Blockchains

Ghada Almashaqbeh
UConn

History

- A whitepaper posted online in 2008: “Bitcoin: A Peer-to-Peer Electronic Cash System,” by Satoshi Nakamoto.
- Described a distributed cryptocurrency system not regulated by any government.
- The system went live on January 2009.
- Now “Satoshi Nakamoto” is only associated with certain public keys on Bitcoin blockchain.
  - She/He/They was/were active on forums/emails/etc. until 2010.
- Currently there are hundreds of cryptocurrencies (https://coinmarketcap.com/).

Cryptocurrencies

- The use of cryptographic primitives and distributed consensus protocols to secure virtual money creation and flow between various parties.
- “A type of unregulated, digital money, which is issued and usually controlled by its developers, and used and accepted among the members of a specific virtual community” - European Central Bank.

Blockchain

- An append only ledger.
  - Simply an immutable record of all transactions and actions performed in the system so far.
  - Each page of this ledger is called a block.
  - These pages are glued together by using a hash chain.
  - Adding a new page on the ledger is done through a process called mining.

Utility of Blockchains

- Initially, the goal was to build a decentralized virtual currency medium.
- Interest has shifted towards providing a decentralized service on top of this medium.
- Lately blockchains on their own (without involving any currency) are used in several applications.
  - Mainly to support transparency and public verifiability.
  - Examples include healthcare, business management, and supply chains.

Bitcoin in a Nutshell I

- A distributed currency exchange medium open to anyone to join.
  - Powered by a peer-to-peer (P2P) network.
- Utilize basic cryptographic primitives to control the money flow in the system.
  - Hash functions and digital signatures.
- Building blocks:
  - Players: miners and clients.
  - Transactions: messages exchanged.
  - Blockchain: an append only log.
  - Mining: extending the blockchain.
  - Consensus: agreeing on the current state of the Blockchain.

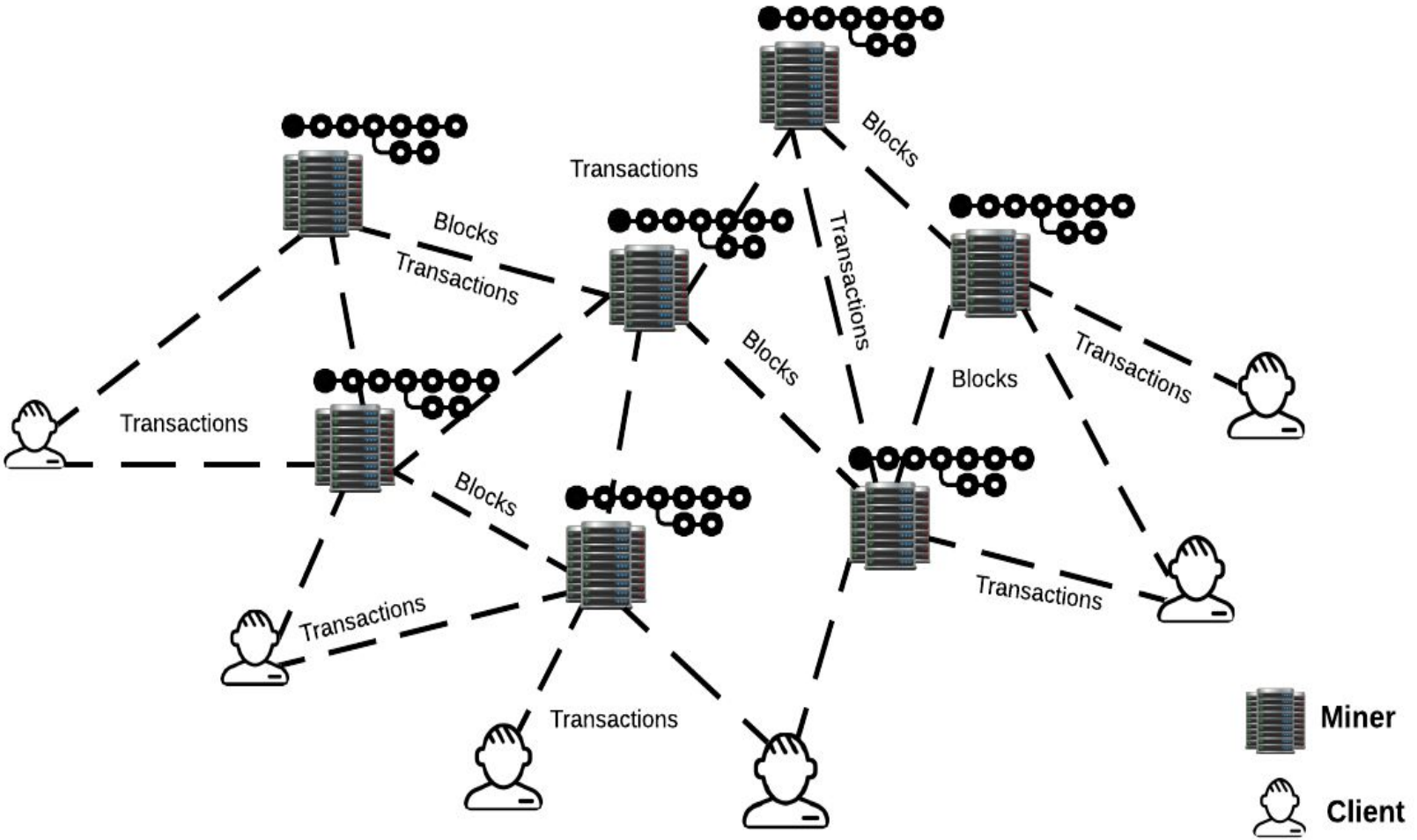
Bitcoin in a Nutshell II

- No real identities are required, just a key pair.
- Owning the private key of the destination address of currency transfer means you own the currency value of that address.
- Losing the private key of a specific address means losing the coins associated to this address forever.
  - Wallets take care of tracking coins, issue transactions, etc.
- Digital signatures are used to prove your ownership of the private key associated to the coins you want to spend.
- Everything is logged on a public ledger called a blockchain.
  - Built basically using a linked list and hash pointers.

Who is Who in Bitcoin

- Two types of nodes in Bitcoin network:
  - **Lightweight nodes or clients:**
    - Also called thin clients or simple payment verification (SPV) clients.
    - The vast majority of Bitcoin nodes are lightweight ones.
    - Do not store the whole blockchain, only specific parts to verify the transactions they care about.
    - They trust the miners in generating trusted and true blocks.
  - **Fully validating nodes or miners:**
    - Must stay permanently connected to the system.
    - Have a good network connectivity to be able to hear all transactions (hopefully).
    - Store a full copy of the blockchain.

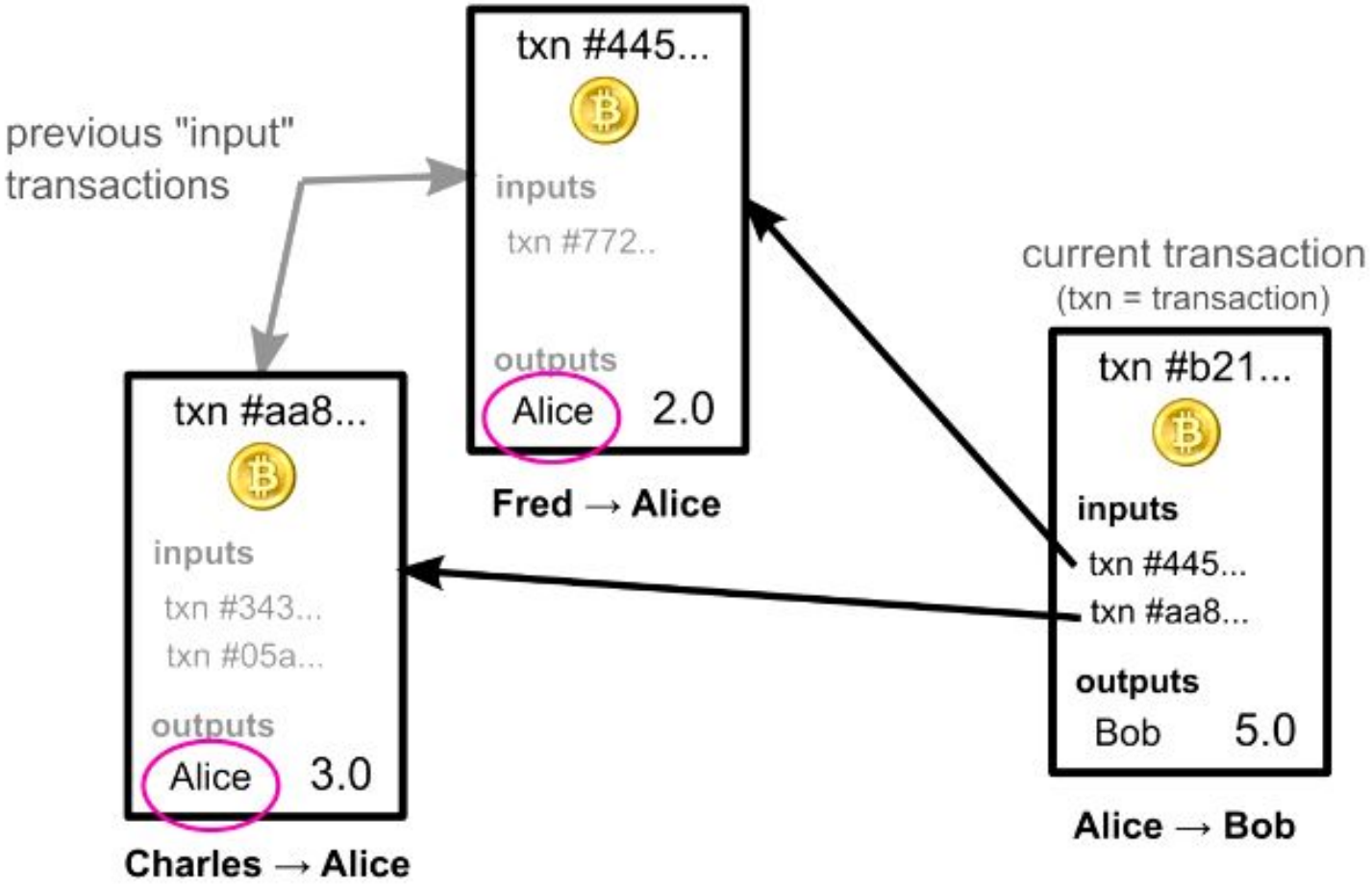
Bitcoin Pictorially



Bitcoin Transactions

- Transactions represent the digital tokens, or virtual coins, in Bitcoin.
- A new transaction is issued by any node as follows:
  - Fill the following fields:
    - Input section: list of pointers to previous unspent transactions owned by the sender.
    - Output section: the address of the receiver or the hash of the output script.
  - Sign the whole transaction (including the output section) using the private keys associated with the inputs.
- The sender then broadcasts the transaction over the network.

Bitcoin Transactions - Pictorially



Source: http://www.imponderablethings.com/2013/07/how-bitcoin-works-under-hood.html

The Public Ledger or Blockchain

- Append only log contains a full record of all transactions.
  - These transactions are recorded in blocks.
  - The blockchain is a linked list of these blocks, linked by their hashes.
- Miners extend the blockchain by mining new blocks.
  - Solve a proof-of-work puzzle.
  - Collect monetary incentives.
- Each block has a header and a body.
  - Header includes meta data, while the body include the list of transactions recorded in a block.

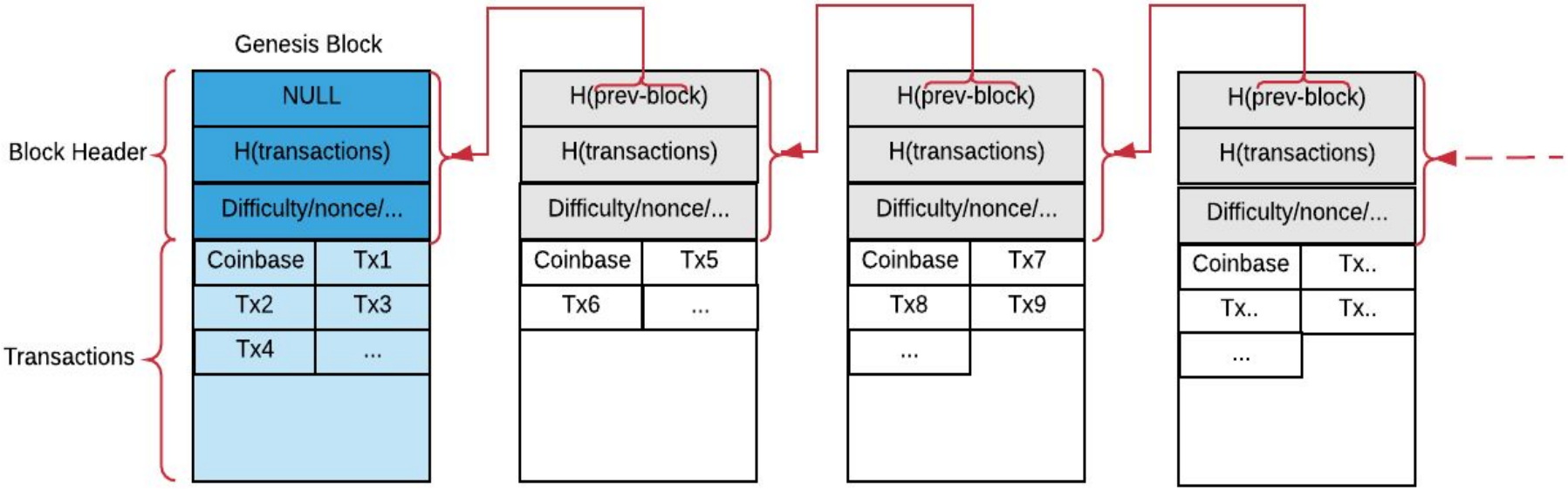
Block Header

- Consists of:
  - 4 bytes ➔ Version: A version number to track software/protocol upgrades
  - 32 bytes ➔ Previous Block Hash: A reference to the hash of the previous (parent) block in the chain
  - 32 bytes ➔ Merkle Root: A hash of the root of the Merkle-Tree of this block's transactions
  - 4 bytes ➔ Timestamp: The approximate creation time of this block (seconds from Unix Epoch)
  - 4 bytes ➔ Difficulty Target: The Proof-of-Work algorithm difficulty target for this block
  - 4 bytes ➔ Nonce: A random value used for the Proof-of-Work algorithm

Block Body

- The content of a block is a set of transactions including:
  - Standard transactions broadcast by the users in the network.
    - Only valid and unspent ones are included.
  - Coinbase transaction with value equals to the mining reward destined to the miner who mines the block.

The Blockchain Structure



Mining I

- The miners extend the blockchain with new blocks (and mint new currency).
- Done through proof-of-work.
  - Needed to prevent Sybil attacks.
- Miners solve a hash puzzle,

  SHA-256(SHA-256 (new block header)) < Difficulty Target

- For secure hash functions, the only way to find the hash with a given property is to try nonce values until a desired hash is found.
  - Hence it is solving a hash puzzle.
- Verification is very easy, other miners check the validity of all transactions in a block, and then verify the solution of the hash puzzle.
  - The latter is a single hash invocation.

Mining II

- Difficulty is adjusted periodically, roughly, every two weeks.
  - Keeps the block generation rate constant, 1 block every 10 minutes.
  - Accommodates the increasing computation power of miners.
    - New strong miners may join the network, hence, they will be able to solve the puzzle faster.
    - Affects the security of the blockchain, strong miners could be able to rewrite the blockchain and change its view.
- Miners are incentivised for mining by:
  - Mining rewards.
  - Transaction fees.

Required Security Properties

- What security properties we require hashes to have to achieve security (namely blockchain immutability)?
  - Collision resistance?
  - PoI?
  - PoC?
- But are not hash functions public and so the blockchain? Why cannot an attacker rewrite the blockchain.
  - Security assumption: honest majority of the mining power