How to Master the Energy Impact of Blockchain?

Prof. Dr. Hans P. Reiser
Christian Berger

University of Passau

UNIVERSITÄT PASSAU

BBC | Sign in | Home | News | Sport | Reel | Worklife

NEWS

Home | Coronavirus | Video | World | UK | Business | Tech | Science | Stories | Entertai

Tech

Bitcoin Mining Council to report renewable energy usage

1 day ago

A new Bitcoin Mining Council has been created to improve the crypto-currency's sustainability, following a meeting of "leading" Bitcoin miners and Elon Musk.

The Tesla CEO tweeted the development was "potentially promising".

It's hoped the council will "promote energy usage transparency" and encourage miners to use renewable sources.

The process of creating Bitcoin consumes large amounts of electricity.

Its value fell earlier this month after Tesla withdrew its support of the crypto-currency, **citing environmental concerns.**

News source:
https://www.bbc.com/news/technology-57240090

CNBC | MARKETS | BUSINESS | INVESTING | TECH | POLITICS | CNBC TV | WATCHLIST

TECH

Elon Musk says Tesla will stop accepting bitcoin for car purchases, citing environmental concerns

PUBLISHED WED, MAY 12 2021·6:20 PM EDT | UPDATED WED, MAY 12 2021·8:26 PM EDT

Lora Kolodny
@LORAKOLODNY

KEY POINTS

- Tesla has "suspended vehicle purchases using bitcoin," out of concern over "rapidly increasing use of fossil fuels for bitcoin mining," according to a tweet from CEO Elon Musk on Wednesday.

News source:
https://www.cnbc.com/2021/05/12/elon-musk-says-tesla-will-stop-accepting-bitcoin-for-car-purchases.html

Could Ethereum Run On Just 0.05% Of It's Current Electricity Levels?! A Potential GAME CHANGER....

Silicon Valley Newsroom 3:30 PM No Comments

Ethereum developer Carl Beekhuizer says *'Ethereum's power-hungry days are numbered'* and explores the energy usage difference that will be seen when Ethereum makes the switch to proof-of-stake(PoS). This replaces the current network's validation method known as proof-of-work (PoW, aka traditional 'mining') and will allow the platform to run on just 0.05% of it's current power usage level, claims Beekuizer.

According to Digiconomist miners currently consume 44.49 TWh per year, and Beekuizer says that could go as low as 0.02 THw by changing to PoS.

News source:
https://www.globalcryptopress.com/2021/05/could-ethereum-run-off-just-005-of-its.html

NEWS PLAN YOUR VACCINE COVID-19 POLITICS U.S. NEWS WATCH NOW

TECH NEWS

Cryptocurrency goes green: Could 'proof of stake' offer a solution to energy concerns?

Bitcoin relies on many computers to crunch difficult math problems. But it doesn't have to.

Mining rigs mine the Ethereum and Zilliqa cryptocurrencies at the Evobits crypto farm in Cluj-Napoca, Romania, on Jan. 22, 2021. Akos Stiller / Bloomberg via Getty Images

May 25, 2021, 6:56 PM CEST / Updated May 25, 2021, 6:58 PM CEST

By Ezra Kaplan

At any particular moment, thousands of computers around the world are humming away, crunching complex math problems that create and sustain bitcoin.

This network gives bitcoin its appeal: decentralized, always on and easily tradeable. But it also means the network is constantly using energy – a sticking point for many of the cryptocurrency's skeptics and critics. And it's not just a bitcoin problem. Other cryptocurrencies and blockchains including Ethereum have similar challenges.

The debate about bitcoin's environmental impact was elevated earlier this month when Tesla CEO Elon Musk, once one of the most notable bitcoin boosters, said his company would no longer accept it for the purchase of vehicles. He cited the use of fossil fuels for bitcoin mining as a reason.

News source:
https://www.nbcnews.com/tech/tech-news/cryptocurrency-goes-green-proof-stake-offer-solution-energy-concerns-rcna1030

Outline of this talk

- **Blockchain basics**
- **Proof-of-work “Nakamoto consensus”**
  - How does it work
  - Energy impact & sustainability
  - Novel PoW variants with less energy consumption
- **Byzantine fault-tolerant (BFT) consensus**
  - The general idea, proof-of-stake blockchains
  - Energy consumption, performance and scalability
  - Selected examples, Algorand and Avalanche
- **Blockchain research at University of Passau**
  - BFT2Chain and AWARE

What is a blockchain? (1)

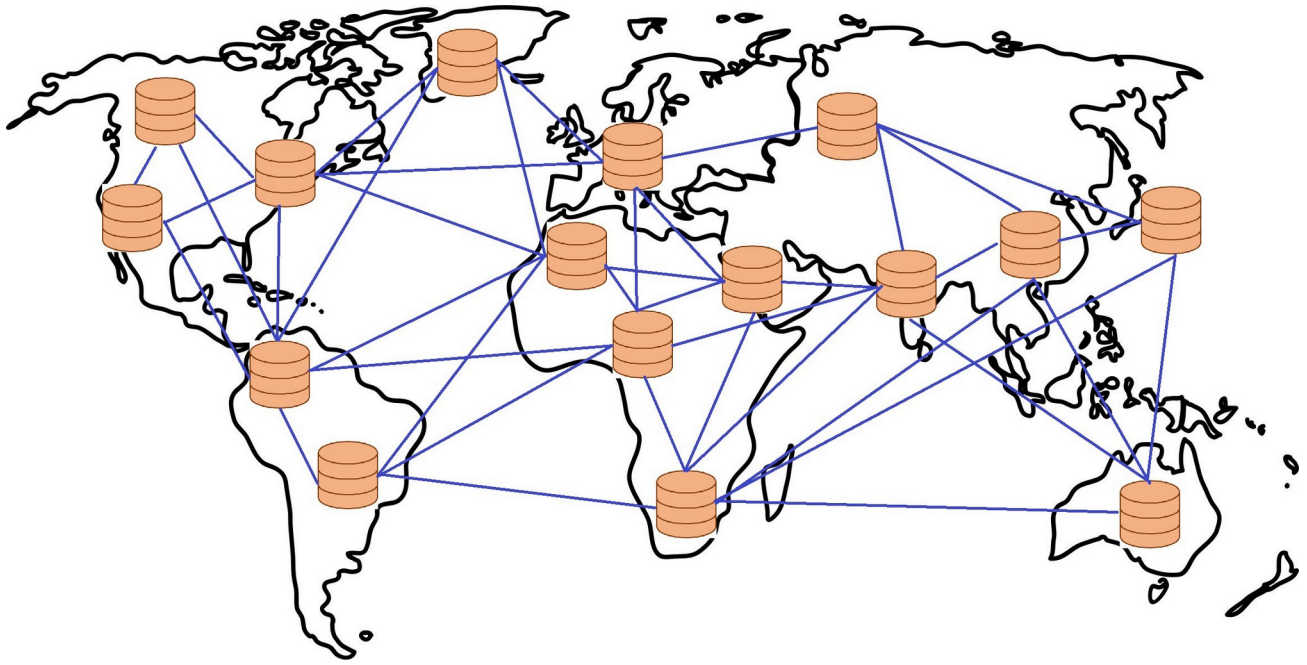
- **A distributed system that manages an**
  - append-only,
  - totally-ordered log
  - of immutable transactions (= the ledger)

  in a “replicated fashion”

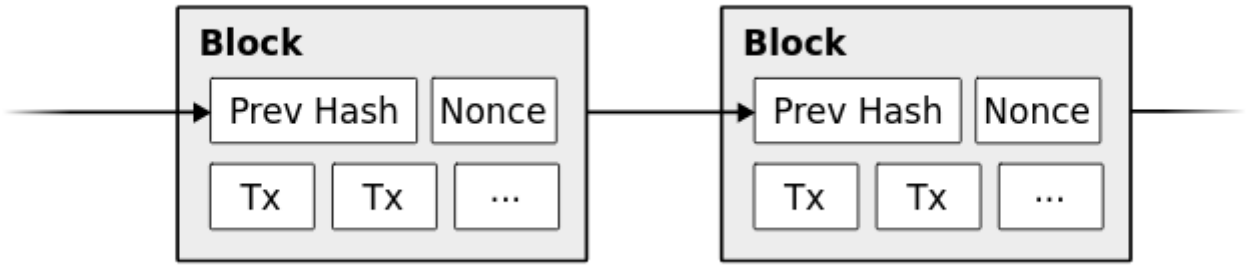
  what does that mean?

What is a blockchain? (2)

- **Several nodes**
  - hold a *consistent* copy of the ledger
  - are involved in *validating transactions*



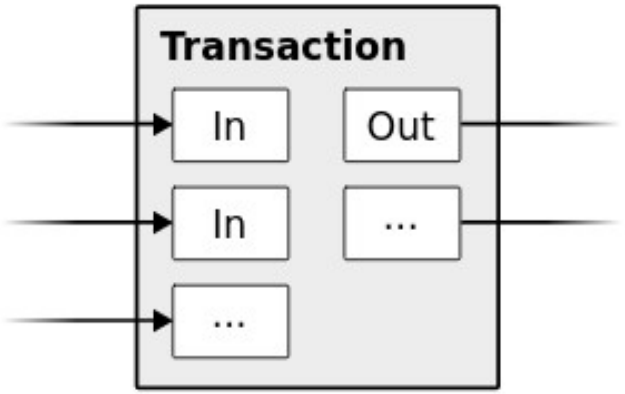
What is a blockchain? (3)



- **To order transactions,**
  - transactions are grouped into *blocks,*
  - blocks are *chained* by each block referencing the *hash* of the previous block,
  - a *consensus* primitive is employed to decide:

    ”which block should be appended next?”

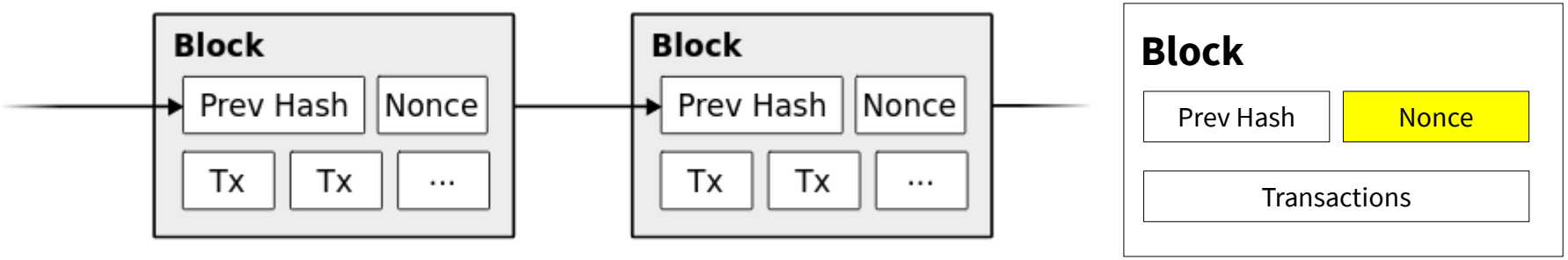
Bitcoin transaction model



- **A *transaction* can combine or split value**
  - Inputs: reference *Unspent Transaction Outputs* (UTXO)
  - Outputs: create new UTXOs
    - A receiver needs to be specified
    - Change can be returned to the sender in a second output
    - Unspecified coins can be rewarded to the miner as *transaction fee*
      - Mining fee is optional but encourages a miner to prioritize a transaction

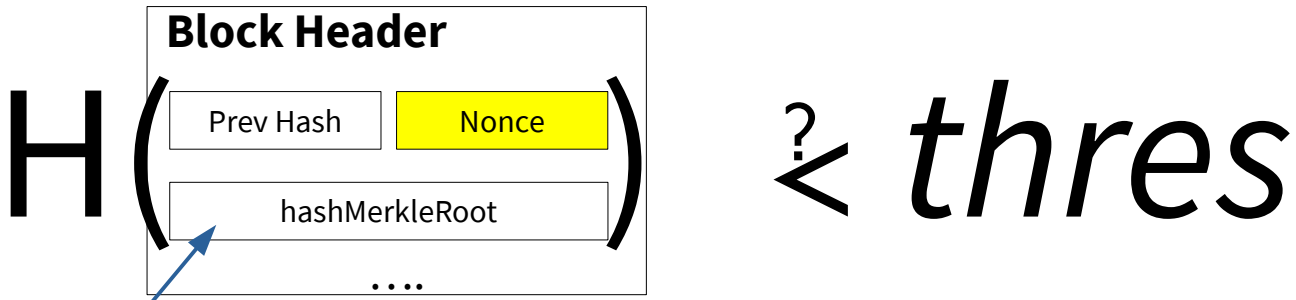
Proof of work: “Nakamoto Consensus”

- **The proof of work**
  - Miner chooses transactions (but must be valid)
    - e.g., no conflicts, such as using the same UTXO as input twice
  - Problem: finding a “fitting” nonce
  - “Found” blocks are broadcasted in the network
    - using gossip
  - Invalid blocks are rejected!



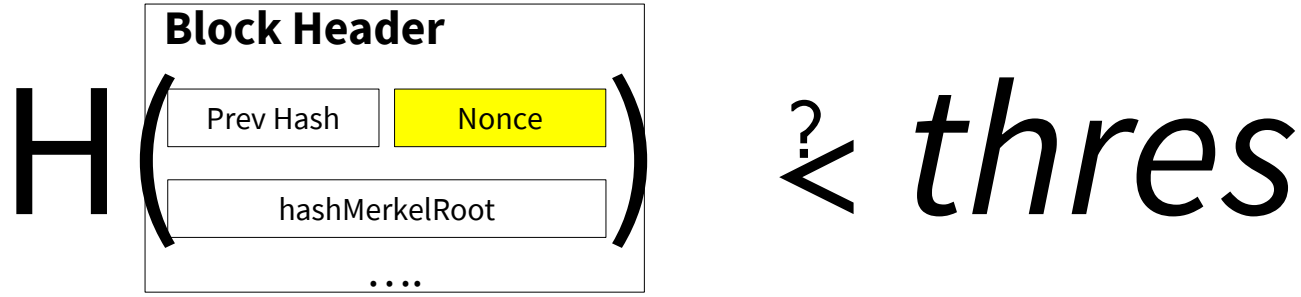
Proof of work: finding a nonce

- **Finding a nonce is hard**
  - We need to “try out” many nonces
  - We *hash* H() the block header and check:



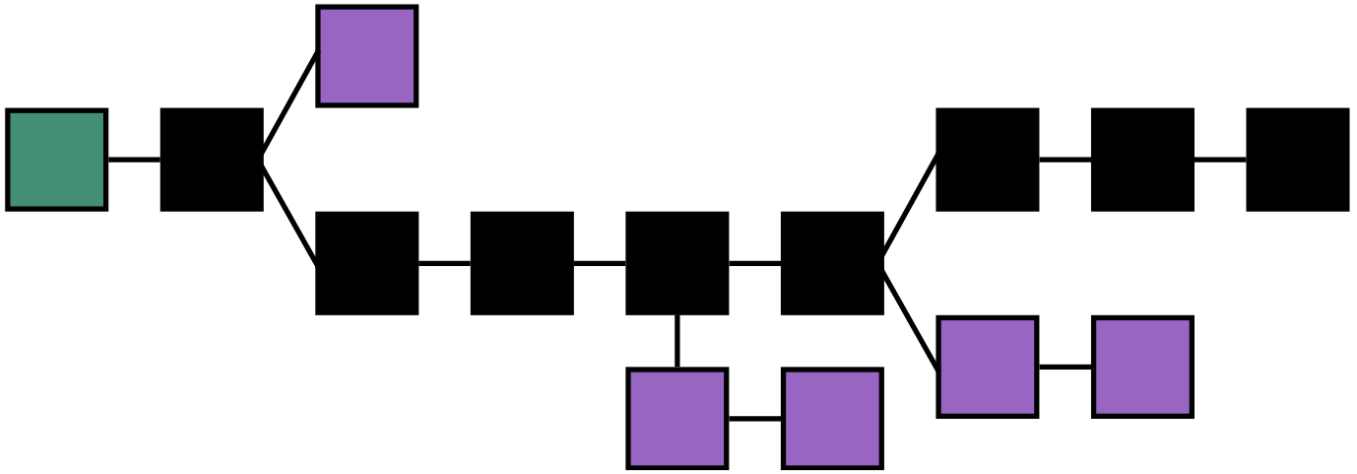
hashMerkelRoot is used instead of including *all transactions*

Proof of work: mining



- **A large number of hashes needs to be calculated**
  - Because hash functions are one-way and can not be reversed easily
- **Threshold depends on the difficulty**
  - Difficulty is regularly adjusted
    - so block generation time is *roughly* 10 minutes
    - If more computational power becomes available (because of more miners joining the network), then difficulty increases
- **Incentive: get Bitcoins for validating Txs**
  - Miner gets transaction fees + block reward

Longest chain rule



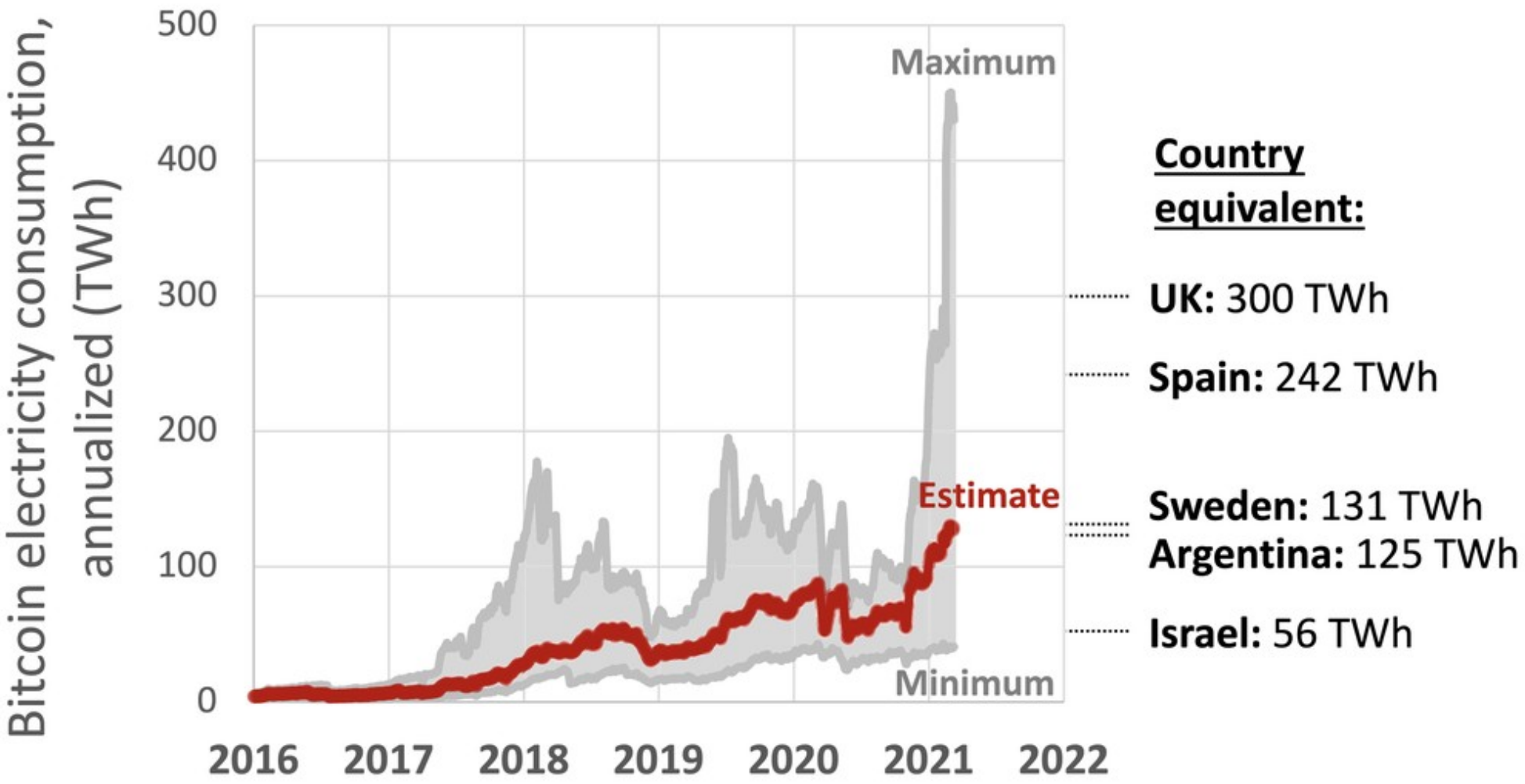
- **What happens if two miners find a solution at the same time?**
  - This can create forks of the blockchain
  - Inbuilt conflict resolution mechanisms:
    - *"Longest chain always wins"*
    - Honest miners always switch to longest chain
      - Eventually majority will work on the same chain again as some fork will grow faster

Bitcoin mining

- **Bitcoin mining is most efficient on ASICs**

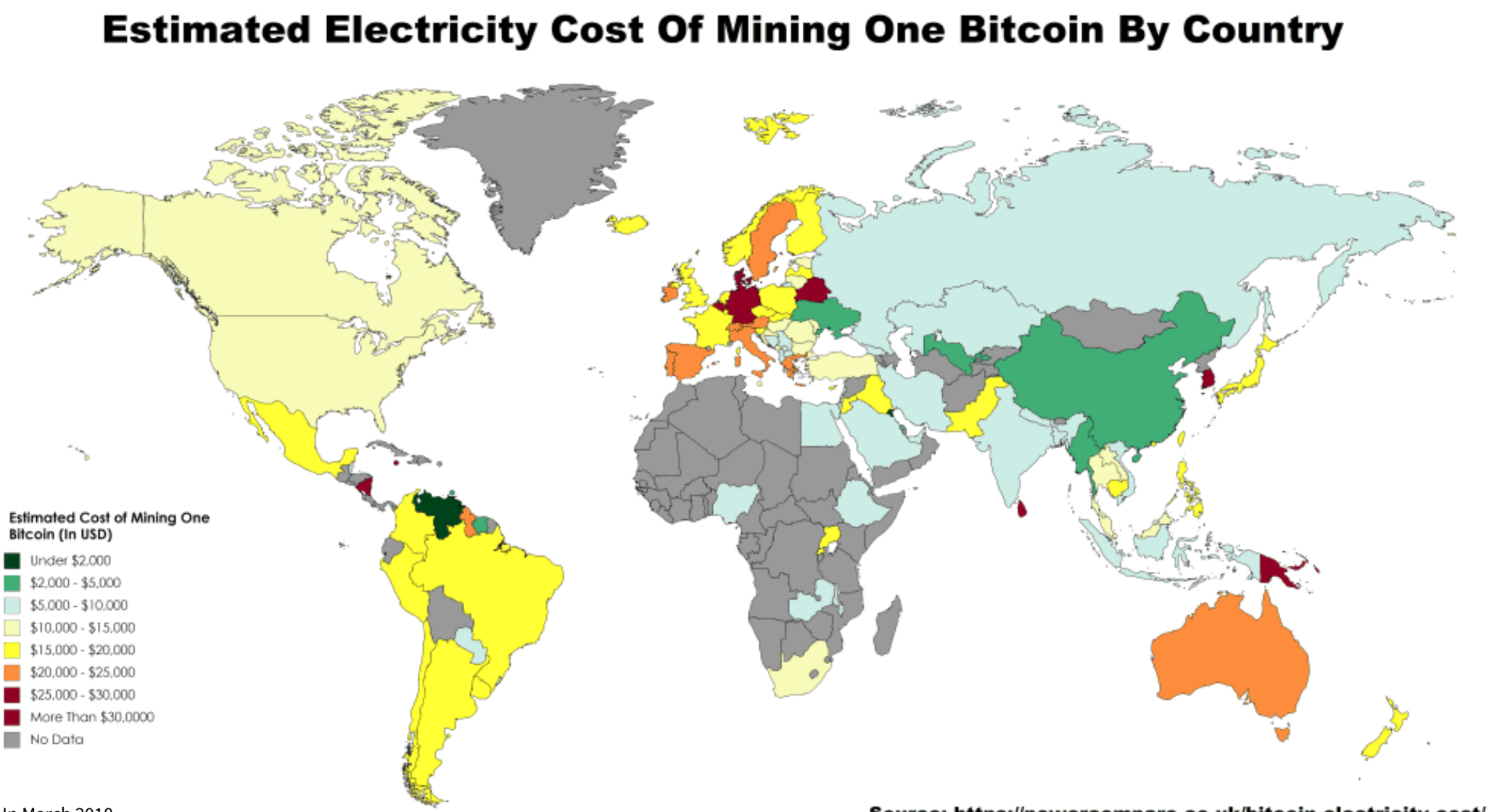
- **Bitmain Antminer S19**
  - SHA-256
  - 95 Tera hashes per second
  - Energy consumption **3250 Watt**
    - You need a cheap electricity price to become profitable
  - Costs only **9.250 €**

Bitcoin: energy impact



Source: https://cbeci.org/

Energy costs per country

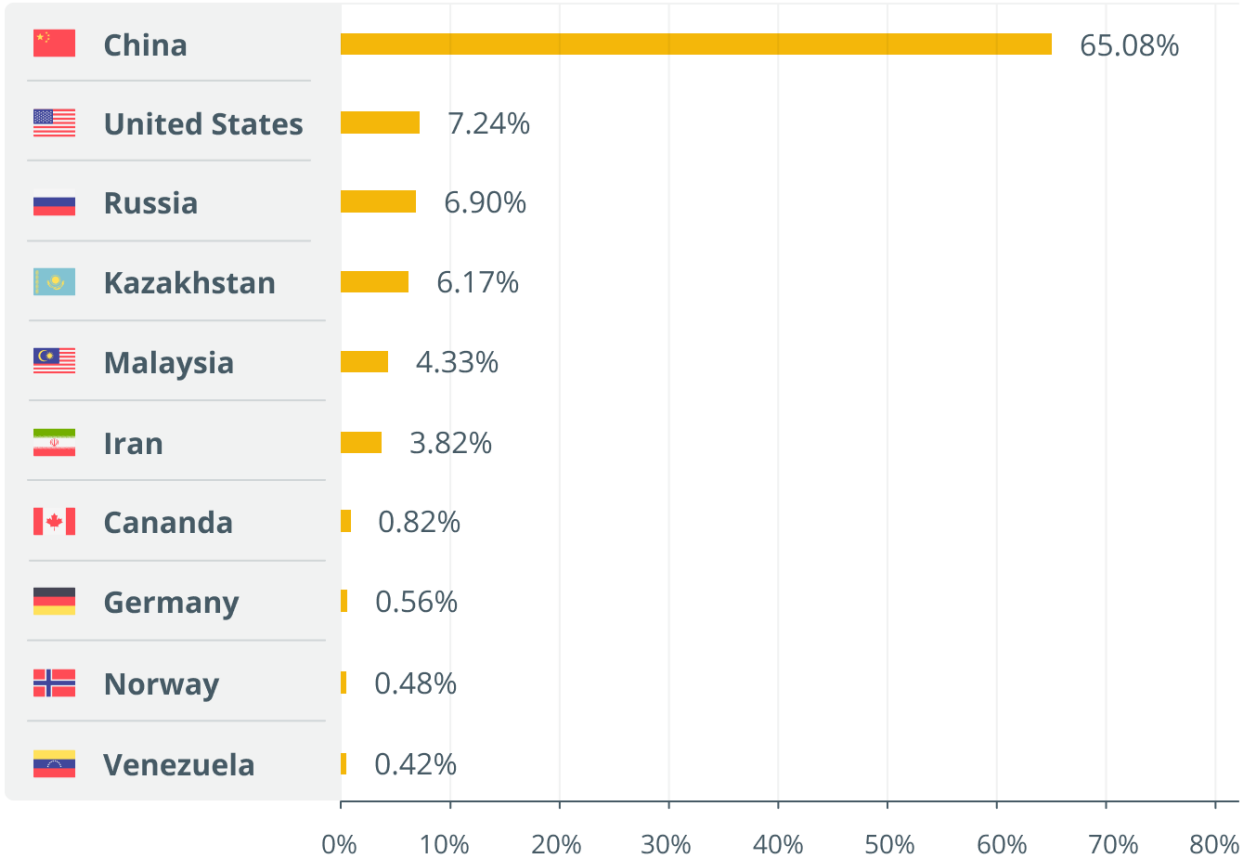


In March 2018

Source: https://powercompare.co.uk/bitcoin-electricity-cost/

Bitcoin hash rate per country

Global hash rate distribution



cointelegraph.com

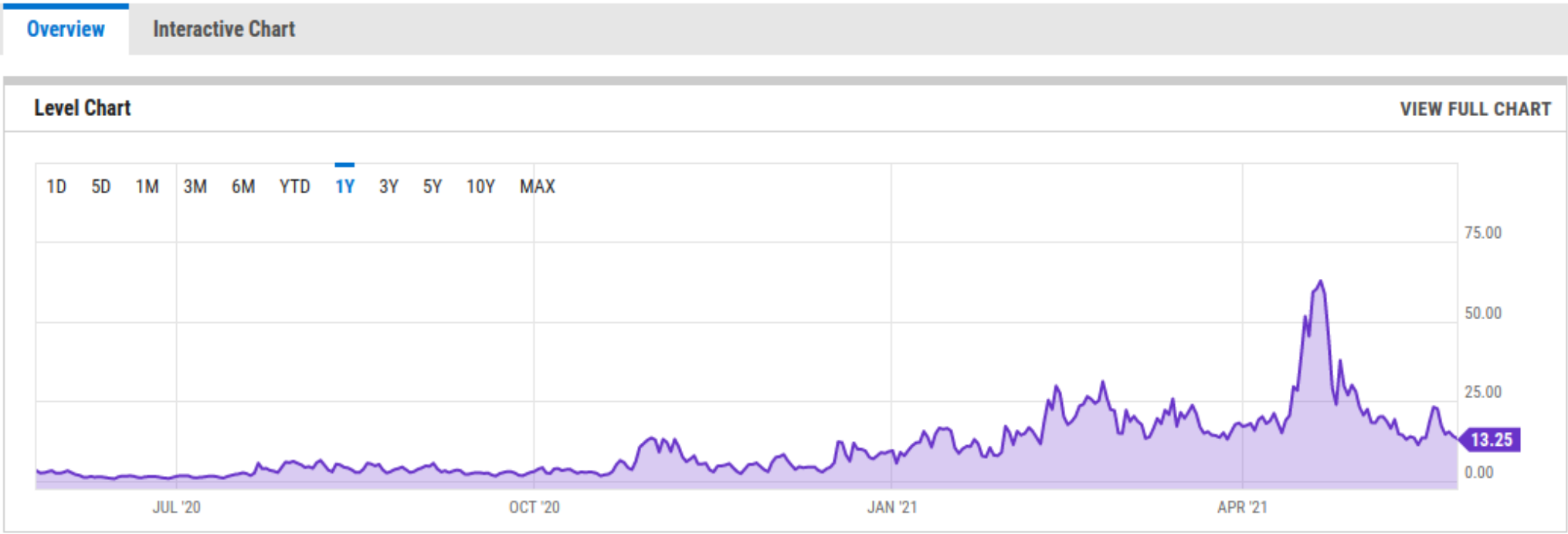
source: **Cbeci.org**

Sustainability: Bitcoin transaction CO_2

- **A single bitcoin transaction has a carbon footprint of 735 kg CO_2**
  - equivalent to the carbon footprint of 1.628.322 VISA transactions
  - Or 122.448 hours of watching YouTube
  - or driving a gasoline car ca. 3000 km

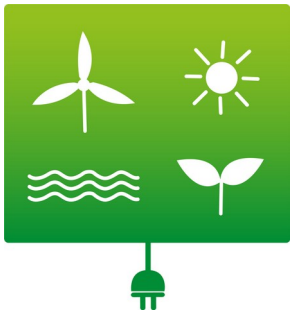
Estimated by Digiconomist (June 2021)
https://digiconomist.net/bitcoin-energy-consumption/

Bitcoin Average Transaction Fee
13.25 USD/tx for May 26 2021

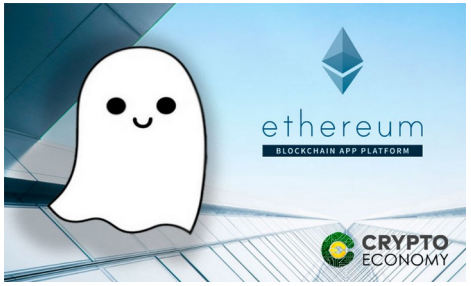


Solving the Bitcoin environmental problem?

- **Use green energy instead of coal**
  - This is currently discussed: CO_2-neutral PoW?
  - Yet, a huge energy waste still remains :(



- **Switch from proof-of-work to a different consensus method**
  - e.g., proof-of-stake, Ethereum does this now!



- **Think about less energy-demanding proof-of-work variants or alternatives**
  - The “work” should not require energy, but other “resources” than computation, like time or disk space

chia

Proof-of-ellapsed-time (PoET)

- **Work replaced**
  - with waiting for a random amount of time
- **Requires**
  - secure random number generation and attested proof of elapsed time
  - PoET program executed in trusted execution environment (Intel SGX)
- **Hyperledger Sawtooth**
  - currently provides support for PoET

Proof-of-space-and-time (Chia)

- **Proof-of-space**
  - A challenge is broadcasted in the network
  - Each “farmer” checks if they have the hash that is closest to the challenge
  - Probability of winning a a block is tied to space being available for farming
- **Proof-of-time**
  - implemented by a verifiable delay function
  - Sequential computation in which parallelisation does not yield benefits
  - A few such VDF servers are sufficient. Fastest honest server determines the speed
  - Eco-friendly as not much energy is needed

Outline of this talk

- Blockchain basics
- Proof-of-work “Nakamoto consensus”
  - How does it work
  - Energy impact & sustainability
  - Novel PoW variants with less energy consumption
- **Byzantine fault-tolerant (BFT) consensus**
  - The general idea, proof-of-stake blockchains
  - Energy consumption, performance and scalability
  - Selected examples, Algorand and Avalanche
- Blockchain research at University of Passau
  - BFT2Chain and AWARE

Byzantine fault-tolerant (BFT) consensus

- **Byzantine faults**
  - Faulty components may behave arbitrarily
    - This includes “malicious behavior”

- **Consensus**
  - is a well-studied problem in distributed systems
  - Simply put:
    - *All correct* nodes need to eventually decide on a single, identical value v and make their decision only once
    - v must have been proposed by some node initially

Byzantine fault-tolerant (BFT) consensus

- **Byzantine faults**
  - Faulty components may behave arbitrarily
    - This includes “malicious behavior”

- **Consensus**
  - is a well-studied problem in distributed systems
  - Simply put:
    - *All correct* nodes need to eventually decide (*Termination*) on a single value *v* (*Agreement*) and make their decision only once (*Integrity*)
    - *v* must have been initially proposed (*Validity*) by some node

Byzantine fault-tolerant (BFT) consensus

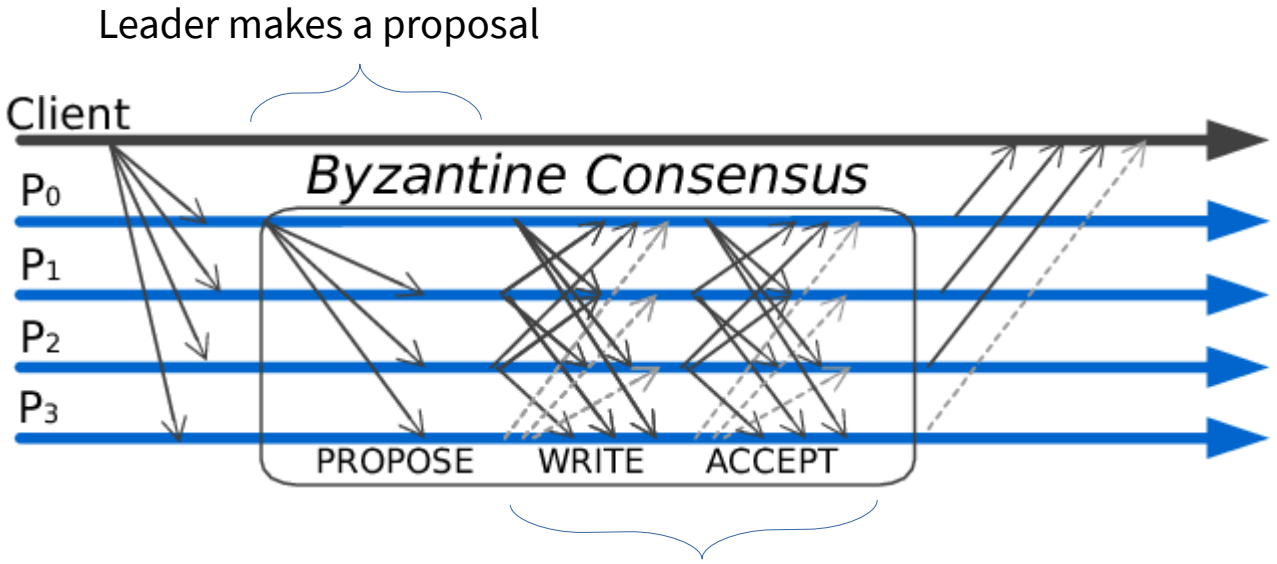
Consensus

- is a well-studied problem in distributed systems
- Simply put:
  - *All correct* nodes need to eventually decide *(Termination)* on a single value *v* *(Agreement)* and make their decision only once *(Integrity)*
  - *v* must have been initially proposed by some node *(Validity)*

<u>Discussion:</u> Does Bitcoin's proof-of-work consensus guarantee all these properties, too ?

Characteristics of BFT consensus

- **Communication based:**
  - Nodes talk to each other to solve consensus

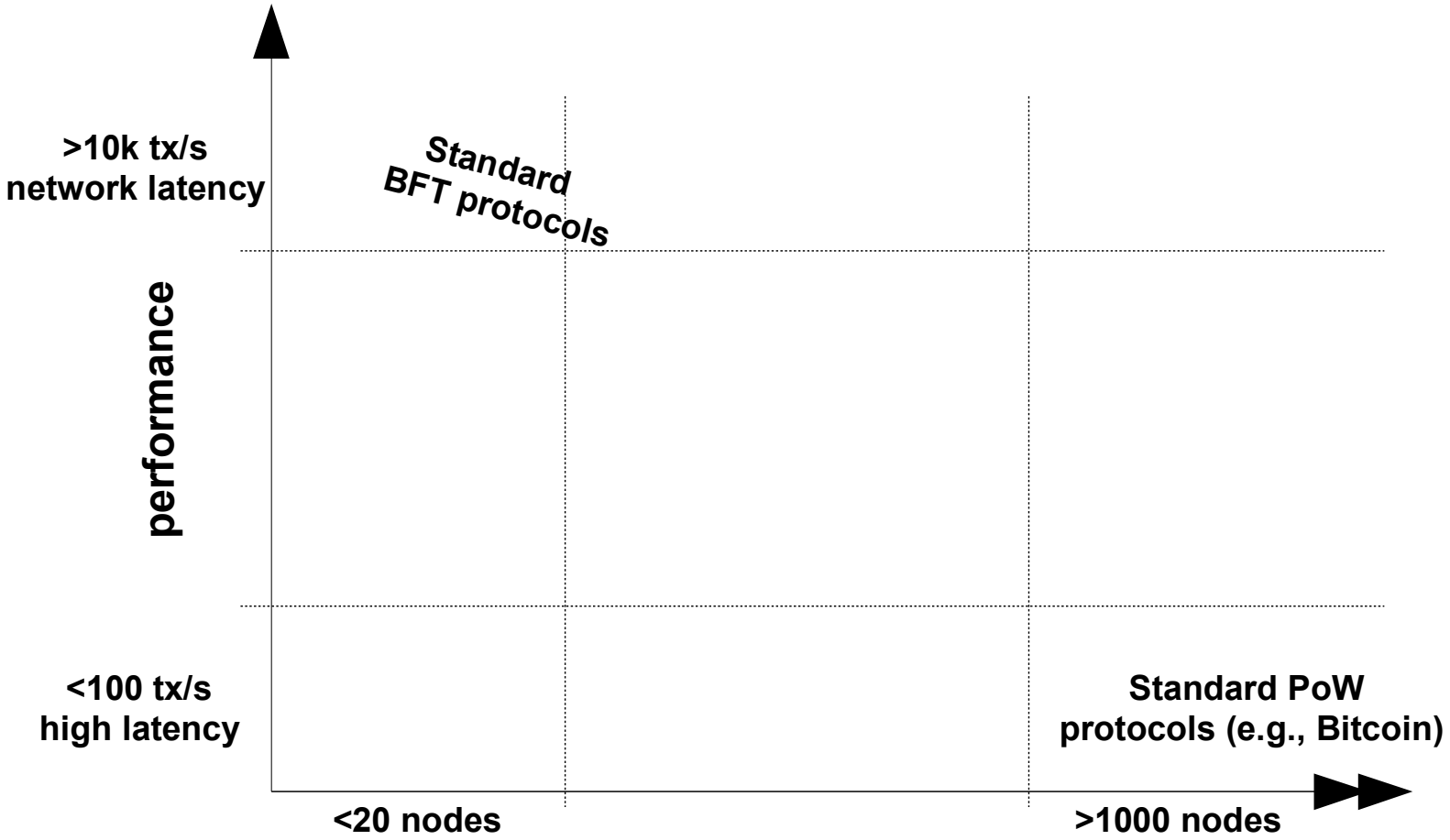


2-Phase commitment:
- Nodes collect votes
- Quorums ensure agreement

Characteristics of BFT consensus

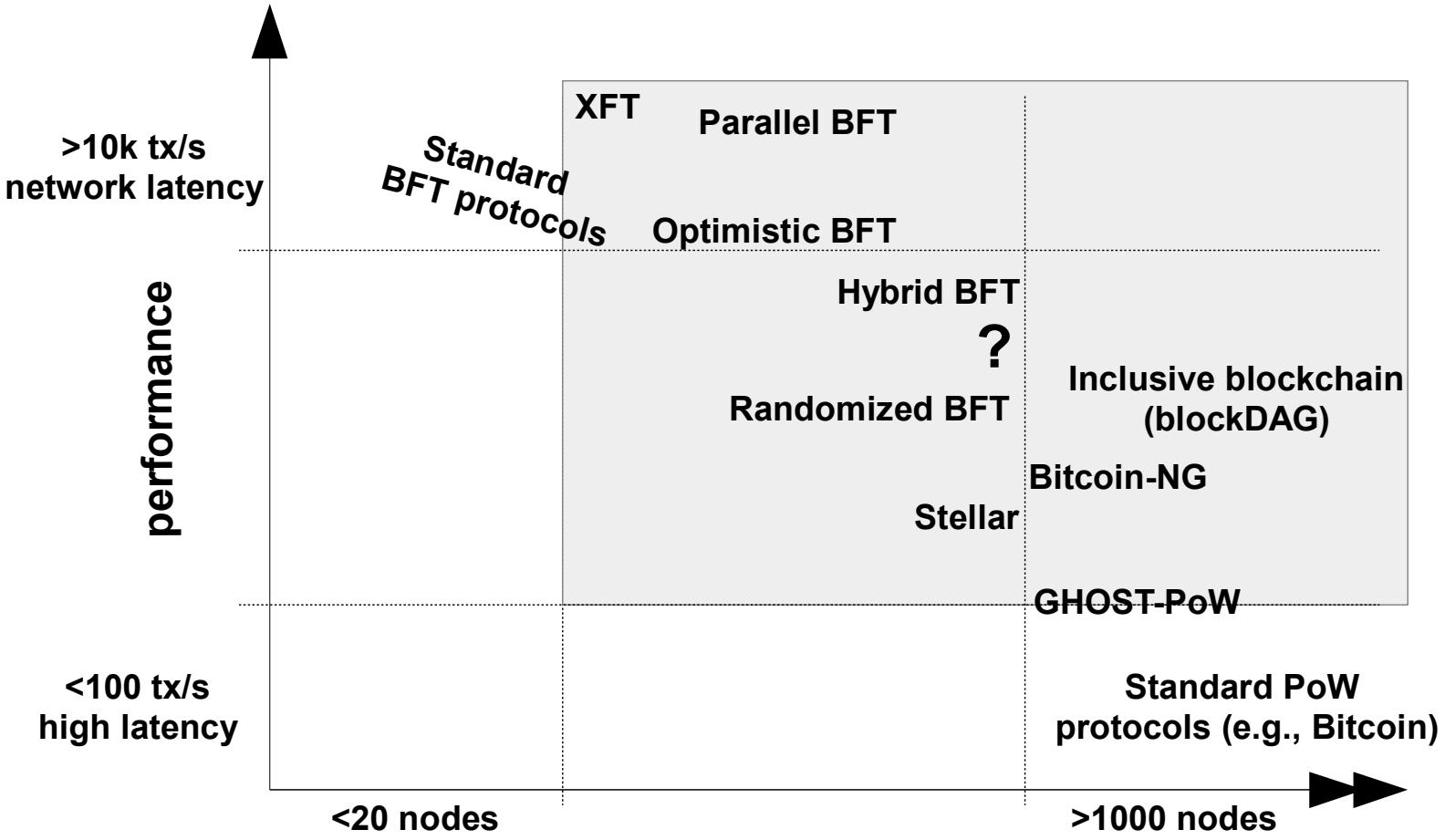
- **Communication based:**
  - Nodes talk to each other to solve consensus
- **Energy efficiency**
  - Because consensus is not tied to a competition of wasting computation power
- **Performance is good**
  - High throughput (multiple thousand Tx/s)
  - Comparable low latency possible (a few seconds)

BFT replication vs. PoW



M. Vukolic: The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication

BFT replication vs. PoW



M. Vukolic: The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication

BFT replication vs. PoW

Proof-of-work

(+) scales well for a large number of nodes

(-) typically slow transaction speed and few throughput

(-) mining wastes energy

vs.

BFT consensus

(-) traditional protocols scale poorly for a large #nodes

(+) typically fast transaction speed and high throughput

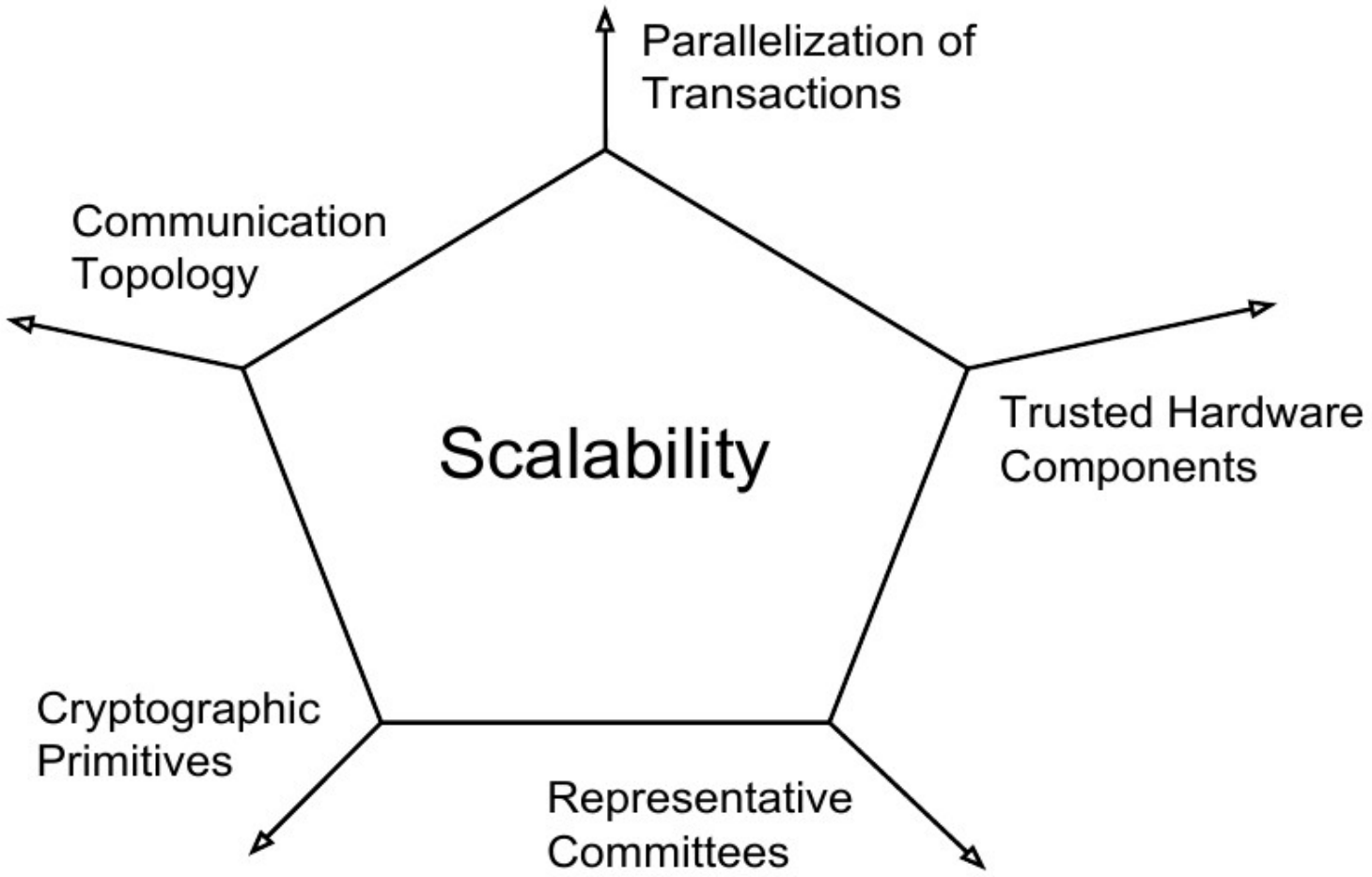
(+) works energy-efficiently

BFT consensus + blockchain ?

- **But how can we maintain security in a permissionless environment ?**
  - Sybil attack: An attacker may create a large number of fake identities in the network
  - Proof-of-stake: Participation is coupled to having stake (native crypto currency of a blockchain)

- **Scalability**
  - Requiring a lot of communication / coordination between nodes limits the scalability of consensus
  - There are techniques for increasing scalability

Scaling Byzantine consensus



Communication topology

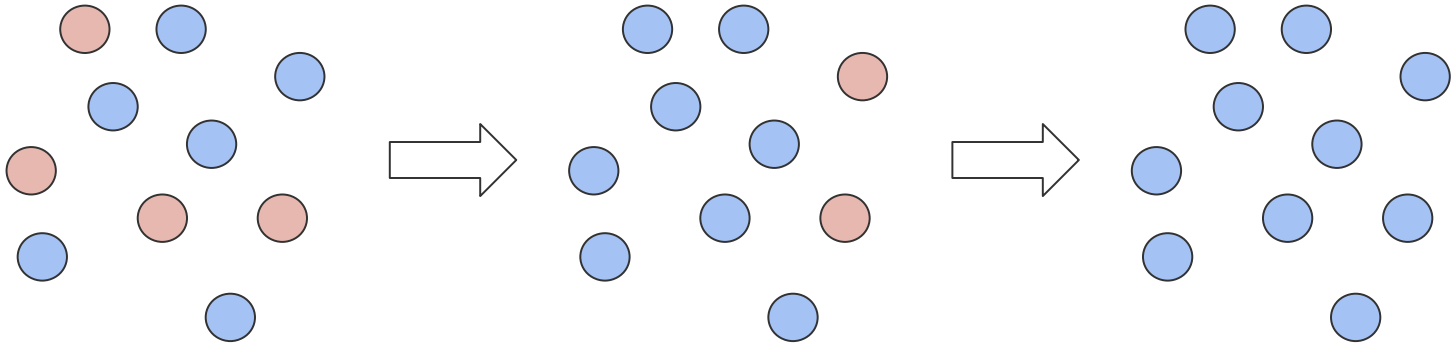
- Who talks with whom?

- **Key ideas**
  - flat-structured communication (HotStuff)
  - tree-structured communication (ByzCoin)
  - overlay networks and gossip (Algorand, Gosig)
  - leader-less communication (Avalanche)
  - federated Byzantine agreement (Stellar)

Leader-less communication (Avalanche)

Avalanche's* idea relies in a metastable mechanism

- Nodes repeatedly sample *k* randomly chosen other nodes and adapt their value to a certain majority
- Thus, correct nodes are being guided towards the same consensus value



*Team Rocket. "Snowflake to Avalanche: A Novel Metastable Consensus Protocol Family for Cryptocurrencies." (2018)

Representative committee

Key idea:

- Announce a committee of delegates with *active* roles (e.g. proposers and acceptors)
- A major portion of the nodes stay passive, i.e., they only learn about the agreement value
- Important: the selection process should **not require coordination** among the nodes

Representative committee

Cryptographic sortition algorithm*

- Choosing a random subset of users according to per-user weights
- In a system with *n* users, for user *i* with weight w_i the probability being chosen is proportional to

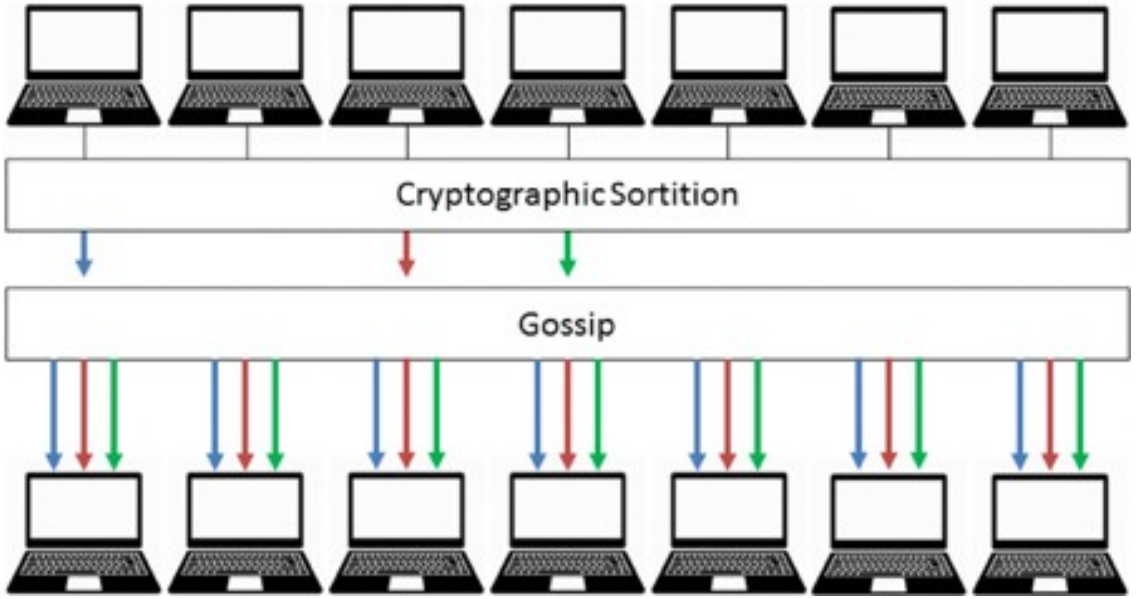
$$\frac{w_i}{\sum_{j=0}^{n-1} w_j}$$

- Delegates are **chosen privately** to avoid being the target of an attacker

* Gilad, Yossi, et al. "Algorand: Scaling Byzantine agreements for cryptocurrencies." *Proceedings of the 26th Symposium on Operating Systems Principles*. ACM, 2017.

Algorand

- **Proof-of-stake**
  - Gives reasonable security guarantees
- **Combines**
  - Committee (selected by cryptographic sortition)
  - Gossip



Scalable Byzantine consensus protocols

- **Specifically designed for large-scale blockchain infrastructures**
- **Differ in their assumptions and ambitions**
- **Use and combine several novel techniques for scaling Byzantine consensus**

	ByzCoin	FastBFT	Stellar	HoneyBadgerBFT	Algorand	Gosig	OmniLedger
Scalability (evaluated with)	1004	199	currently running ca 100	104	**up to 500k**	up to 10k	1800
Throughput (transactions/s)	700 (n=1004)	370 (n=199)	1000 (n ca. 100)	1200 (n=104)	<1000	4000 (n=140)	**≥ 4000 (n=1800)**
Latency	30s	**< 1s (1 Gbps LAN)**	few seconds	100s	1 minute	<1 minute	< 2s
Synchrony	weakly synchronous	weakly synchronous	asynchronous, but progress depends on synchrony	**asynchronous**	weakly synchronous	asynchronous, but provable liveness only under weak synchrony	synchronous
Consensus determinism	deterministic	deterministic	deterministic	probabilistic	probabilistic	probabilistic	probabilistic
Approaches for scaling consensus	communication tree + collective signatures	hardware-based TEE + secret sharing, tree topology	federal Byzantine agreement with hierarchical structure	novel ACS reduction with threshold encryption, efficient RBC with erasure codes	committee (cryptographic sortition) + gossip	multi-signatures + gossip	communication tree, collective signatures, parallelizing transactions

Permissioned blockchains

- **Are based on a well-defined consortium of participators**
  - A “native” crypto currency or proof-of-stake mechanism is not needed!
- **Employ “traditional” consensus mechanisms**
- **Build resilient distributed applications on top of it**
- **A popular open-source platform currently is Hyperledger Fabric**

Conclusions

- **Proof-of-work wastes a lot of energy**
  - This really can become an environmental problem
- **The energy problem of blockchains can be solved**
  - Other novel alternatives based on time and/or space
  - Proof-of-stake & scalable BFT consensus
  - Permissioned blockchain & BFT consensus

Our Current and Future Research

Research Questions

- How can the environmental adaptivity of BFT consensus be improved without diminishing resilience?
- How can we design BFT systems that can deliver a steady and predictable performance?
- How can the design process be enhanced by suitable validation techniques to ensure implemented BFT systems work as intended?

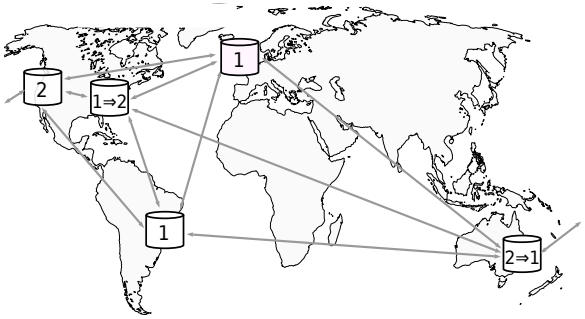
Research Project: BFT2Chain

Design and Validation of Scalable, Byzantine Fault-Tolerant Consensus Algorithms for Blockchains

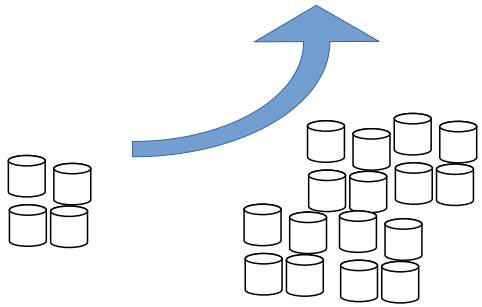
A project funded by DFG Deutsche Forschungsgemeinschaft

Research Focus

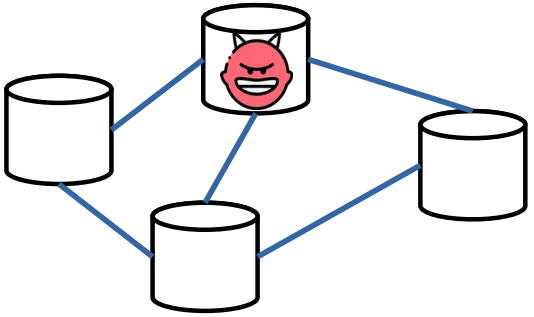
- **Our work focuses on**
  - the **practical aspects** of *BFT consensus* protocols when employed within distributed ledger technology
  - … this also means exploring realistic deployment scenarios and understanding the practical constraints they involve



Geographic dispersion



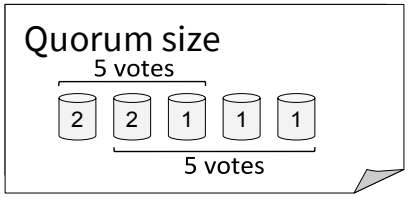
Scalability (#nodes)



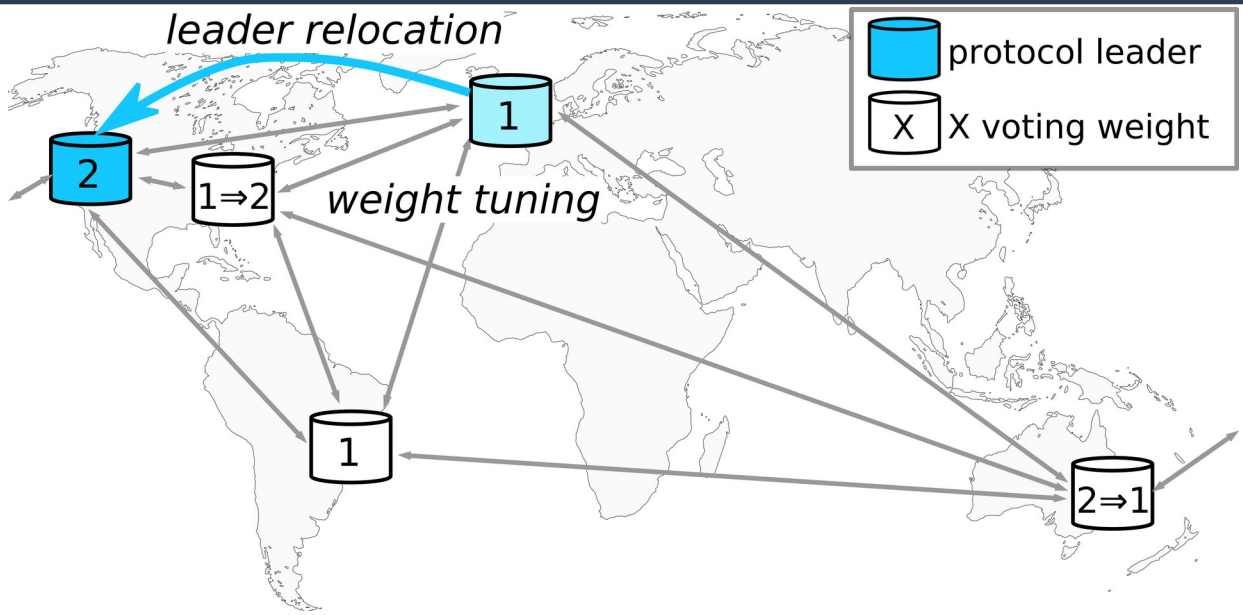
Resilience against attacks

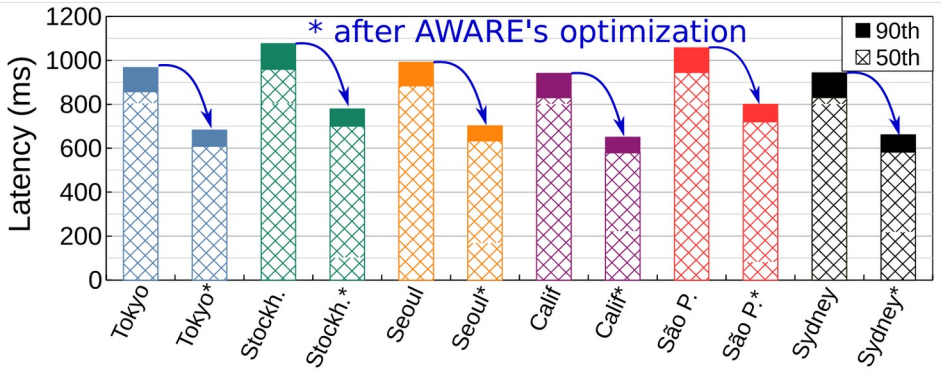
Current Research: AWARE

- **A**daptive **W**ide-**A**rea **RE**plication (AWARE)[1]
  - Uses voting weights



- employed in **Hyperledger Fabric** as consensus substrate[2]
  - To speed up ordering

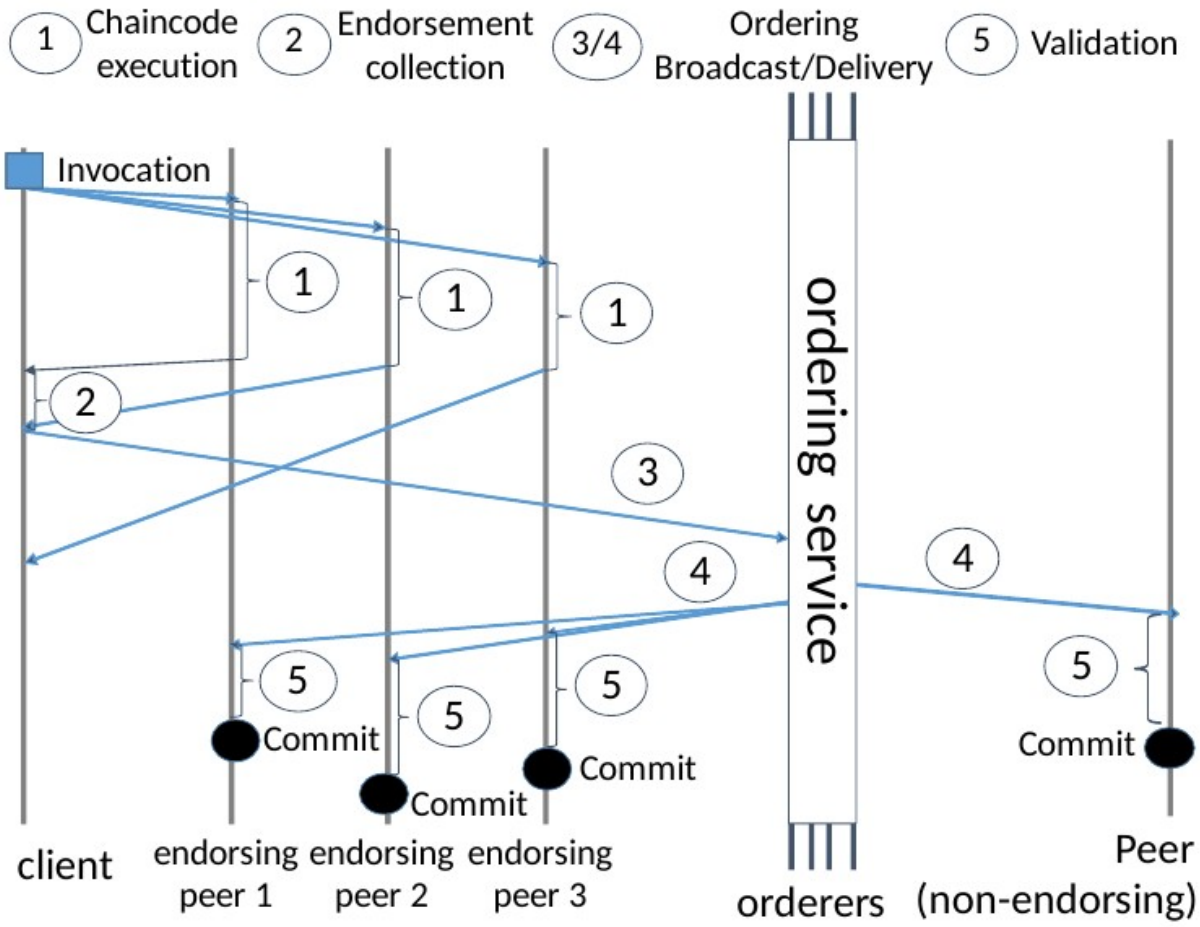




1. Christian Berger, Hans P. Reiser, João Sousa, Alysson Bessani. **Resilient Wide-Area Byzantine Consensus Using Adaptive Weighted Replication**. *SRDS'19: The 38th IEEE International Symposium on Reliable Distributed Systems*. October 2019.

2. Christian Berger, Hans P. Reiser, João Sousa, and Alysson Bessani. **AWARE: Adaptive Wide-Area Replication for Fast and Resilient Byzantine Consensus**. *IEEE Transactions on Dependable and Secure Computing*. Accepted in October 2020.

Hyperledger Fabric



Androulaki, E., et al.: Hyperledger fabric: a distributed operating system for permissioned blockchains. In: Proc. of the 13th EuroSys Conf. pp. 1–15. ACM (2018)

Future Research

- **Scaling consensus**
  - separate management of suitable communication topology from BFT protocol
- **Prediction models for BFT protocols**
  - e.g. simulation of consensus, considering malicious attacks, different consensus protocol patterns ...
- **Validating practical eligibility**
  - test scenario generator
  - automated testing procedures (deployment + benchmarking, faultloads)

Discussion