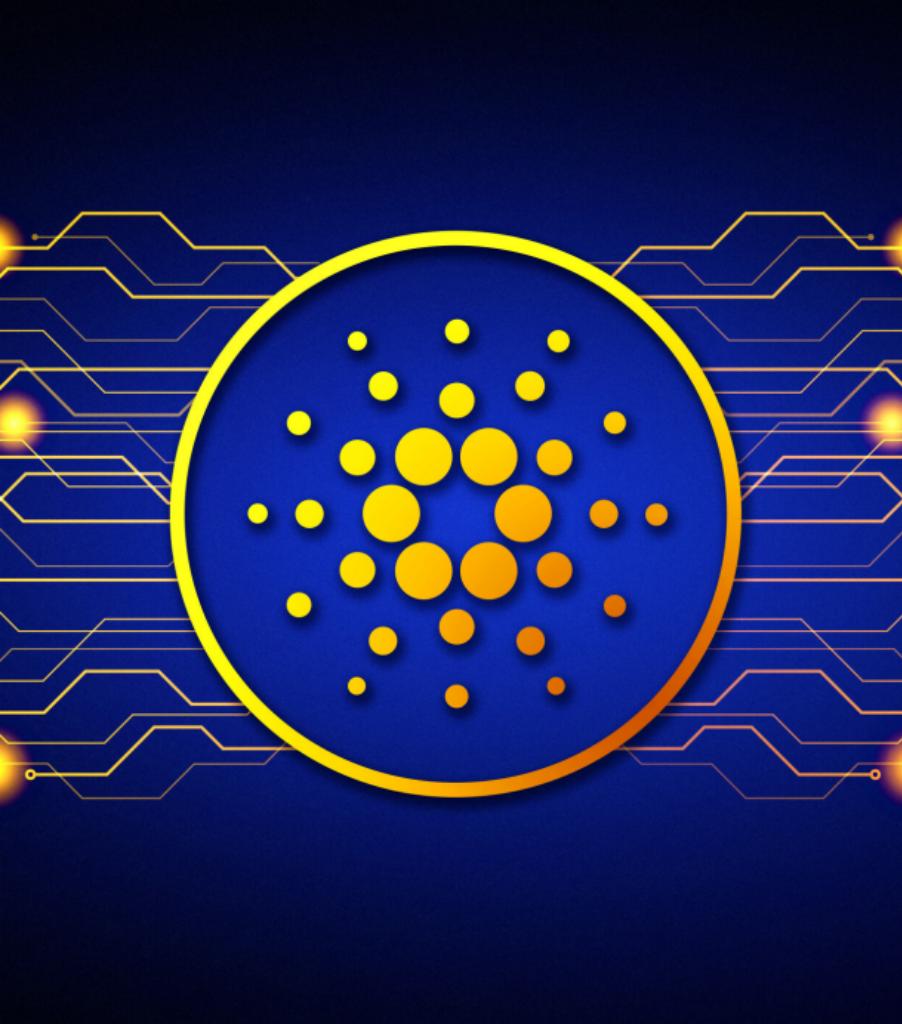
Staking and Governance: ADA holders can participate in staking, where they can delegate their ADA to a pool to help secure the network and earn rewards. Cardano also has a treasury system called Project Catalyst, which allows the community to propose and vote on projects to be funded.



Here are some key aspects of Cardano(Cont...)

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.





Here are some key aspects of Cardano(Cont...)

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.



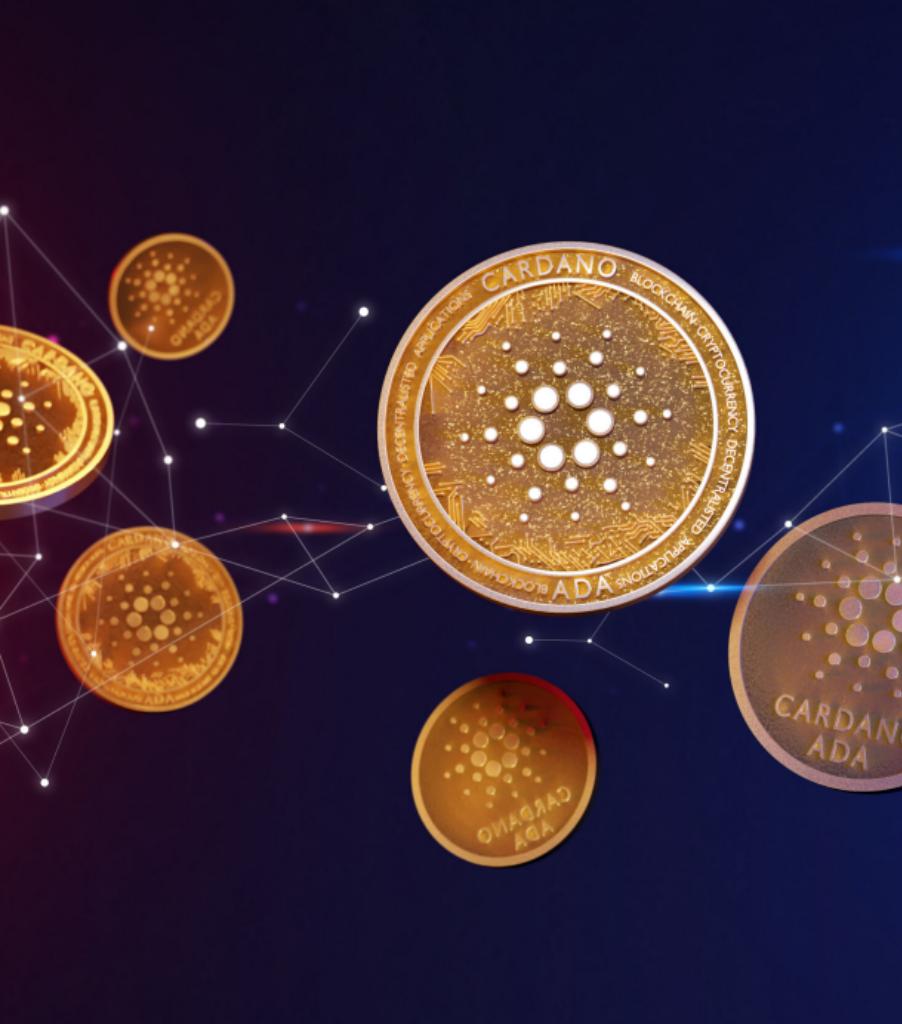
Here are some key aspects of Cardano(Cont...)

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.



Here are some key aspects of Cardano(Cont...)

The eutxo model offers unique 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.



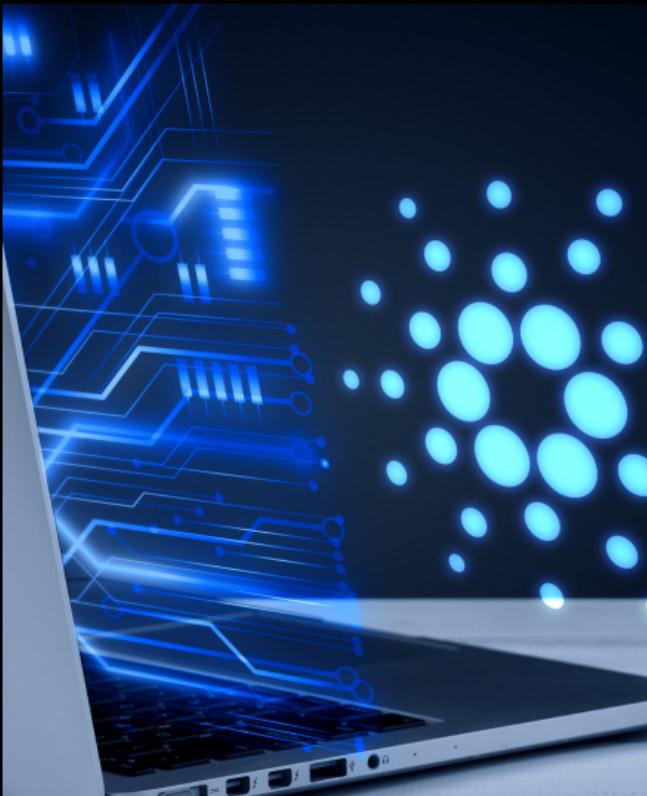
Here are some key aspects of Cardano(Cont...)

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.

How does the EUTXO model extend UTXO?

EUTXO extends the basics utxo model in two directions:

- 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 outputs address and will execute the script if the transaction can use output as an input.



How does the EUTXO model extend UTXO? (Cont...)

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



Plutus Core

The implementation of Eutxo includes two key elements that differentiates it from an account mode.

Script and Data



Plutus Core

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. Indeed, 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)



A dark background featuring two glowing, metallic-looking rings, one blue and one purple, intertwined in a complex, swirling pattern. The rings appear to be made of a reflective material, possibly glass or polished metal, with bright highlights and deep shadows. The background is a dark, solid color, making the glowing rings stand out.

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(Cont...)

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.

A dark background featuring three glowing, metallic-looking rings in shades of blue and purple. The rings are intertwined and appear to be floating in space. The lighting creates bright highlights and deep shadows, giving them a three-dimensional, reflective appearance.

EUTXO as a springboard to scale Cardano in 2022(Cont...)

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.

Wallets in a block-chain network

Producing digital signatures and managing secret credentials can be tedious.

- Custodial and
- Noncustodial Wallets

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

- Hot and
- cold storage





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.
- **Yoroi:** Yoroi is a light wallet developed by Emurgo. Yoroi is available as a browser extension and mobile app.



Cardano Wallets(Cont...)

- **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.



Cardano Staking(Cont...)

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.



Cardano Staking(Cont...)

- **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.



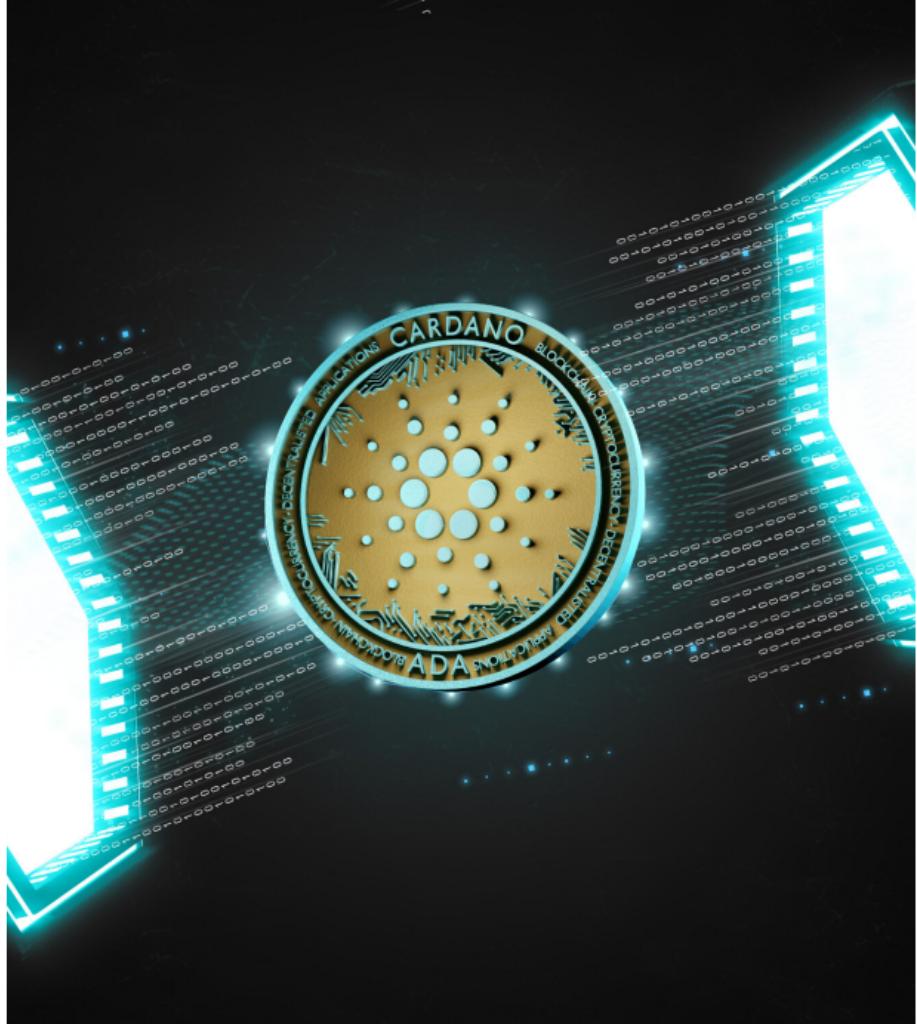
Governance

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.



Conclusion

As we conclude, it's evident that Cardano is at the forefront of revolutionizing the blockchain landscape. Its commitment to **security, sustainability, and innovation** positions it as a driving force in the future of decentralized technologies.

Thanks!

Do you have any questions?