Introduction to Cardano

https://cardano.org

December 2020

- What is blockchain?
- Introduction to the Cardano blockchain

What is blockchain?

- An immutable distributed financial ledger
- Individual financial transactions are protected via cryptographic algorithms
- Individual blocks contain multiple transactions protected via cryptography
- Time is divided in slots
- During a slot a block is assigned to a slot leader, also known as miners or block producers
- Multiple nodes in the network are competing with each other to become slot leader and be able to solve the cryptographic puzzle
- The node that solves the cryptographic puzzle gets a reward for adding a new verified block to the chain
- Consensus is required in order for a block to be added to the chain
- Different consensus algorithms, most known PoW and PoS

What are the advantages of a blockchain?

- Advantages:
  - Immutable an append only, all block are time stamped in chronological order
  - Cryptographic protected
  - Storage of data is decentralized, data on the ledger can’t be lost
  - Transparency, provenance of data
  - Very strong protection against fraud and hacking
  - Verification without the need of third parties, delivers trust
  - Automation via smart contracts
  - Allows for financial inclusion, everyone can participate

What are the disadvantages of a blockchain?

- Disadvantages:
  - 51% attack
  - Difficult to adopt changes (hard forks)
  - Possibility of loss of private keys
  - Inefficiency (PoW)
  - Growing storage over time

Introduction to the Cardano blockchain

- Third generation blockchain platform also known as the Japanese Ethereum
  - Blockchain evolved out of scientific philosophy and research first driven approach
  - Only truly peer reviewed project - by academics outside of the project
    - review the code and check the validity that is been done
  - Open source - progress and code can be verified https://github.com/input-output-hk
  - Clear goals and roadmap
  - Written in the functional programming language Haskell - delivers the resilience necessary for mission critical systems (used in aerospace, defense, and financial industry)

Third generation blockchains

- Solving the problems of first and second generation blockchains
  - Proof of Stake vs Proof of Work
  - Energy efficient
  - Lower transaction fees
  - On and off-chain processing
  - Tokens are first class citizens (native)
  - Multiple layer solutions
  - Better scalability, more transactions per second (parallel processing)
  - Better security
  - etc.

Unique aspects of Cardano

- New PoS algorithm called Ouroboros - first proof of stake protocol that has been mathematically proven secure to the level of bitcoin
  - leader election process is done by way of a secure multiparty implementation of a coin flipping protocol
- Post-quantum cryptography - resistant against attacks by a quantum computer
- Multi-layer protocol
  - settlement layer - unit of account
  - control layer - runs the smart contract (recognize identity, assisting compliance)

Unique aspects of Cardano

- Protocol is tunable by setting parameters
- Support of native tokens - ERC-20 convertor
- Metadata support (ownership can not be recorded in the Bitcoin blockchain)
  - handy for certification and validation
  - samples: ownership provenance, intellectual ownership, supply chain tracking
  - 40 - 80 bytes extended to 16 kilo byte
- Post quantum cryptography - resistant against attacks by quantum computers
- Hardfork combinator - reliable way to switch the protocol from one version to another

Unique aspects of Cardano

- Treasure system - ensures sustainability of the protocol
- DevNet launch ~ 10th of Dec 2020
  - EVM - Ethereum interoperability, support for ETH tools and language
- IELE LLVM adoption strategy for all main programming languages
- Currency - ADA lovelace
  - 1 ADA = 1.000.000 lovelaces (0.000001 ADA = 1 lovelace)
  - Total supply 45 billion ADA
    - 1 BTC = 10^8 sats vs 1 ADA = 10^6 lovelaces
    - 21 million x 10^8 sats = 21^{14} satoshis
    - 45 billion x 10^6 lovelaces = 45^{15} lovelaces (~21x more supply than BTC)
  - Current circulation supply ~31.1M from which 63,1% is currently staked

Goal of Cardano

- Building the financial system of the future

Status of the Cardano blockchain

- Under development, roadmap https://cardanoroadmap.com/en/

- Phases
  - Byron - settlement layer protocol
  - Shelley - decentralization and stake pools
  - Goguen - smart contracts
  - Basho - scaling
  - Voltaire - governance

- Current phase: Goguen

Status of the Cardano blockchain

- **Byron**
  - Settlement layer protocol
  - Currency support
  - UTXO transactions
  - Daedalus wallet, https://daedaluswallet.io

Status of the Cardano blockchain

- **Shelley**
  - Decentralization - delegation, incentive scheme, reward scheme for stake pools, eUTXO
  - Community runs stake pools to secure the network
  - Ouroboros protocol enhancements
  - Daedalus wallet enhancements

Status of the Cardano blockchain

- BFT - Byzantine Fault tolerance consensus over the state of the network and next steps to be taken by nodes to avoid collapsing of the distributed network

- PRAOS - through private leader selection and forward security, key-evolving signatures avoid the prediction of next slot leader to avoid a planned attack

- GENESIS - security under dynamic availability, a novel chain selection rule that enables parties to join or rejoin the execution chain from the genesis block without requiring any trusted party or checkpoint preventing long-range attacks. In short a long range attack is a scenario where an adversary creates a branch on the blockchain starting from the genesis block and overtakes the main chain, this branch may contain different transactions and blocks also known as alternative history or history revision. https://blog.positive.com/rewriting-history-a-brief-introduction-to-long-range-attacks-54e473acdba9

Status of the Cardano blockchain

- **Goguen**
  - smart contracts
  - allows technical and non-technical people to write smart contracts
    - Plutus smart contract framework on basis of the functional programming language Haskell
    - Marlowe, a domain specific language to write smart contracts based on Plutus that non programmers can use to write financial smart contracts

Status of Cardano blockchain

- **Goguen**
  - Native tokens support. Addition of a multi-currency ledger enabling user to create new tokens, fungible and non fungible, supporting creation of new cryptocurrencies and tokenization of many types of digital and physical assets
  - ERC-20 convertor, migration of Ethereum tokens to Cardano

Allows for creation of Enterprise level, mission critical, decentralized smart contract applications, going to be operational mid 2021

Status of the Cardano blockchain

- **Basho**
  - Scaling
  - Side chains and offloading from the main chain to increase the capacity
  - Interoperability with other blockchains

Hydra is the result of a five year European-funded collaborative research project and can scale to a million of transactions per second, this is comfortably in excess of current global payment systems such as VISA. “Scalability is blockchain’s holy grail”.

Status of the Cardano blockchain

- **Voltaire**
  - Governance
  - Will make the Cardano blockchain a self sustaining system
  - Voting and treasury system

Q&A

THANKS!

In case you have questions?

contact us:
info@madelintwente.nl
https://madelintwente.nl

ada4profit@gmail.com
telegram: t.me/ada4profit_stakepool
https://ada4profit.com