Blockchain: Some Basics

Raja Velu

February,2021

Map

- Motivation
- Basics
- Applications
- Myths
- Questions

What is Possible?

- Instant, secure, costless, decentralized transfer of information and ownership
- How Potential to
  - Disrupt the functioning of oligopolistic institutions
  - Eliminate transaction costs
  - Enhance growth as innovators can find new ways to raise capital.

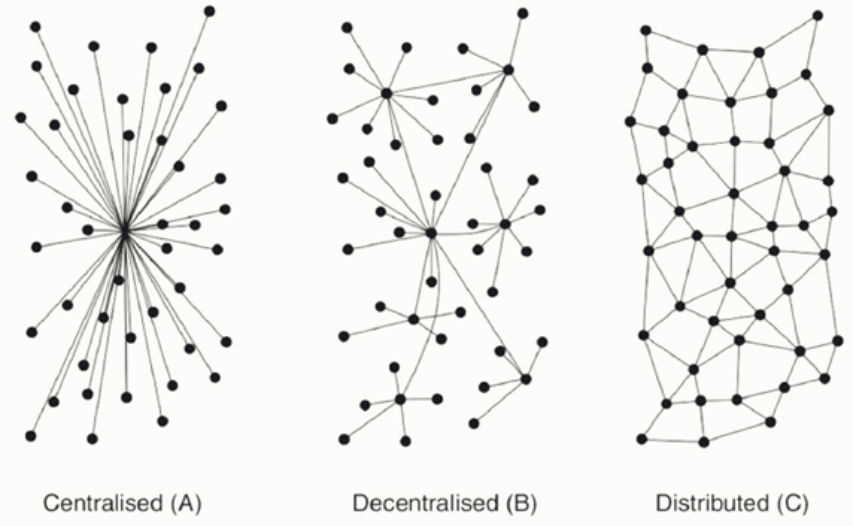
Blockchain in a Technology

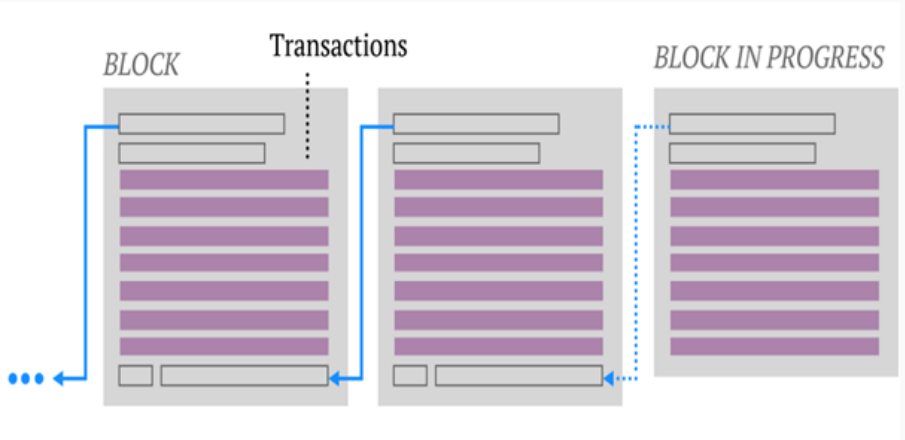
- Concept proposed in Haber and Stornetta (1991): Time-Stamping Digital Documents/ Cryptography
- Blockchain is not Bitcoin!

Blockchain is a Ledger

A very special ledger

- Quickly and easily accessed and shared by many – distributed
- Various levels of transparency depending on application
- Immutable (you can only add to it – you cannot alter history)
- Cryptographically secured

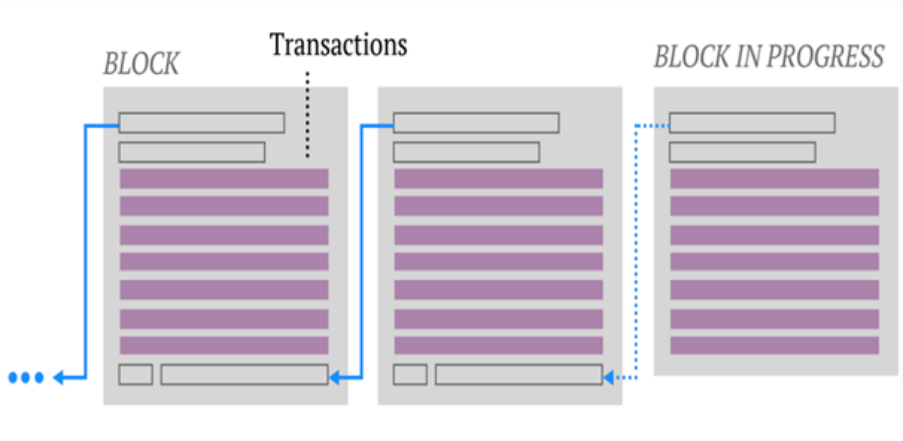




How do public blockchains work?

Cryptographic security

– Last line (hash) is repeated as the first line in the next block. This is why it is called "chain". Altering any data in say block 1, means the last line will change and will not match the first line in block 2.



What can blockchain technology do?

Solves many problems

- Verification of ownership (quickly check the immutable history recorded on a blockchain to see if someone owns something)
- Efficient exchange of ownership (direct transactions without middle person, everybody treated the same whether customer, retailer or banker).

Applications

- Payments (new SWIFT, implications of micropayments)
- Financial inclusion
- Tokenization of assets (stocks, bonds, etc.)
- National currencies
- Proof of ownership (property, rental)
- Proof of identity (license, SSN, passport, $\cdots$) [with zero knowledge]
- Monetization of personal data
- Supply chain
- Securing private information (health records)
- Dispensing drugs
- Financial statements
- Digital twins
- IoT
- Community markets

Blockchain myths (if time)

- Satoshi Nakamoto invented blockchain in 2008
- There is one blockchain: "the" blockchain
- Blockchains are routinely hacked
- Blockchains are anonymous
- Cryptocurrencies are ideal for illegal transactions
- Blockchain will never go anywhere because it is energy inefficient
- Quantum computing nullifies the impact of blockchain
- You need a computer science degree to understand blockchain technology
- I don't need to stress out about blockchain because it is a technology of the distant future

Prime targets of disruption

Any situation with a thick layer of middle people

– Blockchain is fundamentally a P2P technology.

Types of blockchains

Public blockchains

- Trustless. Original example bitcoin blockchain. Open source code.
- Ethereum blockchain allows for contracting and is the main choice for most corporate applications. Contracts can be conditional, if then statements. Bitcoin blockchain cannot do this.
- Variety of mechanisms to ensure security (Proof of Work, Proof of Stake, Proof of Authority, Zero Knowledge Proof, etc.)

Private blockchains

- Trust required.
- Need to determine if the cost of trustlessness is worth it. Most applications today involve trust. Combining blockchain technology with trust allows for much more efficient transactions (think of payments)

Bitcoin Blockchain (original)

- Distributed, secure, transparent public ledger that establishes ownership, exchange of ownership.
- Decentralized; available to anyone.
- Controlled by no one, monitored by everyone.
- Strong Cryptography, miners provide, rewarded for security.
- Cost of network power?

Hashing: Example

- Mapping data of arbitrary size to fixed size values
- Encode, $a = 1, b = 2, \cdots, z = 26$
- Send a mail with a single word: "HELLO"
  $(8 \times 5 \times 12 \times 12 \times 15 = 86400)$
- Receiver does the same hash to retrieve information.
- "HALLO"=$8 \times 1 \times 12 \times 12 \times 15 = 12280$, doesn't match.
- "OHELL"=86400, results in "collision". Too simple.
- One-way function, not "encryption".
- SHA-2

Blockchain: Some more jargons

- Distributed ledger-spread across all peers holding a copy.
- Cryptographically secure
- Append only; once added, data is immutable.
- Updateable via concensus.
- Block – transactions bundled together.
- NONCE – A number generated for authoritication/encryption.
- Merkle root, Hash of all nodes of a Merkle tree
- Smart contract: Logic to be executed when certain conditions are met.

More Jargons

- Tokenized Blockchains: Standard, generates cryptocurrency via consensus, mining etc. Bitcoin /Ethereum
- Tokenless: No value transfer, transfer of information
- Consensus: Backbone of a Blockchain; process of agreement between distrusting nodes. Decentralized through mining. Byzantines Generals problem.
- Some consensus algorithms: Proof of work, Proof of stake, Proof of deposit
- Methods of Decentralization, platforms: Ethereum, Maidsafe, Lisk etc.

Bitcoin – An Introduction

- First application of Blockchain Technology. Nakamoto (2008) bitcoin.org/bitcoin.pdf
- Main components:
  - Digital Keys
  - Addresses
  - Transactions
  - Blockchain
  - Miners
  - Bitcoin Network
  - Wallets (Client Software)

Steps for sending a payment

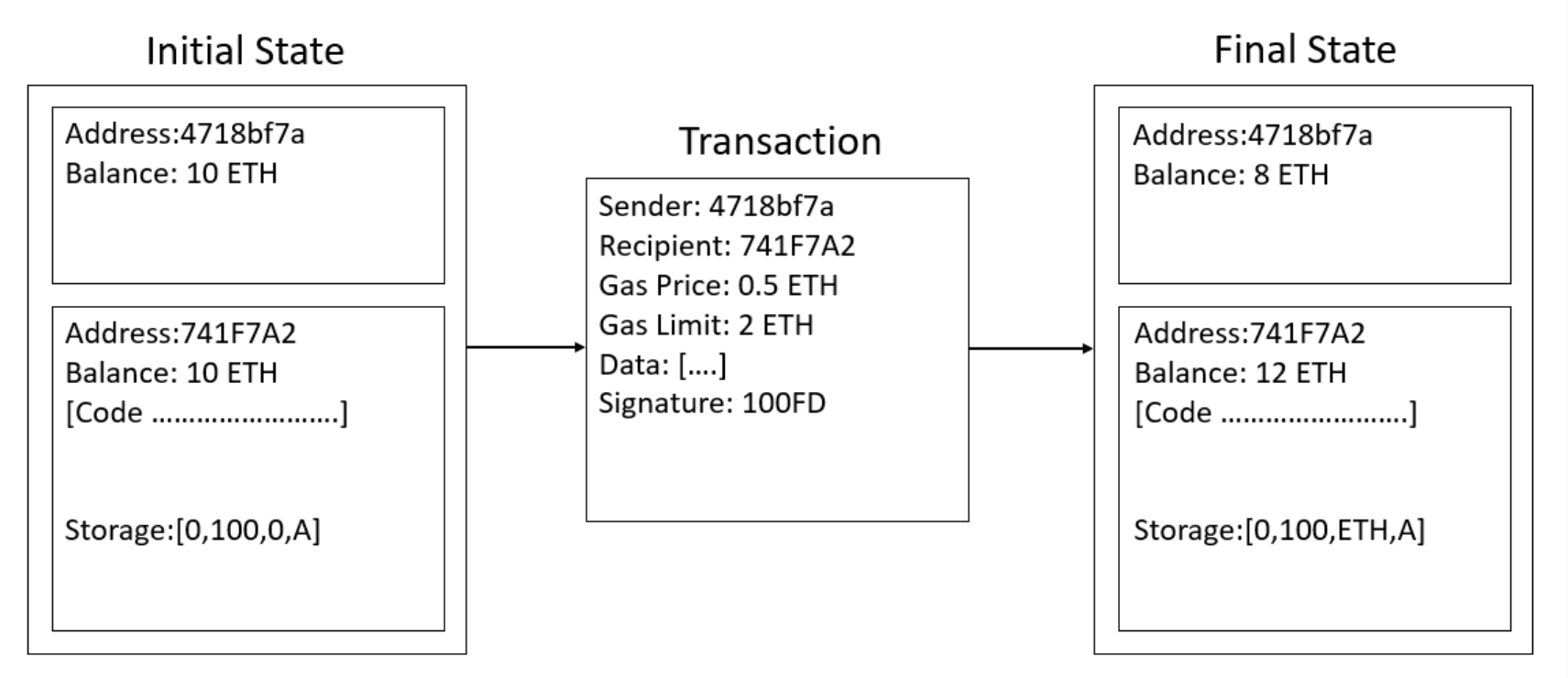
- Sender signs the transaction with a private key
- Transaction serialized/transmitted to the network
- Miners pick up/verify validity
- Transaction added to the candidate block for mining
- Once mined, result is broadcasted to all nodes

More on Components:

- **Private Key:** 256-bit numbers randomly chosen/ converted to QR code.
- **Public Key:** Derived from private keys by mathematical relationship.
- **Address:** Public key hashed twice; address is used only once.
- **Transactions:** At least three conformations are required; Fees vary; Verification is the important part. Double spending, authentication etc.
- **Minding:** Process of adding new blocks/ resource-intensive as proof-of-work verification is difficult; fee depends on the complexity. Block header contains 32-bit nonce field, miners vary the nonce until the resultant hash is less than a predetermined target.

Ethereum Blockchain:(2013)

– Critical Idea: Turing-complete language, allows for arbitrary smart contracts in contrast to Bitcoin.



Economics of Blockchain

- Cost of Verification of State
  - Currently done by a third party. Tracking settlements, Enforcing contracts etc. Results in information sharing and leakage.
  - In Blockchain, information stored on a distributed ledger is easy to verify; trust in the intermediary is replaced with trust in the underlying code/consensus rules (how regularly distribute the true state of the shared data etc)
  - Ether, Filecoin (data storage), BAT (digital ad), Blockstack (digital identify) etc
  - As cost of digital verification falls, it can improve the process of offline verification as well.

Economics of Blockchain (contd)

- Cost of Networking
  - Reduction in the cost of verification is a necessary condition for reduction in the cost of networking, but not a sufficient condition.
  - There is a difference between permissioned and permissionless blockchains.
  - Market power is in the hands of many! Lower Privacy Risk.

Some Useful Links

- https://blog.programster.org/bitcoins-mathematical-problem
- https://www.youtube.com/watch?v=SSo_EIwHSd4
- https://www.youtube.com/watch?v=yubzJw0uiE4
- https://www.bitcoin.com/get-started/
- https://www.nytimes.com/2021/01/26/technology/what-is-blockchain.html?searchResultPosition=1
- https://www.nytimes.com/2021/01/26/technology/big-tech-power-bitcoin.html?searchResultPosition=2
- https://www.wsj.com/articles/cryptocurrency-startup-ripples-future-hinges-on-sec-case-1161
  mod=lead_feature_below_a_pos1
- https://en.wikipedia.org/wiki/Proof_of_work