TIBA

Lecture 4  Limitations and Vulnerabilities

By Samuel Tang, TIBA

Fall 2020 @ Tsinghua University

TIBA

Goal: What are the problems blockchain is facing?

TIBA

Content

- Limitations
  - Societal
  - Technical
- Solutions
- Vulnerabilities

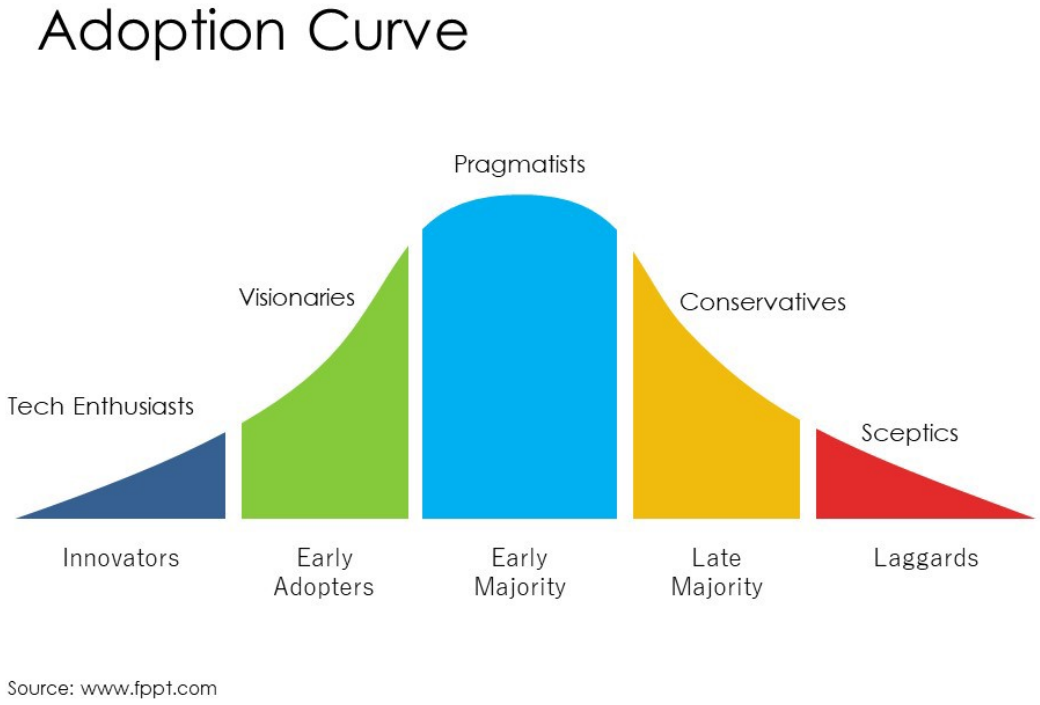
TIBA

Limitations

Adoption – Innovators & Early Adopters

When's the tipping point?

- Some say that the current state of blockchain = internet in the 90s
- Still waiting for "killer apps" outside of cryptocurrency



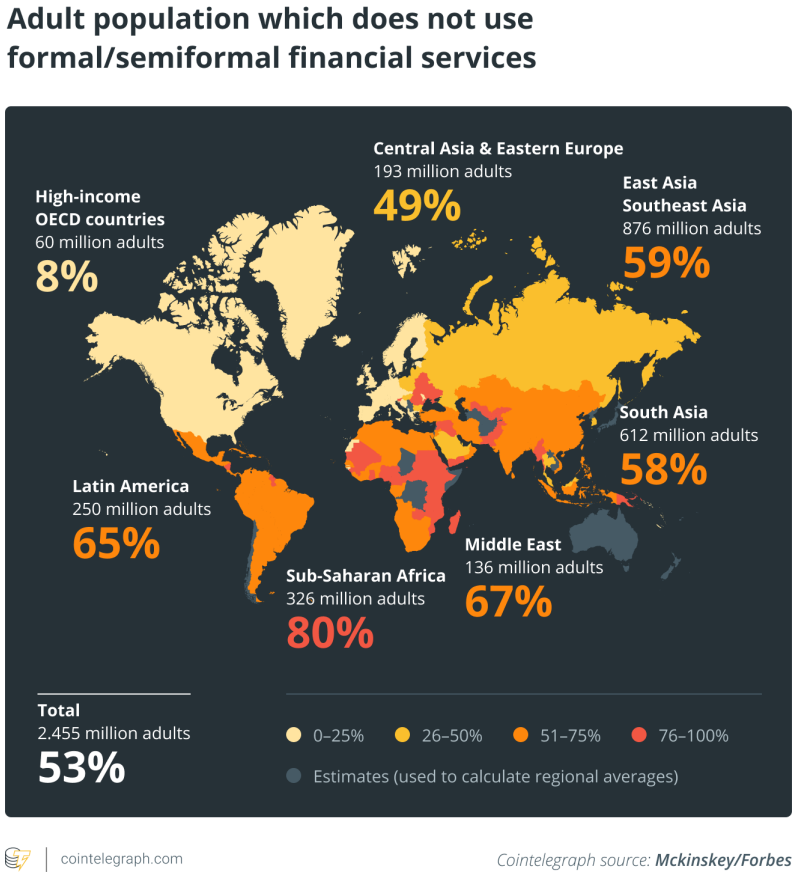
Source: www.fppt.com

Img: https://medium.com/@MeshPay/blockchain-cryptocurrencies-and-icos-dc13ce2e60c4;

Adoption – The Promise of Blockchain

Financial Inclusion

- Blockchain adaption in financial industry
  - Financial access for all
  - Level the playing field
- Current innovation and applications -> next week's lecture!

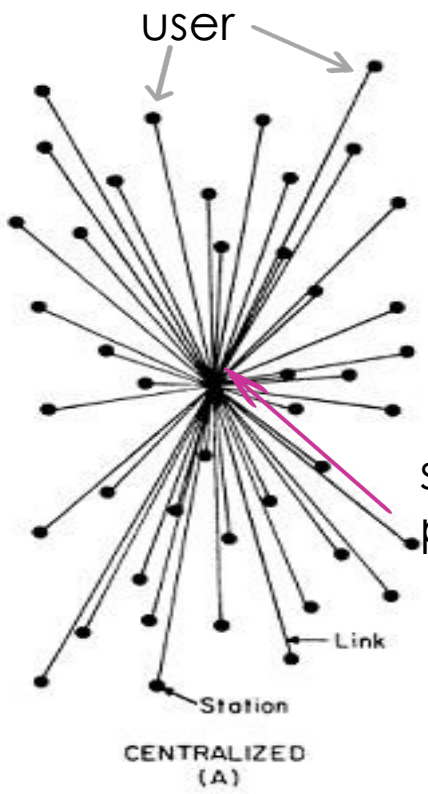


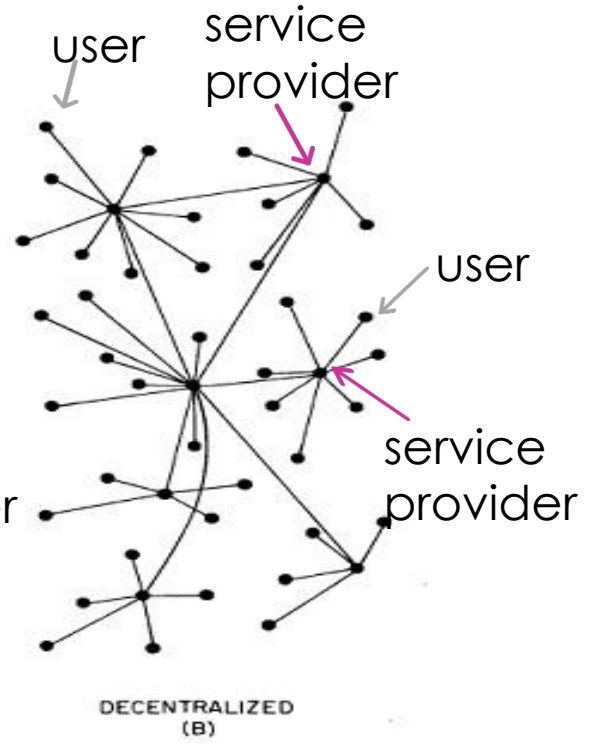
Img: https://cointelegraph.com/news/the-state-of-blockchain-experts-weigh-in-on-adoption-around-the-world

Adaption – User's Perspective

Wait…what's the difference?

- Blockchain's invisibility
- For the most part, user experience is the same regardless of decentralized or centralized





TIBA

Adaption - Decentralized or no?

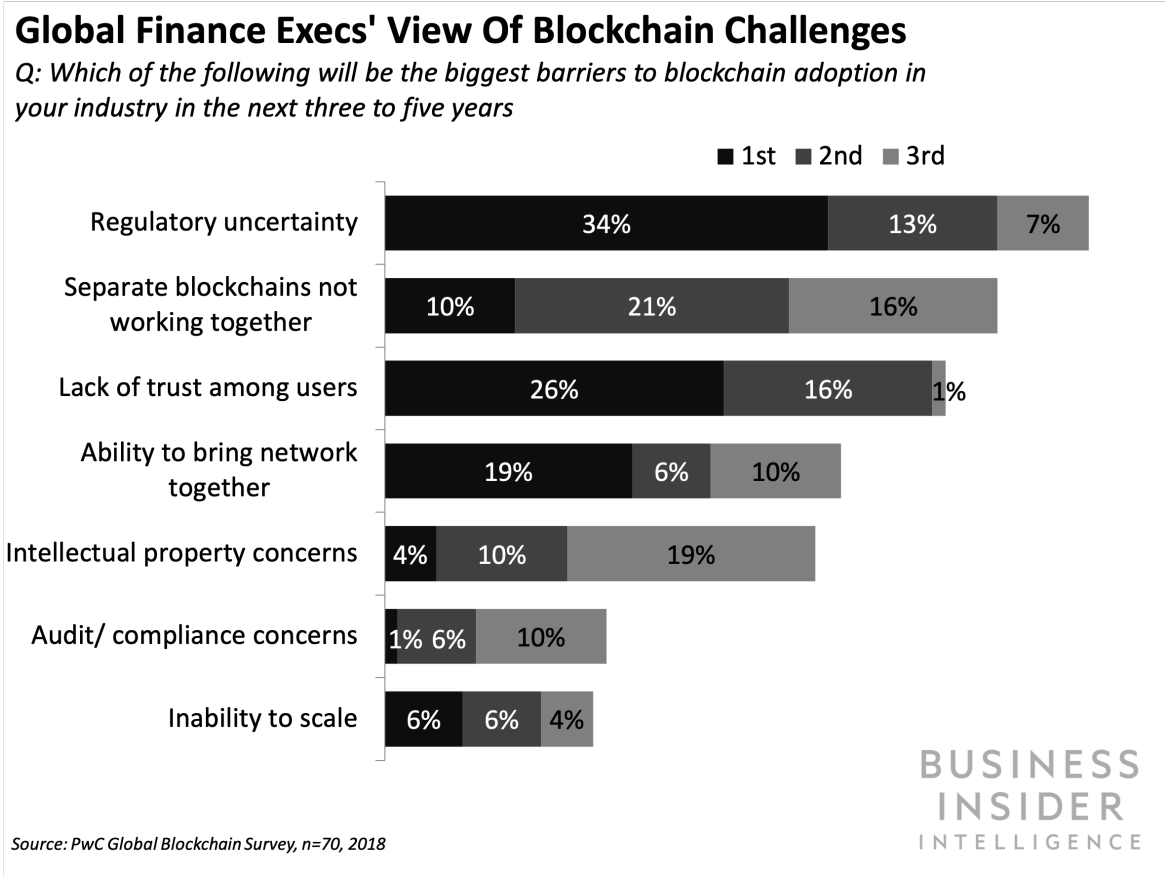
what do people want?

- People still tend to use centralized systems even in systems that's meant to/could be decentralized
  - Crypto exchanges such as Mt. Gox, Coinbase,…
    - no need to remember/store your own private key
    - ease of password reset
    - faster payment system

Regulation

Optimists vs. Skeptics

- Different definitions & perspectives of "cryptocurrency"
  - In the US, Dept. of Treasury, SEC, FTC, IRS, FinCEN
- Lots of "grey area"
  - Is Bitcoin an asset, commodity, or currency?
- KYC (Know Your Customer) and AML (Anti-Money Laundering)
- Facebook's Libra questioned by U.S. Senate



TIBA

Technical Challenge

Measure what Matters

- Speed/Efficiency
  - Bitcoin: 7~10 transactions/second
  - Ethereum: ~20 transactions/second
  - Visa: ~24,000 transactions/second
- Energy Consumption
  - PoW uses significant energy resources
- Things that require low latency or high volumes will be better served by centralized database systems

Source: https://voxeu.org/content/impact-blockchain-technology-finance-catalyst-change

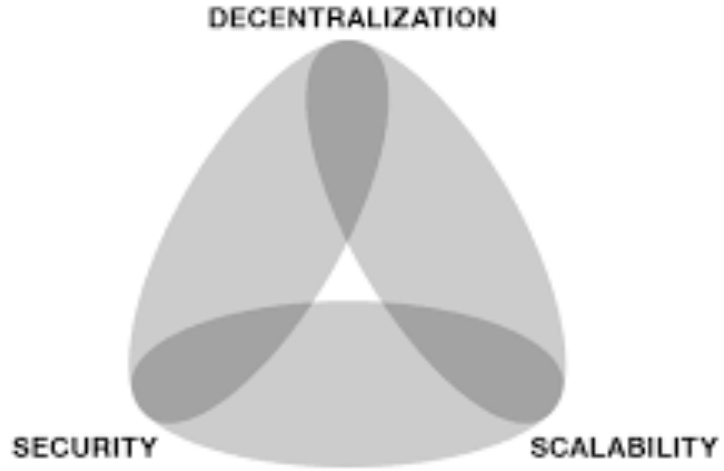
Source: https://howmuch.net/articles/crypto-transaction-speeds-compared

TIBA

Scalability Trilemma

Two out of Three

- Described by Ethereum's Vitalik Buterinan
- For Blockchain systems:
  - Security, Decentralization, Scalability
    - Pick two of the three properties
    - Or pick one side of the triangle
- Some people disagree and think we can achieve all three



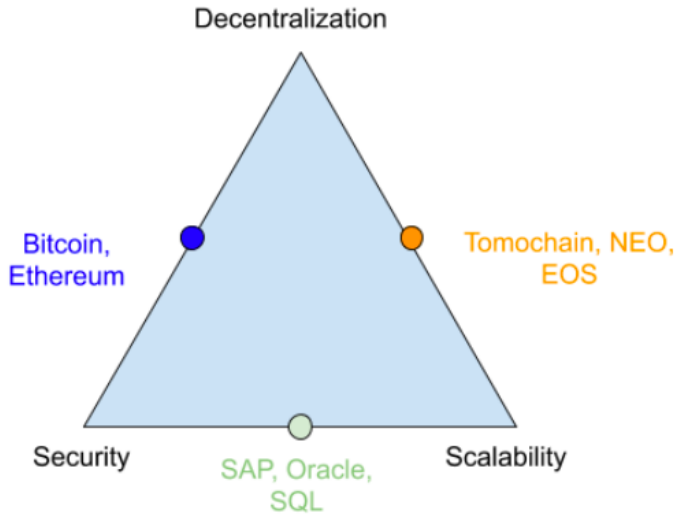
Source: https://steemit.com/ethereum/@icodog/eos-vs-ethereum-where-do-they-differ; Reading: https://thecontrol.co/on-the-scalability-of-blockchains-ec76ed769405

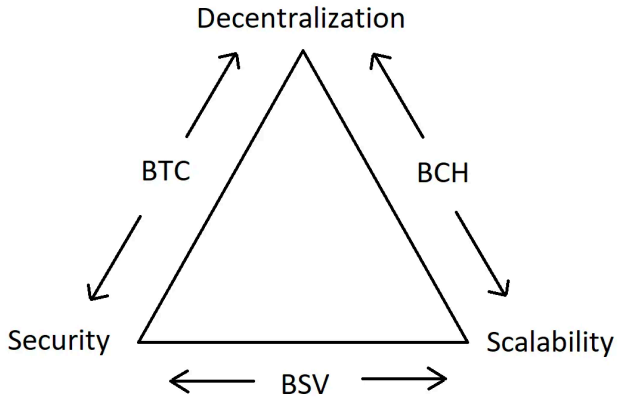
TIBA

Scalability Trilemma

Two out of Three

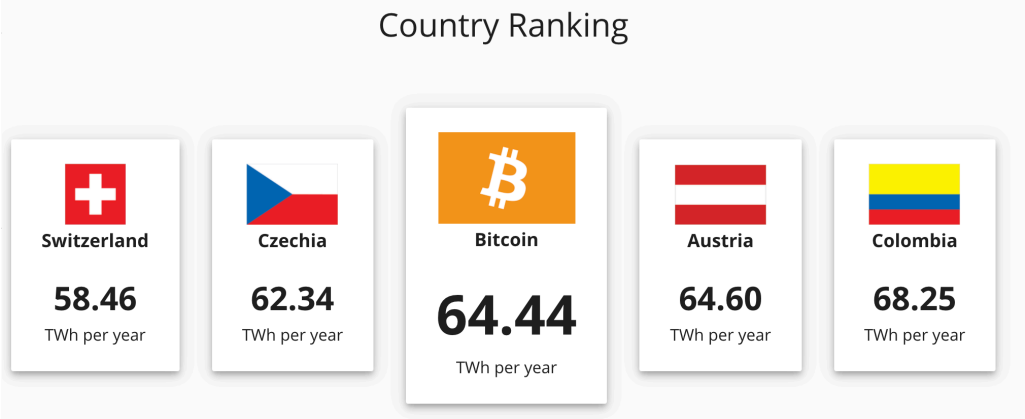
- **Decentralization:** defined as the system being able to run in a scenario where each participant only has access to O(c) resources, ie. a regular laptop or small VPS
- **Scalability:** defined as being able to process O(n) > O(c) transactions
- **Security:** defined as being secure against attackers with up to O(n) resources





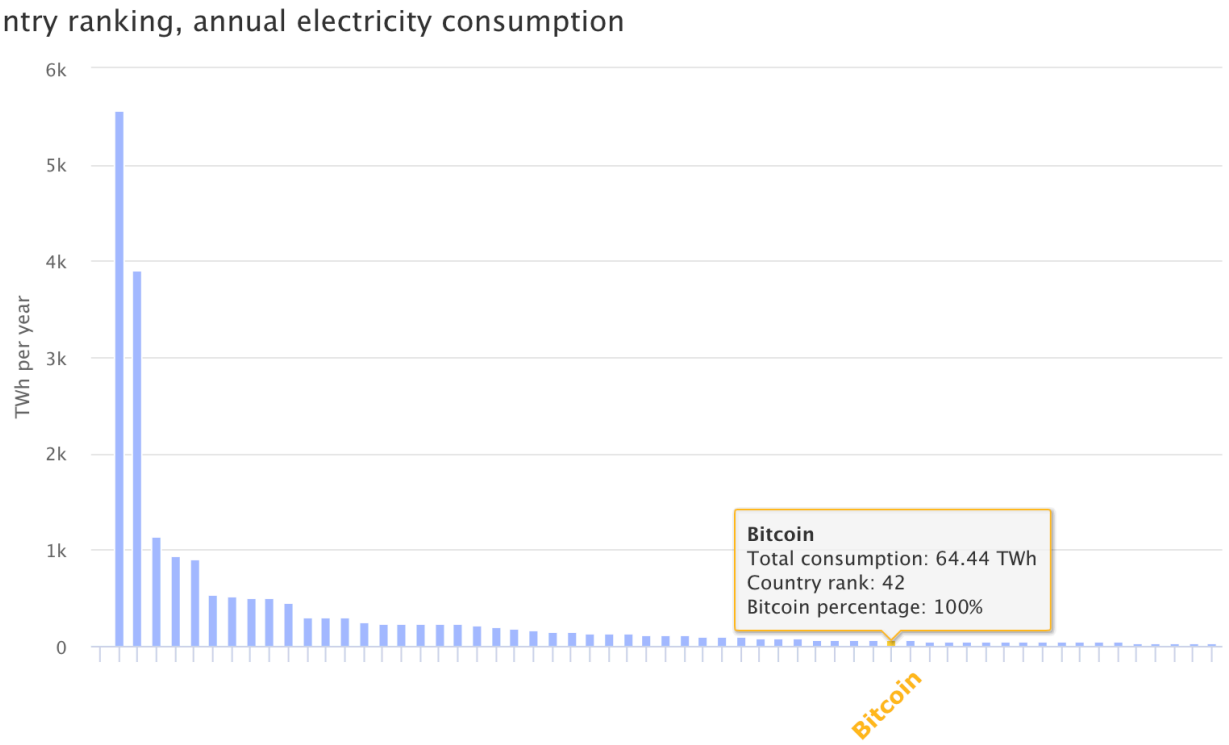
Source: https://www.bitorb.com/campus/what-is-the-scalability-trilemma/; https://eatsleepcrypto.com/the-bitcoin-trilemma/

Environment – Proof of Work



The amount of electricity used annually by the Bitcoin network could **satisfy the energy needs** of the University of Cambridge for ...

168 years



Source: Cambridge Bitcoin Electricity Consumption Index, https://www.cbeci.org/

TIBA

Solutions

Potential Solutions

Solutions

- Scalability
  - ‘Layer 2’
  - Permissioned blockchain
- Environment
  - Alternative Consensus Protocols
- Disagreement
  - Forks

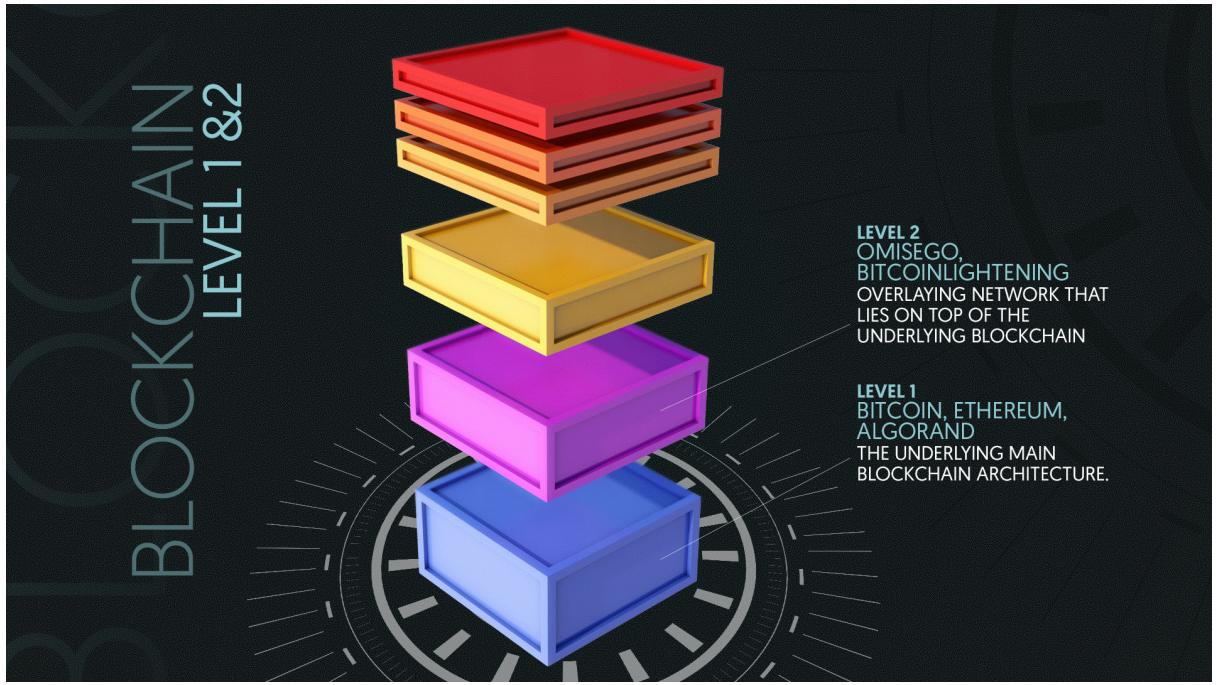
Source: https://voxeu.org/content/impact-blockchain-technology-finance-catalyst-change; Reading: https://dci.mit.edu/lightning-network

TIBA

Scalability Solution - Layer 2

Solutions

- ‘Layer 2’ (aka Sidechain)
  - Shifting small transactions to a cryptographically secure ‘off-chain’ and untimely settle ‘on-chain’
  - Bitcoin Lightning Network, Ethereum Plasma and Casper



Img: https://medium.com/the-capital/layer-1-vs-layer-2-what-you-need-to-know-about-different-blockchain-layer-solutions-69f91904ce40;

TIBA

Scalability Solution - Enterprise Blockchain

Centralized + Decentralized ?

- Distributed Ledger Technology (DLT)
- Permissioned Blockchain
  - Operates based on private members
  - Types:
    - Federated/Consortium blockchains
    - Private blockchains

TIBA

Permissionless vs. Permissioned

Types of Blockchain

- **Permissionless**: where anyone can join and have full rights to use the blockchain
  - Bitcoin, Ethereum, …
- **Permissioned**: a person needs to meet certain requirements to perform certain actions on the blockchain
  - pre-verified users who have already proven they are who they say they are
  - Or allow anyone to join, but only let trusted identities verify transactions on the blockchain

Source: http://intersoftkk.com/industries/blockchain-solutions/

TIBA

Permissioned Blockchain

Types of Permissioned Blockchain

- **Private**: Allows one party to have full control and they will select a few nodes that are predetermined
- **Federated/Consortium**: Provides many of the same benefits of the private blockchain (efficiency and transaction privacy, etc), without consolidating power with only one party

Source & Reading: https://medium.com/blockchain-strategy-and-use-cases/public-private-and-consortium-blockchains-whats-the-best-flavour-7728834a4b1c

Types of Blockchain

	Blockchain type		
	Public	**Private**	**Consortium**
Permissionless?	Yes	No	No
Who can read?	Anyone	Invited users only	Depends
Who can write?	Anyone	Approved participants	Approved participants
Ownership	Nobody	Single entity	Multiple entities
Participants known?	No	Yes	Yes
Transaction speed	Slow	Fast	Fast

Source & Reading: https://academy.binance.com/blockchain/private-public-and-consortium-blockchains-whats-the-difference#consortium-blockchains

Environment Solution – Alternative Consensus Protocols

- Proof of Stake (PoS)
  - validators pledge coins in exchange for a chance of creating new block
- Proof of Burn ("PoW that doesn't consume energy")
  - miner "burns" or "destroys" coins, which enables them to "mine" and verify transactions
- Proof of Capacity
  - similar to PoW, but uses storage instead of computation
- Proof of Elapsed Time
  - given a random amount of time to wait, the first person to be done waiting gets to determine the next block
- …and many others

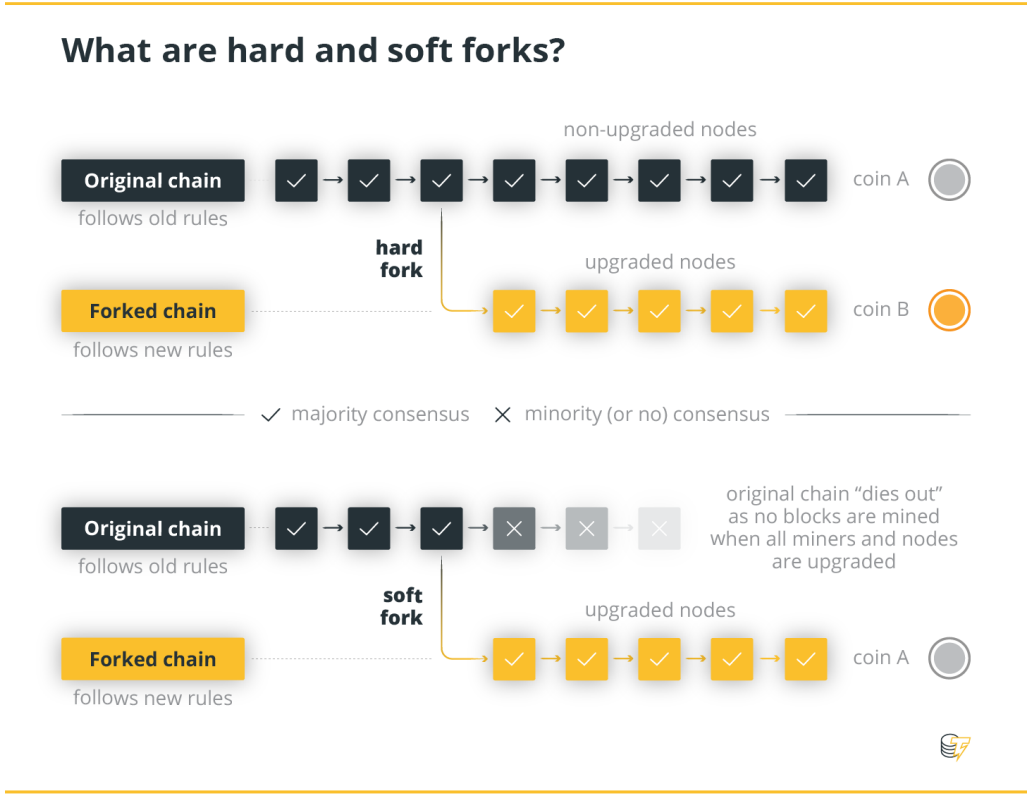
Source: https://hackernoon.com/alternative-blockchain-consensus-mechanisms-40c1509af39e

TIBA

Disagreement Resolution: Forks

Going Separate Paths

- **Fork** - "what happens when a blockchain diverges into two potential paths forward" or "a change in protocol"
- Two types:
  - Hard Fork
  - Soft Fork



Source: https://cointelegraph.com/news/can-crypto-exchanges-be-trusted-with-hard-forks; https://en.wikipedia.org/wiki/Fork_(blockchain);

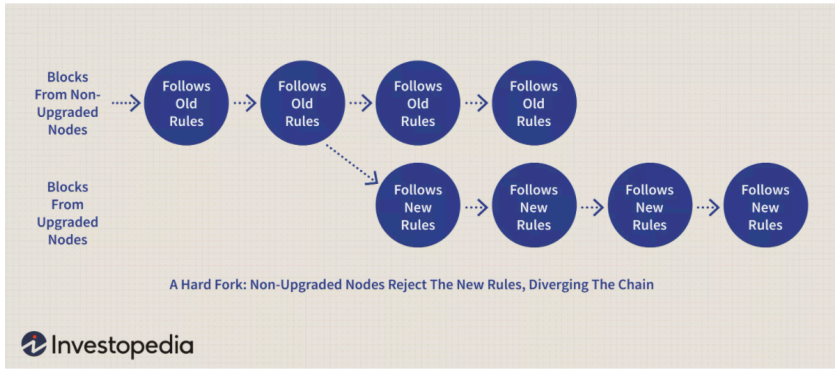
Disagreement Resolution: Forks

Going Separate Paths

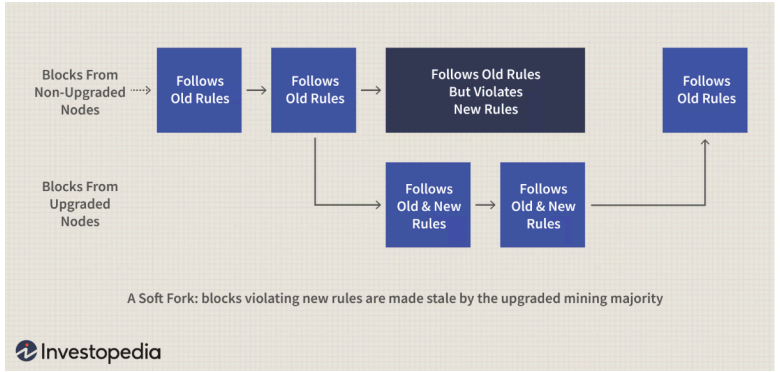
- **Hard Fork: backward-incompatible software updates**
  - upgraded nodes can only communicate with others that operate the upgraded version

- **Soft Fork: backward-compatible software upgrade**
  - upgraded nodes can still communicate with the non-upgraded ones

Hard Fork



Soft Fork



Source: https://academy.binance.com/en/articles/hard-forks-and-soft-forks; https://www.investopedia.com/terms/s/soft-fork.asp; https://www.investopedia.com/terms/h/hard-fork.asp;

TIBA

Vulnerabilities

TIBA

Attacking Blockchain

Hacking the "Immutable"

- Peer-to-Peer Network-based Attacks
  - Eclipse attack
  - Sybil attack
- Smart Contract-based Attacks
  - The DAO attack
- Wallet-based/Identity Attack
  - Parity Multi-sig Wallet attack
  - Dusting attack
- Consensus Mechanism and Mining-based Attacks
  - Selfish mining attack
  - Mining malware
  - 51% attack
  - Timejack attack
  - Finney attack
  - Race attack

Source: https://blogs.arubanetworks.com/solutions/10-blockchain-and-new-age-security-attacks-you-should-know/

TIBA

Attacking Blockchain

Hacking the "Immutable"

- Eclipse attack - aims to obscure a participant's view of the peer-to-peer network
- Sybil attack - flood the network with fake peers
- Selfish mining attack (aka block withholding attack) - miner or mining pool attempts to withhold a successfully validated block from being broadcast to the rest of the network
- Mining malware – malware on computers that are mining
- 51% attack – majority dishonest nodes controlling the network
- Timejack attack – eclipse attack and provide false timestamp information
- Finney attack – double spend by keeping transactions in stealth and mining a block
- Race attack – submit multiple transactions with the same coin at once
- The DAO attack - exploit smart contract bug
- Parity Multi-sig Wallet attack – exploit smart contract bug
- Dusting attack - hackers try to break the privacy of cryptocurrency users by sending tiny amounts of coins to their wallets

Source: https://blogs.arubanetworks.com/solutions/10-blockchain-and-new-age-security-attacks-you-should-know/

TIBA

PoW's 51% Attack

When does Decentralized become Centralized?

- PoW assumes a majority of honest nodes
  - (majority >= 51 % of hashing power)
- **51% Attack** – malicious node(s) (miner or mining pool) control more than 50% of the hashing power
  - 51% hashing power = always outpace the rest in terms of creating blocks

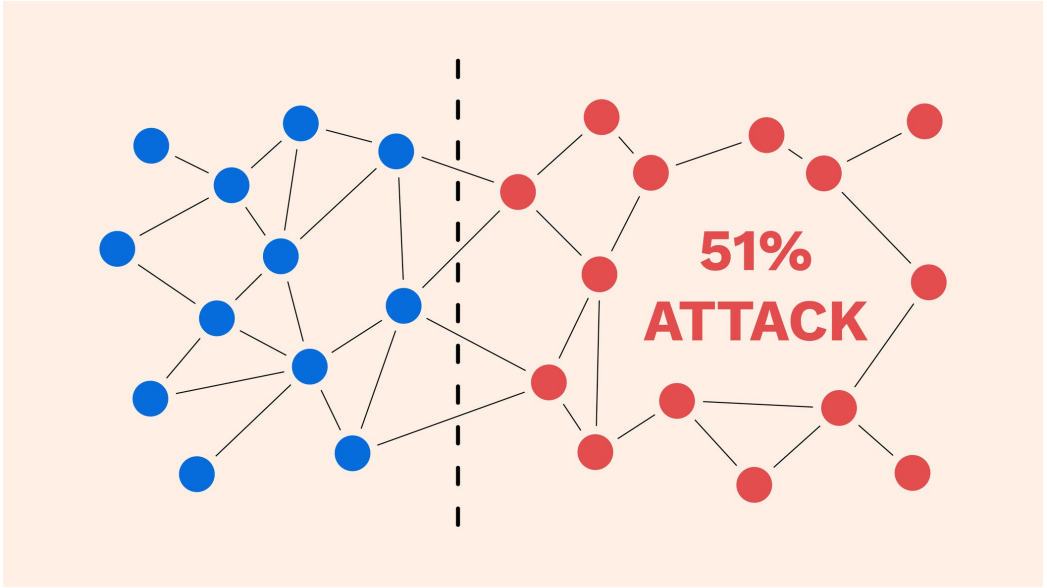


Image: https://www.bitpanda.com/academy/en/lessons/what-is-a-51-attack-and-how-is-it-prevented/;

Bitcoin Mining Map

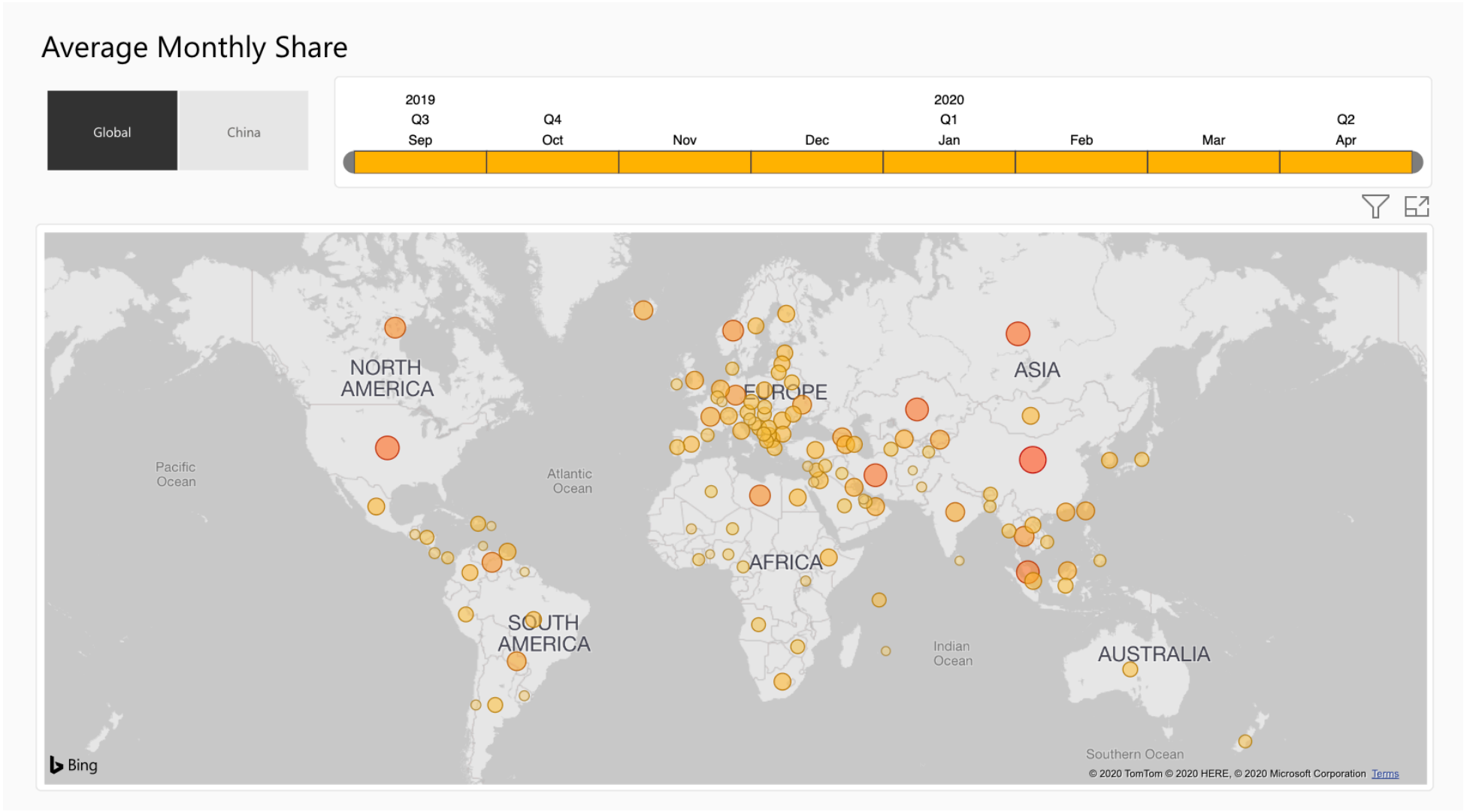


Image: University of Cambridge, https://www.cbeci.org/mining_map

TIBA Average monthly hashrate breakdown by country

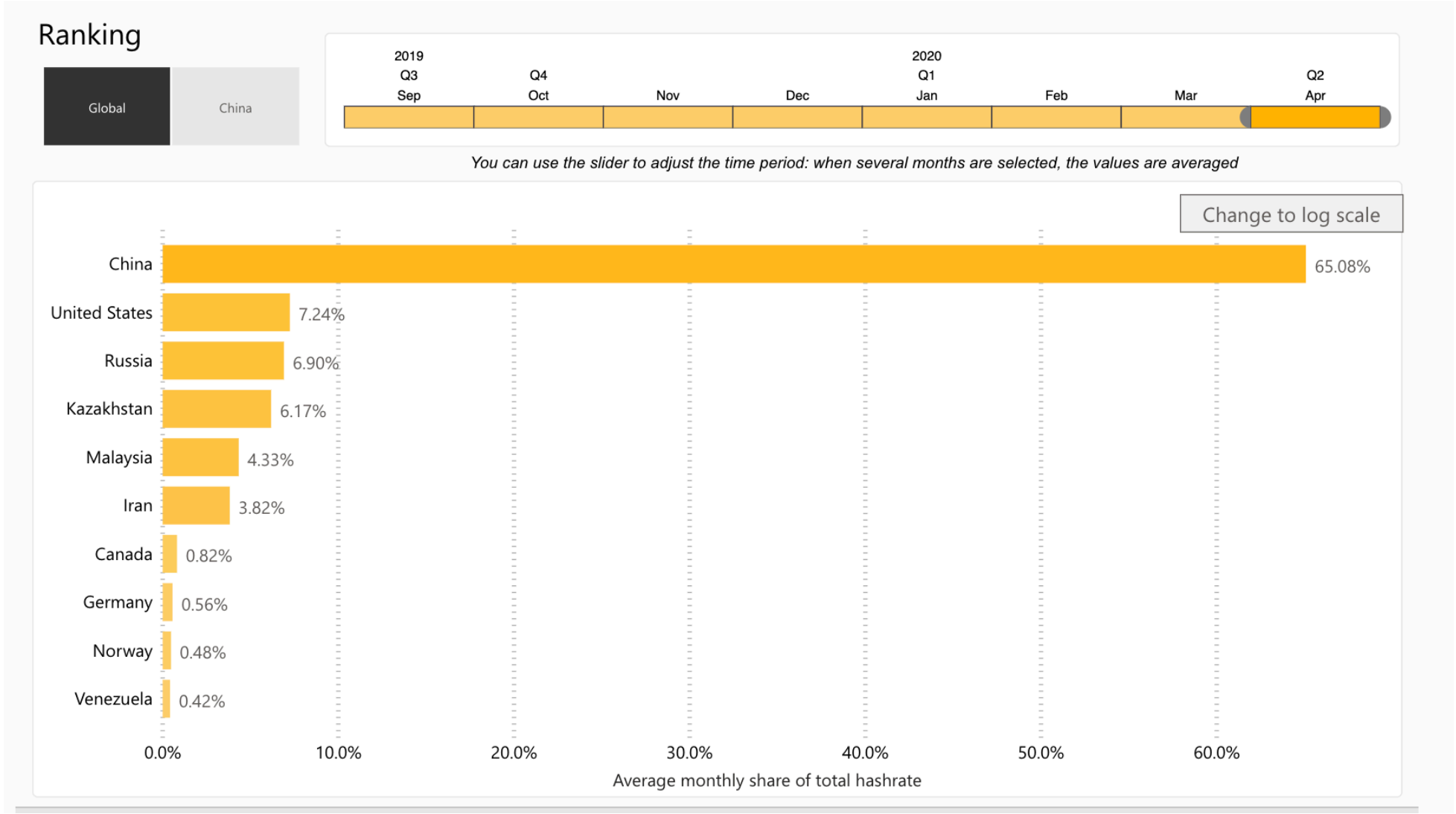


Image: University of Cambridge, https://www.cbeci.org/mining_map

TIBA

PoW's 51% Attack

When does Decentralized become Centralized?

- A miner employing a 51% attack can:
  - Double spend their coins
  - Prevent transactions from being confirmed

- A miner employing a 51% attack can **NOT**:
  - Reverse confirmed transactions.
  - Create false transactions (that never occurred)
  - Steal funds from a certain address
  - Create new coins without mining

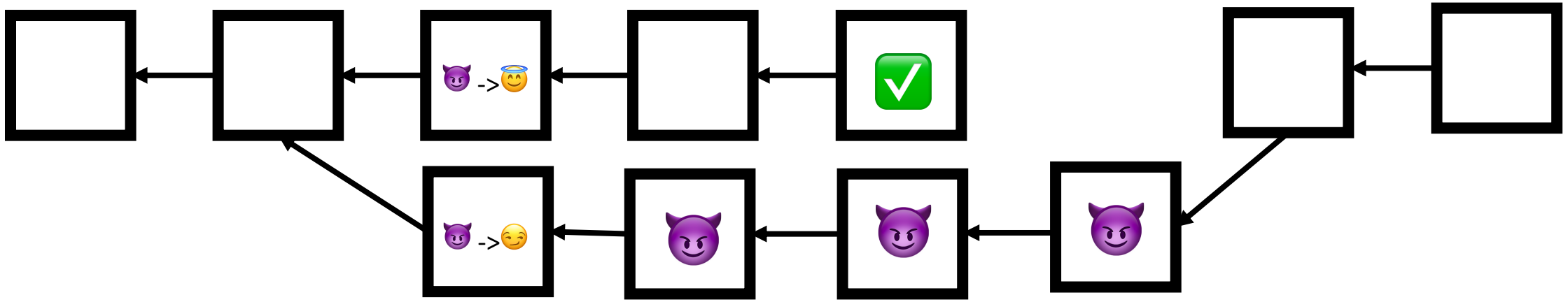
Source: From 51% Attack Explained Simply + Real Life Example (2020 Updated); https://99bitcoins.com/51-percent-attack/

TIBA

PoW's 51% Attack – Double Spend

When does Decentralized become Centralized?

😈 wants to use the same coin to buy from 😇 and 😏

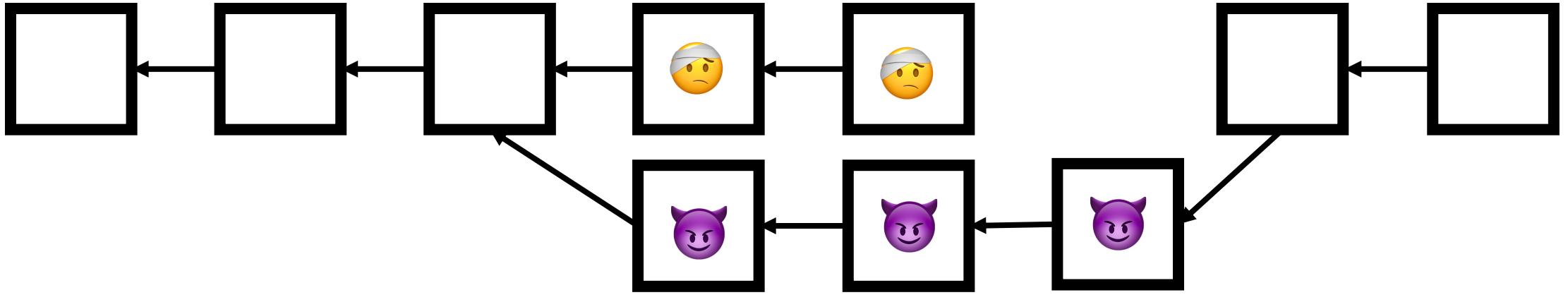


TIBA

PoW's 51% Attack – Blocking Transactions

When does Decentralized become Centralized?

😈 wants to blacklist 🤕



TIBA

Questions?

TIBA

Homework Assignments

- Medium, On the Scalability of Blockchains
- Business Insider, How the laws & regulations affecting blockchain technology and cryptocurrencies, like Bitcoin, can impact its adoption
- Harvard Business Review, The Truth About Blockchain
- Forbes, The Tipping Point For Mass Blockchain Adoption
- Hard Forks and Soft Forks Explained
- Cambridge Bitcoin Electricity Consumption Index & Mining Map
- MIT Media Lab, 51% attacks

TIBA

Blockchain Limitations and Vulnerabilities by Samuel Tang

Thank you for listening!
See you next week!