INCS-741: Blockchain and Cryptocurrencies

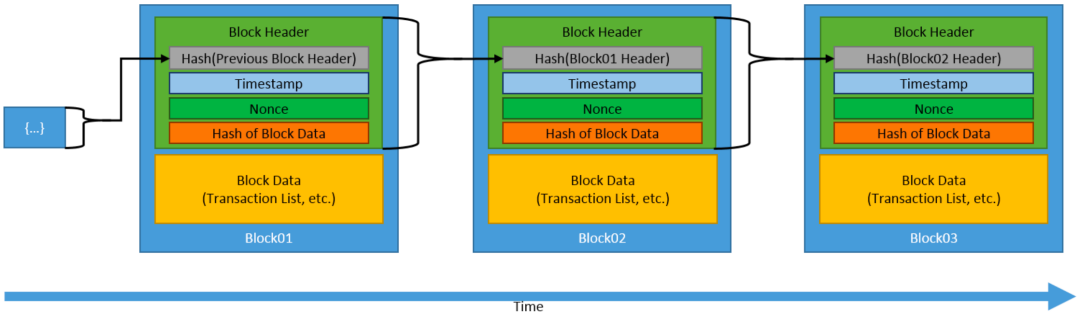
1

Definitions - Blockchain

- ***Blockchains*** are tamper evident and tamper resistant digital ledgers implemented in a distributed fashion (i.e., without a central repository) and usually without a central authority (i.e., a bank, company, or government) – ***NIST***
- A **blockchain** is a continuously **growing list of records**, called blocks, which are linked and secured using cryptography. Each block typically contains a hash pointer as a link to a previous block, a timestamp and transaction data.

2

Blockchain



- Generic Blockchain

3

Blockchain: Uses

- Cryptocurrencies
  - Digital currencies based on blockchain technology that rely heavily on cryptographic functions for their implementation
  - Bitcoin (2009), Ethereum (2015), Ripple (2012), Bitcoin Cash (2017), Litecoin (2011)
- Smart Contracts
  - Software deployed on the blockchain and executed by computers running that blockchain
  - They allow the enforcement of contracts between parties without the involvement of the parties or a third party
- Distributed Digital Ledgers

4

Cryptocurrency

- According to Jan Lansky, a cryptocurrency is a system that meets six conditions:
  1. The system does not require a central authority, its state is maintained through distributed consensus.
  2. The system keeps an overview of cryptocurrency units and their ownership.
  3. The system defines whether new cryptocurrency units can be created. If new cryptocurrency units can be created, the system defines the circumstances of their origin and how to determine the ownership of these new units.
  4. Ownership of cryptocurrency units can be proved exclusively cryptographically.
  5. The system allows transactions to be performed in which ownership of the cryptographic units is changed. A transaction statement can only be issued by an entity proving the current ownership of these units.
  6. If two different instructions for changing the ownership of the same cryptographic units are simultaneously entered, the system performs at most one of them.

5

Cryptocurrency: Cryptographic Technologies

- Cryptographic hash functions:
  - Creating unique identifiers
  - Securing block data – blocks store a hash of their data in the header
  - Securing block header

6

Cryptocurrency: Cryptographic Technologies

- Asymmetric-Key Cryptography:
  - Private keys are used to digitally sign transactions
  - Public keys are used to derive addresses
  - Public keys are used to verify signatures generated with private keys
  - Asymmetric-key cryptography provides the ability to verify that the user transferring value to another user is in possession of the private key capable of signing the transaction
- Address Derivation

public key → cryptographic hash function → address

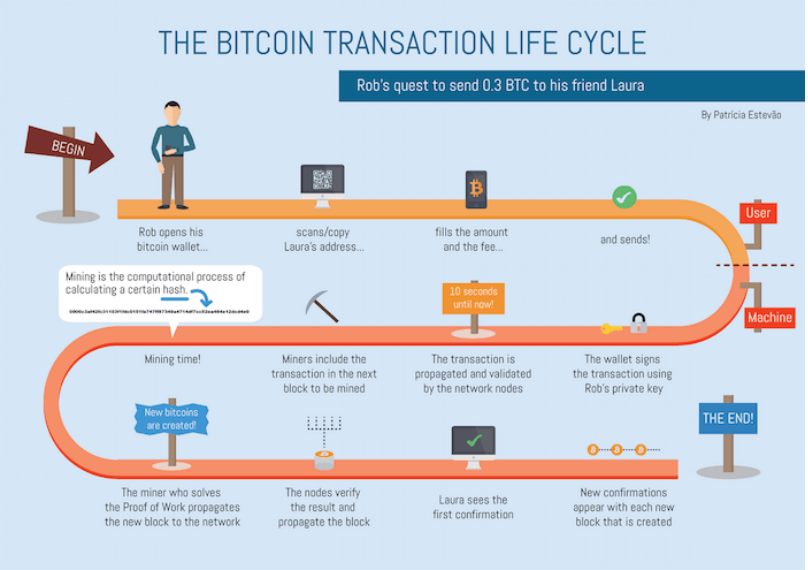
7

Cryptocurrency Wallets

- It is a program, implemented in hardware or software that stores a blockchain users private and public keys
- It interacts with various blockchains to enable users to send and receive digital currency and monitor their balance
- If you want to use Bitcoin or any other cryptocurrency, you will need to have a digital wallet
- Examples include:
  - Atomic Wallet
  - Bread Wallet
  - Mycelium
  - Exodus
  - Copay etc.

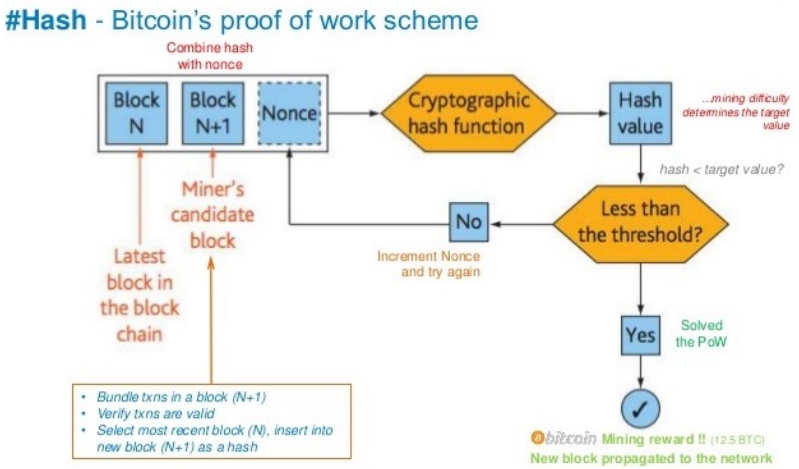
8

Bitcoin- Transactions



9

Bitcoin- *Proof-of-work*



10

Simulation Tools

- Coins2Learn - https://coins2learn.com/
- Shadow - https://shadow.github.io/
- Bitcoin Simulator - https://arthurgervais.github.io/Bitcoin-Simulator/
- BlockSim - https://github.com/blockbirdLabs/blocksim
- Live Monitoring - https://blockstream.info/

11

References

- D. Yaga, P. Mell, N. Roby, and K. Scarfone, “Blockchain Technology Overview,” NIST Draft NISTIR 8202, January 2018, available on https://csrc.nist.gov
- Z. Zheng, S. Xie, H. Dai, X. Chen and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," 2017 IEEE International Congress on Big Data (BigData Congress), Honolulu, HI, 2017, pp. 557-564.

12

Blockchain: Categories

- Permissionless
  - Anyone can read and write to the blockchain without authorization
- Permissioned
  - Limits participation to specific people or organizations

13