BLOCKCHAIN 101: INTRODUCTION TO BLOCKCHAIN

BROUGHT TO YOU BY SMU BLOCKCHAIN CLUB

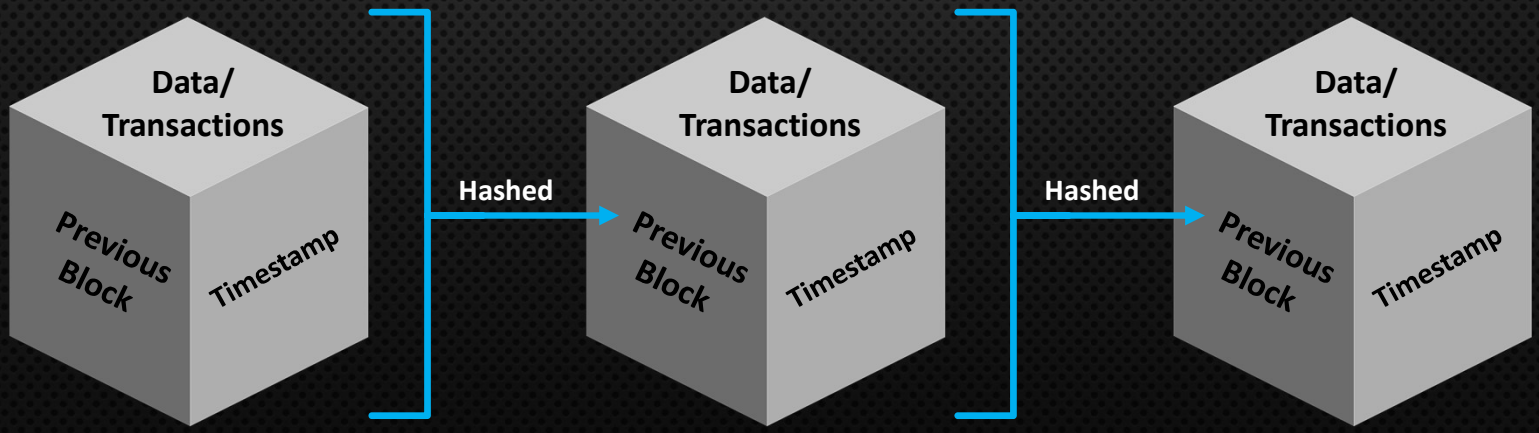
AGENDA

- Background
- Where it all started
- Purpose
- Concerns
- Public vs Consortium vs Private Blockchain
- Proof of Work vs Proof of Stake
- Next: Applications of Blockchain

BACKGROUND

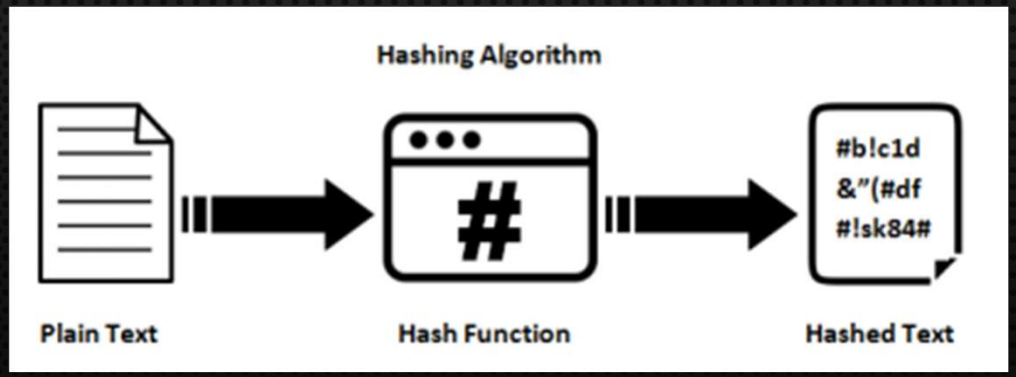
BACKGROUND

- Block = Storage of data or transactions
- Timestamps the transaction, blocks are **IMMUTABLE**
- Blockchain = Irreversible chain of blocks
- All blocks are unique and links to the previous one

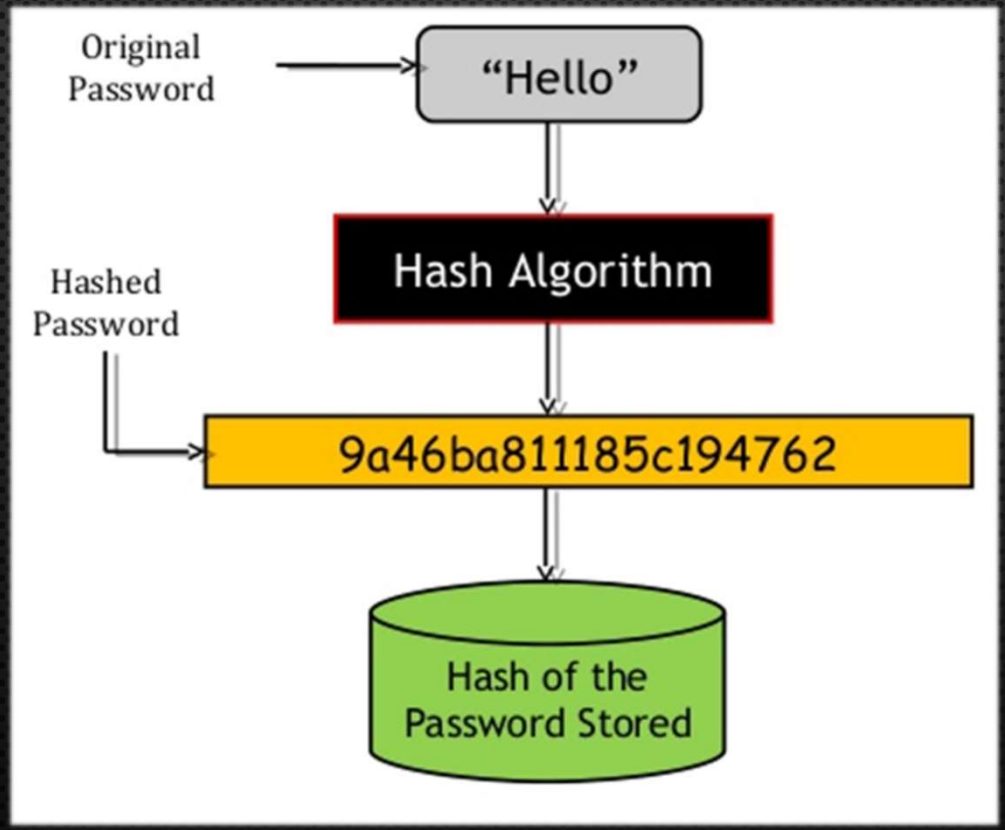


BACKGROUND - HASHING

- HASHING IS GENERATING A VALUE OR VALUES FROM A STRING OF TEXT USING A MATHEMATICAL FUNCTION
- ONE WAY
- PREVENTS TAMPERING
- NOT TO BE CONFUSED WITH ENCRYPTION/DECRYPTION



BACKGROUND - HASHING

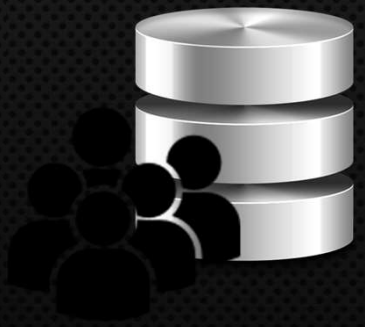


BACKGROUND

- With Distributed Ledger Technology (DLT), Blockchain can act as a digital infrastructure for various purposes

BACKGROUND - DLT

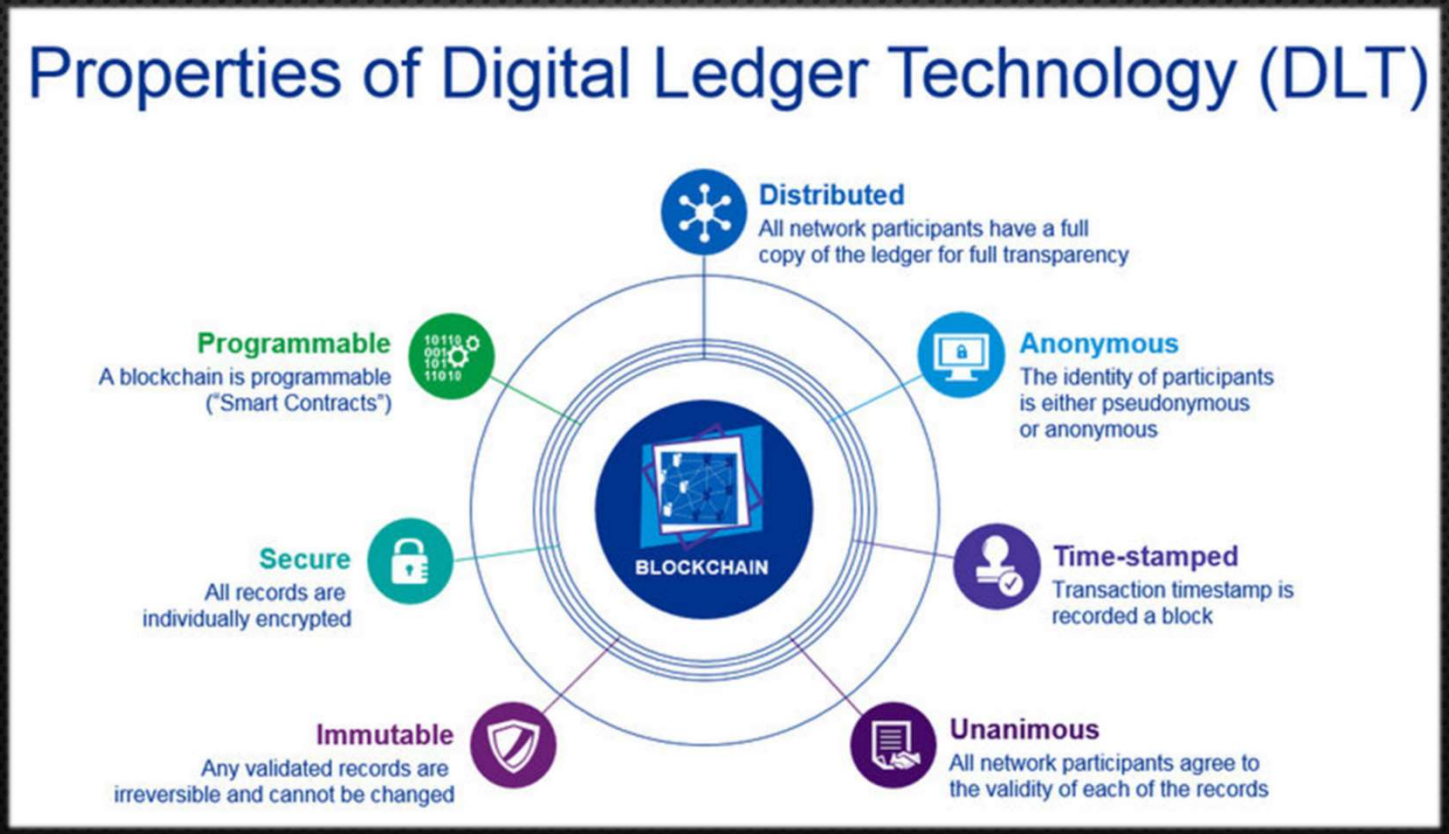
- A DATABASE THAT IS CONSENSUALLY SHARED AND SYNCHRONIZED ACROSS NETWORK SPREAD ACROSS MULTIPLE SITES, COUNTRIES, OR INSTITUTIONS
- ALLOWS TRANSACTION TO HAVE PUBLIC "WITNESSES", MAKING CYBERATTACK DIFFICULT
- ANY CHANGES MADE TO LEDGER ARE REFLECTED AND COPIED TO ALL PARTICIPANTS.



BACKGROUND - DLT

- No central administrator or centralized data storage
- Requires peer-to-peer network and consensus algorithms to ensure replication
- Allows creation of cryptocurrencies, smart contracts, file storages, applications, etc.

BACKGROUND - DLT



Where it all started

WHERE IT ALL STARTED

- TECHNOLOGY FIRST FORMALLY IMPLEMENTED IN 2008 BY SATOSHI NAKAMOTO

WHERE IT ALL STARTED - SATOSHI NAKAMOTO

- Founder of Bitcoin and initial creator of the Original Bitcoin client
- Entirely unknown outside of Bitcoin
- Satoshi = “wisdom”/“reason”
- Nakamoto = “central source”
- 2007-2010

WHERE IT ALL STARTED - SATOSHI NAKAMOTO

"Yes, [we will not find a solution to political problems in cryptography,] but we can win a major battle in the arms race and gain a new territory of freedom for several years.

Governments are good at cutting off the heads of a centrally controlled networks like Napster, but pure P2P networks like Gnutella and Tor seem to be holding their own.

It's very attractive to the libertarian viewpoint if we can explain it properly. I'm better with code than with words though."

- Satoshi Nakamoto, 2008

ROUND 1

HASHING GAME

WHERE IT ALL STARTED

- Bitcoin introduced in 2009
- First digital currency using a trustless system to solve double spending problem without a central authority

WHERE IT ALL STARTED – BITCOIN – DIGITAL CURRENCY

- Digital currency
  - A form of currency
  - Available only in digital or electronic form, and not in physical form
  - Also called digital money, electronic money, electronic currency, or cyber cash
  - Intangible
  - Only be owned and transacted in by using computers or electronic wallets connected to the Internet or the designated networks
  - Cryptocurrency = Virtual currency = Digital currency → But not the other way round

Where it all started – Bitcoin – Digital Currency

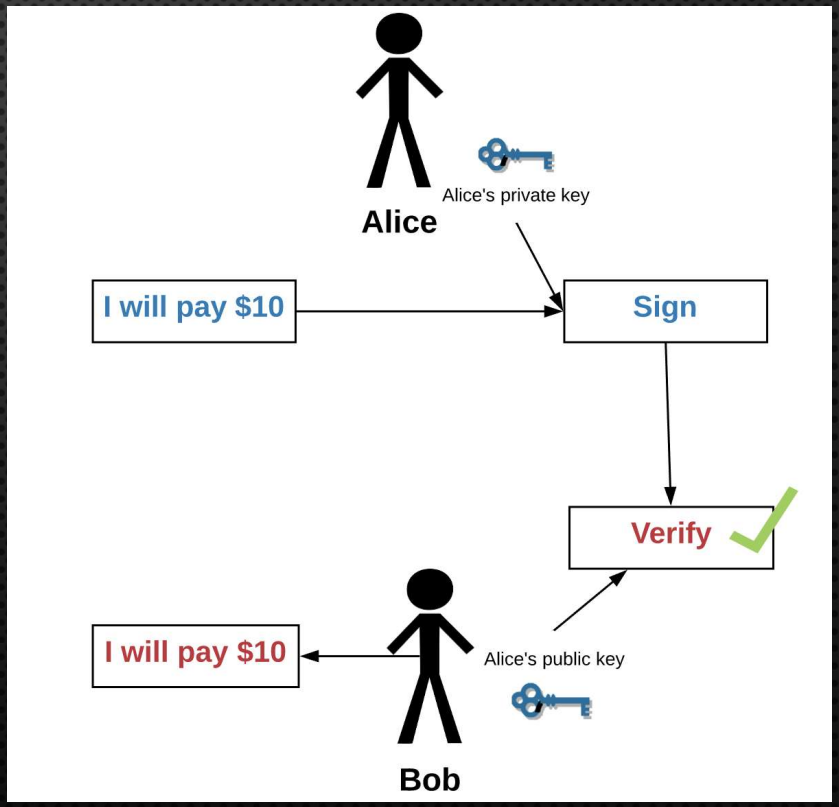
- Virtual Currency
  - unregulated form of digital currency
  - May be under the control of the currency developer(s), the founding organization, or the defined network protocol, instead of being controlled by a centralized regulator
  - i.e. cryptocurrencies, coupon-linked/rewards-linked monetary systems
- Cryptocurrency
  - Uses cryptography to secure and verify transactions and to manage and control the creation of new currency units
  - i.e. Bitcoin, Ethereum, etc.

WHERE IT ALL STARTED – BITCOIN – TRUSTLESS

- Ability to send transact with someone else without the need to know exactly who the actual person is physically
- "Trust" is shifted from intermediary to the ecosystem itself
  - Instead of trusting third party (i.e. DBS Bank), trust to transact is now placed in the public-key cryptography and consensus mechanism

WHERE IT ALL STARTED – BITCOIN – TRUSTLESS

- PUBLIC-KEY CRYPTOGRAPHY
  - PUBLIC KEY IS VISIBLE TO ANYONE
  - PRIVATE KEY IS VISIBLE ONLY TO ITS OWNER
  - TO ENCRYPT: SIGN PLAINTEXT WITH PRIVATE KEY TO GET CIPHERTEXT
  - TO DECRYPT: VERIFY CIPHERTEXT WITH PUBLIC KEY TO GET PLAINTEXT



Where it all started – Bitcoin – Trustless

- Consensus mechanism
  - Needed to preserve a digitally shared truth
  - Prevents double spending
  - Using mathematics, economics, and game theory to incentivize all parties in the system to reach a "consensus", or coming to an agreement on a single state of this ledger.
  - I.e. Bitcoin uses Proof of Work consensus algorithm

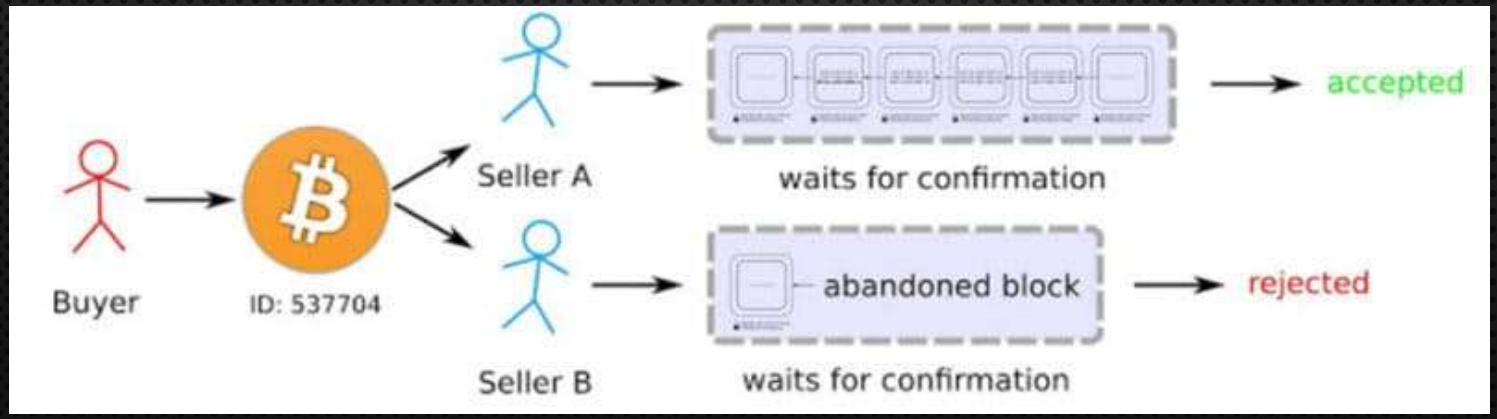
WHERE IT ALL STARTED – BITCOIN – TRUSTLESS

"TRUSTLESS"

- MECHANISMS IN PLACE BY WHICH ALL PARTIES IN THE SYSTEM CAN REACH A CONSENSUS ON WHAT THE CANONICAL TRUTH IS
- POWER AND TRUST IS DISTRIBUTED AMONGST STAKEHOLDERS RATHER THAN A SINGLE ENTITY

WHERE IT ALL STARTED – BITCOIN – DOUBLE SPENDING

- NOT ALLOWING SOMEONE FROM SPENDING SAME ASSET TWICE



WHERE IT ALL STARTED – BITCOIN – DOUBLE SPENDING

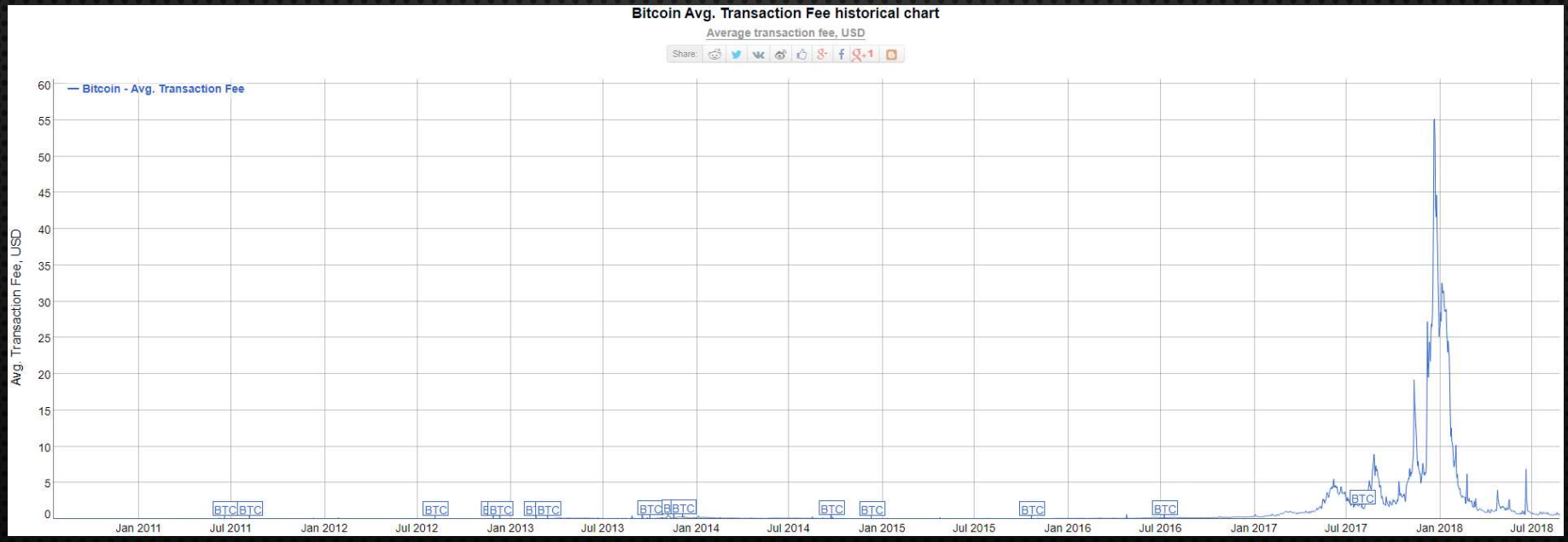
- Scenario 1:
  - You sent the same 1 BTC to merchant A and merchant B
  - Both transactions go into the unconfirmed pool of transactions
  - First transaction got confirmations and was verified by miners in the next block
  - Second transaction will not get enough confirmations because the miners judged it as invalid, so it was pulled from the network
  - Double spending problem solved

WHERE IT ALL STARTED – BITCOIN – DOUBLE SPENDING

- Scenario 2:
  - You sent the same 1 BTC to merchant A and merchant B
  - Both transactions go into the unconfirmed pool of transactions
  - Both transactions are taken simultaneously by the miners and got confirmations
  - Only the one with the most number of confirmations will be included in the blockchain
  - Double spending problem solved, if merchants wait for a **minimum of 6 confirmations**
    - As of current, it is computationally impossible and/or ridiculously expensive for double-spender-wannabe to go back and reverse all transactions in the 6 blocks that have been added after their transaction

WHERE IT ALL STARTED – BITCOIN – MINER FEE

- MINER FEES ARE TRANSACTION FEES THAT SPENDERS MAY INCLUDE IN ANY BITCOIN TRANSACTION
- LOW COST COMPARED TO TRADITIONAL REMITTANCE



WHERE IT ALL STARTED - BITCOIN

- Ease of use - only requires internet
- every update is live and final
- Supply: 21 million BTC that can be mined, 2140.

Round 2

HASH GAME

PURPOSE

PURPOSE

- Privacy
  - One can own multiple addresses
  - No link to name, email, address or any personal info
- Secure
  - Combination of random numbers and letters for both public and private
- Trustless
  - No need for mutual trust before transaction
  - Smart contracts can help escrow payments
- Decentralisation
  - No need for third-party reliance
  - Incorruptible

PURPOSE

- Minimal fee
  - Little to no transaction fees
- Transparency
  - Proof of transaction/information (receipts, copyrights)
- Backups
  - No fear of misplacing data on one machine
- Tamper proof
  - Not able to manipulate data for individual interests

CONCERNS

CONCERNS

- Money laundering
  - Untraceable
- Terrorism funding
  - Anonymous
- Irreversible
  - Typos, scams, etc.

PUBLIC VS CONSORTIUM VS PRIVATE BLOCKCHAIN

Public blockchain

- "Fully decentralised"
- Anyone can read
- Anyone can send
- Anyone can participate in consensus process
- Good for global currency, etc.

Consortium blockchain

- "Partially decentralized"
- Right to read may be restricted
- Right to sent may be restricted
- Consensus controlled by preselected nodes
- e.g. one might imagine a consortium of 15 financial institutes, each of which operates a node and of which 10 must sign every block in order for the block to be valid.
- Good for limiting public queries, etc.

PRIVATE BLOCKCHAIN

- "Fully private"
- Right to read may be restricted
- Right to sent may be restricted
- Write permission kept centralised to one organisation
- Good for database management, auditing, etc.

PUBLIC VS PRIVATE BLOCKCHAIN

	Public Blockchain	**Private Blockchain**
Access	Open read/write. Allows anyone to participate, execute contracts, run node, become a miner	Permissioned read/writes. All participants and nodes needs to be approved.
Consensus	Proof of Work (PoW), Proof of Stake (PoS), etc	Custom: PBFT (Practical Byzantine Fault Tolerant), multi-signature, etc
Currency	Mostly required. Used for transactions, rewarding miners and other utility (PoS)	Not required
Apps	Commonly known as dApps (decentralized Apps), they are decentralized, guarantee privacy and anonymity. Execution costs currency (to reward miners) and take time for data to verified across all nodes. Equivalent to open Internet.	Apps are built to custom business needs. Private Blockchain tech helps cut down processing times, less data redundancy and introduce efficiency between (or within) systems or organizations, and the same time restrict public access to sensitive data.
Examples	You can build something which serves everyone: from fun games like Crypto Kitties to important services like universal KYC (Civic), decentralized file storage (Storj, Filecoin), Anonymous SSO	Popular examples could be banks sharing a common ledger for fraud detection, international forex transactions, medical institutions storing and sharing patients health data with each other, etc.
Popular platforms	Ethereum, Bitcoin, NEO, Ripple, Stellar	Hyperledger, Corda, Multichain
Languages (Smart Contracts)	Ethereum: Solidity	Hyperledger: Chaincode
	NEO: VB.net, C#, Java, Python	Corda: Kotlin
Frameworks and Development Tools	Ethereum: Truffle, Metamask, Mist Wallet	Hyperledger: Hyperledger-Compose, Visual Studio
		Corda: Flow

PUBLIC VS PRIVATE BLOCKCHAIN - ADVANTAGES OF EACH

Public	Private
Transparency of application codes	Rules are easy to change
Network effects	Known Validators
	Cheaper transaction fee
	Faster transaction speeds
	Can hide from public

PROOF OF WORK VS PROOF OF STAKE

PROOF OF WORK

- A protocol that aims to deter cyber-attacks such as a distributed denial-of-service attack (DDoS) which has the purpose of exhausting the resources of a computer system by sending multiple fake requests
- a requirement to define an expensive computer calculation called mining

Proof of Work - Mining

- Mining verifies legitimacy of a transaction and creates new digital currencies via miner rewards
- Steps:
  1. Transactions bundled together into a block
  2. Miners verify that transactions within each block are legitimate, by solving a mathematical puzzle known as proof-of-work problem
  3. A reward is given to the first miner who solves each blocks problem
  4. Verified transactions are stored in the public blockchain

Proof of Stake

- A different way to validate transactions based and achieve the distributed consensus
- The creator of a new block is chosen in a deterministic way, depending on its wealth or age (stake)
- There is no block reward
- Many types of POS algorithms
  - I.e. Ethereum plans to introduce bonding stake for its POS plans

PROOF OF WORK VS PROOF OF STAKE

PROOF OF WORK	PROOF OF STAKE
	
The probability of mining a block is determined by how much computational work is done by the miner.	The probability of validating a new block is determined by how large of a stake a person holds (how many coins they possess).
	
A reward is given to the first miner to solve the cryptographic puzzle of each block.	The validators do not receive a block reward, instead they collect network fees as their reward.
	
Network miners compete with one another using computational power. Mining communities tend to become more centralized over time.	Proof of Stake systems can be much more cost and energy efficient than Proof of Work systems, but are less proven.

3iQ Research Group

Next: Applications of Blockchain

- Will blockchain be the next Internet
- Why it matters to you
- How your jobs will change

THANK YOU