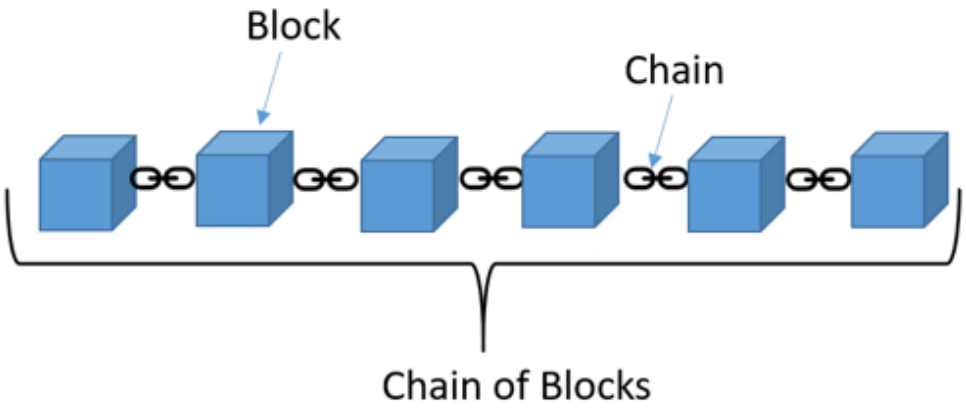
Blockchain

Slide set 10
Distributed Systems
Graduate Level

K. N. Toosi Institute of Technology
Dr. H. Khanmirza
h.khanmirza@kntu.ac.ir

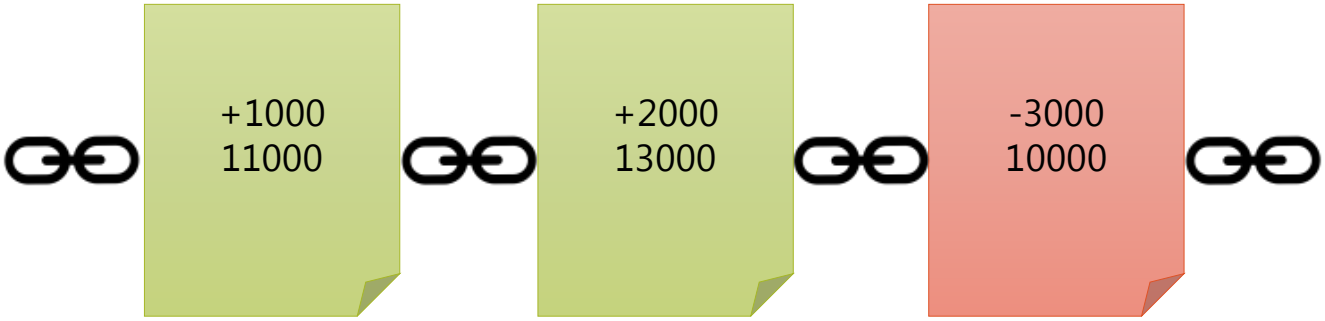
Blockchain

- Essentially is a series of data blocks chained together
  - Each block is chained to its previous block by embedding information from the previous block
- Blockchain is immutable or append only
  - Once a data recorded in a block it cannot be changed
- Blockchain is a peer-to-peer system in its core
  - No central administration
  - No third party in exchanging info, cash, file, ...



Blockchain

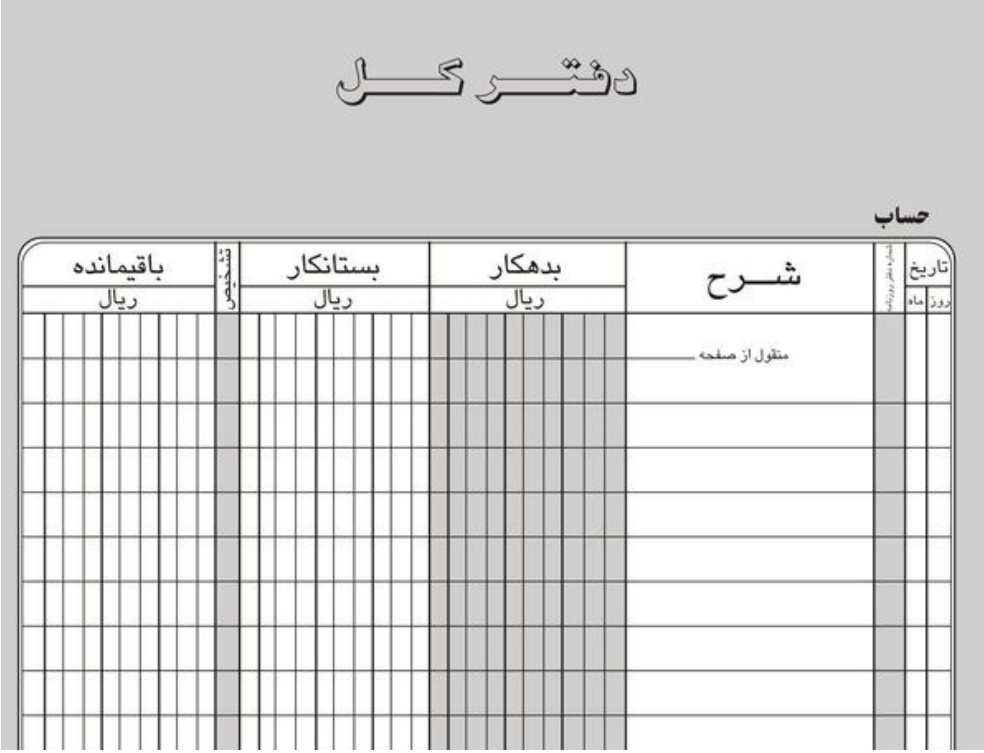
- We may use Chained Blocks concept to build a ledger
  - Suppose we keep transactions of an account in series of blocks
  - Each block consists of two pieces of information
    - Amount of transaction (debit or credit)
    - Remaining



Distributed Ledger Technology (DLT)

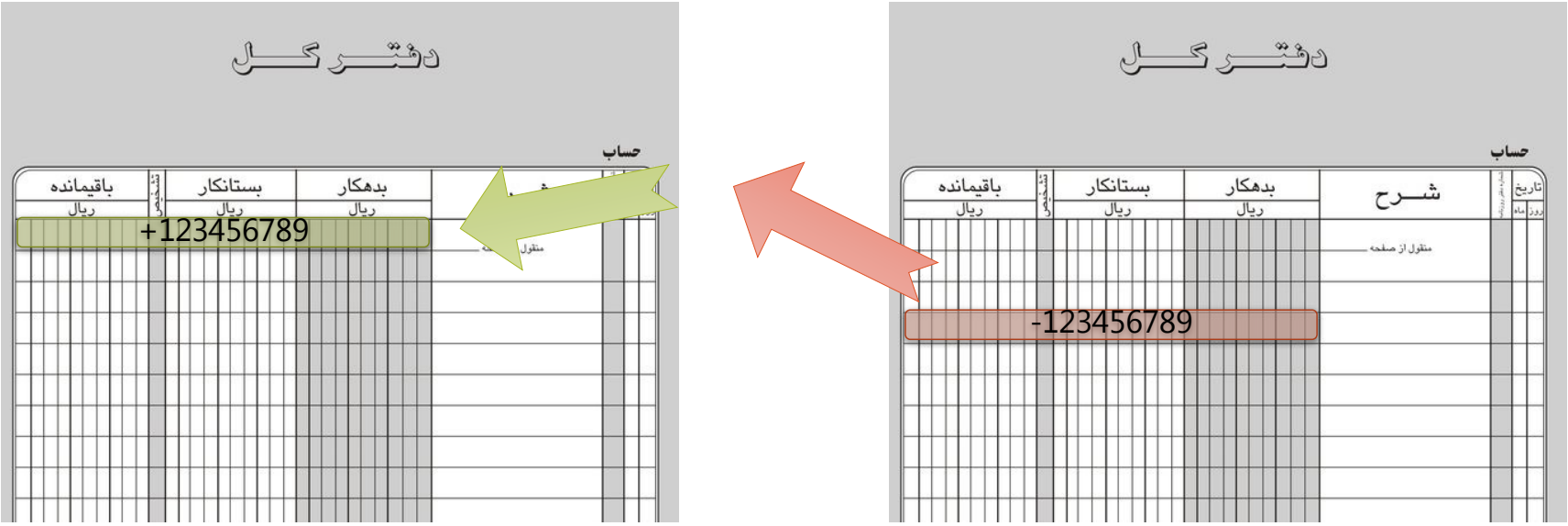
- Single entry ledger first appeared around 3,000 B.C has a debit or credit column

- Double entry ledgers appeared in 1340 (A.D.) has both columns



Distributed Ledger Technology (DLT)

- When one row in a ledger is debit then a row in another ledger is credit

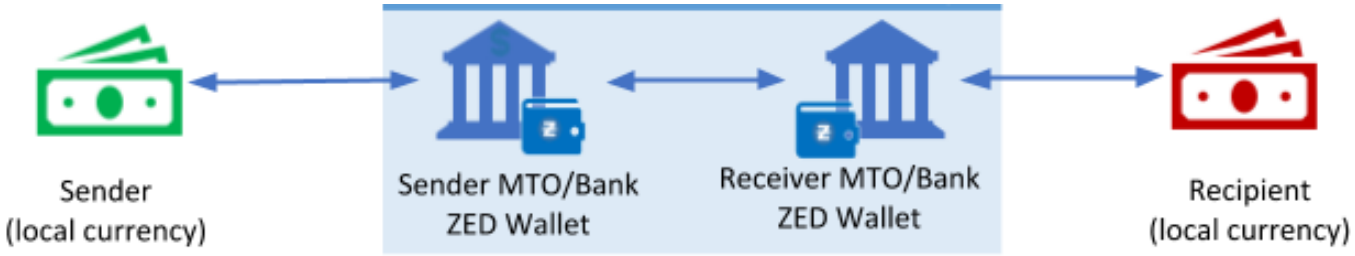


Distributed Ledger Technology (DLT)

- What if two ledgers had contradiction?
  - Here a third party comes in to the picture like Banks
  - For each business there may be a dispute resolution reference

Contradiction Resolution

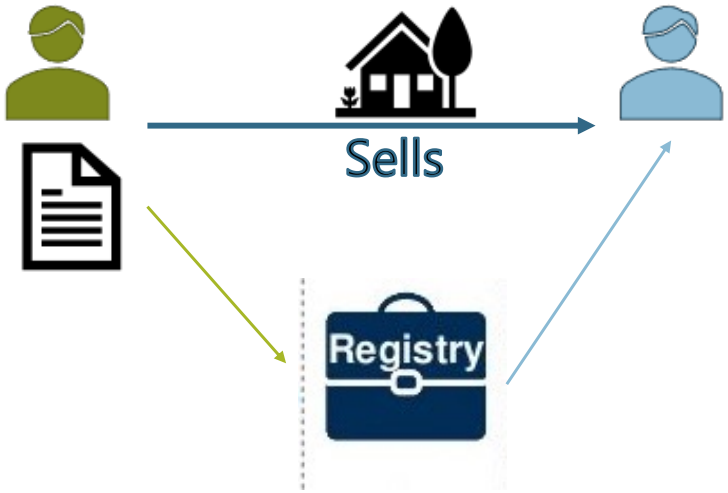
- Some businesses are only the third party trusted by mediators



Contradiction Resolution

- Some businesses are only the third party trusted by mediators

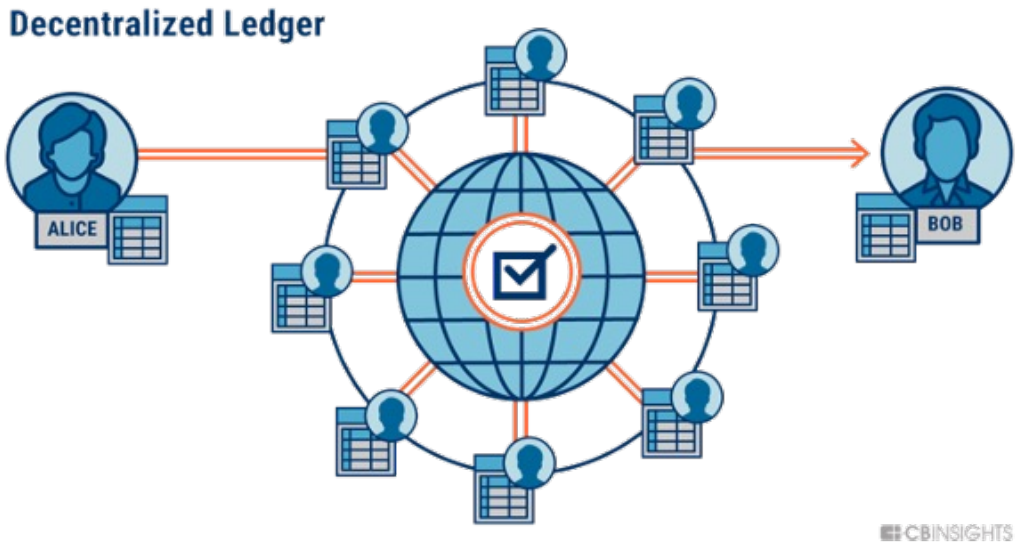
A is the owner of a house based on a document issued by a registry



The process of transferring ownership should be registered in the registry

Contradiction Resolution

- How could we remove the role of third party trust-intermediaries?
- What if large number of people keep track of every transaction in the world?
- What if everyone have copy of others ledger



Contradiction Resolution

- If majority of people verify a transaction, then we could ensure correctness of that transaction
- No one can cheat, otherwise he must convince +50% of ledger-keepers
- Few ledger-keepers may lie, but they must be more than 50% to change the majority-driven consensus

Contradiction Resolution

- How ledger-keepers could trust to some people claiming they had transactions with each other?

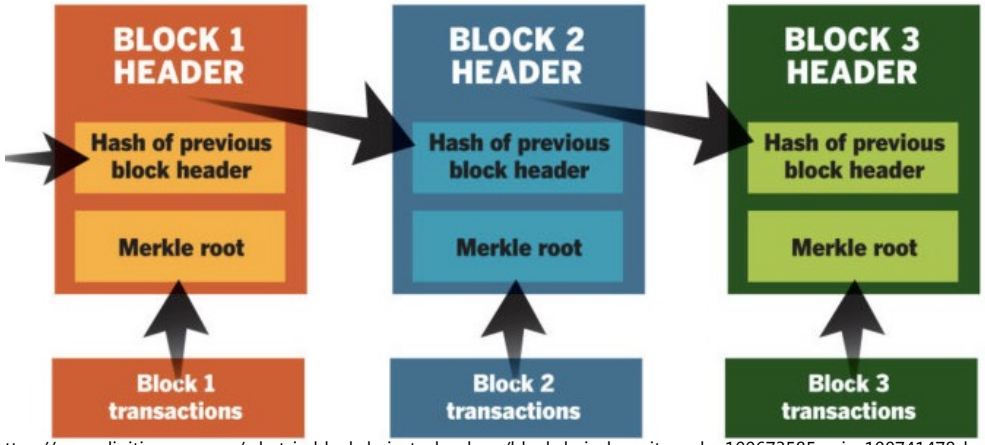
- Simple! all parties must sign the transaction and send a copy to all ledger-keepers

Distributed Ledger Technology (DLT)

- DLT Technology Enablers (sum-up)
  - All contributors must have sign to be distinguishable
  - A copy of all transactions is kept by all contributors
    - Any transaction must be announced to contributors
  - Transactions are open to read by anyone but they are signed

Distributed Ledger Technology (DLT)

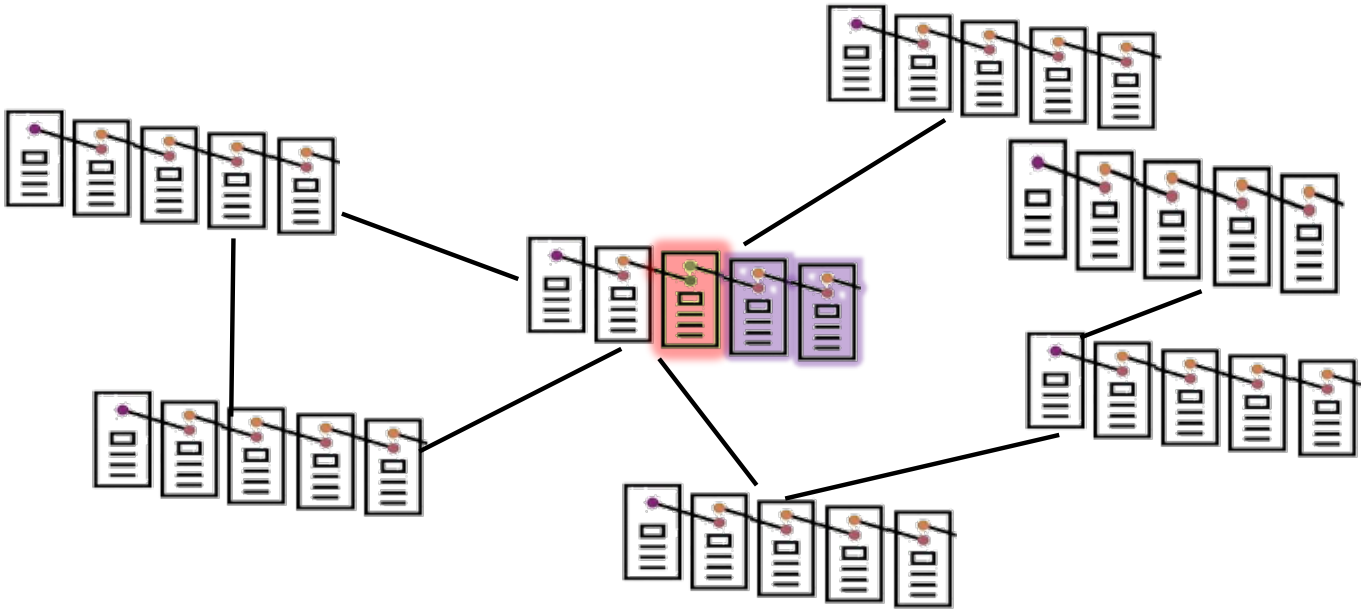
- Triple entry ledger introduced by Nakamoto (BitCoin creator)
- Third column is an immutable link to all past debits and credits



https://www.digitisenow.com/what-is-blockchain-technology/blockchain-how-it-works-100673585-orig-100741478-large/

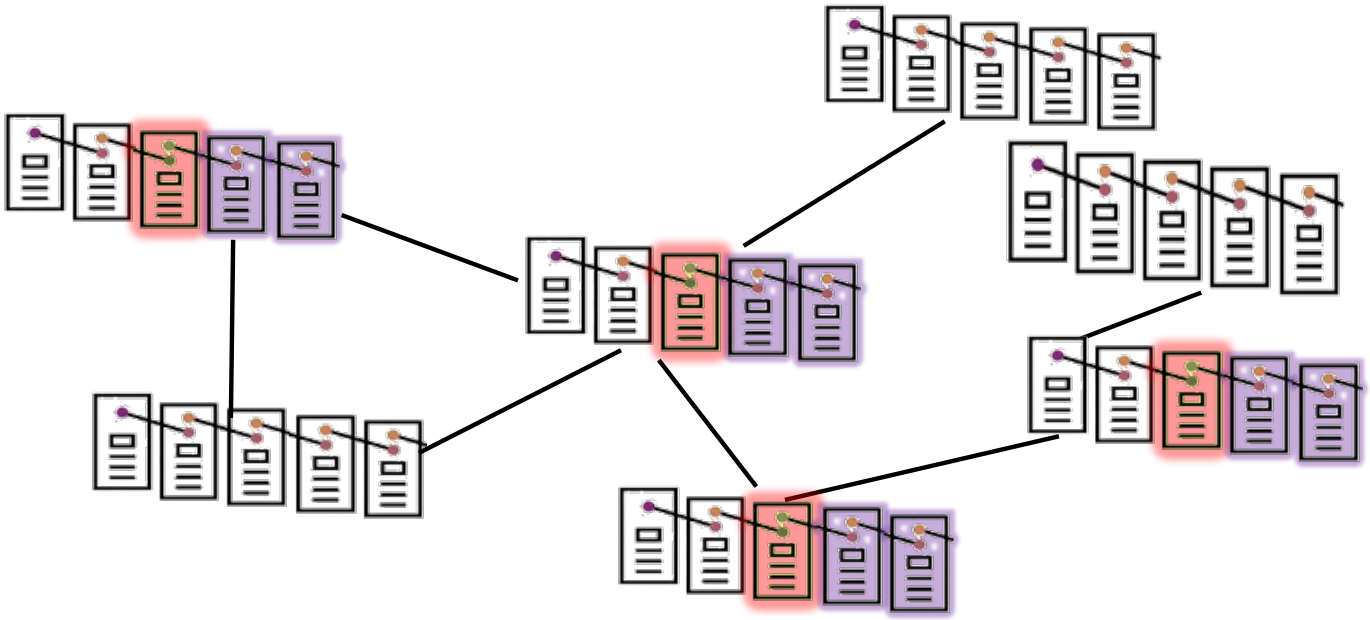
Distributed Ledger Technology (DLT)

- For altering a transaction someone must change several blocks of transactions
- This makes cheating much more difficult



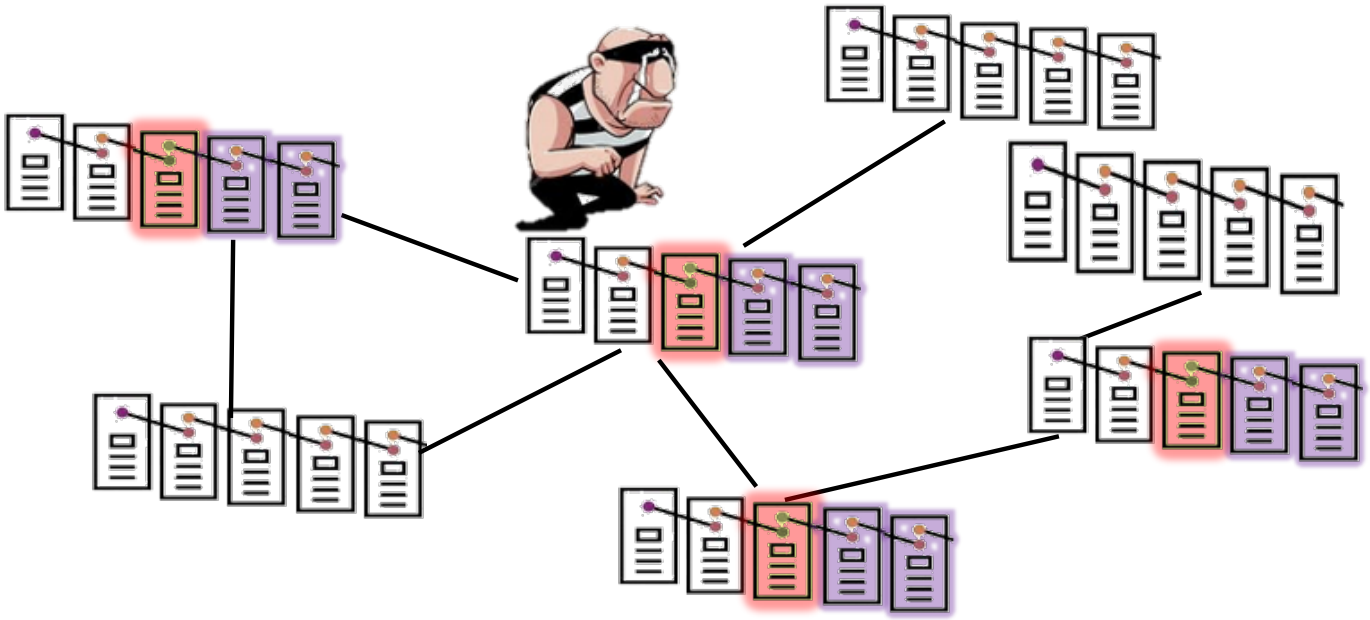
Distributed Ledger Technology (DLT)

- For altering a transaction someone must change all the previous transactions in more than 50% of ledgers scattered throughout the world



Distributed Ledger Technology (DLT)

- Looks impossible



Blockchain

"Blockchain is a peer-to-peer, distributed ledger that is cryptographically-secure, append-only, immutable and updateable only via consensus among peers"

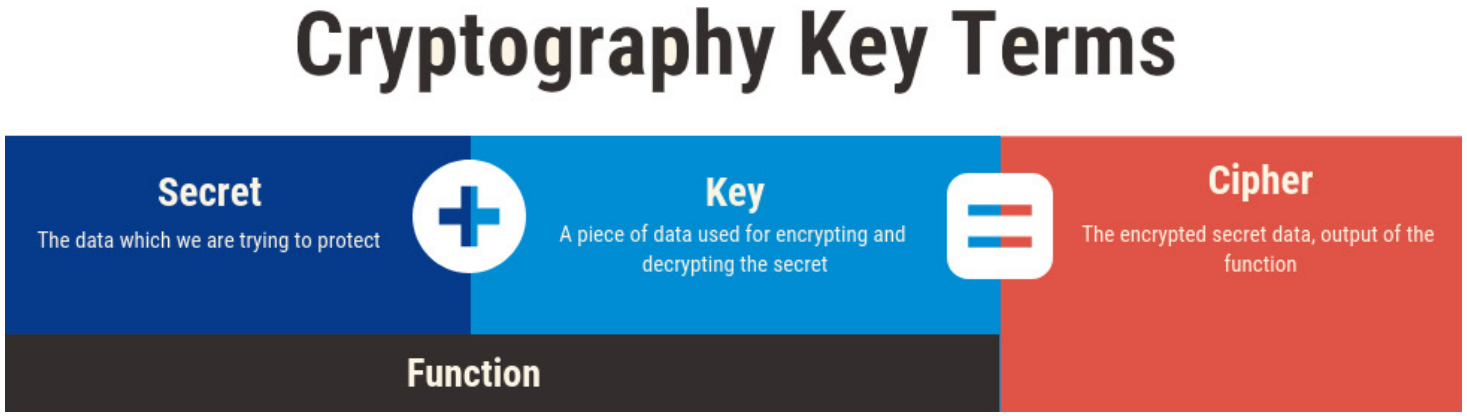
Blockchain

- How blocks are chained together?

Cryptography Basics

- Secret: The data we are trying to protect
- Key: A piece of data used for encrypting and decrypting the secret
- Function: The process or function used to encrypt the secret
- Cipher: The encrypted secret data, the output of the function

- Blockchain makes use of several different types of cryptography



Public Key Cryptography

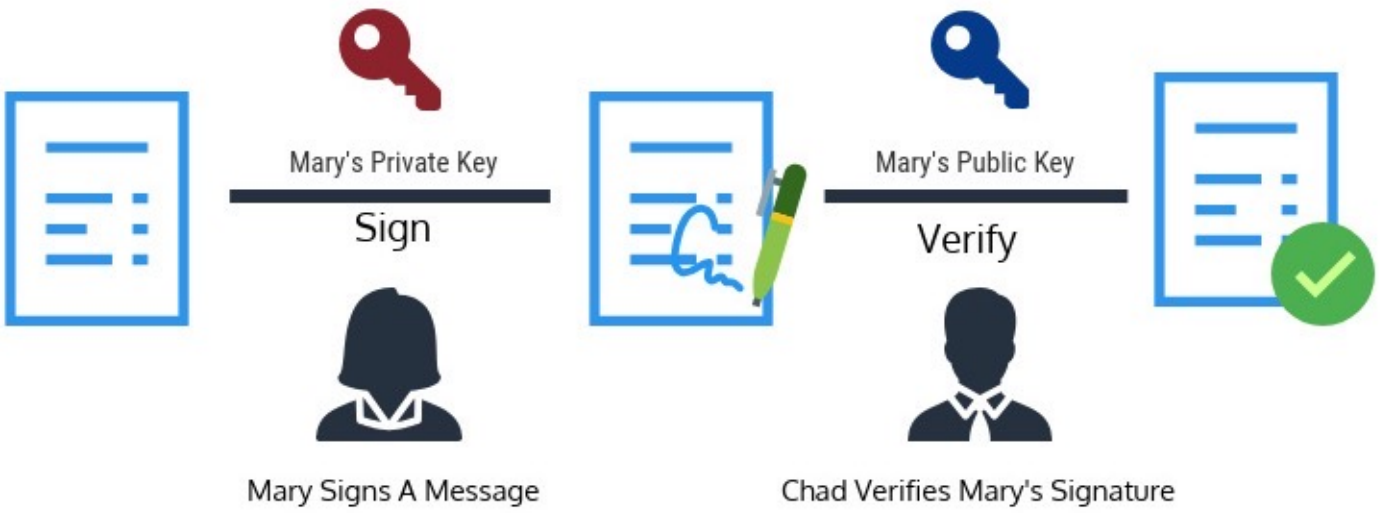
- Pair of public and private keys used for encryption and digital signatures
- It is extremely difficult to reach from one key to another
- Public key is distributed publicly
- Private must be kept secret

Public Key Cryptography

- Confidentiality use case
  - When one encrypts a content with someone's public key then it can only be opened with the corresponding private key
  - This is used to send a secret message to someone

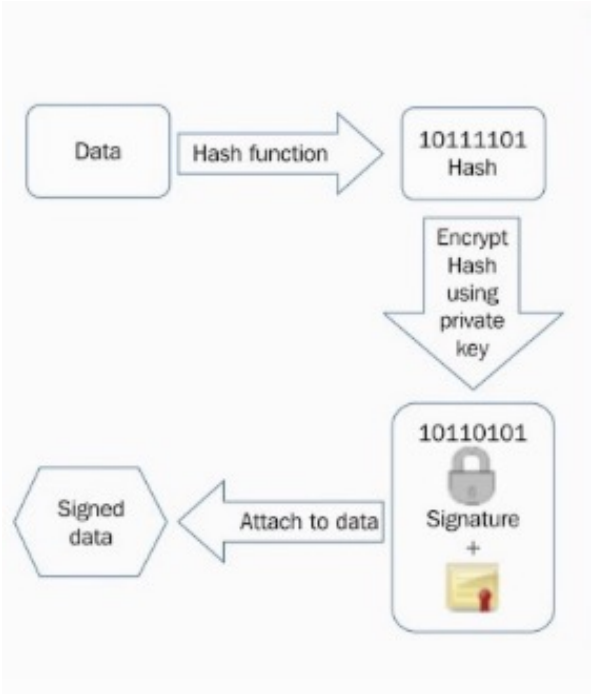
Public Key Cryptography

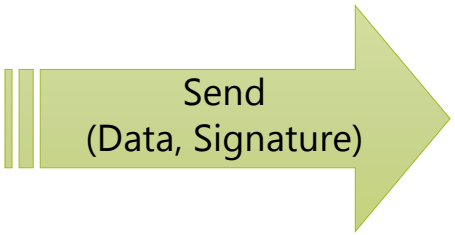
- Integrity & Digital signing use case
  - When one encrypts a content with his private key then it can only be opened with his corresponding public key
  - Receivers of the message can reliably determine the identity of the sender

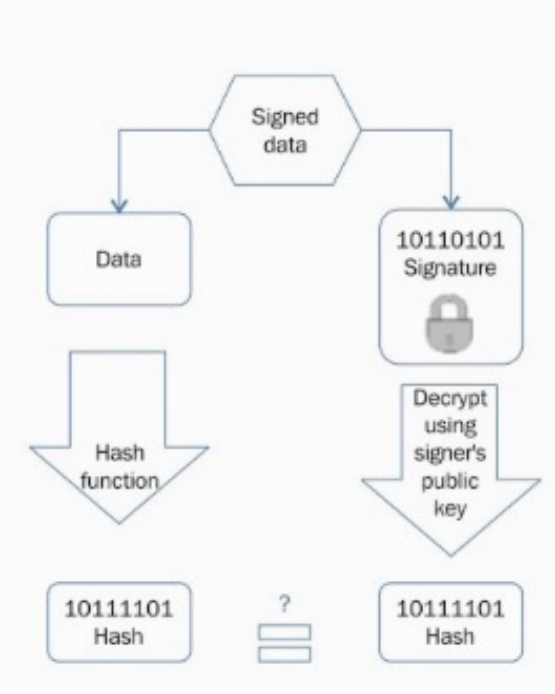


Public Key Cryptography

- Secure digital signing use case







Hash Functions

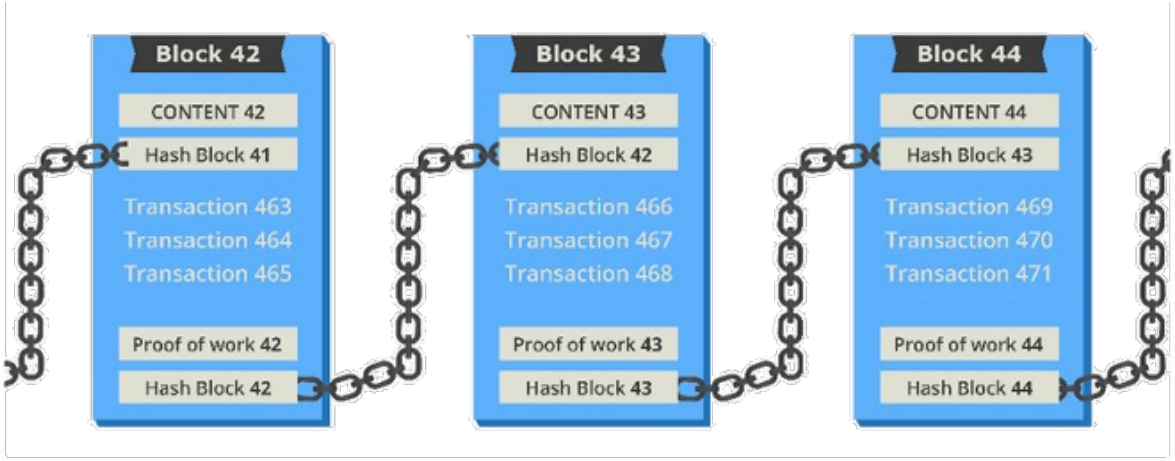
- One-way pseudo-random mathematical functions
- Takes an input and produce a fixed size sequence of bits
- Hashes produce a fixed size output for even very long inputs, then hash of data can be considered as a compressed signature of data

Hash Functions

- Calculating hash is simple but it is practically impossible to determine the input
- Changing a single bit in input, produces an output that differs by half of bits on average
- Finding two inputs that have equal hashes are very hard
- Using hashes we are able to compare two pieces of data without knowing their actual value

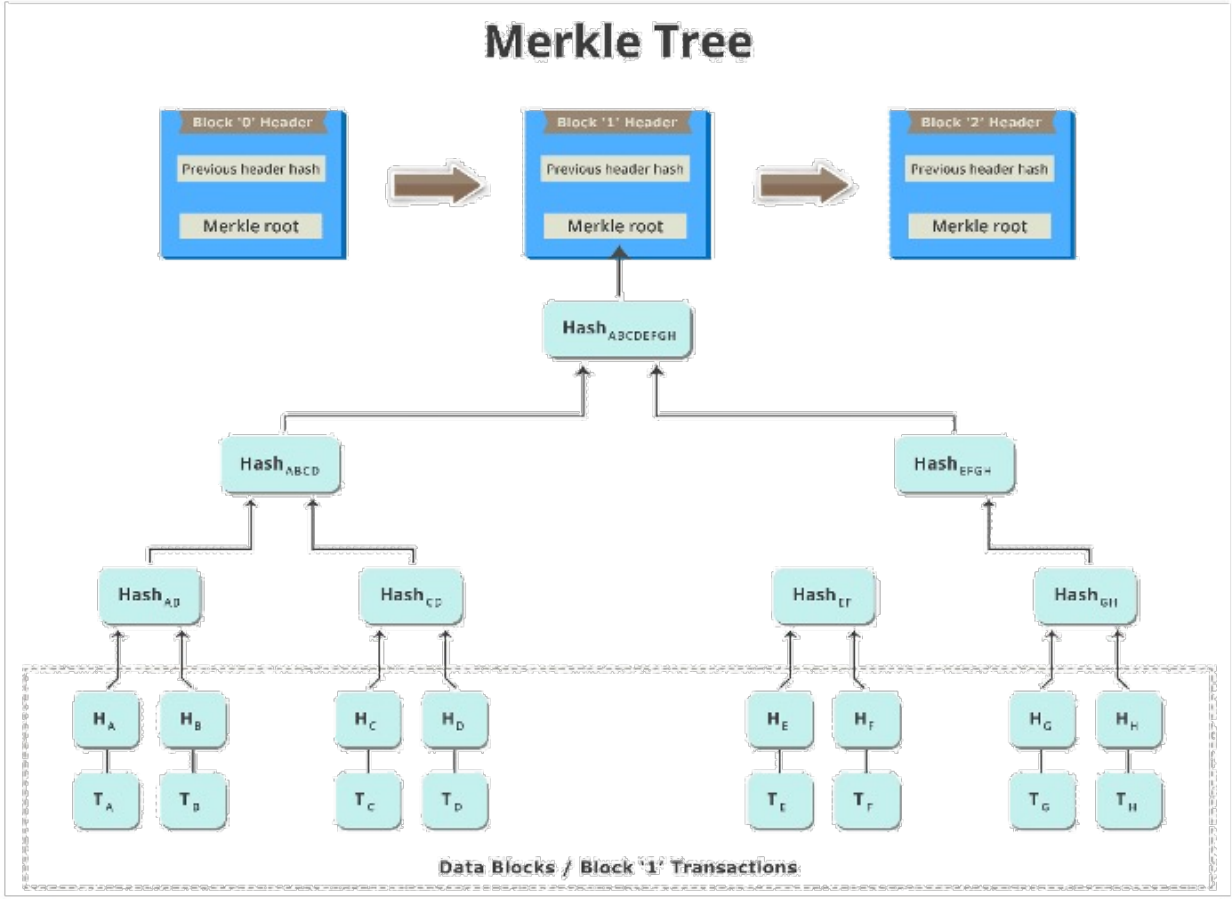
Chaining Blocks

- How blocks are chained together
  - Hash of a block is calculated
  - It is used in the next block
  - First block is called Genesis block



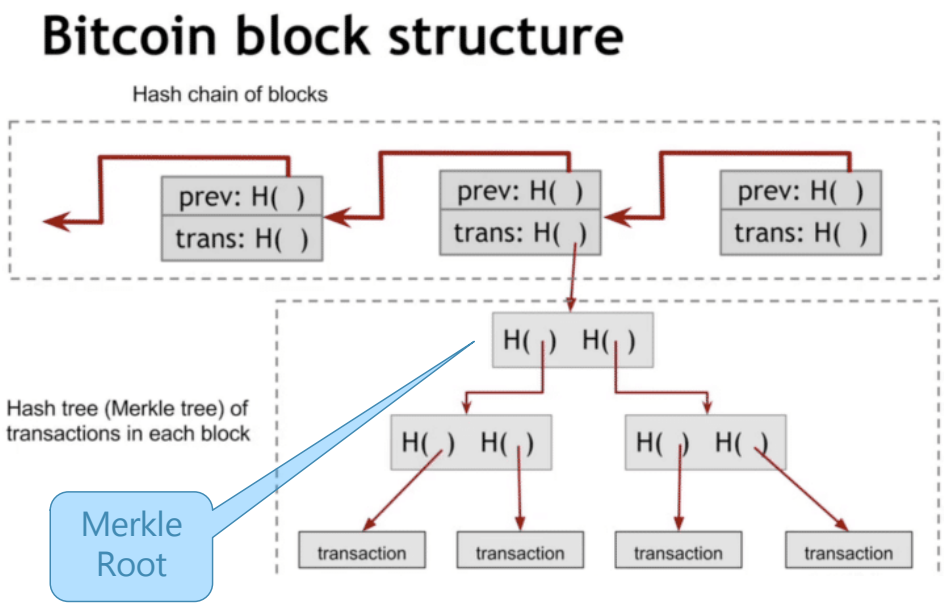
Chaining Blocks

- Merkle Tree
  - Also hash-tree
  - Leaf nodes are hash of data
  - Non-leaf nodes are hash of hash of its children



Chaining Blocks

- Merkle Tree (cont.)
  - A block may contain data of several transactions in a block
  - For each block a Merkle tree is computed and saved in block header
  - This makes comparing of blocks between two nodes very simple, just compare Merkle Roots
  - No need to have the entire block data



Elements of Generic Blockchain

Elements of Blockchain

- Address
  - Unique identifier for each user
  - Users may have several identifiers
  - Often identifier is users' public key

- Transaction
  - A transfer of an asset between two addresses

Elements of Blockchain

- Nonce
  - A number generated and used only once.
  - Used extensively in many cryptographic operations to provide replay protection, authentication, and encryption

- Block
  - Composed of several transactions beside timestamp, nonce and previous block hash

Elements of Blockchain

- Node
  - In a blockchain network performs various functions depending on the role that it takes on
  - Can propose and validate transactions and perform mining to facilitate consensus and secure the blockchain
    - This goal is achieved by following a consensus protocol
  - Can perform other functions such as simple payment verification (lightweight nodes) and validation
  - Do transactions

Mining

- Miners validate new transactions and record them on the global ledger

- It is a mechanism that allows the blockchain to perform decentralized security

https://dev.to/damcosset/blockchain-what-is-mining-2eod

Mining

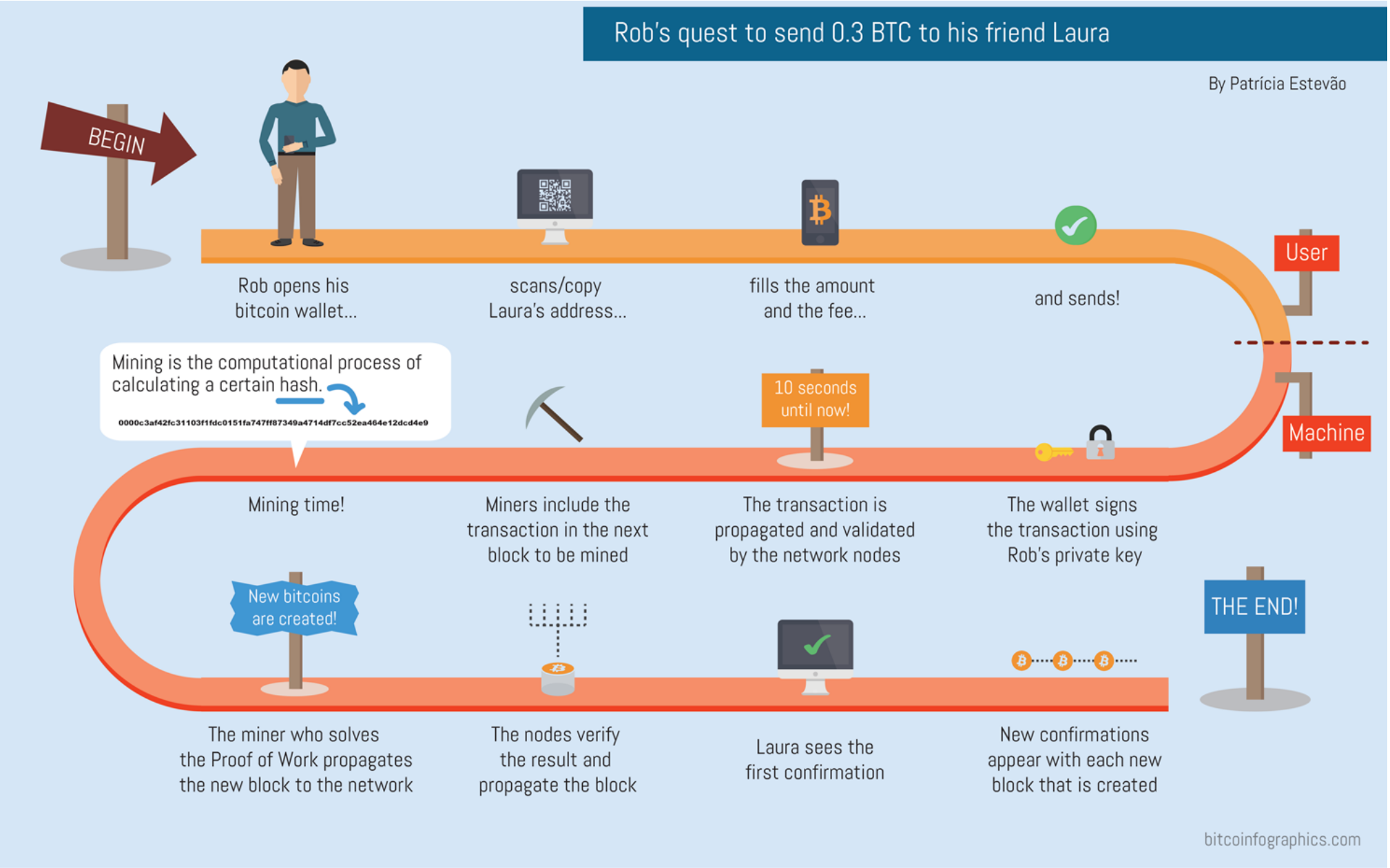
- Miners compete to solve a difficult mathematical problem based on a cryptographic hash algorithm

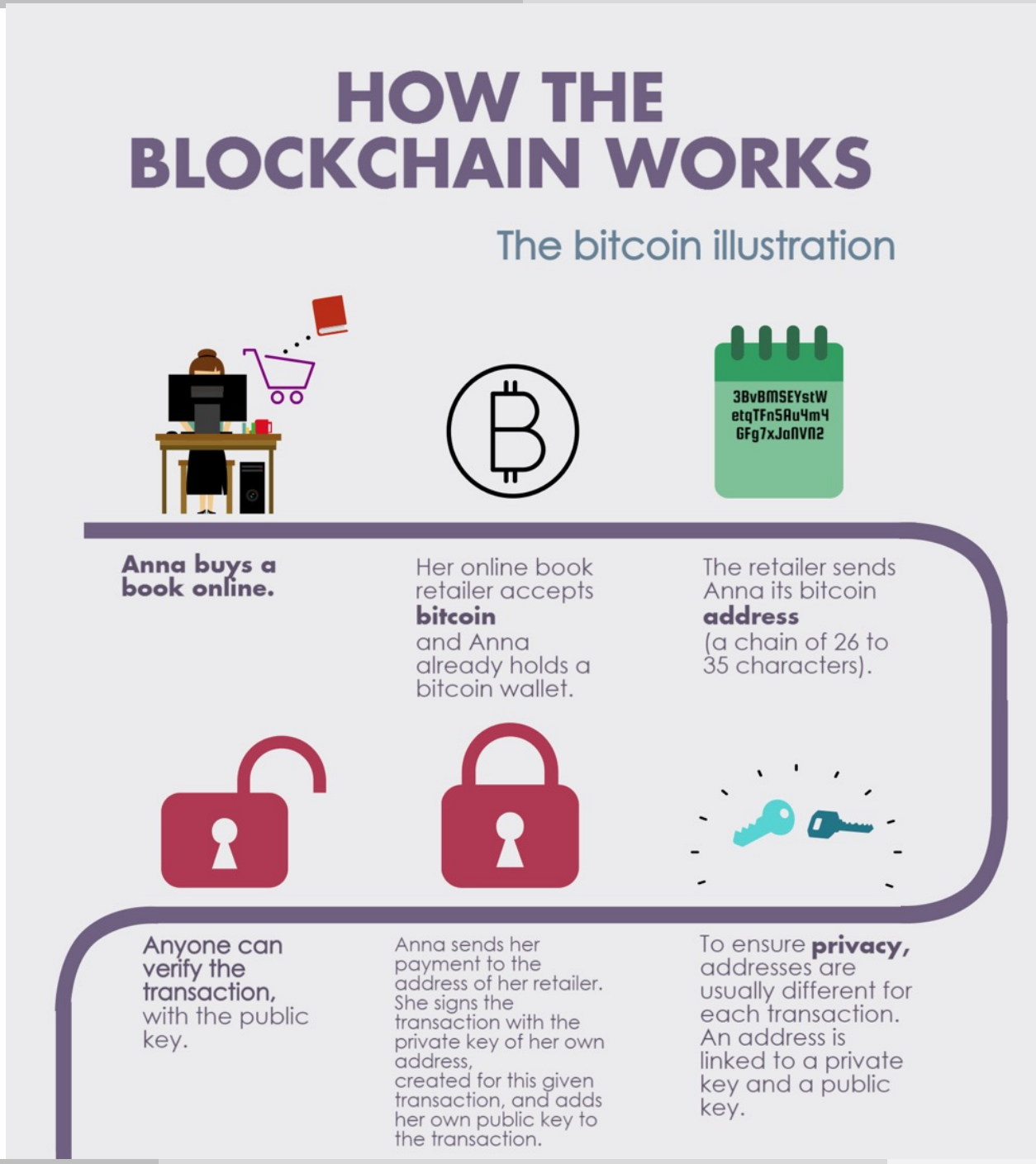
- This proof proves that a miner did spend a lot of time and resources to solve the problem and is rewarded

https://dev.to/damcosset/blockchain-what-is-mining-2eod

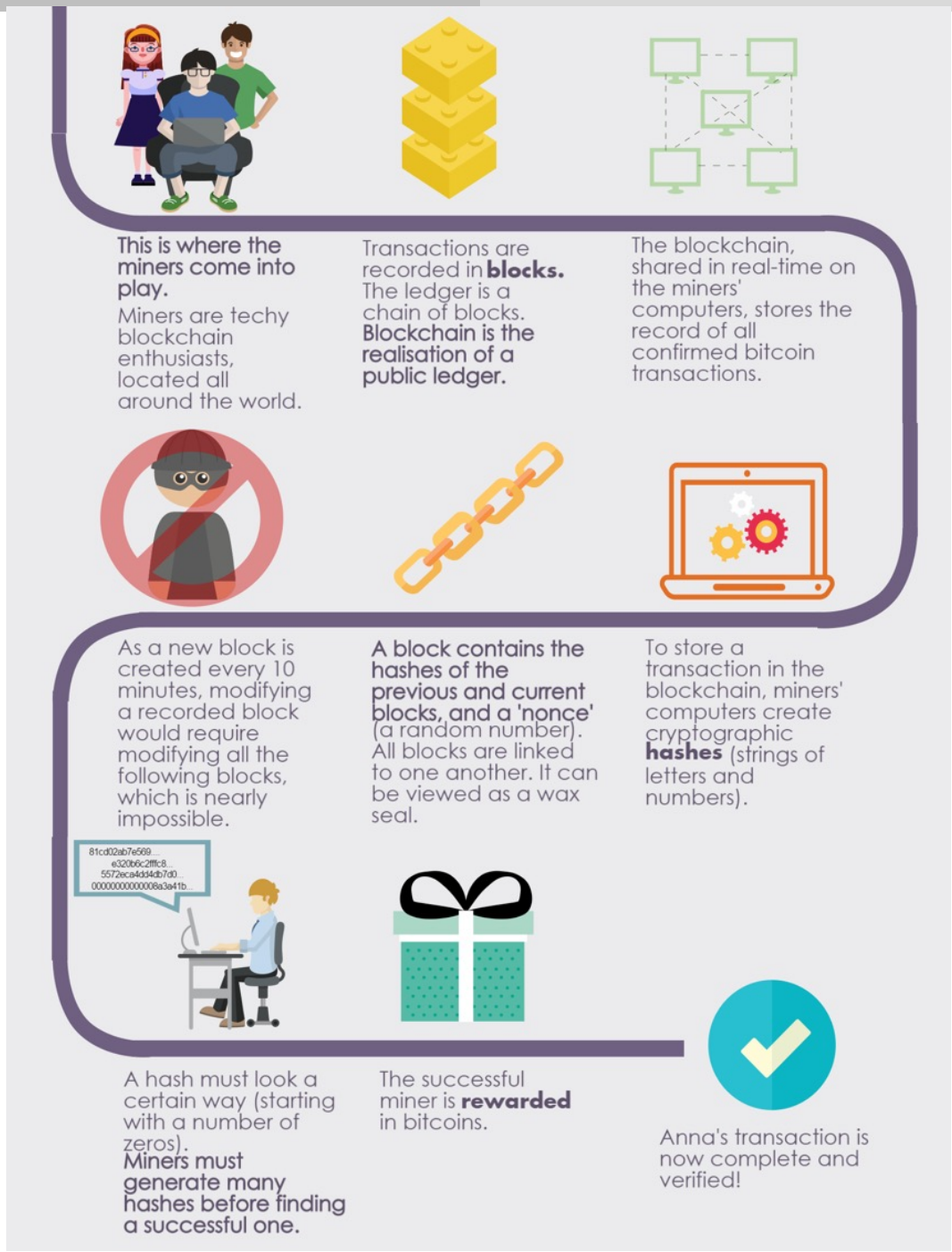
Transaction Flow

- A node starts a transaction with creating and signing it with its private key
- Transaction is flooded into the Blockchain network with a Gossiping protocol
- Several miners validate the transaction
- Transaction is appended into a block and is propagated throughout the network
- In this step, transaction is confirmed
- A transaction is finalized if several blocks created after this block


Rob's quest to send 0.3 BTC to his friend Laura
By Patrícia Estevão
BEGIN
Rob opens his bitcoin wallet...
scans/copy Laura's address...
fills the amount and the fee...
and sends!
User
Machine
Mining is the computational process of calculating a certain hash.
0000c3af42fc31103f1fdc0151fa747ff87349a4714df7cc52ea464e12dcd4e9
10 seconds until now!
Mining time!
Miners include the transaction in the next block to be mined
The transaction is propagated and validated by the network nodes
The wallet signs the transaction using Rob's private key
New bitcoins are created!
THE END!
The miner who solves the Proof of Work propagates the new block to the network
The nodes verify the result and propagate the block
Laura sees the first confirmation
New confirmations appear with each new block that is created
bitcoinfographics.com


HOW THE BLOCKCHAIN WORKS
The bitcoin illustration
3BvBMSEYstW etqTFn5Au4m4 GFg7xJaNVN2
Anna buys a book online.
Her online book retailer accepts bitcoin and Anna already holds a bitcoin wallet.
The retailer sends Anna its bitcoin address (a chain of 26 to 35 characters).
Anyone can verify the transaction, with the public key.
Anna sends her payment to the address of her retailer. She signs the transaction with the private key of her own address, created for this given transaction, and adds her own public key to the transaction.
To ensure privacy, addresses are usually different for each transaction. An address is linked to a private key and a public key.

Transaction Flow



Blockchain vs. Bitcoin

- Bitcoin and cryptocurrencies are great use cases for blockchain

- There are many more use cases that utilize blockchain technology

Blockchain Types

Blockchain Types

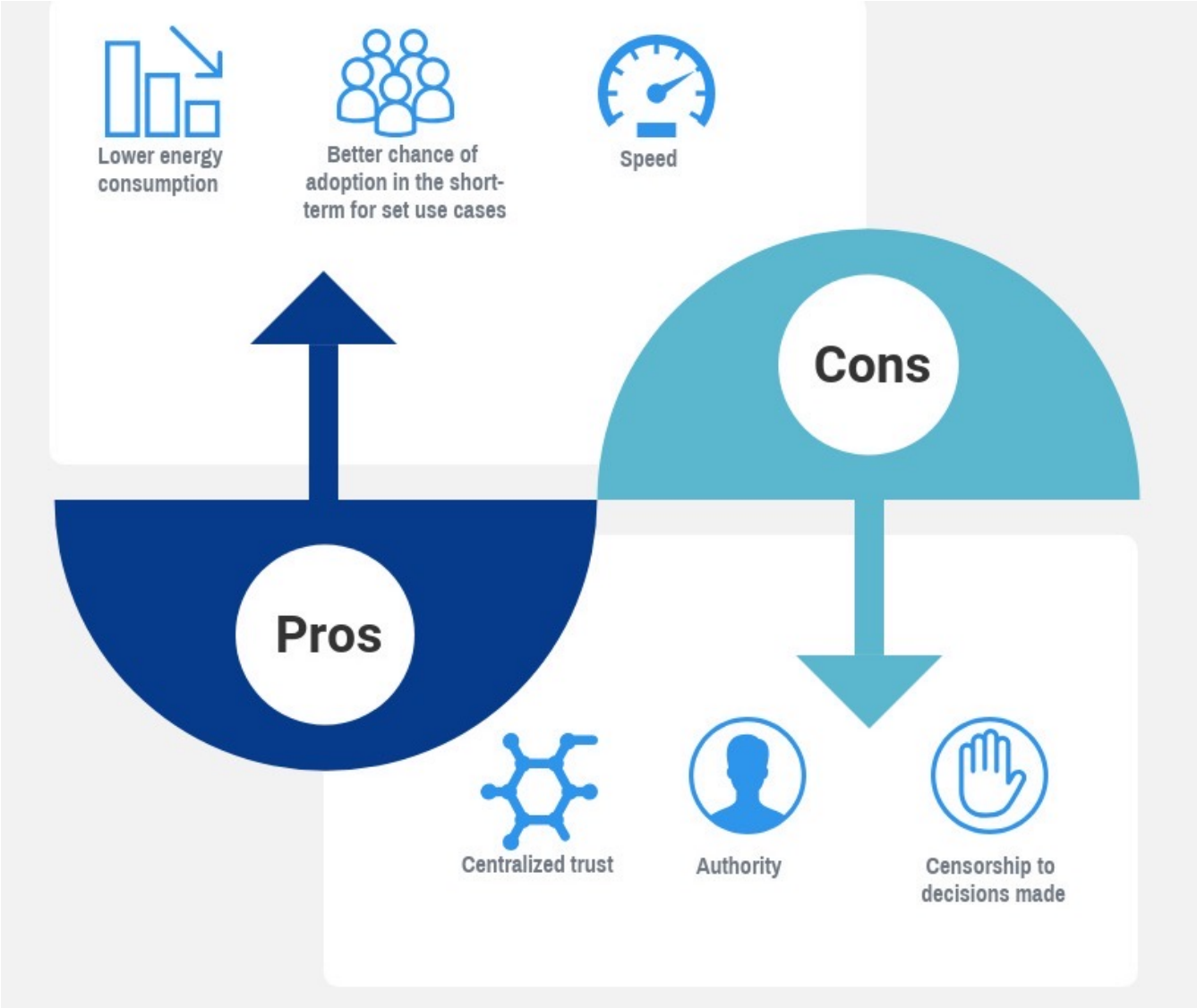
- Public
  - Everyone can join the network without limitation
  - Just download the related software and start
  - Like Bitcoin, Ethereum, ...

Blockchain Types

- Consortium
  - Grouping of institutions (possibly individuals) getting together to achieve a mutual goal
    - Each participant shares resources and promise to stick to the rules
  - Only certified identities can participate
    - Called shared permissioned blockchains
    - Consortium of Banks
  - Consensus protocols are much simpler as there is no traitor
  - Like: Stellar, Ripple, Hyperledger, Corda

Blockchain Types

- Consortium



Blockchain Types

- Private
  - Permissioned
  - Inside an organization among fully trusted entities

- Why one may use private blockchain instead of a central database?

Blockchain Types

- Private blockchain vs. Central DB

Immutability

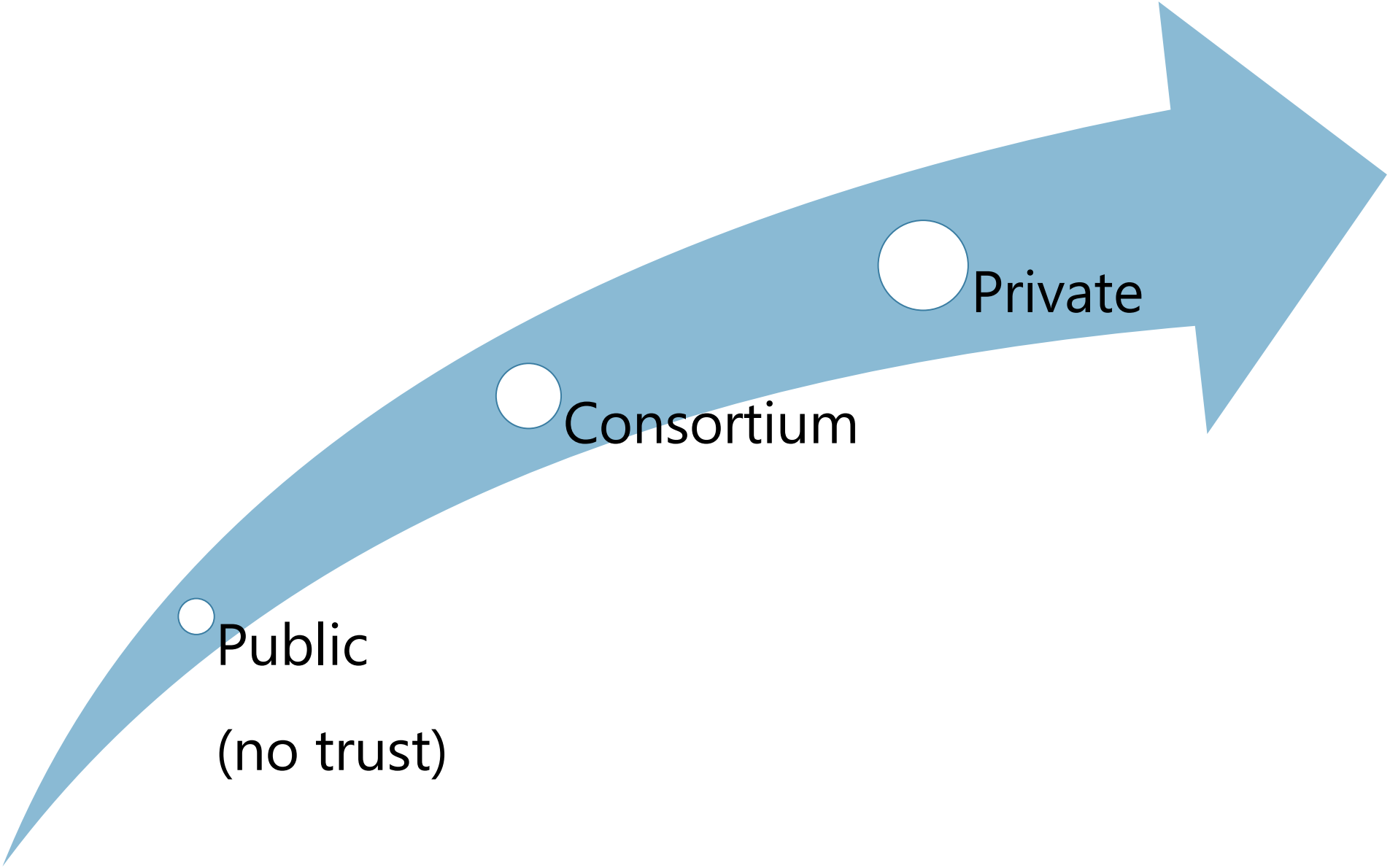
- Records are immutable forever

Transaction identity

- Identity of records can be identified and is undeniable

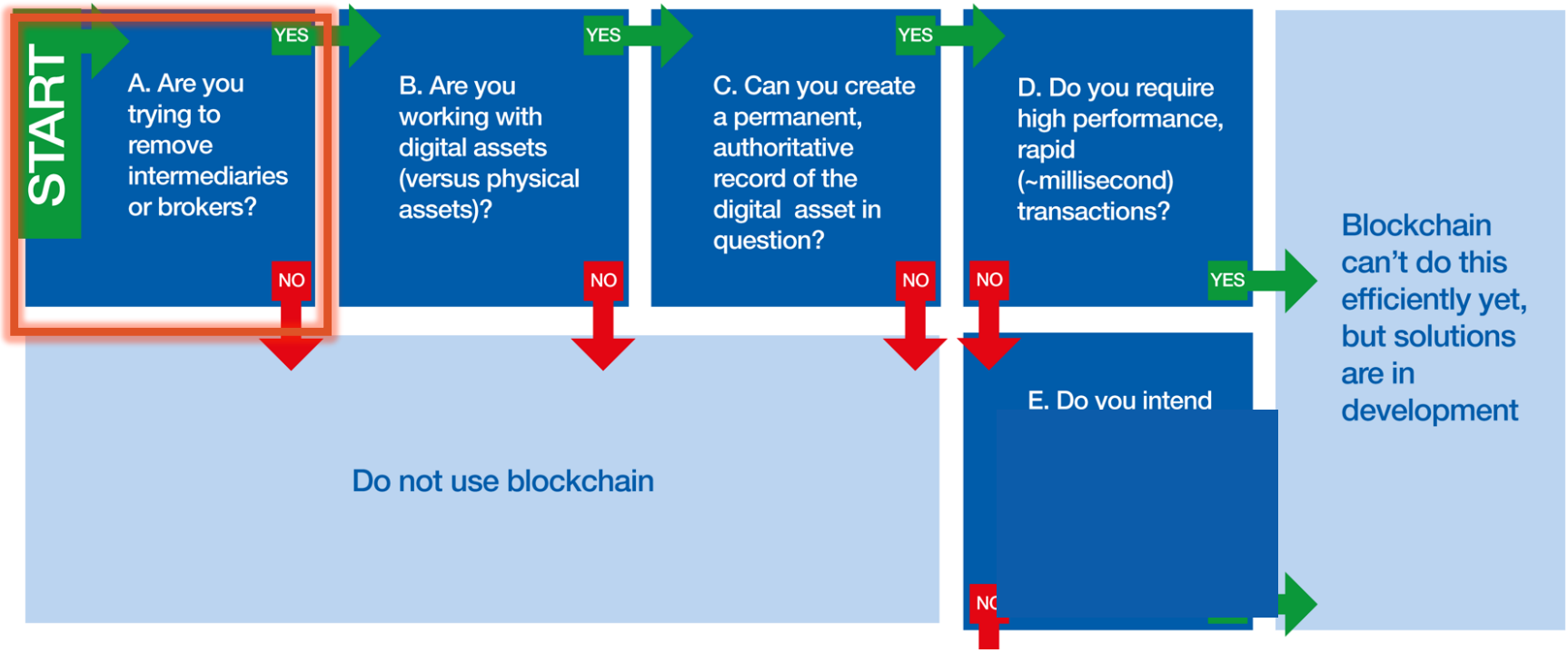
Cryptographic auditability

Trust in Blockchains

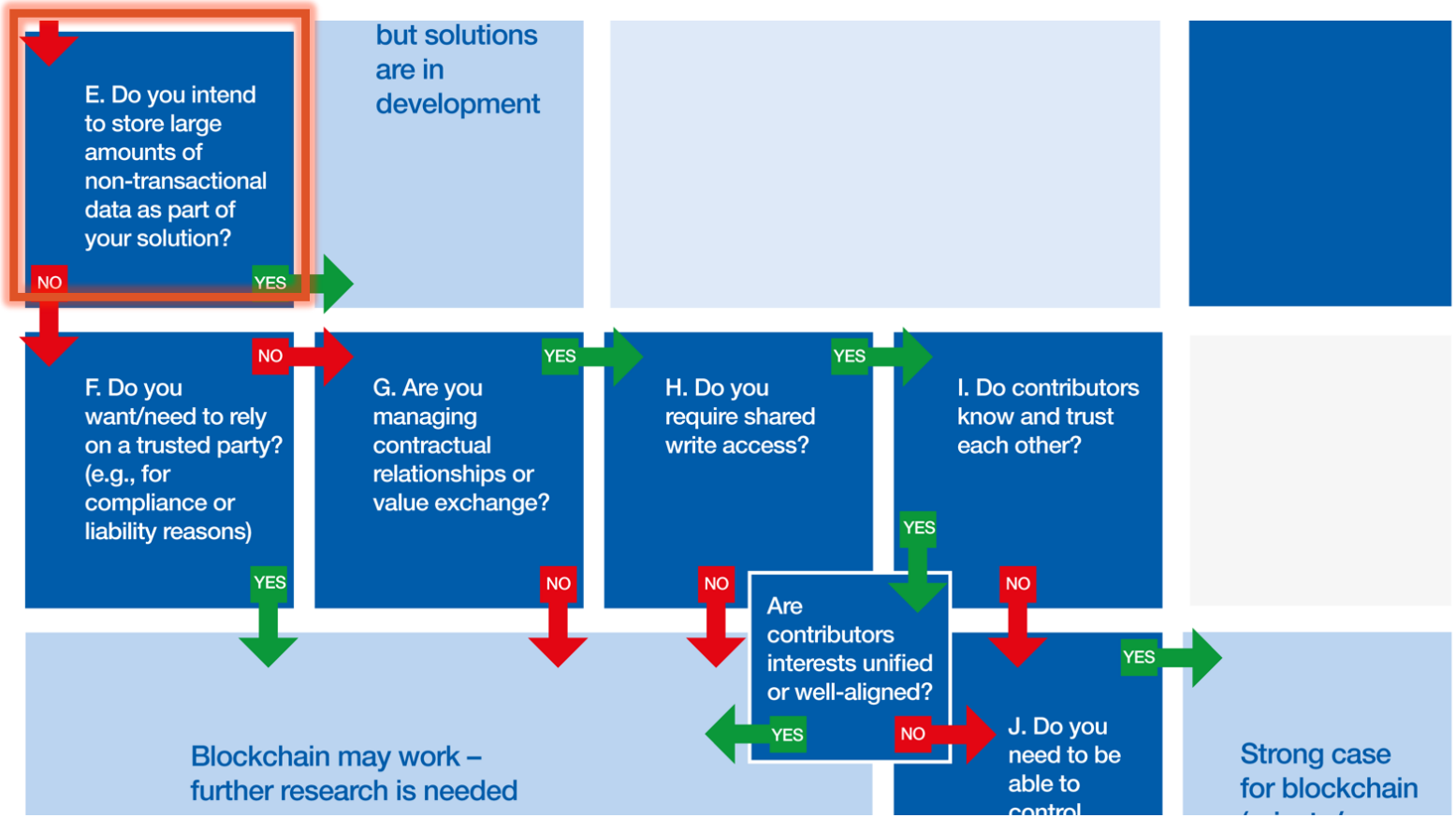


When to use Blockchain

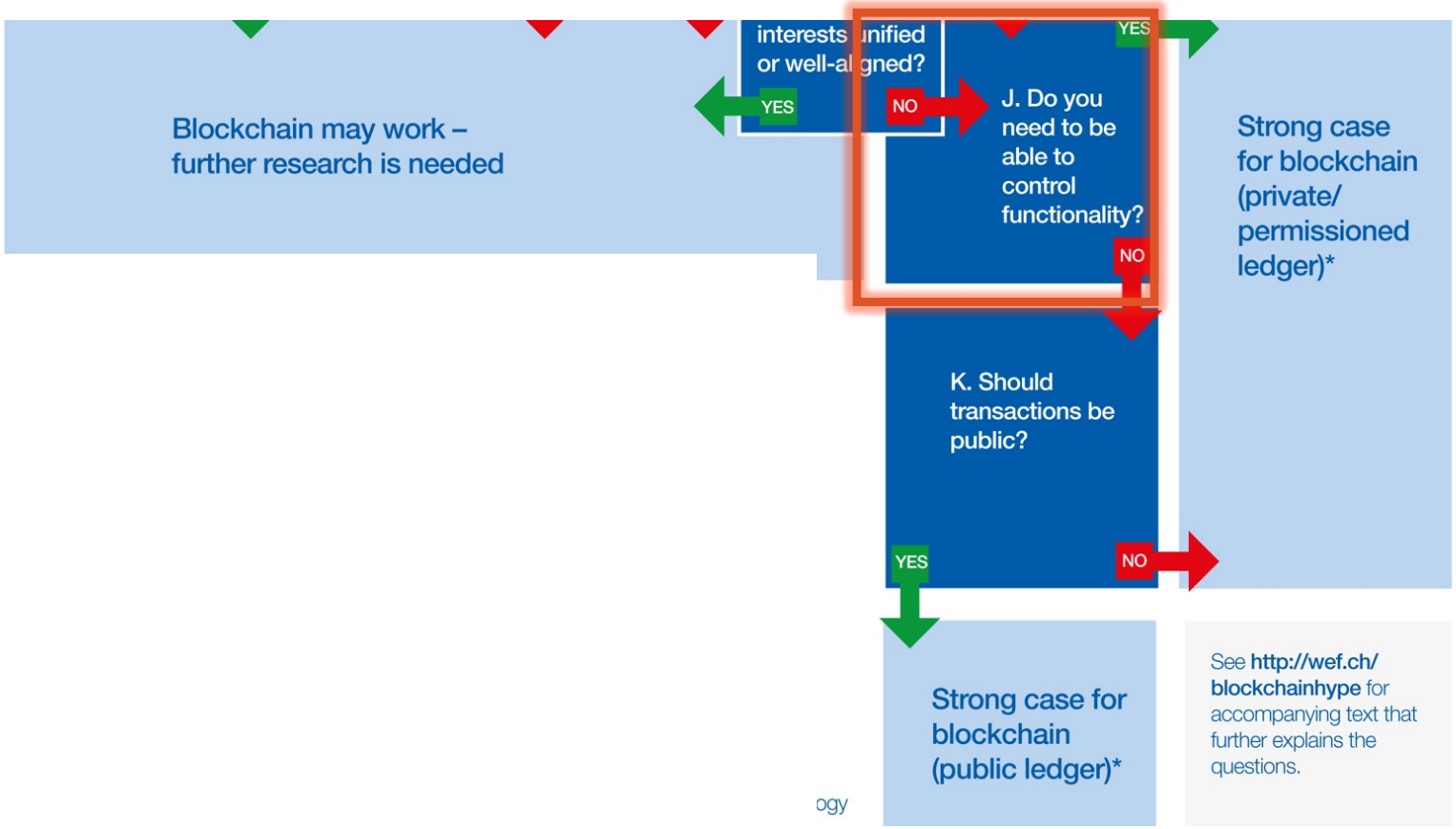
When to use Blockchain



When to use Blockchain



When to use Blockchain



Smart Contracts

Smart Contracts

- Also known as Chaincode

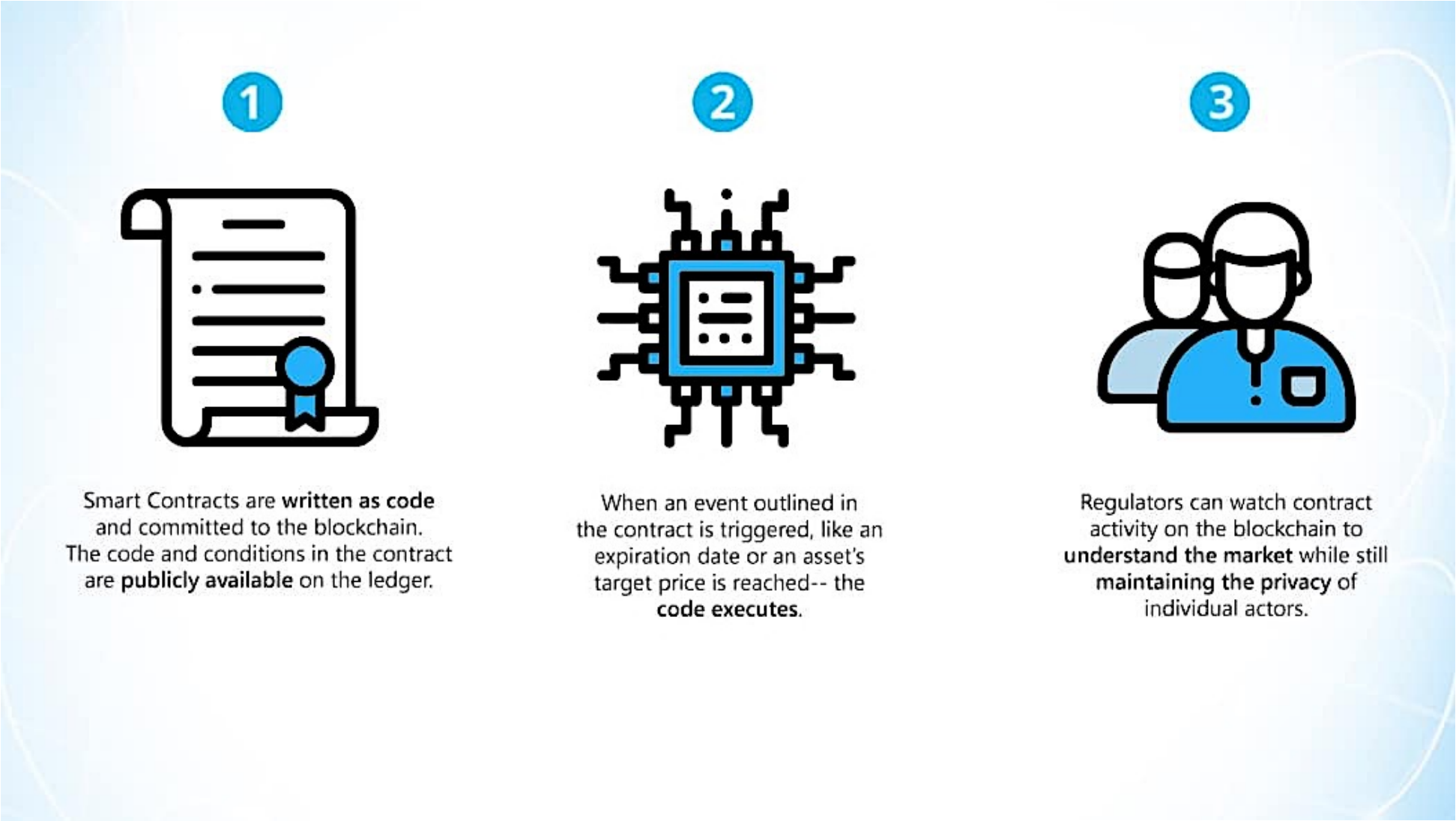
- Automate transactions and ensure they are all following the same rules

- Anyone can write a smart contract by the scripting language of the blockchain and upload it into the blockchain

Smart Contracts

- Anyone can read and call contracts
- Once created they are executed without intervention of intermediaries

Smart Contracts



https://blockgeeks.com/guides/smart-contracts/

Smart Contracts

- A sample Smart Contract written with Solidity language for Ethereum blockchain

```
contract NameRegistry {
  mapping(bytes32 => address) public registryTable;
  function claimName(bytes32 name) {
  if (msg.value < 10) {     // if has been paid 10 wei (the smallest
  currency)
    throw;
  }
  if (registryTable[name] == 0) {
    registryTable[name] = msg.sender;
  }}}
```

Smart Contracts

- Dapp (pronounced Dee-app)
  - Decentralized Application

- Essentially Dapp = frontend +smart contracts

- Executing Daaps is expensive
  - Anything run on the network has to be run on every node.
  - This means that contracts and logic must be simple, streamlined and efficient
  - It is only useful for a small subset of applications

Smart Contracts

- Decentralized Autonomous Organization (DAO)
  - A DAO is an organization that runs on a stack of computer programs
    - Smart contracts in the blockchain world
  - Rules are proposed by people inside community
  - Once it is accepted by majority it is placed in stack or operational rules
  - There is no such thing as a completely autonomous DAO
    - There are specific parts that are autonomous and others that are not so autonomous.

Cryptocurrency

Cryptocurrency

- What is Money?
- Why Money has Value?
- What is Value?

Cryptocurrency

- Over time people have used different kind of things to denote value
  - Salt
  - Peppercorn
  - ...
  - Gold

- What makes them valuable in their time?
  - They were Uncommon and scarce
    - Think about if soil could be the currency?
  - People collectively agree that something is valuable

Cryptocurrency

- What about paper dollar bills?
  - They're just scarce
  - Hard to reproduce
  - All agree that they have value
- Add to this power of economy, army, …

Cryptocurrency

- Digital currencies now has the same properties
  - Scarcity: Mining Difficulty
  - Reliability: Network Consensus
  - Tradability: Digital Signing

Cryptocurrency

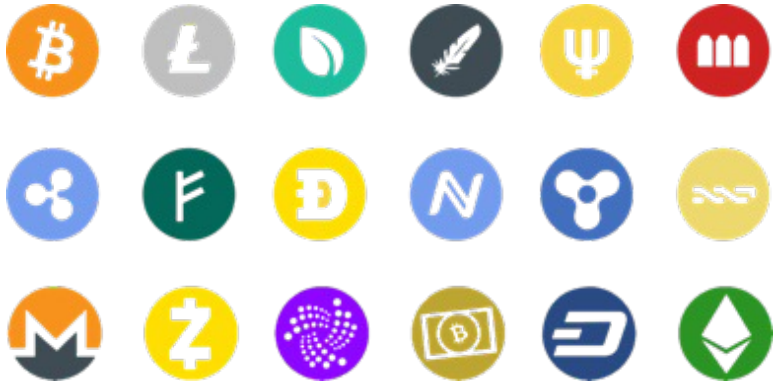
- Currency, Digital Currency
  - Something has value intrinsically
  - Just like Dollar

Cryptocurrency

- A digital asset designed to work as a medium of exchange that uses strong cryptography to secure financial transactions, control the creation of additional units, and verify the transfer of assets.

- Use decentralized control as opposed to centralized digital currency and central banking systems

- Uses DLT on a blockchain to implement decentralization
-
- Not all blockchains have an associated currency
  - Bitcoin and Ether currencies are associated with their blockchain network



Coin

- A coin is a unit of cryptocurrency associated with a given blockchain network

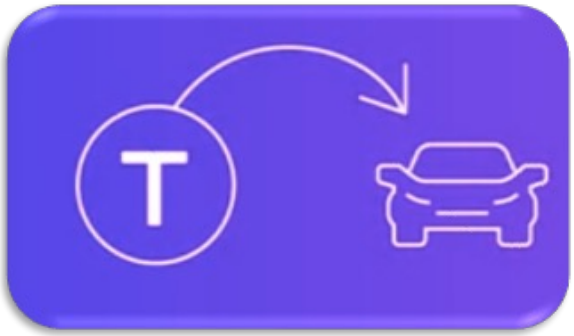
Token

- Something tradable, sellable, own-able
- Can be seen as a proof of an ownership of stake in something which has value
  - Like a share in a company
- Value of the token is extrinsic to it and that is in contrast to the value intrinsic to a coin
- You buy tokens with coins of that blockchain
  - You buy Ethereum tokens with Ether coins

Token

- Tokens are a mechanism to represent a physical item or value in the digital realm.

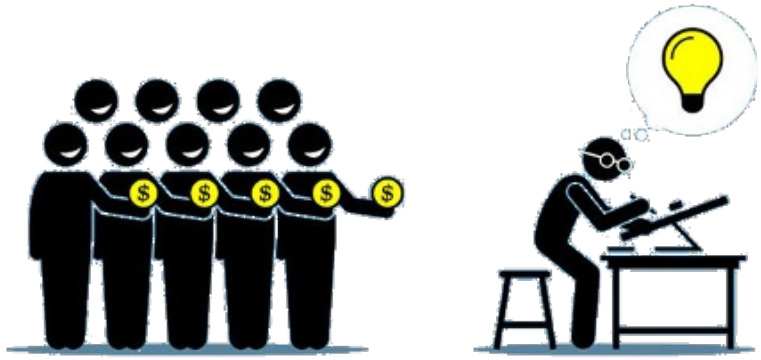
- A token enables the movement or trading of the value or asset the token represents.



Token

- You have a project and want to be invested by people
  - Crowd funding
- You can create a token with a new name on a blockchain

- People buy it with the currency of that blockchain
- Having your tokens, is a proof that some one holds some share on your Dapp project
  - Like voting right



Token

- You provide some online services
- People can buy different tokens to use various services you provide
- These tokens have monetary value

- The possibilities of tokenized ownership are one of the potentially revolutionary aspects of blockchain technology

Token

- Ethereum network defines ERC-20 and recently ERC-223 standards
- Standards define a minimum set of functions for a token
- They are optional but recommended

Initial Coin Offering (ICO)

- An ICO is like a crypto version of an IPO (Initial Public Offering)
- In an IPO, accompany offers ownership shares to the public in order to raise money
- The ICO is the same, it's a way for projects to get funded in exchange for shares of ownership

Initial Coin Offering (ICO)

- ICO is also a process by which new cryptocurrencies can be introduced to the public.
- Instead of selling an ownership stake in something else, it's an offer to buy a new currency, with the hope that the associated blockchain will grow in popularity, making that currency more valuable.
- This would be most similar to buying foreign currency and hoping that the issuing country's economy strengthens.

Example of Dapps & Tokens

- Golem
  - Builds world-scale supercomputer
  - Rent part of your CPU power and get GNT (Golem Network Token)
  - Buy GNT token to use the network

- Meridio
  - Slice total value of a house into small shares
  - You buy shares with Ether coins and receive tokens
  - Later you may exchange tokens for other currencies

Example of Dapps & Tokens

- Brave Browser
  - Chrome-base browser
  - Gives BAT (Business Attendance Token) for people watching contents (Ads, any content)
  - Secure and respects privacy
  - What is the business?
    - When users of the platform increases, BAT value is also increase

Consensus

Consensus

- Consensus is a process of agreement between distrusting nodes on the final state of data

- The choice of the consensus algorithm is also governed by the type of blockchain in use
  - Not all consensus mechanisms are suitable for all types of blockchains

Consensus Types

- Leader Election-based
  - Also called proof-based, lottery-based, ...
  - Nodes compete to be leader and then the elected leader proposes the final value
  - Like in Paxos

  - It is mostly used in public and permissionless Blockchains

Consensus Types

- BFT-Based (Byzantine Fault Tolerant)
  - Works based on voting rounds

  - Nodes send and receive signed-messages
  - If enough similar messages gathered, the agreement is reached

  - Works well with limited number of nodes
  - Mostly used in consortium (permissioned or enterprise) blockchains

Consensus Types

- Proof-of-Work (PoW) consensus
  - Also Nakamoto consensus, used in Bitcoin and Ethereum networks
  - Accounts on scarcity of computational resources
  - Miners must race to solve a hard cryptographic problem
    - Consumes a high amount of resources including computing power and electricity
    - Secures the system against frauds and double spending attacks while adding more virtual currency to the Bitcoin ecosystem
  - Once a miner found a solution, broadcasts in network to be included in the chain

PoW

- Roughly one new block is created (mined) every 10 minutes to control the frequency of generation of bitcoins.

- This frequency needs to be maintained by the Bitcoin network and is encoded in the bitcoin core clients in order to control the money supply.

Consensus Types

- Miners are rewarded with new coins if and when they discover new blocks by solving PoW.
- This is how new coins are injected into the Bitcoin network
- Miners are also paid transaction fees in return for including transactions in their proposed blocks.

PoW

- The rate of creation of new bitcoins decreases by 50%, every 210,000 blocks, roughly every 4 years by adjusting difficulty of cryptographic puzzle

- When bitcoin was initially introduced, the block reward was 50 bitcoins
- In 2012, this was reduced to 25 bitcoins.
- In July 2016, This was further reduced to 12.5 coins (12 coins)

- The next reduction was done on July 4, 2020.
- This will reduce the coin reward further down to approximately six coins

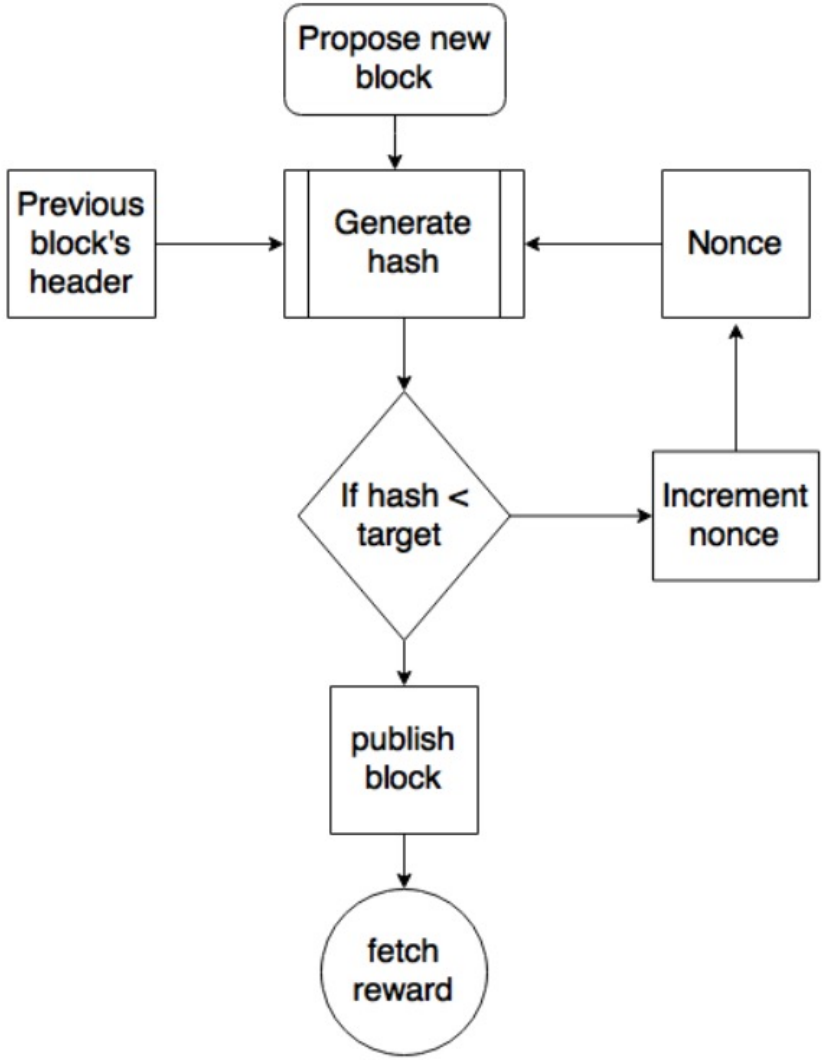
PoW

- Approximately 144 blocks(= 1,728 bitcoins) are generated per day
- Bitcoin supply is also limited and in 2140, almost 21 million bitcoins will be finally created and no new bitcoins can be created
- Around 130 years to mine all Bitcoins
- Bitcoin miners, however, will still be able to profit from the ecosystem by charging transaction fees

PoW Cryptographic Puzzle

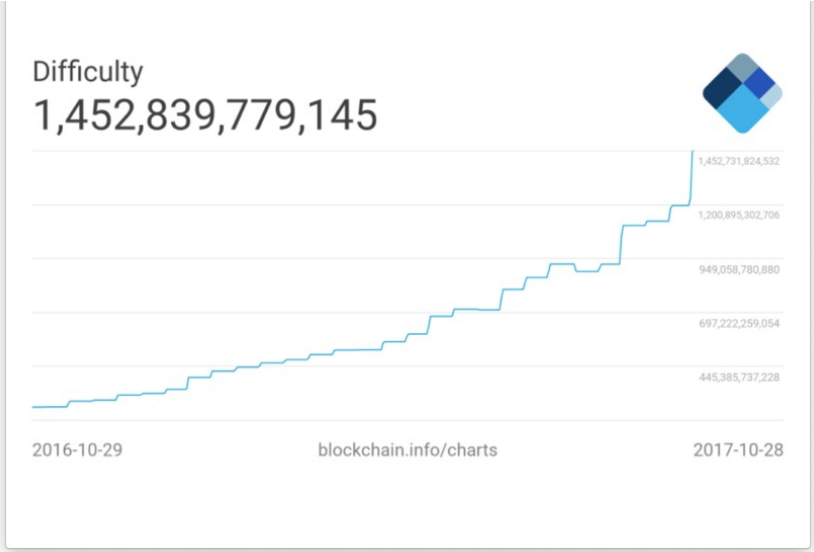
- **H(N || P_hash || Tx || Tx || . . . Tx) < Target**
  - Where N is a nonce
  - P_hash is a hash of the previous block
  - Tx represents transactions in the block
  - Target is the target network difficulty value.
    - H(block) < target value
  - The only way to find this nonce is the brute force method.
  - Once a certain pattern of a certain number of zeroes is met by a miner, the block is immediately broadcasted and accepted by other miners

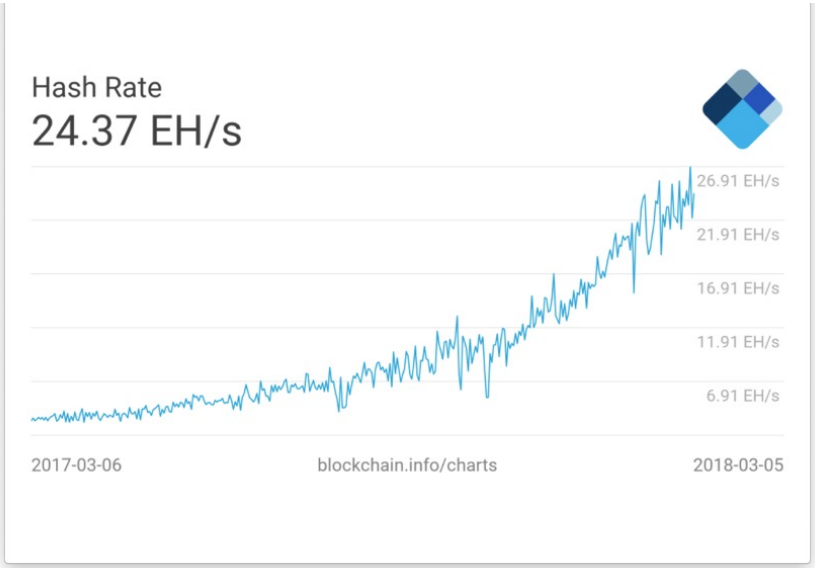
PoW Cryptographic Puzzle



PoW Cryptographic Puzzle

- Target value is updated every two weeks to adjust difficulty to ensure 10-minute block generation time is maintained





PoW

- Mining Tools
  - CPU
  - GPU
  - FPGA
  - ASIC
  - Mining Pools

Consensus

- What if a malicious leader is elected?
  - Others validate the proposal and do not include in their database
  - Leaders must spend power horse on computation to prove they are not malicious!
- Assumes no-one (or consortium) holds more than 51% of resources
  - Otherwise, the miner has a high probability of finding an acceptable solution to the mining puzzle before anyone else for every
  - This gives the miner complete control of the blockchain and breaks the decentralization of blockchain

Consensus Types

- Proof-of-Stake (PoS)
  - The principle idea behind PoS is that users are required to demonstrate possession of a certain amount of stake in network
  - For example how much they have stake in the coin of this blockchain
  - Amount of coins that a network may require changes just like the difficulty in PoW.

PoS

- Works based on scarcity of given cryptocurrency
- If someone (a group) hold majority percent of cryptocurrency can forge most of blocks and takes the control
- Since cryptocurrency is a limited asset, buying up enough of it is expensive, making attacks economically infeasible
- Having stake in a network, convince person to behave trustfully, otherwise value of his stake will decrease

PoS

- How miners are selected?

- Randomized Block Selection
  - Next leader (forger) is selected pseudo-randomly from all users with a stake
  - All nodes has synchronized algorithm state and execute it independently
  - Probability of being selected is roughly proportional to the size of the user's stake

PoS

- Age-based (Proof-of-Coinage)
  - Coinage: The age of a coin is the time since the coins were last used or held
  - Age of held coins is reset every time a block is mined
  - A number generated from the product of the number of coins multiplied by the number of days the coins have been held
  - Next leader is selected pseudo-randomly from the highest generated numbers
  - Coins must be blocked for 30 days up to maximum of 90 days
    - Prevents domination of very old or very large collections

PoS

- If a forger decide to cheat
  - Loses the blocked stake
  - Loses rights to forge

PoS

- PeerCoin is an implementation of Proof-of-Coinage
  - Peercoin works with combination of coinage and PoW
  - The difficulty of mining puzzles (PoW) is inversely proportional to the coinage
  - If miners consume some coinage using coin-stake transactions, then the PoW requirements are relieved.

PoS

Pros

- Speed
- Efficiency (consumes less energy)
- Less hardware (doesn't need a supercomputer)
- Less centralization due to the forger being chosen at pseudo random

Cons

- Vulnerability (investing in the destruction of the network)
- The rich get richer (stake based consensus)

BLOCKCHAIN TRAINING ALLIANCE

Consensus Types

- Proof-of-Activity
  - For a new block miners race with PoW
    - Block contains miner address and his reward plus other header info
  - When a new block mined, a group of validators are selected by PoS to validate and sign
  - The more cryptocoins a validator stakes, the more chances he or she has for being selected as a signer

Consensus Types

- Proof-of-Burn
  - Considered as a variant of PoS
  - Participants must "burn" some their coins
    - Burning a coin means sending it to a randomly selected address which is unlikely to be under control of any participant
  - The amount of burned coins then serves as an everlasting ticket in a lottery for the right to publish
  - Participants can then engage in a proof-of-work-style puzzle whose difficulty is inversely related to the amount of burned coins

Consensus Types

- Proof-of-Capacity
  - Implemented by BurstCoin
  - Uses HDD capacity
  - It has two major steps
    - Plotting Step:
      - A large data set is generated and stored in user's hard drive
      - These are can be seen as the pre-computed hashes and all things required to forge blocks
      - This phase may take days or weeks to complete
    - Mining Step
      - Through some mathematical processes user scans his Plot files and finds a deadline time
      - Waits for the defined deadline time and if no one forge a block he can start forging
  - Having larger capacity helps to find smaller deadline time

Consensus Types

- Proof-of-space
  - Allows prover to convince verifier that the miner has spent some storage resources

Consensus Types

- Proof-of-Retrievability (PoRet)
  - Allows prover to check that the server is still storing the data
  - Makes the proofs themselves leak pieces of the data so that the verifier can issue some number of challenges and then reconstruct the data from the proofs

Proof-of-Retrievability

- Permacoin
  - A PoRet system developed by Microsoft Research
  - Modifies Bitcoin to repurpose its mining resources to achieve a distributed storage of archival data.
  - It requires clients to invest both computational and storage
  - Miners are required local, random access to a copy of a file
  - A large file F is broken into several segments distributed by a trusted dealer

Proof-of-Retrievability

- Permacoin
  - Computer Merkle root for the file where tree leaves are segments
  - Select a random nonce and compute
  - h1 = H(prev_block||mrkl_root||pk||nonce)
  - With h1 select K psuedo-randomly file segments to store
  - Compute h2 based on the nonce and the file content:
  - h2 = H(prev_block||mrkl_root||pk||nonce||F)
  - The miner wins if h2<target

Consensus Types

- PBFT (Practical Byzantine Fault-Tolerance)
  - Provide strong guarantees in that either all honest nodes will adopt a block or none will
  - PBFT does not scale well, useful for small networks

Consensus Types

- Proof of Elapsed Time (PoET)
  - Works like a lottery system, the next leader is elected randomly
  - Gives chance to all participators
  - Each node have a timer, it is assigned a random time to wait
  - The node finished its waiting time commits the next block

Proof of Elapsed Time (PoET)

- Hyperledger
  - A project started by Linux Foundation and involves several blockchain projects mostly for enterprises
- Hyperledger Sawtooth
  - A modular project to inject any consensus algorithms and permissions, …
  - Currently it has Intel-contributed PoET and PBFT

Proof of Elapsed Time (PoET)

- PoET in Hyperledger Sawtooth
  - Sawtooth relies on Intel Trusted Execution Environment, SGX
    - SGX is like a VM with special privileged instructions
  - Waiting time is generated by random and checked by SGX
  - The validator with the shortest wait time for a particular transaction block is elected as leader
  - Leader creates, finalizes, signs and broadcast block
  - Block is validated by validators

Proof of Elapsed Time (PoET)

- PoET in Hyperledger Sawtooth (cont.)
  - It is very energy-efficient
  - Disadvantages
    - Needs a special hardware
    - Having several SGX environments means having more tickets in lottery
    - Attacker with compromised environment may win always

Consensus Types

- Ripple Network
  - Mostly for consortium blockchains
  - The rival of SWIFT system for exchanging
  - Mainly designed for exchanging with its native currency XRP
  - Uses the Ripple protocol consensus algorithm (RPCA) which is variant of PBFT
  - There are two node types: clients and servers
  - Clients only issue transactions

Ripple Network

- Servers maintain a UNL (Unique Node List) which is a list of trusted nodes
- Servers collect valid transactions (candidate set) and send to other UNL nodes (about every few seconds)
- They collect candidate sets from others
- Transactions accepted by 80% of UNL nodes are applied to the ledger

Consensus Types

- Stellar Network
  - Launched by one the cofounders of Ripple
  - Uses Federated Byzantine Agreement (Variant of PBFT)
  - Similar to Ripple, but allows participants to choose their trusted list called quorum slice
  - Set of quorum slices form Quorums which are nodes that is sufficient for network if they reach consensus
    - A quorum is a non-empty set of nodes containing at least one quorum slice for each of its non-faulty members
  - FBA mandates Quorums must share at least one honest node

List of Crypto-Currencies

MOST ACTIVE CRYPTOCURRENCIES

DOLLAR EURO

NAME CURRENCY	PRICE	+/-	%	LAST UPDATED	MARKET CAP	CIRCULATING SUPPLY	VOLUME	1 MON. CHART
Bitcoin	7,186.7500	-19.89	-0.28 %	10:36:00 PM	129.88 B	18,072,712	18.88 B	
Ethereum	127.4152	-0.86	-0.67 %	10:36:00 PM	13.85 B	108,728,346	7.37 B	
Ripple	0.1934	0.00	-0.92 %	10:36:00 PM	8.37 B	43,299,885,509	1.27 B	
Tether	1.0054	0.00	-0.06 %	10:32:00 PM	4.13 B	4,108,044,456	21.23 B	
Bitcoin Cash	187.2741	-0.06	-0.03 %	10:36:00 PM	3.40 B	18,138,300	1.42 B	
Litecoin	39.9779	-0.18	-0.44 %	10:36:00 PM	2.55 B	63,728,213	2.67 B	
EOS	2.4785	-0.02	-0.81 %	10:32:00 PM	2.34 B	942,129,908	1.49 B	
Binance Coin	13.5432	0.00	-0.03 %	10:32:00 PM	2.11 B	155,536,713	195.90 M	
Bitcoin SV	87.5976	-0.87	-0.98 %	10:32:00 PM	1.58 B	18,068,415	390.69 M	
Stellar	0.0448	0.00	-3.20 %	10:32:00 PM	897.63 M	20,054,779,554	227.56 M	
Tron	0.0134	0.00	-0.87 %	10:32:00 PM	893.07 M	66,682,072,191	1.30 B	
Cardano	0.0339	0.00	0.57 %	10:32:00 PM	879.60 M	25,927,070,538	59.59 M	
Monero	46.2166	-0.54	-1.17 %	10:36:00 PM	800.91 M	17,329,479	154.01 M	

References

- Imran Bashir, Mastering Blockchain, 2nd Edition
- edx course
- https://www.cbinsights.com/research/what-is-blockchain-technology/
- https://dev.to/damcosset/blockchain-what-is-mining-2eod
- https://www.weforum.org/agenda/2018/04/questions-blockchain-toolkit-right-for-business/
- https://www.investopedia.com
- https://tokens-economy.gitbook.io/consensus/
- Blockchain: Foundations and Use Cases, https://www.coursera.org/learn/blockchain-foundations-and-use-cases/home/welcome
- https://burstwiki.org/
- Salimitari M, Chatterjee M. A Survey on Consensus Protocols in Blockchain for IoT Networks. arXiv preprint arXiv:1809.05613. 2018.
- https://medium.com/@ppio/proofs-relevant-to-storage-a747ff477d8c
- http://learningspot.altervista.org/blockchain-mining-proof-of-useful-work/
- https://www.stellar.org/developers/guides/concepts/scp.html
- http://www.scs.stanford.edu/~dm/blog/simplified-scp.html

The End!