blockchain.taltech.ee

BLOCKCHAIN AND CONSENSUS

27.06.2021

AGENDA

- Introduction of Distributed Systems
- Introduction of Money
- Bitcoin Motivation
- Importance of Digital Disruption
- Consensus as a Solution
- Introduction of CAP Theorem
- Blockchain Consensus

DEFINITION OF DISTRIBUTED SYSTEMS

- According to Leslie Lamport "A distributed system is one that prevents you from working because of the failure of a machine that you had never heard of."
- More data rate due to simultaneous read/write.
- Concurrent computation results in higher performance.
- Smaller latency because of improved load balancing.
- Higher availability because of replicating application process.
- Higher reliability due to multiple computation and crosscheck
- Higher stability because of no singe point of failure.

DISADVANTAGE OF DISTRIBUTED SYSTEMS

- **Distributed systems has high overall system complexity because of following-**

  - Heterogeneity- over a heterogeneous collection of computers and networks.

  - Larger attack surface- more nodes, the bigger the attack surface.

  - More people involved- results no consensus and more misunderstanding.

  - Smaller reliability-more and remote failure modes can cause smaller reliability.

  - Scalability-must be scalable as the number of user increases.

MAIN TASK OF DISTRIBUTED SYSTEMS

- Contain the inherent complexity
- Use the advantages while avoiding their price.

DISTRIBUTED SYSTEM
CONSENSUS

- Consensus mechanism is used to achieve reliable system in a distributed system.
- This ensures that the system is fully decentralized; are trusted nodes or PKI required?
- Determines and identifies how, when, and which model failed.
- Detection of synchronous, asynchronous, and bounded communication model.
- Confirms whether or not the model was terminated or failed.

DISTRIBUTED SYSTEM
WHY CONSENSUS IS DIFFICULT?

- Distributed systems has following limitations-
  - Impossible to prove termination.
  - Impossible to prove correctness.
  - Impossible to pinpoint the location of the failure.
  - Impossible to detect failure.

MONEY

- It is a measure of value.
- Medium of value of exchange
- Deferring value of exchange
- Money as a unlimited optionality
- Money as a abstract data type
- Monetary system

BITCOIN

- Protect against inflation

  - To maintain monetary stability by constraining political decisions
- Protect against next Lehman crisis

  - Satoshi Nakamoto's solution was trustless money.
- Escape negative interest rates

  - Urge consumers to spend
  - Undermine financial decision autonomy of citizen
- Denial of service based on policy or identity

BITCOIN ARCHITECTURE

- Fully decentralized P2P with no single point of action
- Open to anonymous & private participation of everybody
- Governed by a majority consensus of participating entities
- Highly replicated and thus robust against attacks
- Cryptography is used to secure data, not human trust or social power.
- The majority of nodes constantly adhere to majority-decided governance.

DIGITAL DISRUPTION
EMAIL

- Data is essential.
- Data are overhyped.
- Everyone uses data in some way.

Limitation:

- Nobody modifies the processes.
  - Using email to send holiday photos to friends
  - Introducing "digital teaching" by disseminating PDFs

DIGITAL DISRUPTION
INTERMEDIARIES

- Recognize and accommodate special needs.
- Utilize scenarios in processes.
- Uber, Tinder, AirBnB, Facebook, Google & Co. introduce specialized solutions.
- Everyone enters their preferences and personal information.
- Everything becomes freely available.

Limitation:

- TOS user lock-in.

  - What precisely are they doing with my data?
  - Why can not I have my way about it? (No ads, spam filters, adaptation of user interface, migration platform, data sovereignty,...)

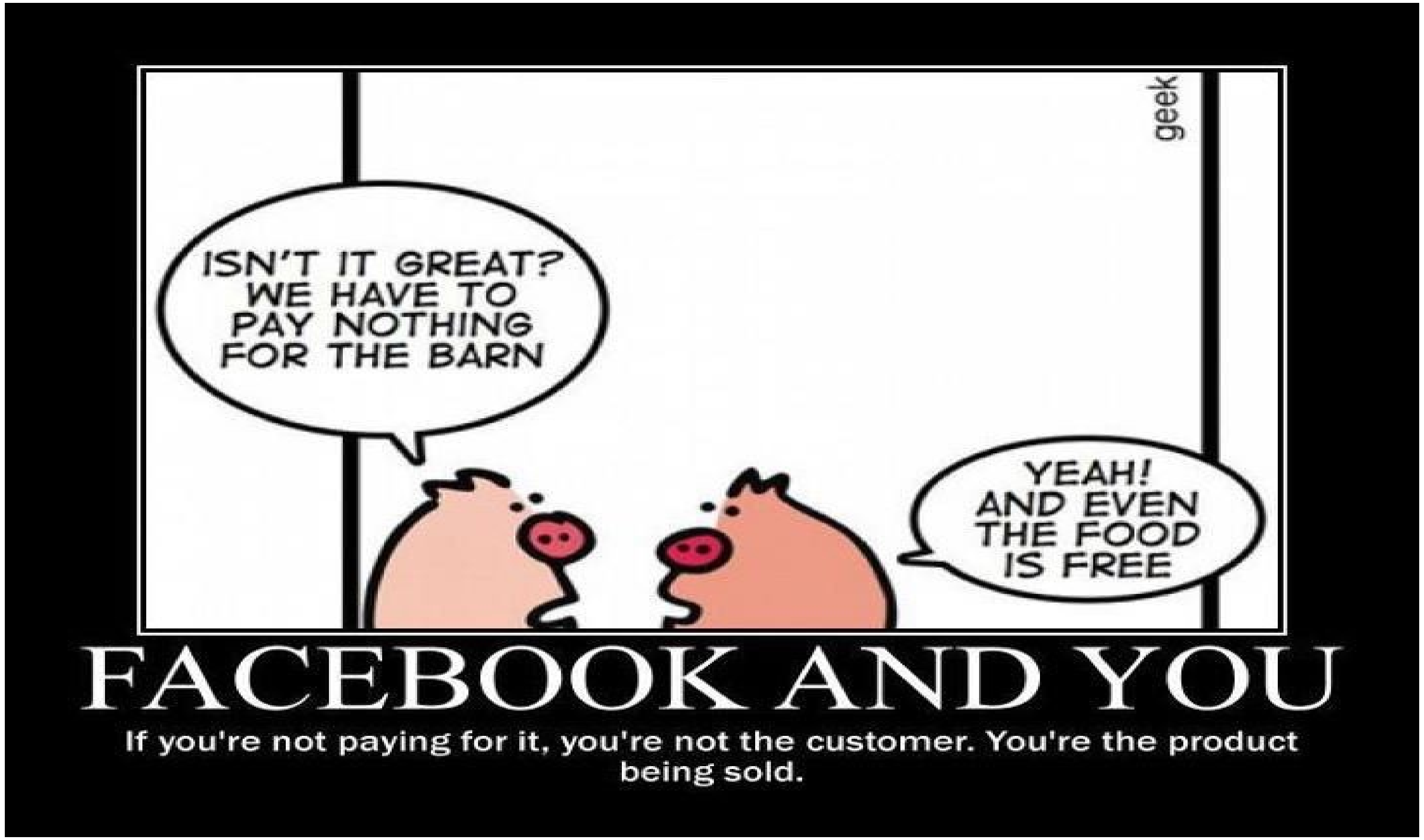

Figure 1: You are being sold if you do not pay for it.

DIGITAL DISRUPTION
OBSTACLES

- **Value generation-** There are no incentives for value generation for intermediaries:
  - dissemination & marketing & branding
  - un-nerding & mainstreaming
  - user studies on UI quality
  - bug removal & feature proliferation & language localization
- **Adherence to community standards-** How can we apply open democratic standards to Community rules?
  - Consensus
  - Benevolent dictator

DIGITAL DISRUPTION
BITCOIN AS A SOLUTION

- **Value generation-**

  - Bitcoin blockchain comes with Bincluded.

- **Adherence to community standards-** Bitcoin began with this goal for the monetary system and has successfully achieved it.

  - Bitcoin upholds a community standard:

  - Σ total amount deposited- Σ total withdrawls=balance , where balance>=0

- Ethereum enforces intricate community standards (aka smart contracts)

```
pragma solidity >=0.4.22 <0.6.0;

contract SimpleAuction {
    // Parameters of the auction. Times are either
    // absolute unix timestamps (seconds since 1970-01-01)
    // or time periods in seconds.
    address payable public beneficiary;
    uint public auctionEndTime;

    // Current state of the auction.
    address public highestBidder;
    uint public highestBid;

    // Allowed withdrawals of previous bids
    mapping(address => uint) pendingReturns;

    // Set to true at the end, disallows any change.
    // By default initialized to `false`.
    bool ended;

    // Events that will be emitted on changes.
    event HighestBidIncreased(address bidder, uint amount);
    event AuctionEnded(address winner, uint amount);

    // The following is a so-called natspec comment,
    // recognizable by the three slashes.
    // It will be shown when the user is asked to
    // confirm a transaction.

    /// Create a simple auction with `_biddingTime`
    /// seconds bidding time on behalf of the
    /// beneficiary address `_beneficiary`.
```

Figure 2: Simple open auction smart contract specification
https://docs.soliditylang.org/en/v0.5.3/solidity-by-example.html

BLOCKCHAIN IMPROVES DIGITAL DISRUPTION

- **Every individual creates their own identity.**
  - Nobody was unfairly omitted.
  - Create a public-private key pair at random (e; d)
  - Very small chance of collision of random key pairs
- **A bitcoin node can/may be operated by anyone.**
  - There is always a bitcoin bank available to you.
- **Everyone broadcasts and stores all transactions and responds to inquiries about account status.**
  - Storage that is robust and available in the face of node failures and network partitions

MAIN SOURCE OF BLOCKCHAIN CONSENSUS PROBLEMS

- **Network and processing latencies are an unavoidable side effect.**
  - A transaction is generated, signed, and broadcasted by Alice.
  - Carol has not heard from it yet, but Bob has.
  - Donald has started a new block, but Eric has yet to hear from it
- **Double spending attack**
  - Mallory sends conflicting transactions to different nodes on purpose.
- **Attack from Malicious nodes**
  - Mallory provides inconsistent responses to requests on purpose.
- **Attack from Sybil nodes**
  - Mallory takes on the roles of Mallory-1, Mallory-2, and Mallory-3 in order to influence "majority" consensus.

BYZANTINE GENERAL PROBLEMS

- Each general has army and that each group is situated in different locations.
- All generals reach consensus, ice, agree on a common decision.
- After the decision is made, it cannot be changed.
- The communication take place with another through messages.
- Messages can get somehow delayed, destroyed or lost
- General represents a network nodes and nodes to reach consensus.
- Majority of participants have to agree and execute the same action.
- If majority of participants decide to act maliciously, the system is susceptible to failure or attacks.

CAP THEOREM

- **CAP theorem, also known as Brewer's theorem, was introduced by Eric Brewer in 1998**

  - **Consistency (C)** ensures that all nodes have a single, current, and identical copy of the data.

  - **Availability (A)** means that each node has data, and the nodes are responding to requests.

  - **Partition tolerance (P)** ensures that even if a network fails, the distributed system continues to function properly.

- **Blockchain manages to achieve all of these properties.**

  - To achieve fault tolerance, replication is used.

  - Consistency is achieved using consensus algorithms which ensure that nodes have the same copy of the data.

  - Consistency (C) on the blockchain is not achieved simultaneously with Partition tolerance (P) and Availability (A), but it is achieved over time

HOW TO DEAL WITH CAP?

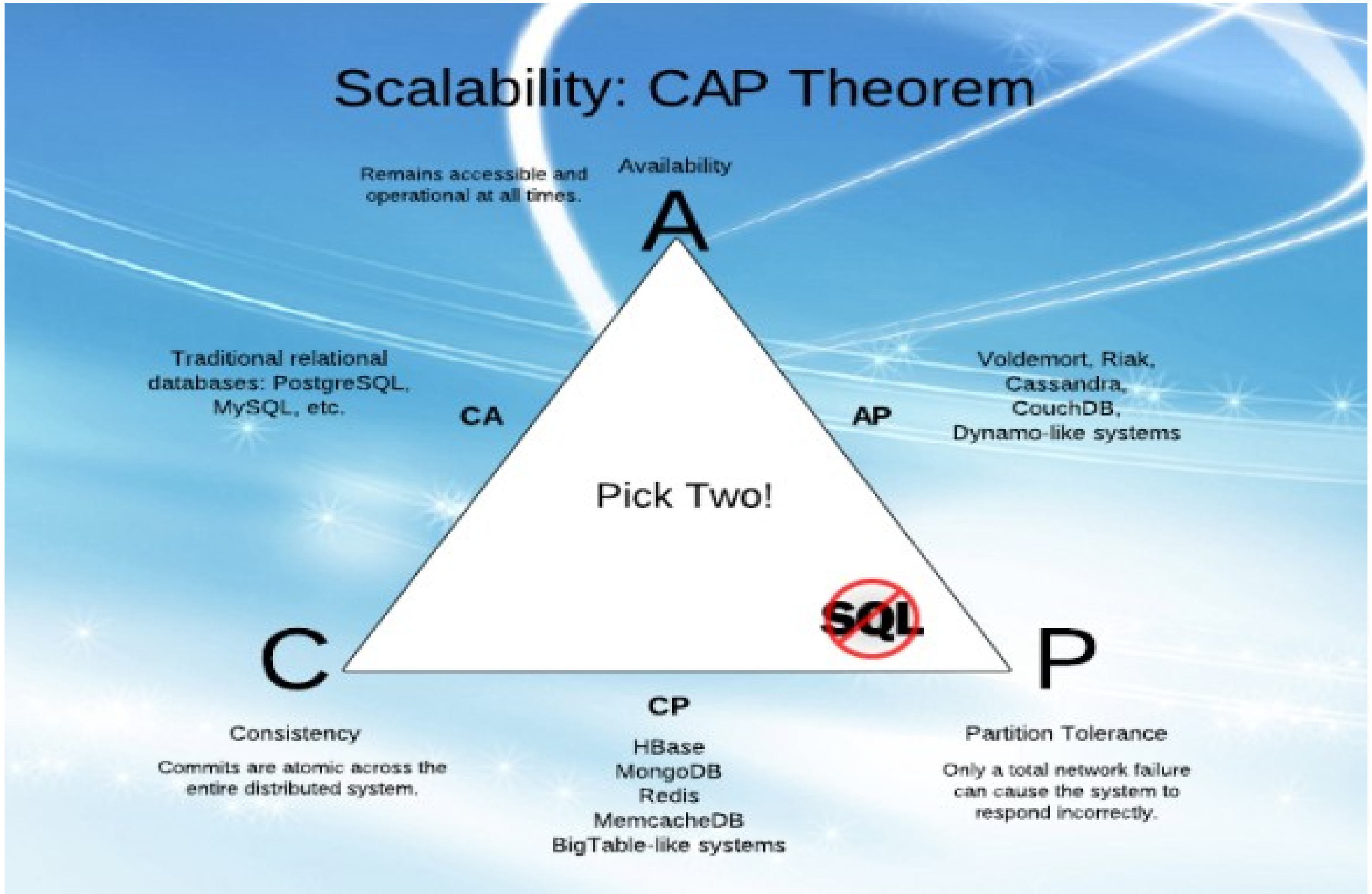

Figure 3: CAP problem is depicted in a nicely equilateral triangle. Source: Image source

HOW TO DEAL WITH CAP THEOREM

- **CA systems drop partition tolerance**

  - Put everything related to a single transaction on a single node or in an atomically failing cluster.

  - Does not scale well.

  - Is not resistant to site and/or connectivity loss.

- **AP systems drop consistency**

  - Consistent systems occasionally accept outdated responses.

  - The most recently written value will finally be reached.

- **CP systems drop availability**

  - Until the data has become consistent, avoid partition events.

  - Degraded network partition detection.

ACID VERSUS BASE FOR DATABASE TRANSACTION

- **Database transactions should be:**

  \- **A**tomic: Everything in a transaction succeeds or the entire transaction is rolled back.

  \- **C**onsistent: A transaction cannot leave the database in an inconsistent state.

  \- **I**solated: Transactions cannot interfere with each other.

  \- **D**urable: Completed transactions persist, even when servers restart etc.

- **An alternative to ACID is BASE:**

  \- **B**asic Availability- but not necessarily guaranteed availability

  \- **S**oft-state- No hard guarantees on a state

  \- **E**ventual consistency- State will sooner or later converge.

CAP THEOREM

- **BASE offers**
  - Simpler syatem design
  - Faster transactions
  - Better scalability
  - Higher availability
  - Smaller downtime
- **Price to pay: Only weak consistency, which means..**
  - Data may be delayed: Data was that way before.
  - Data can be stale: State is shown, but does not exist.
  - Mechanisms are required to detect and fix this

ROLE OF BLOCKCHAIN STRUCTURE ON CAP THEOREM

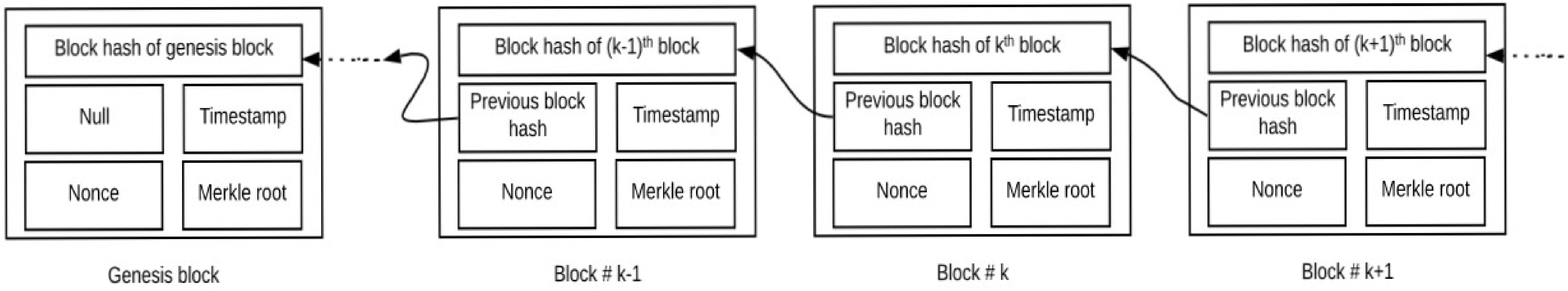

Figure 4: States of Blockchain in time.

ROLE OF BLOCKCHAIN STRUCTURE ON CAP THEOREM

- **Chain provides a sequence of states**

  - There may be several transactions involving the same account arriving at different nodes at different order.

  - Resolution by real-time clocks.

  - Resolution by time-stamp algorithm.

- **Resolution in bitcoin**

  - By random winner of PoW for locally

  - Selfish nodes prefer the longest branch globally.

- **Additional roles of chain**

  - Conflict resolution by "rule of longest branch"

  - The block chain must be reset from the genesis block

  - Redoing entire chain is very costly

BLOCKCHAIN CONSENSUS ALGORITHM

- **Classical consensus algorithms include:**
  - Proof of Work (PoW)
  - Proof of Stake (PoS)
  - Proof of Authority (PoA)
- **Four others types includes:**
  - Proof of Weight (PoW)
  - Byzantine Fault Tolerance (BFT)
  - Directed Acyclic Graphs (DAG)
  - Delegated Proof of Stake (DPoS)

PROOF OF WORK (POW)

- An insulating method from fraudulent transactions, except in the event of a 51% attack.
- A group of miners with a majority of network computing power conspires to obstruct transactions.
- Proof of work is based on math equations, which the nodes, or miners, on a network race to solve.
- First miner to solve the mathematical equation receives freshly minted Bitcoin.
- To guarantee equal probabilities, proof of work equations must be solved by brute force.
- Bitcoin, Litecoin uses Proof of Work algorithm.

PROOF OF WORK (POW): ENERGY CONSUMPTION

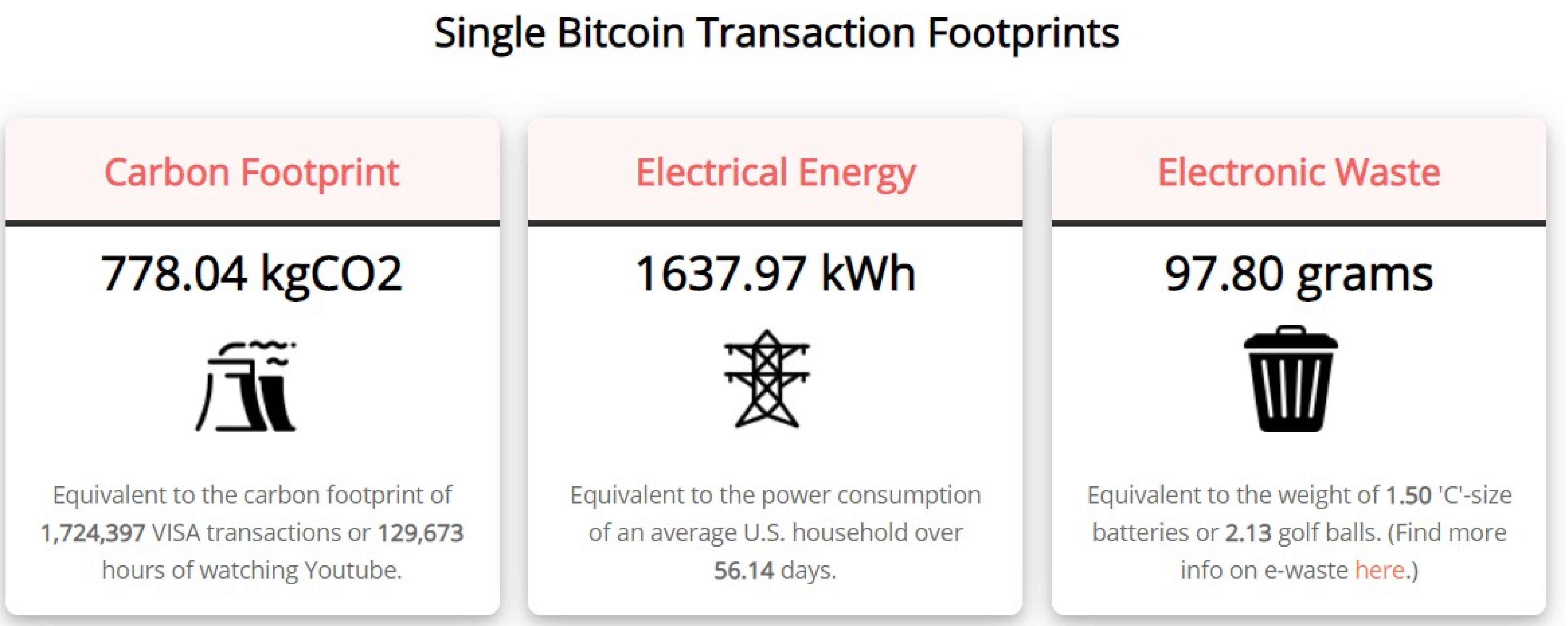

Figure 5: Bitcoin Energy consumption

PROOF OF WORK (POW): ENERGY CONSUMPTION

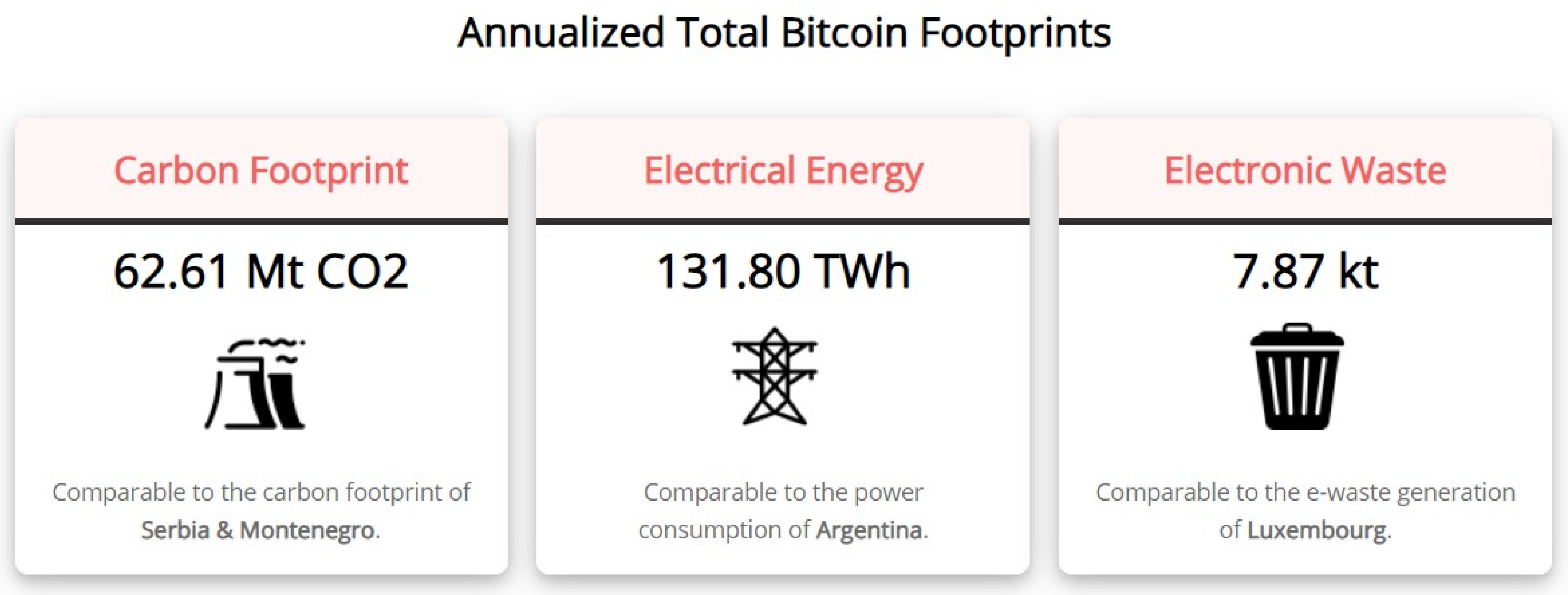

Figure 5: Bitcoin Energy consumption

PROOF OF STAKE (POS)

- Depend on how much cryptocurrency a node or validator already owns and stakes.

- Created in response to the increasing computational power required by the PoW.

- Elimination of racing to solve a mathematical equation as in PoW

- Nodes select a percentage of transactions based on their stake of ownership in the network.

- Eliminates the need to leverage (and waste) exorbitant amounts of computing power

- Ethereum 2.0, Peercoin uses the Proof of Stake.

PROOF OF AUTHORITY

- Combination of PoS and PoW, stakeholders is selected in a pseudorandom.
- More energy-efficient mechanism than the PoW.
- Small and designated number of blockchain actors the power to validate transactions or interaction with the network.
- Each new block of transactions is validated by one or more validation machines.
- It does not require a lot of computing power and does not use a lot of electricity.
- It is often favoured by private or consortium blockchains.

PROOF OF WEIGHT

- **Concepts:** Next block minting is based on some weighted value, not necessarily coupled to system tokens like PoS.

  - Filecoin's Proof-of-Spacetime is weighted on how much IPFS data you're storing.
- **Used in**: Filecoin, Chia, Algorand
- **Pros-**

  - Customizable; scalable
- **Cons-**

  - Incentivization can be a challenge

PBFT (PRACTICAL BYZANTINE FAULT TOLERANCE)

- Algorithm for state machine replication that tolerates Byzantine faults
- The algorithm offers both liveness (client finally receiving correct replies to their requests) and safety, provided:

  - At most '(n-1)/3' nodes are faulty out of 'n' nodes

  - Delay 't' does not grow faster than indefinitely.
- Delays occur when a message is sent for the first time, and when it has been received by its destination
- PBFT is currently used in Hyperledger fabric along with the Kafka ordering system

DIRECTED ACYCLIC GRAPH

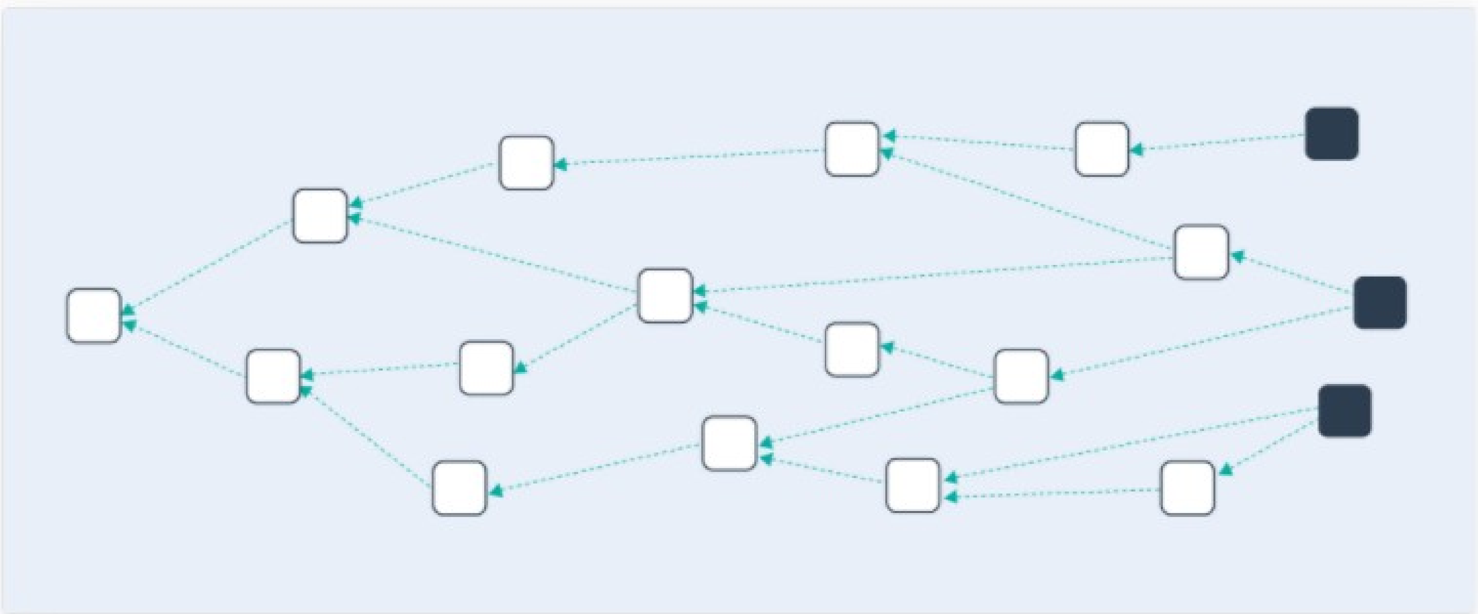

Figure 6: DAGs emphasized front-covering instead of one-tree-focused DAGs.

DIRECTED ACYCLIC GRAPH

- Acyclic just means that no node in the graph can reference back to itself; it can’t be its own mother node.
- This data structure resembles a flow chart where all points are headed in one direction.
- The first crypto project we must mention when talking about DAG is IOTA.
- IOTA is an excellent example of a DAG based cryptocurrency.
- Suitable for IoT devices.
- Centralization might be a requirement.

DELEGATED PROOF OF STAKE (DPOS)

- Users of the network vote and elect delegates to validate the next block.
- Delegates are also called witnesses or block producers.
- Staking your tokens in a pool grants you voting rights to delegates.
- Staking services provider in a staking pool (in place of "you transfer your tokens to another wallet").
- Much better scalability
- Centralization might be a requirement.
- Much faster transaction clearance (up to 1 block/sec)

TAL TECH

Thank you very much for your attention!
Q & A?

Reference: Arumaithurai M., Introduction to Blockchains, Tallinn, Estonia 2019, https://tinyurl.com/n2y3k5pu