CSCI 6313 – Introduction to Blockchains

Prof Peter Bodorik

Email: Peter.Bodorik@dal.ca

Faculty of Computer Science, Dalhousie University,

Halifax, NS Canada

Adopted from: https://www.forbes.com/advisor/investing/cryptocurrency/what-is-blockchain/

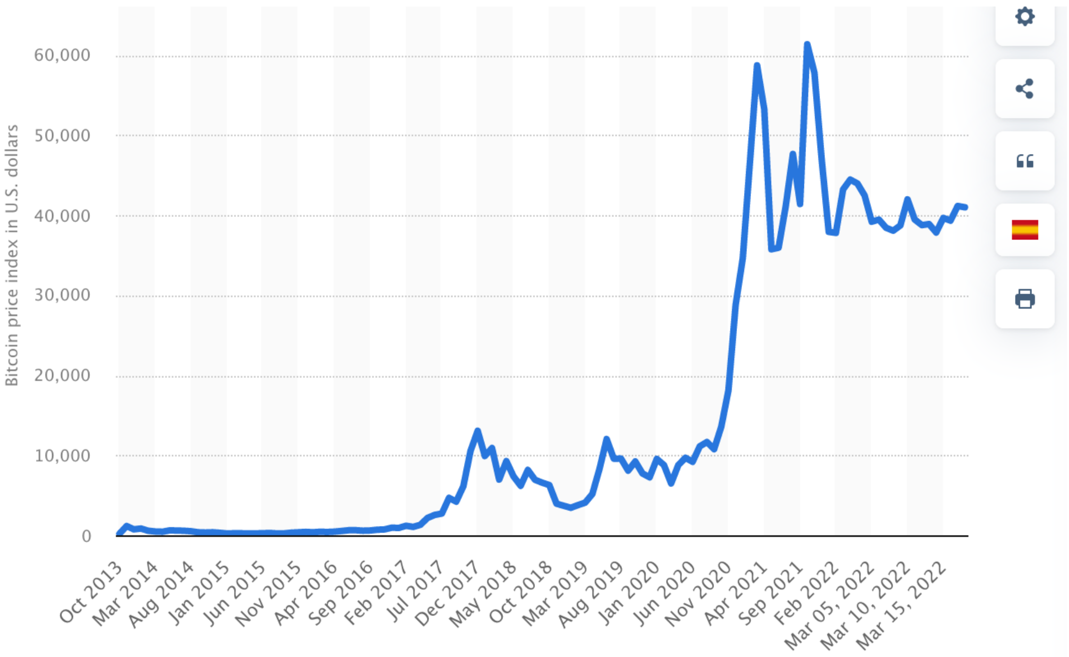
- Introduction
- History
- Block, Chain, Consensus
- Permissioned, non-permissioned
- Smart contracts
- Tokens
- ICOs
- Are B-chains safe and lasting?
- Blockchain Challenges

Bitcoin

- 2008: Satoshi Nakamoto Bitcoin white paper
- 2009: Bitcoin Network goes live
- 2010: First cryptocurrency stock exchange for trading Bitcoin

  …
- 2017 … Crypto crash ?

  …
- 2021 … Crypto crash ?



© Statista 2022

Blockchains: Are they safe?

- Blockchain vulnerabilities
  - 51% attacks
    - Miner collude … need 51% of miners
    - Problem for smaller chains
  - Blockchain infrastructure creation errors
    - Configurations
    - Coding
  - Insufficient security
    - Wallets, trading, …
    - Smart contracts … as any other code … e.g., re-entrancy attack (DAO attack)
- Blockchains are safe …
  - As for any software … best security practices must be followed …
  - Most attacks … social engineering & code vulnerabilities exploits
- Smart contracts security? … More later

Failed currencies … introduce Bitcoin

Digital Currencies That Failed

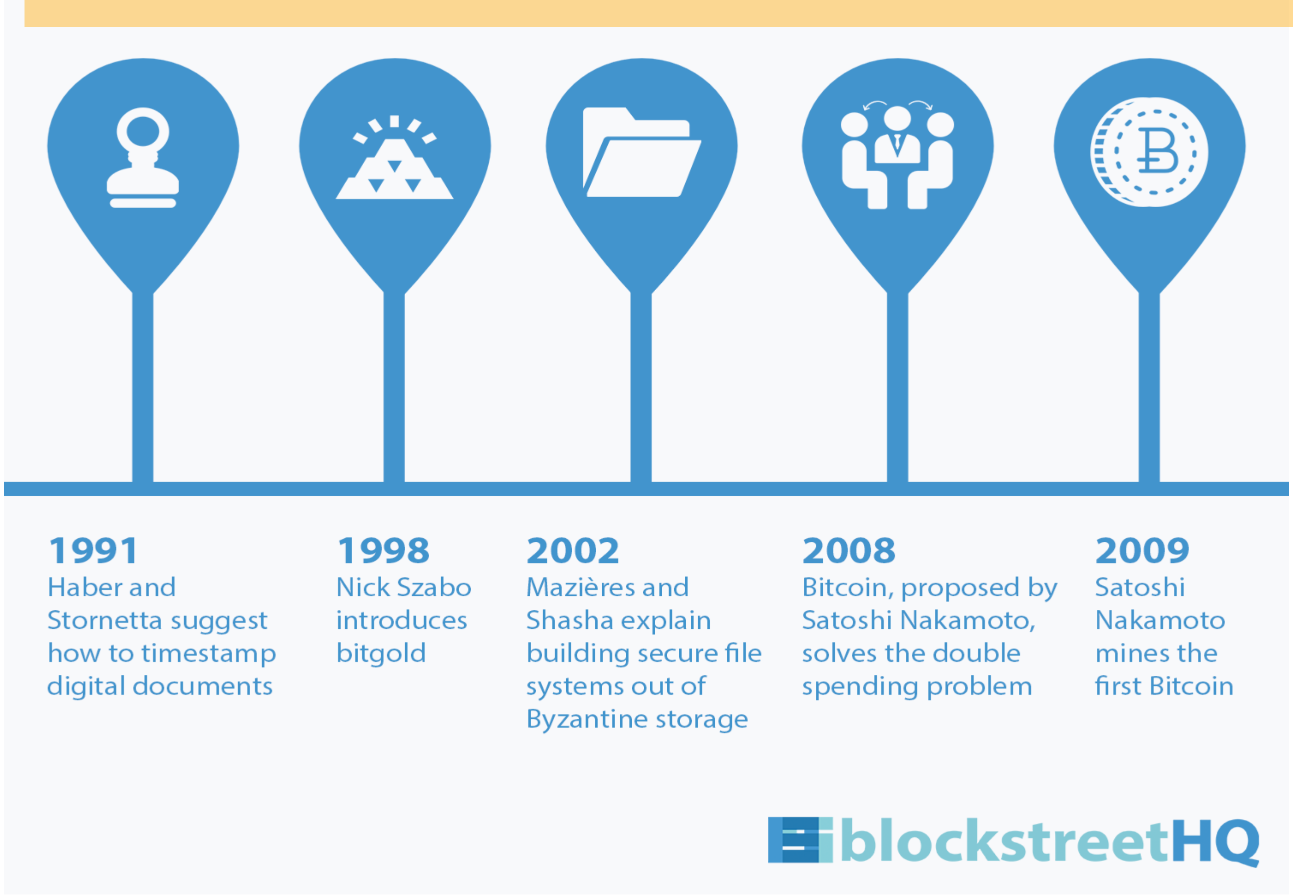
- DigiCash – 1989
- Mondex -1993
- E-gold – 1996
- Hashcash – 1997
- Bit Gold – 1998
- Lucre – 1999

Bitcoin

- 2008: Bitcoin White Paper by "Satoshi Nakamoto"
- 2009: The Bitcoin Network goes live and the first Bitcoins are mined
- 2010: The first cryptocurrency stock exchange for trading Bitcoin is launched

Intro to Blockchains - History

Historical timeline



1991
Haber and Stornetta suggest how to timestamp digital documents

1998
Nick Szabo introduces bitgold

2002
Mazières and Shasha explain building secure file systems out of Byzantine storage

2008
Bitcoin, proposed by Satoshi Nakamoto, solves the double spending problem

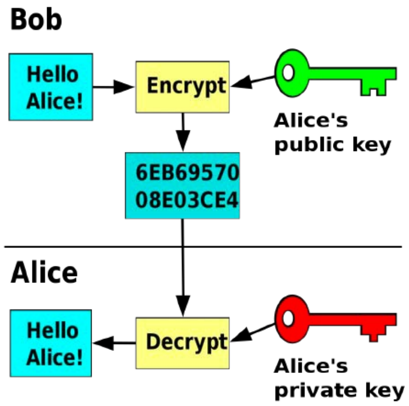
2009
Satoshi Nakamoto mines the first Bitcoin

https://medium.com/blockstreethq/before-blockchain-there-was-distributed-ledger-technology-319d0295f011

Innovations

- Internet protocols (TCP/IP 1994; HTTP 1990)
- Peer to peer computing, distributed computing, …
- Cryptography
  - Hashing
  - Asymmetric (public-key) cryptography

Wikipedia … Public domain



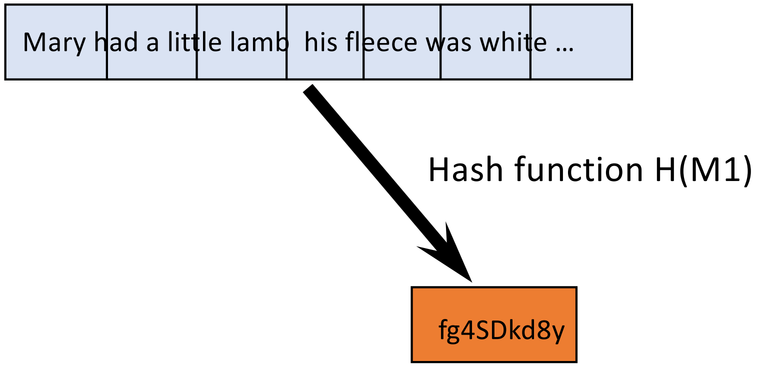
Wikipedia … Public domain

Hashing

Hashing

- Hash function – easy to compute
- Hashing function transforms/maps information contained in a file (could be large) to a single large number (e.g., 128 bits or 256 bits)
- Given a hash-code (256 bits) … ***not known how to find plaintext that will hash to that hash-code***

M1 plaintext message … long file … megabytes



Mary had a little lamb his fleece was white …

Hash function H(M1)

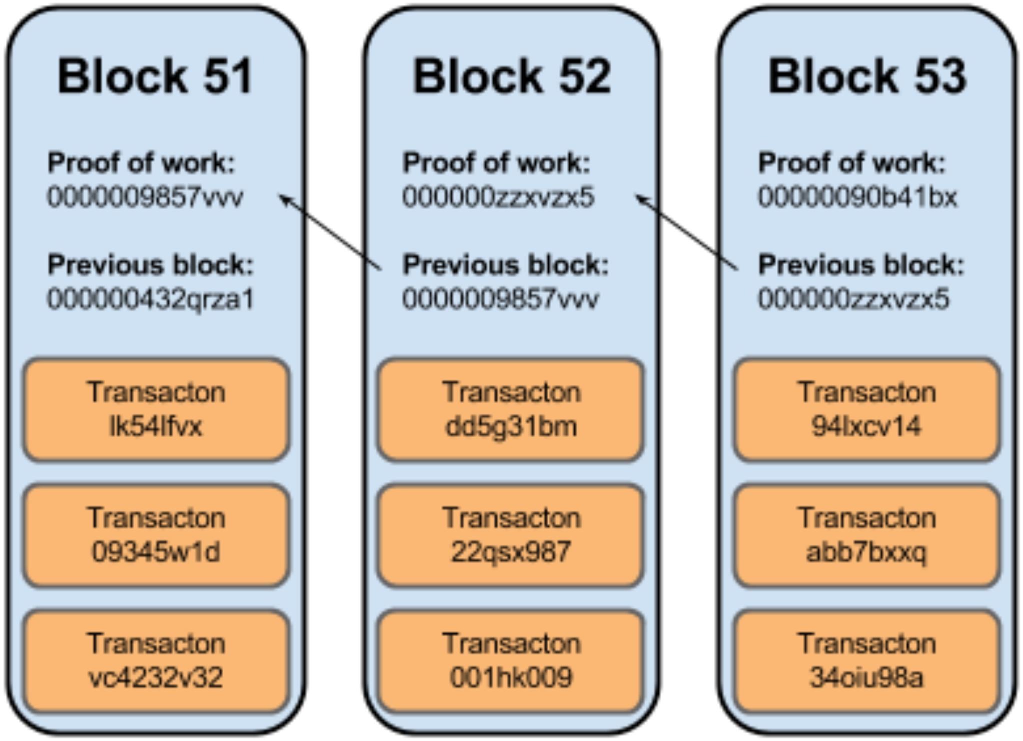
fg4SDkd8y

Message Digest … Hash-code… 256 bits => 2^{256} codes … 1.1579209e+77

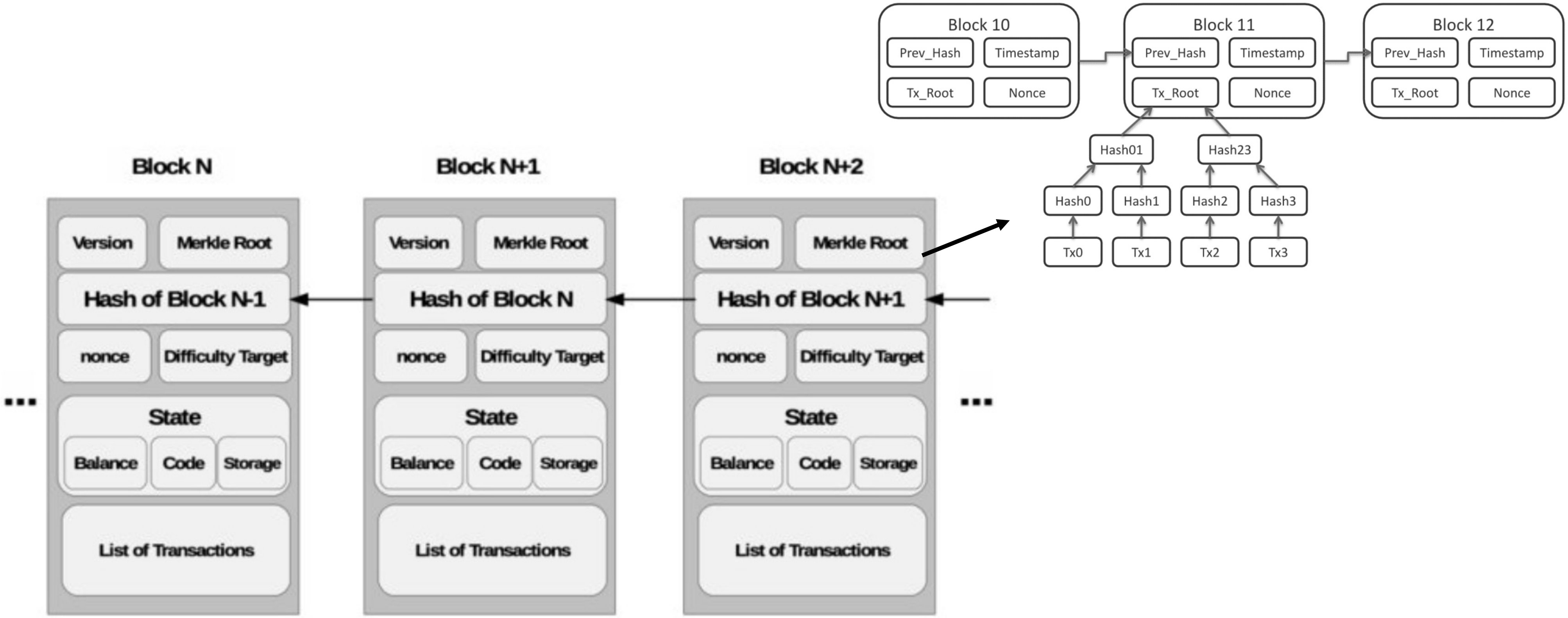
2^{150} = 1 427 247 692 705 959 881 058 285 969 449 495 136 382 746 624 ≈ 1000^{15}

Blockchain – Append only Chain of Blocks

- Block
  - Transaction writes are recorded in blocks
  - Cryptographic methods in transactions
  - Block contains link to previous block in the
  - Chain grows as new information is added
  - Shared digital ledger
  - Immutable updates and append-only
- Smart contract … program
  - Stored on the blockchain
  - Executed by EVM



Potpourri - Block details



Block 10

Prev_Hash | Timestamp

Tx_Root | Nonce

Block 11

Prev_Hash | Timestamp

Tx_Root | Nonce

Block 12

Prev_Hash | Timestamp

Tx_Root | Nonce

Hash01 | Hash23

Hash0 | Hash1 | Hash2 | Hash3

Tx0 | Tx1 | Tx2 | Tx3

Block N

Version | Merkle Root

Hash of Block N-1

nonce | Difficulty Target

State: Balance | Code | Storage

List of Transactions

Block N+1

Version | Merkle Root

Hash of Block N

nonce | Difficulty Target

State: Balance | Code | Storage

List of Transactions

Block N+2

Version | Merkle Root

Hash of Block N+1

nonce | Difficulty Target

State: Balance | Code | Storage

List of Transactions

...

...

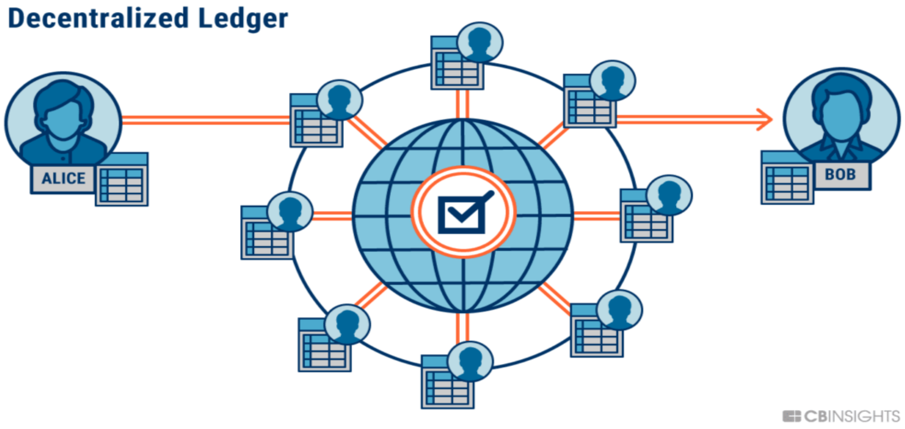
https://www.researchgate.net/publication/321017113_IoT_Security_Review_Blockchain_Solutions_and_Open_Challenges/figures?lo=1

Blockchain – Decentralized Ledger

- Blockchain

  … replicated chain of blocks

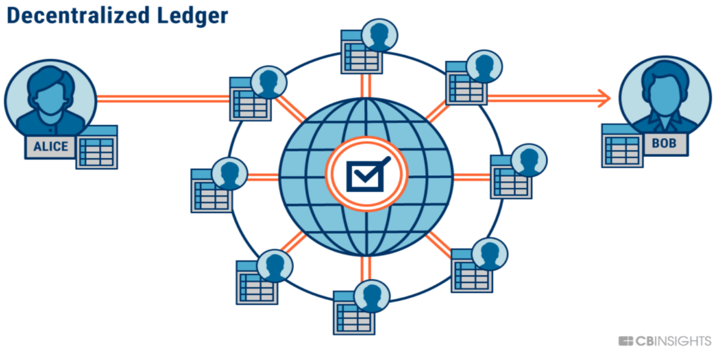
- Nodes
  - Node … executing client node software
  - Contains a copy of the blockchain
  - Assist in forming consensus
  - Who can join? => public, private, permissioned
  - User connects to a node to transact



Adopted from: https://www.cbinsights.com/research/what-is-blockchain-technology/

Blockchain – Decentralized Ledger … continued

- Adding a block to the chain … consensus
  - General agreement by majority of parties on the state of the distributed ledge
    - Proof-of-Work and Mining (large coin burn)
    - Proof-of-Stake … PoAuthority, PoCapacity, PoActivity, PoElapsedTime, PoBurn, …
- Blockchains categories … later
  - Public vs. Private
  - Permissioned vs. non-permissioned



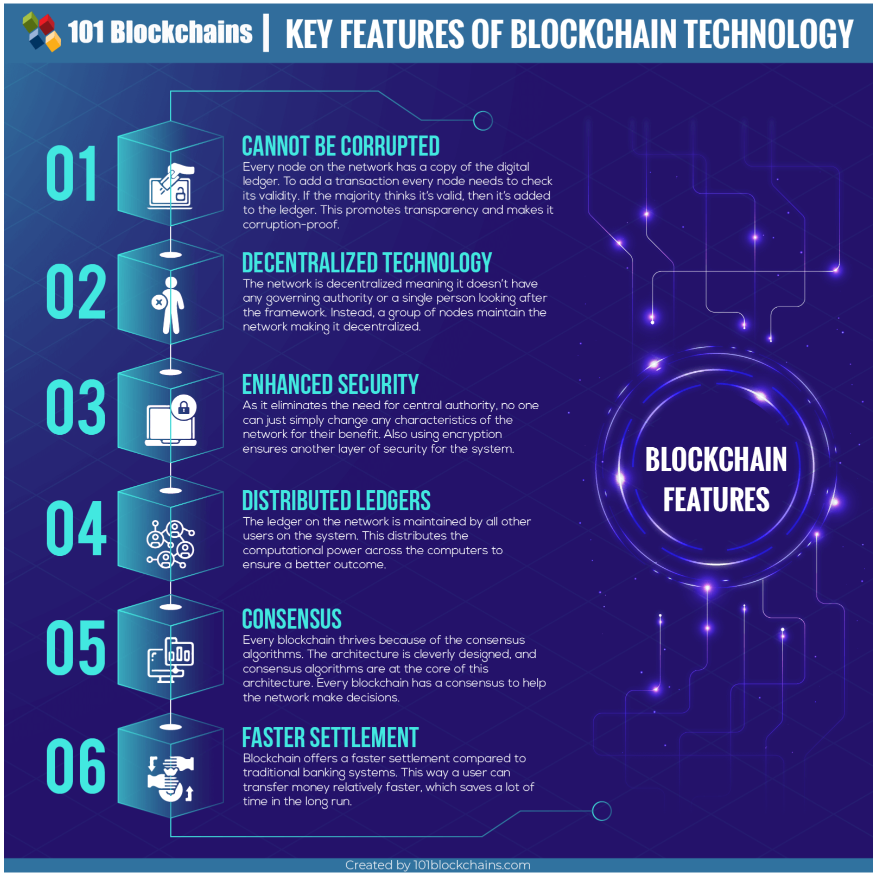
Adopted from: https://www.cbinsights.com/research/what-is-blockchain-technology/

Blockchain Features

Trust => Key Feature

Blockchain

- Improves trust
- Eliminates Trusted Third Parties
- Facilitates faster settlements



101 Blockchains | KEY FEATURES OF BLOCKCHAIN TECHNOLOGY

01 CANNOT BE CORRUPTED

Every node on the network has a copy of the digital ledger. To add a transaction every node needs to check its validity. If the majority thinks it's valid, then it's added to the ledger. This promotes transparency and makes it corruption-proof.

02 DECENTRALIZED TECHNOLOGY

The network is decentralized meaning it doesn't have any governing authority or a single person looking after the framework. Instead, a group of nodes maintain the network making it decentralized.

03 ENHANCED SECURITY

As it eliminates the need for central authority, no one can just simply change any characteristics of the network for their benefit. Also using encryption ensures another layer of security for the system.

04 DISTRIBUTED LEDGERS

The ledger on the network is maintained by all other users on the system. This distributes the computational power across the computers to ensure a better outcome.

05 CONSENSUS

Every blockchain thrives because of the consensus algorithms. The architecture is cleverly designed, and consensus algorithms are at the core of this architecture. Every blockchain has a consensus to help the network make decisions.

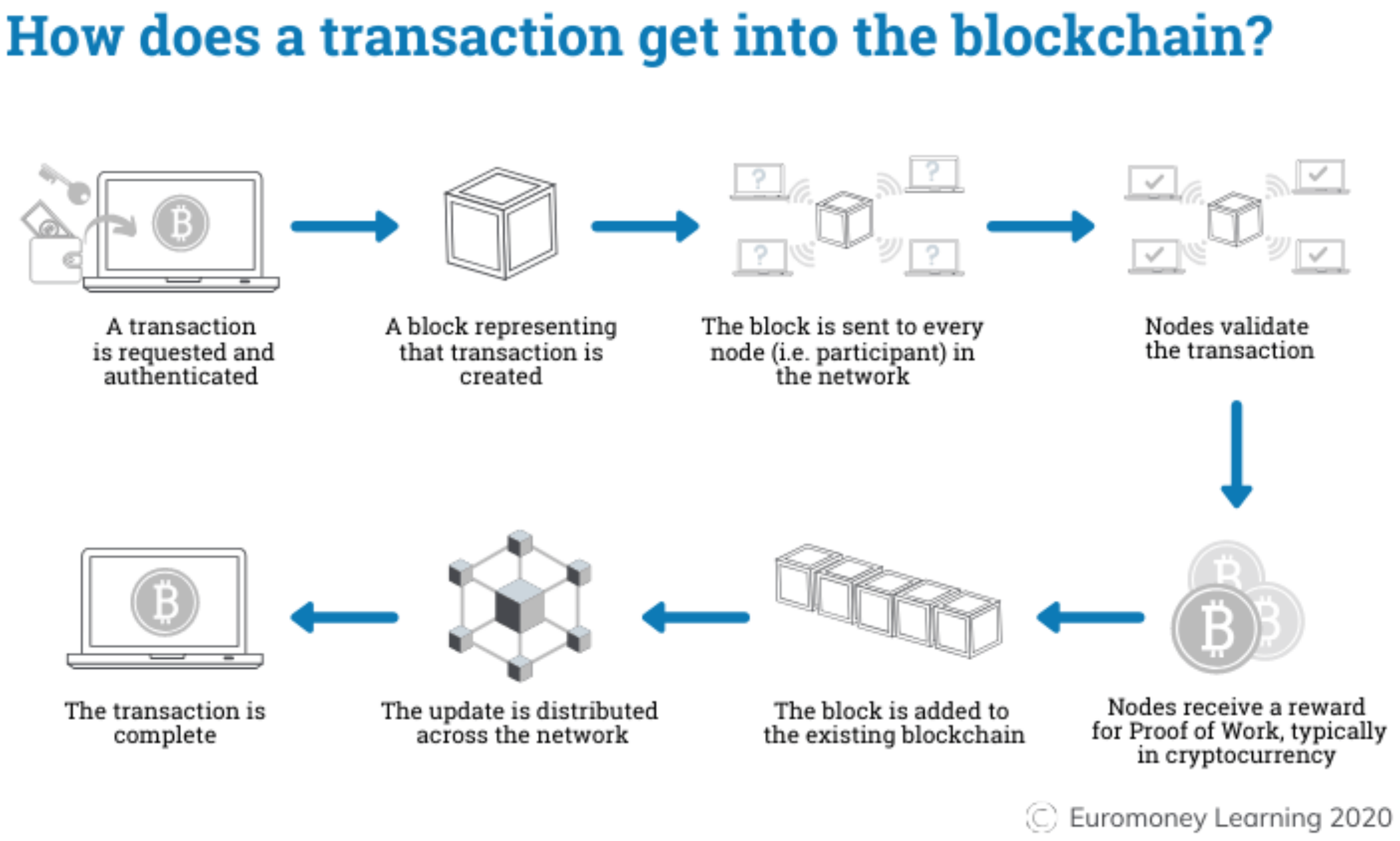
06 FASTER SETTLEMENT

Blockchain offers a faster settlement compared to traditional banking systems. This way a user can transfer money relatively faster, which saves a lot of time in the long run.

Created by 101blockchains.com

https://101blockchains.com/introduction-to-blockchain-features/#prettyPhoto/2/

Bitcoin: Adding a Block - Consensus Algorithm



How does a transaction get into the blockchain?

1. A transaction is requested and authenticated
2. A block representing that transaction is created
3. The block is sent to every node (i.e. participant) in the network
4. Nodes validate the transaction
5. Nodes receive a reward for Proof of Work, typically in cryptocurrency
6. The block is added to the existing blockchain
7. The update is distributed across the network
8. The transaction is complete

Ⓒ Euromoney Learning 2020

Adopted from: https://www.euromoney.com/learning/blockchain-explained/how-transactions-get-into-the-blockchain

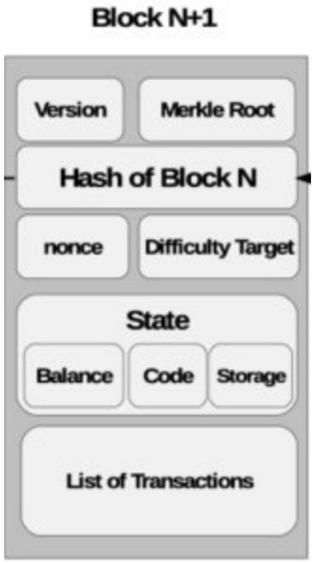
Consensus / Validation

- Which block is added

PoW – Puzzle, Solution, Checking

Note on Block Creation

- Each transaction is *broadcast*
- When a node receives a transaction (from a connected user or another node), it validates the transaction information
  - Eventually the transaction is appended to a block
- When the node's block is full, the node starts mining
  - There may be many miners trying to solve the PoW puzzle simultaneously
  - Each miner has its own block of transaction
  - A transaction in one miner's block may or may not appear in another miner's block.
  - If the same transactions appear in two or more blocks, they may appear in different orders in those blocks.



Proof of Work (PoW)

- Find NONCE (32-bit value) and store it in the block; NONCE must be such that
  - Hash of the block (includes nonce, Target difficulty, …) < Target difficulty

- Once a node solves the puzzle (finds the nonce bit pattern satisfying the above), the block (that includes the nonce and difficulty) is broadcast
- When a node receives the block with solution
  - It checks the solutions (using its hash of its own previous block or checks the hash of previous block of the solution with the hash of the previous block in its own chain)
  - Executes each transaction in the block

Video: transaction added to block & block validation

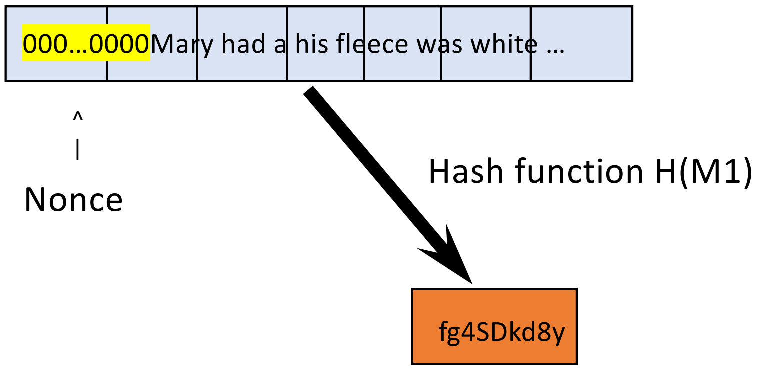
Video: Ethereum PoS & Sharding

Hashing

Hashing

- Hash function – easy to compute
- Given a hash-code (256 bits) … *not known how to find plaintext that will hash to a particular hash-code*
- *Even if a large part of plaintext is known, it is difficult to find the full plaintext from a hash-code*

M1 plaintext message … long file … megabytes



Message Digest … Hash-code… 256 bits => 2^{256} codes … 1.1579209e+77

2^{150} = 1 427 247 692 705 959 881 058 285 969 449 495 136 382 746 624 ≈ 1000^{15}

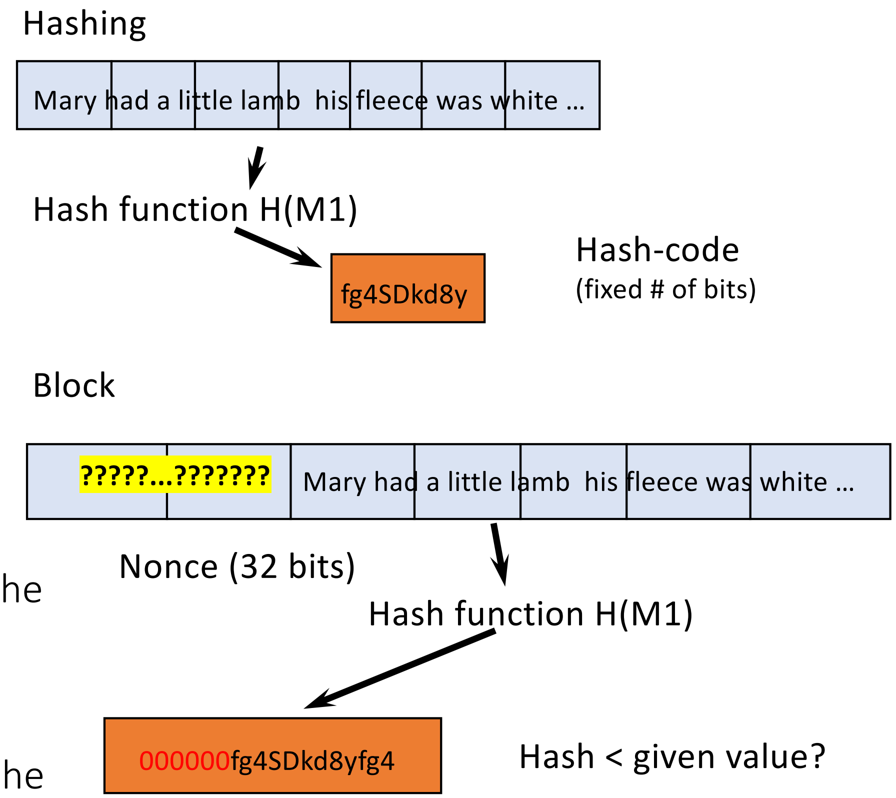
Consensus: Proof of Work … Mining

Proof of work

- Hard puzzle
  - Given X, find n, such that
    hash ((hash(n) append X) is less than Y
    - Smaller Y … harder the puzzle
- Solution by guessing
- Puzzle difficulty?
  - Depends on the value Y … smaller the value, smaller the number of solutions available
  - Hash function value must be less than Y (binary)

⇒ Number of tries/attempts inversely proportional to the number of leading zeros in the hash code

⇒ Smaller # of zeros (in hash code) more attempts required



Hashing

Mary had a little lamb his fleece was white …

Hash function H(M1)

fg4SDkd8y

Hash-code
(fixed # of bits)

Block

?????…???????

Mary had a little lamb his fleece was white …

Nonce (32 bits)

Hash function H(M1)

000000fg4SDkd8yfg4

Hash < given value?

Message Digest … Hash-code… 256 bits => 2^{256} codes

Consensus

- In the absence of a central trusted party, how to achieve agreement?

- *Consensus : A*greement by majority of nodes on the state of the distributed ledger

- A solution … *Proof-of-Work* … *Mining*
  - Difficult … guessing is used to find solution
  - Guessing by different miners … random =>
    - Different winners in different rounds

Mining

Proof of Work

- Performed by miners
  (nodes that perform Proof of Work (PoW))
- Ensure consensus and validity of transactions
- Miners rewarded with
  - *Newly minted cryptocurrency units*
  - *Transaction fees*
- Appends data to blockchain

https://www.yuantalks.com/another-chinese-province-cleans-up-cryptocurrency-mining-amid-nation-wide-crackdown/

Proof of Work: Control of Puzzle Difficulty

As number of miners increases

=> more miners … more hash power … more rewards

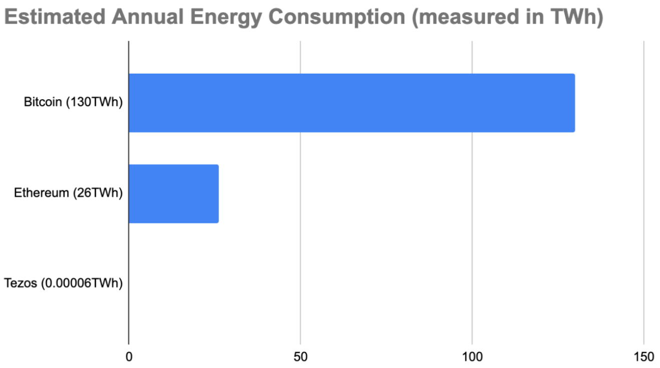
=> puzzle solved faster

=> more rewards means inflation

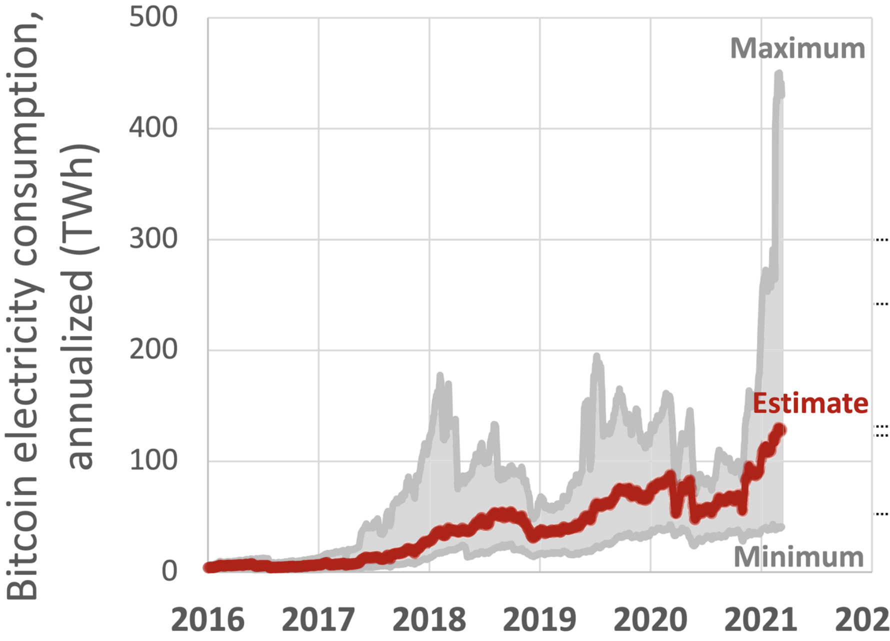
=> every 2 weeks Bitcoin adjusts the difficulty of mining (number of leading zeros in a nonce)

Public Blockchain with PoWork

- Mining … Proof of Work … Large burn of electricity to solve the puzzle
- Estimates



https://medium.com/tqtezos/proof-of-work-vs-proof-of-stake-the-ecological-footprint-c58029faee44



Country equivalent:

UK: 300 TWh

Spain: 242 TWh

Sweden: 131 TWh

Argentina: 125 TWh

Israel: 56 TWh

Cambridge Bitcoin Electricity Consumption Index (CBECI)". www.cbeci.org. Retrieved 2020-02-20

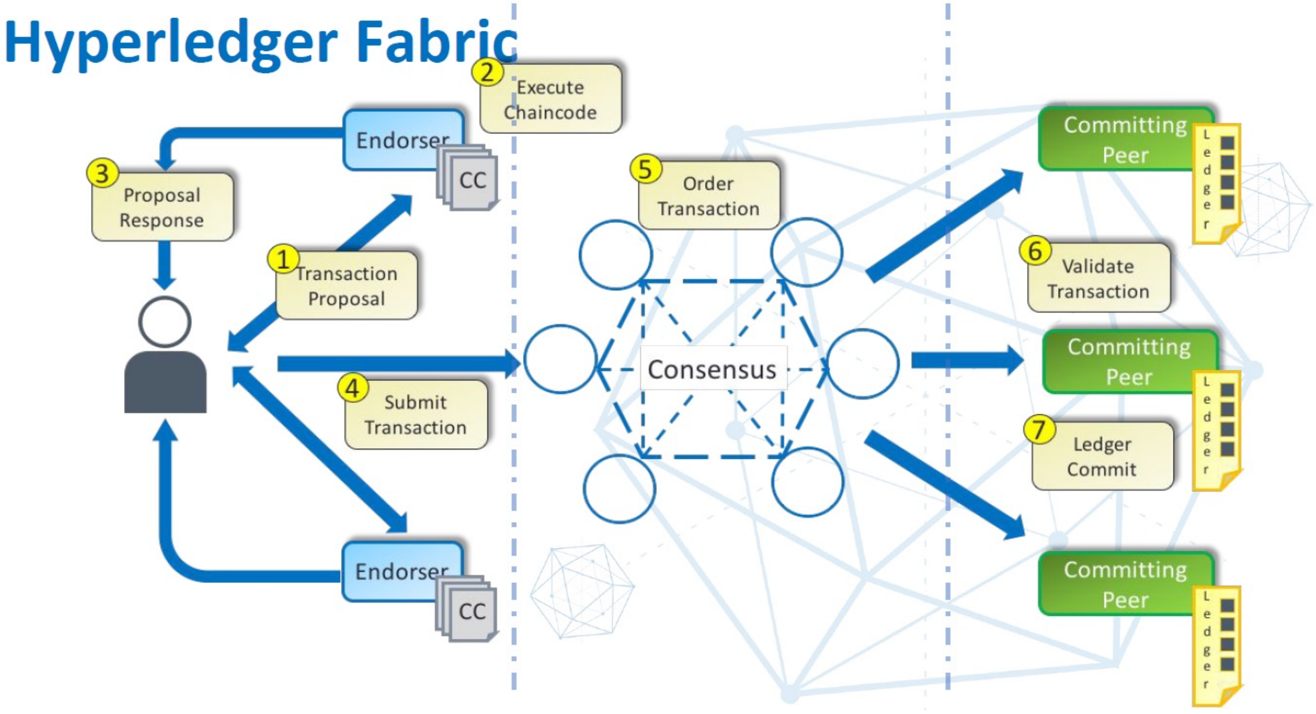
Consensus Algorithms

- Consensus algorithm … randomization
  - Proof of Work … solve a difficult puzzle … winner posts block
    - Suppose there is collusion and 51% attack is successful and all currency stolen => crash?
  - Proof of Stake – Stake in Native Currency
  - Proof of Activity -Hybrid of POW and POS
  - Proof of Burn – Validation comes with Burning of Coins (punish bad actors & reward good ones)
  - Proof of Capacity (Storage space)

Hyperledger Fabric

- Distributed Ledger technology & smart contracts
- Part of Hyperledger Project
- Smart contracts – Turing complete
- No native currency
- Aims to focus on:
  - Permissioned membership
  - Modular consensus and identity management
  - Privacy and confidentiality of transactions

Hyperledger Fabric – Permissioned – Adding a block



Nodes

Peers: Maintain Ledger state, transactions & contain *chaincode*

Endorsers: Accept and grant/deny transaction endorsements

Orderers: Store transactions in blocks and send blocks to peers for committing to ledger.

Channels

Transactions carried out on channels

Distributed ledger and transactions occur within scope of a channel

Membership Services

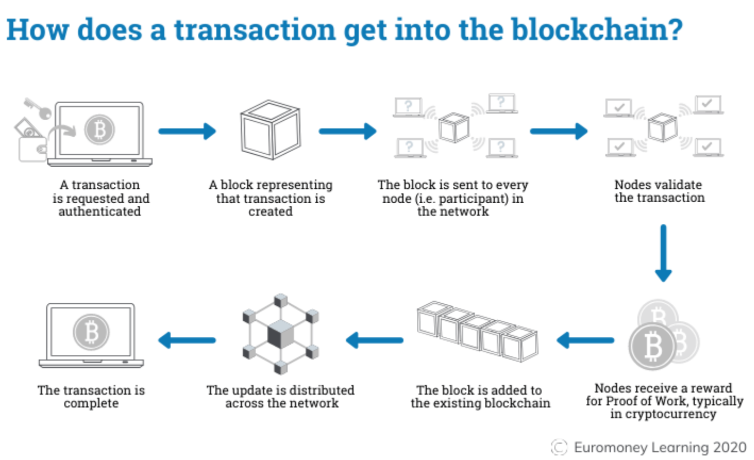
Identities for Peers, Orderers and clients

Issuance, validation and revocation of credentials to interact on Fabric

Permissioned vs. Public Blockchain

- Public (non-permissioned)
  - Anyone can have a node
  - Users anonymous (in chain)
  - NO privacy

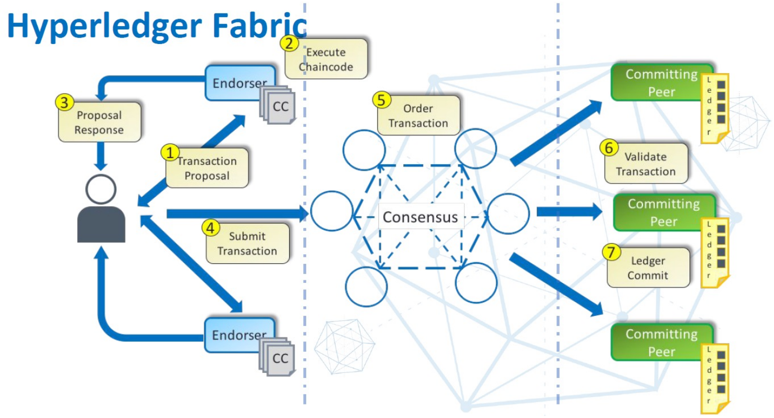
- Permissioned
  - Nodes are authenticated
  - Users are authenticated
  - Privacy



How does a transaction get into the blockchain?

A transaction is requested and authenticated
A block representing that transaction is created
The block is sent to every node (i.e. participant) in the network
Nodes validate the transaction
Nodes receive a reward for Proof of Work, typically in cryptocurrency
The block is added to the existing blockchain
The update is distributed across the network
The transaction is complete

Ⓒ Euromoney Learning 2020



Hyperledger Fabric

Public and Permissioned Blockchains - Examples

- Public blockchains
  - Rated at: https://blog.fasset.com/public-blockchain-in-the-cryptocurrency-world/
  - Bitcoin
  - Ethereum
  - Neo
  - Qtum
  - Waves … Custom tokens

- Permissioned blockchains
  - Hyperledger project (Linux foundation)
    - Fabric
    - Sawtooth … Option: Po Elapsed Time (lottery)
    - Besu … Enterprise-grade version
  - R3 Corda ... for financial industry
  - Quorum … fork of Ethereum with
    - Permissioned access, privacy
    - Alternative consensus protocols
  - Enterprise Ethereum

Smart Contracts

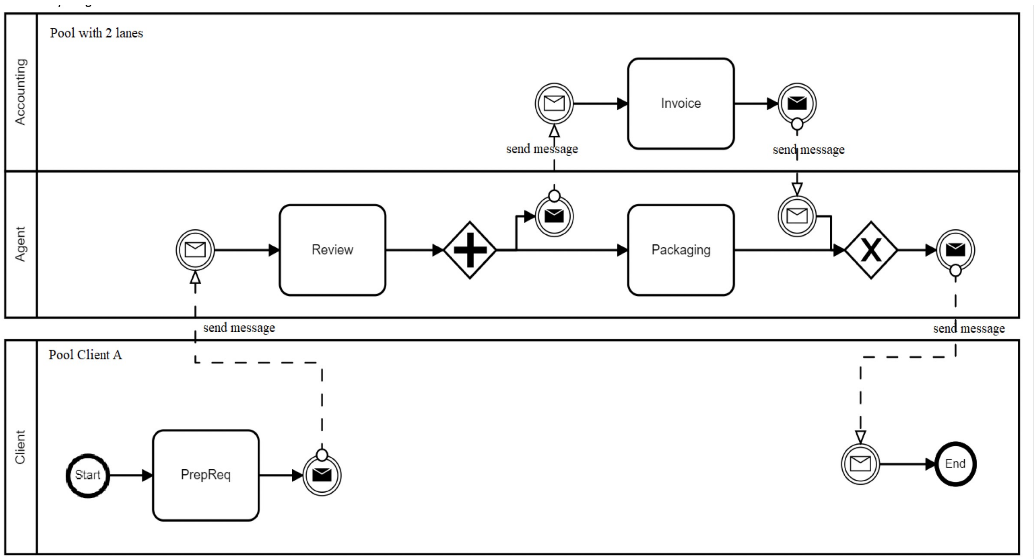
- Smart Contract
  - Computer program/script
  - *Stored on the blockchain* (code cannot be modified … *security*)
  - Does not have access to any external resources
    - Can access only the ledger and communicate with other smart contracts
    - Oracles needed … trusted third parties that are set up to provide only specific info
  - Executed by a virtual machine
  - Results validated … helps in checking correctness of execution

=> Security improved … but smart program may contain bugs

Smart Contracts … continued

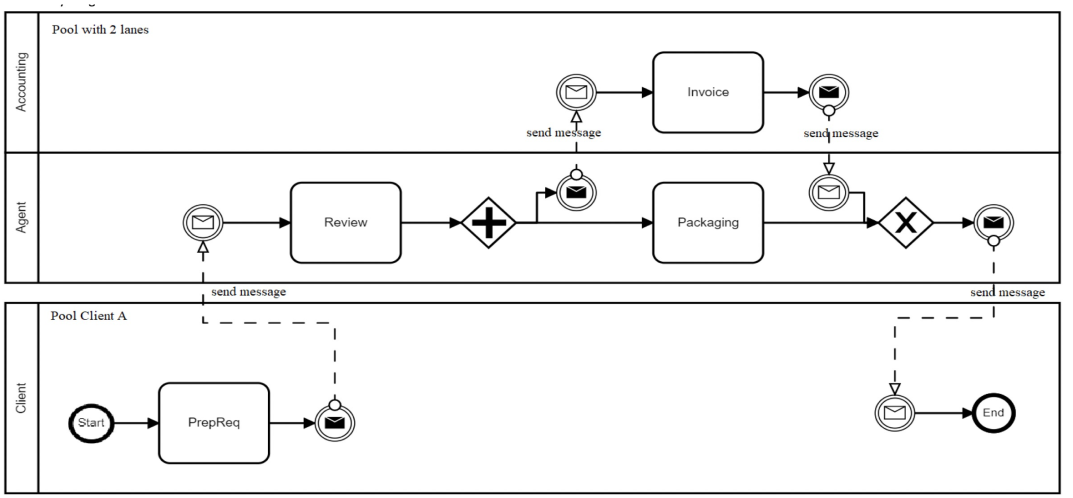
- Smart contract programs
  - More complex to write than “regular” programs
  - Program errors lead to exploits/hacks
- BUT
  - Automated generation of smart contracts from business models
  - Smart contract secured by plugging security holes automatically (for known exploits)

Business Process Management Notation - BPMN



Smart contract vulnerabilities

- Affect only smart contract participants
  - Smart contracts are more
    - complex to write than “regular” programs
  - Program errors … exploits/hacks
  - BUT
    - Automated generation of smart contracts from business models
    - Smart contract secured by plugging security holes



BPMN – Business Process Model and Notation
(Object Management Group (OMG) Standard)

Blockchains: Are they safer? Yes !

- Blockchains are safer than ”regular” software
  - Blockchain infrastructure … for established chains … safe
    - Resiliency improved … if one node is hacked - still safe (two nodes hacked – still safe; f nodes hacked … safe?)
    - Smart contract & data … on blockchain ... replicated … smart contract hacked on one node … safe
  - Smart contract error (design or bug)
    - Smart contract coding errors ? … If programs developed for a single node … same errors when on blockchain
- MOST HACKS:
  - Social engineering
  - Wallets, trading tokens … hacks are NOT due to blockchain

Questions and Answers