Blockchain

SPS110NDD | GROUP#6

MINA, AMIR, MAHARU

Overview

Think of blockchain as a "special" database. In the simplest terms, Blockchain is a chain of blocks, but not in the actual definition of these two words. When we say "block" and "chain", we are actually talking about digital data ("block") stored in a public database ("chain").

In blockchain the data is unique and immutable forever ; digital information cannot get copied. What this means is that each piece of info and data can only have one owner and every change made in those data is added as blocks to the chain. Once an information is stored on a blockchain, it is going to stay for good and it's extremely hard to change or steal it.

Figure 1. Blockchain. (2019). Retrieved from https://www.thestreet.com/technology/what-is-blockchain-15179703

Blockchain is needless of a central control entity. Currently, most people use a reliable middleman such as a bank to make a transaction. Blockchain, on the other side, allows clients and providers to connect directly and remove the need for a third party. These chains and blocks are controlled by no single authority.

Blockchain came into people's conversations when its application Bitcoin was launched, but the invention of blockchain goes back to 2008.

Benefits

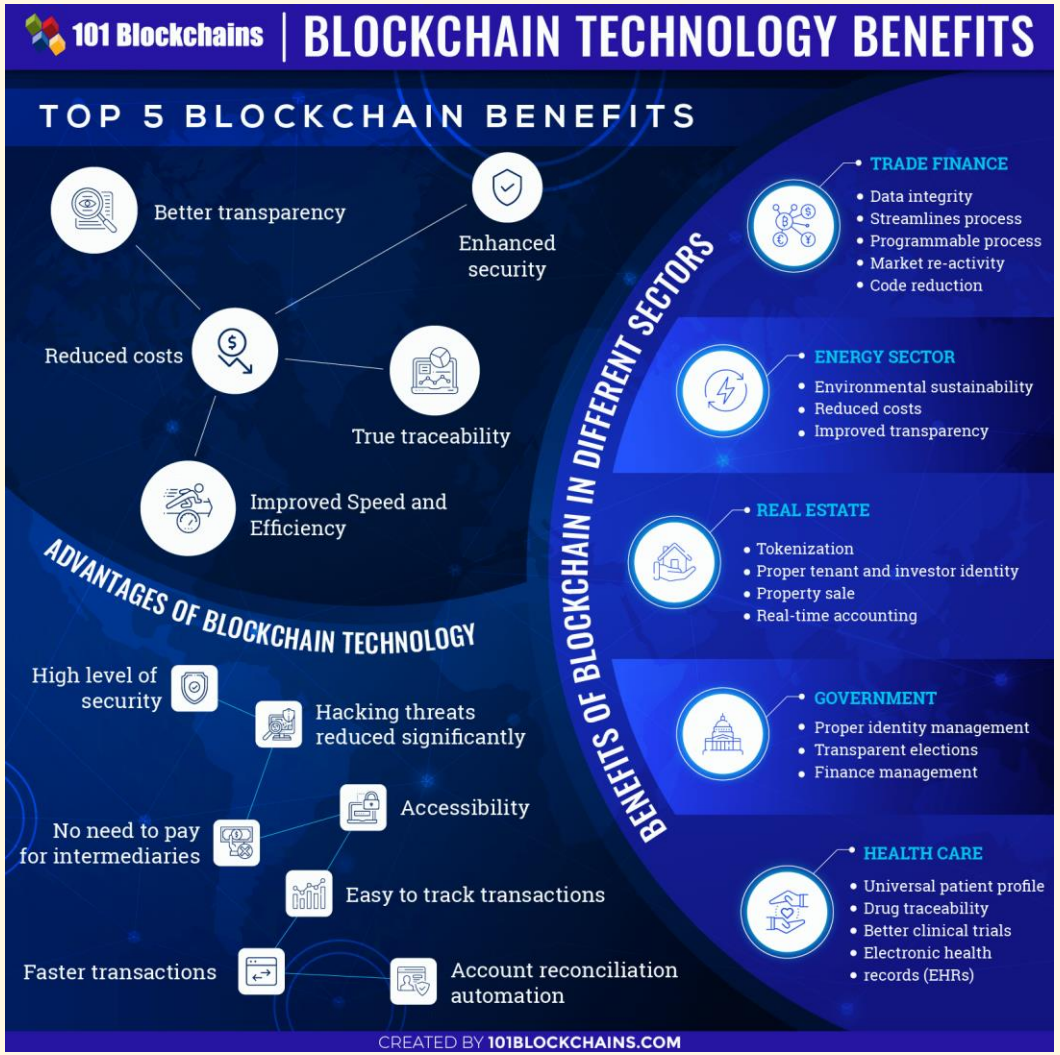


Figure 2. Benefits of Blockchain Technology. (2019)
Retrieved from https://101blockchains.com/benefits-of-blockchain-technology/

- **Transparency**
  - Data is shared across the entire network
  - Available to everyone in the network
  - Everyone share the same documentations instead of separate copies
  - No more confusion around usage rights or administration
- **Traceability**
  - Tracking goods and assets and where they are currently residing
  - Indelible audit trail helps to trace the goods
- **Trust**
  - No control by any single entity
  - Peer-to-Peer network manages all transactions → no point of failure

• Security

- Each transaction is verified within the network using independently verified cryptography
- Agreements can’t be tampered with and transactions can’t be altered

• Efficiency

- No third-party - process transactions between parties without intermediaries
- Faster transactions by allowing p-2-p transfers

• Costs

- No third-party → no need to pay for vendor costs
- Users can transfer millions of dollars worth on blockchain for less than $1

Challenges

Figure 3. Challenges of blockchain. (February, 2019). https://hackernoon.com/five-challenges-of-permissioned-blockchain-solutions-and-the-tools-and-protocols-that-can-help-you-d3e9cf49818a

- **Bad Image**
  - Hard to understand the concept for some people
  - Negative image of cryptography
- **Interoperability**
  - No standard exists
  - More than 6,500 active blockchain projects on GitHub using a range of platforms with different coding languages
- **Complexity & Cost**
  - Intensive computing power and electricity is needed
  - Huge computer rigs are desired
  - All these will result in exorbitant rates and prices

- ## Lack of Talent

- Not enough skilled blockchain developers
- No proper training and tutorials

- ## Integration with Legacy Systems

- In most cases, organizations are required to completely restructure or redesign their previous system

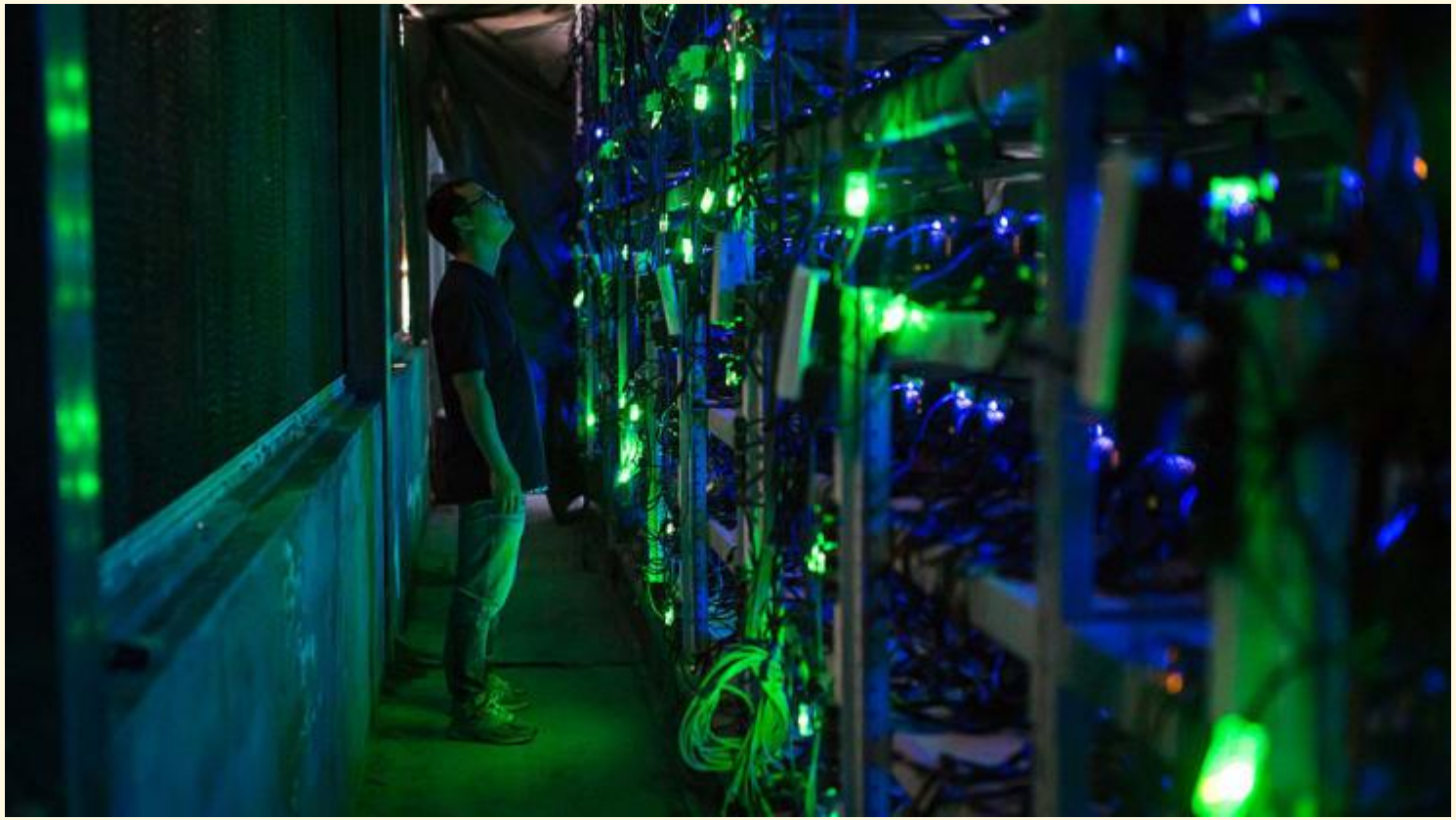
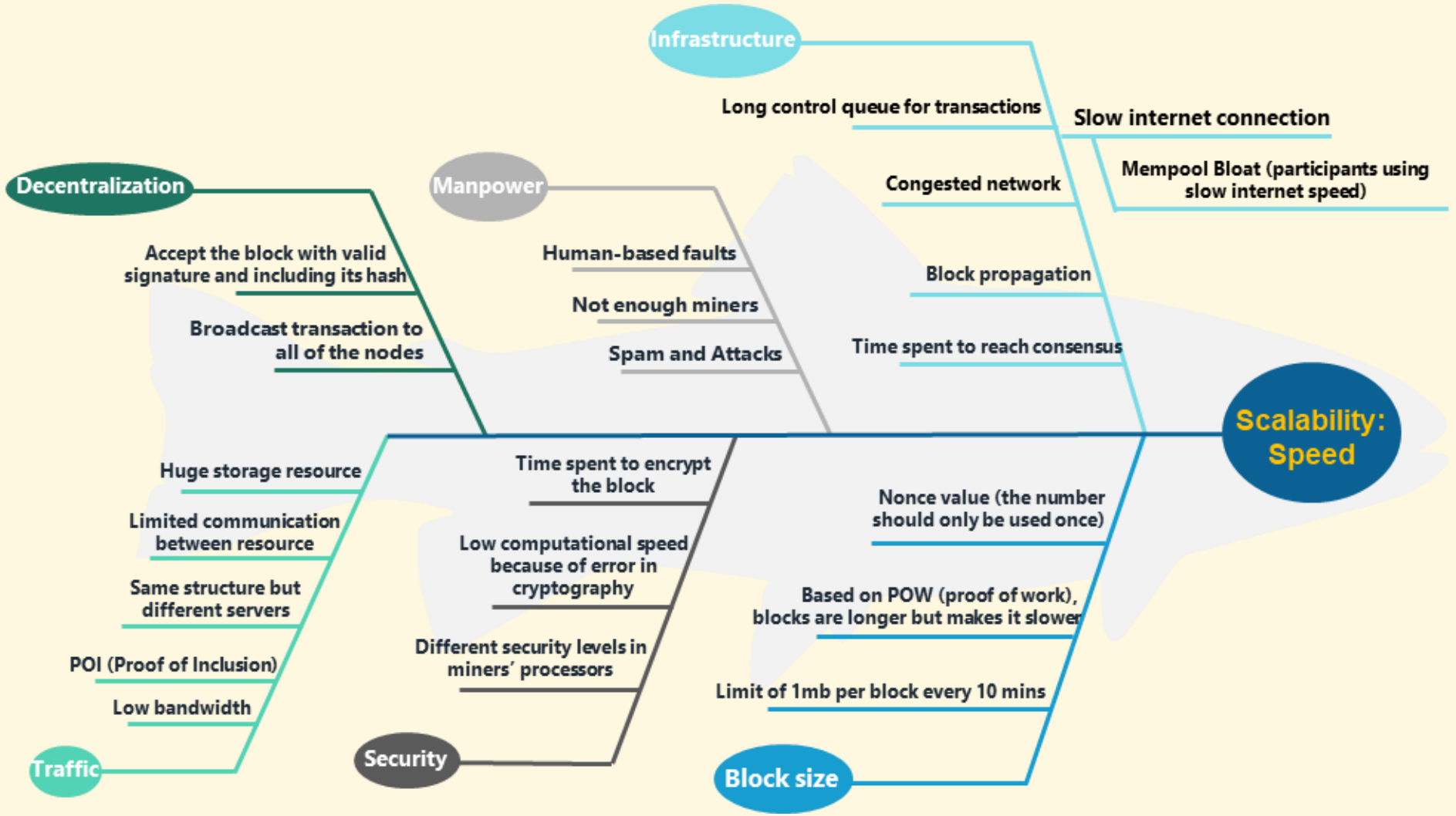


Figure 4. *Paul Ratje.* A bitcoin mine near Kongyuxiang, Sichuan, China. (August 12, 2016). The Washington Post. *Getty Images*

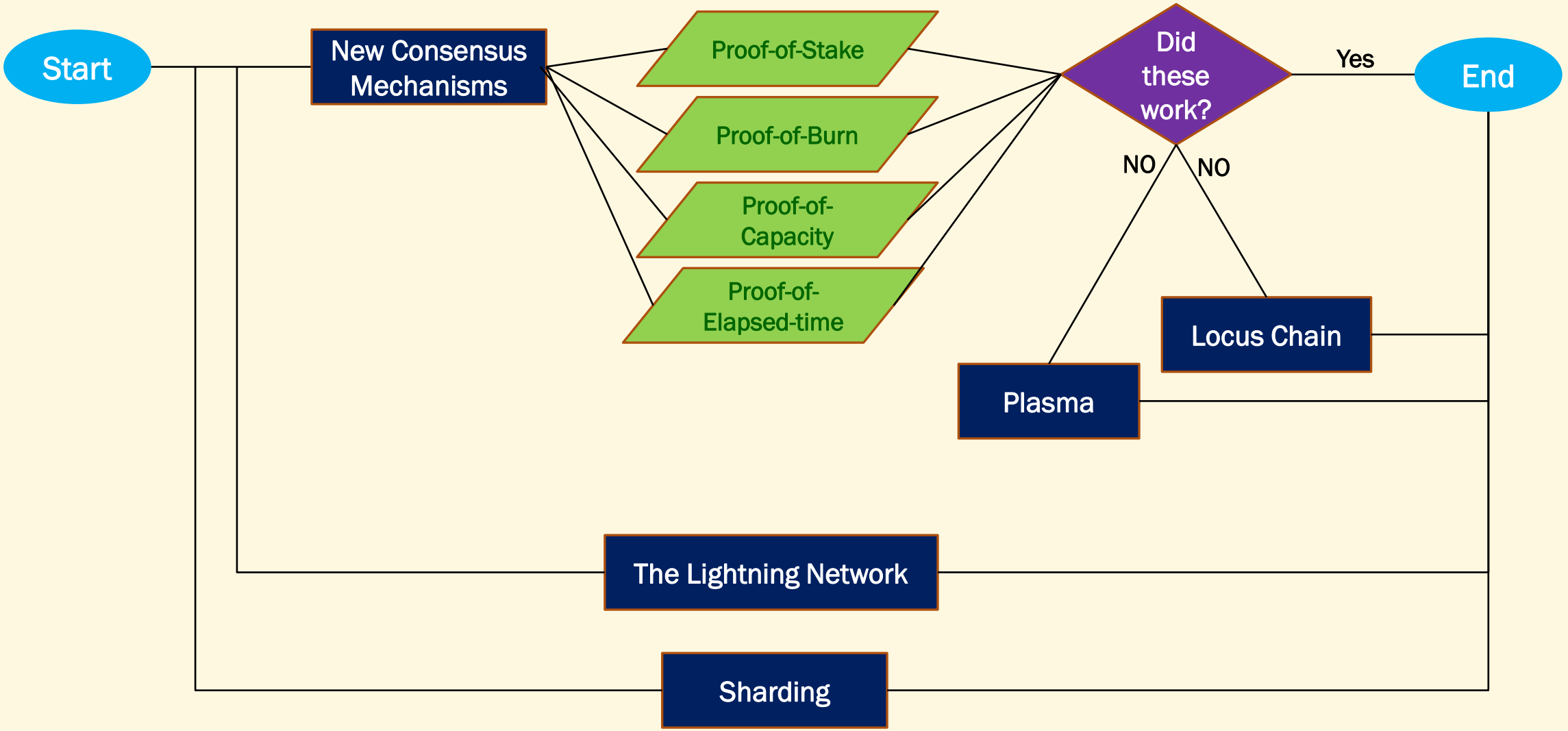
- ## Slow Performance

- Traditional system is much faster
- Bitcoin 3-7 transactions/sec. and Ethereum 13-20 /sec. while Visa 2000 transactions/sec.
- Complexity and encryption results in slower traffic

Fishbone

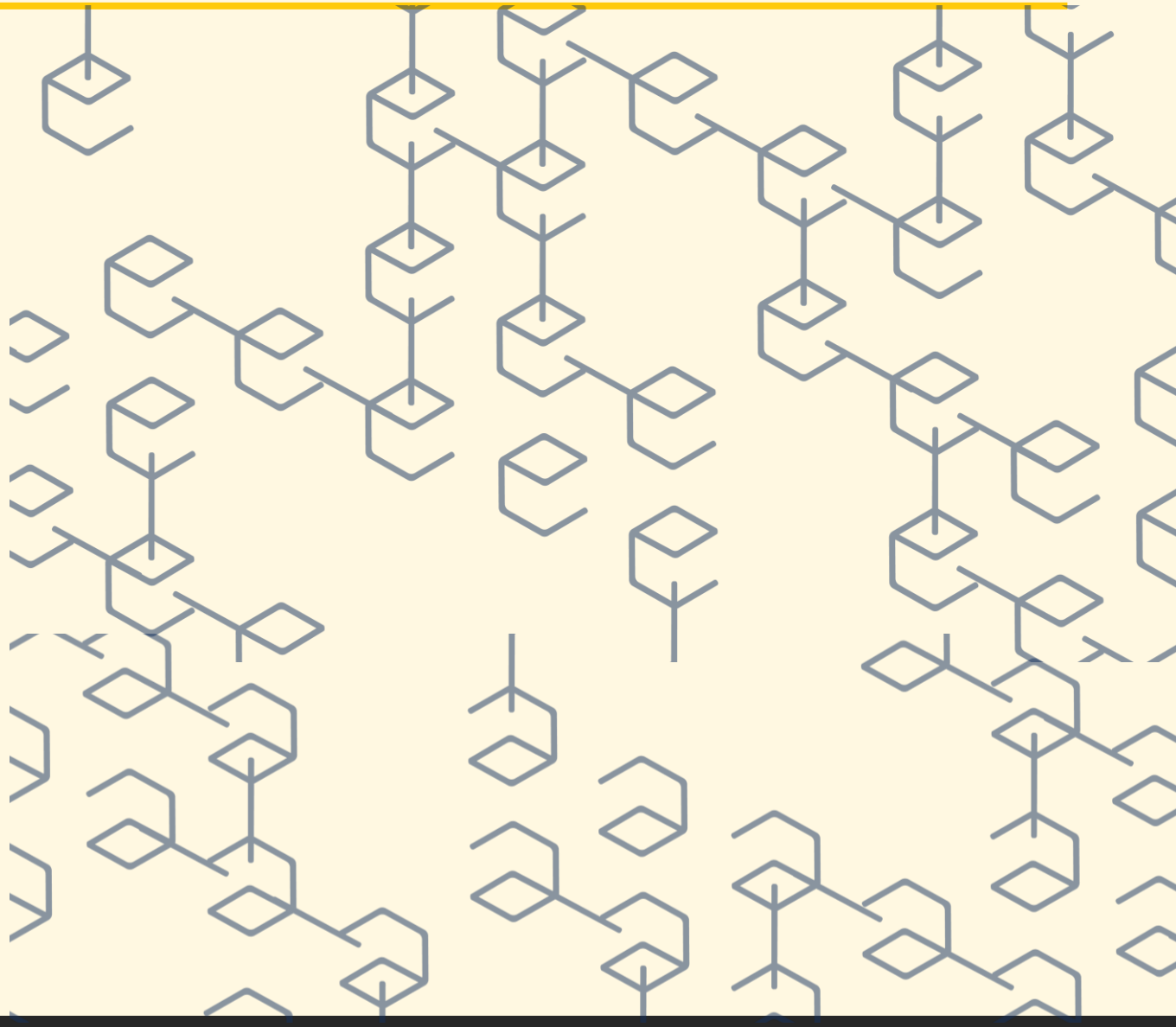

Infrastructure
Long control queue for transactions
Slow internet connection
Mempool Bloat (participants using slow internet speed)
Congested network
Block propagation
Time spent to reach consensus
Decentralization
Accept the block with valid signature and including its hash
Broadcast transaction to all of the nodes
Manpower
Human-based faults
Not enough miners
Spam and Attacks
Scalability: Speed
Huge storage resource
Limited communication between resource
Same structure but different servers
POI (Proof of Inclusion)
Low bandwidth
Traffic
Time spent to encrypt the block
Low computational speed because of error in cryptography
Different security levels in miners' processors
Security
Nonce value (the number should only be used once)
Based on POW (proof of work), blocks are longer but makes it slower
Limit of 1mb per block every 10 mins
Block size

Flowchart


Start
New Consensus Mechanisms
Proof-of-Stake
Proof-of-Burn
Proof-of-Capacity
Proof-of-Elapsed-time
Did these work?
Yes
End
NO
NO
Locus Chain
Plasma
The Lightning Network
Sharding

Future

- Smart Contracts
- Ethereum
- Alternative for Money
- Recruitment



- **DLT-Based Government Systems**
  Distributed ledger technology - Dubai has vowed to replace all government systems with DLT-based structures by 2020

- **Autonomous Negotiation And Trade**

- **Ultimate Transparency Across Industries**
  spot hacking attempts and reduce the messiness

- **Private Data**

- **Blockchain-as-a-Service**
  BaaS will help brands like Walmart track food production

References

- Dughi, Paul. (Feb 3, 2018). A simple explanation of how blockchain works. Retrieved from https://medium.com/the-mission/a-simple-explanation-on-how-blockchain-works-e52f75da6e9a
- https://hackernoon.com/blockchain-technology-explained-introduction-meaning-and-applications-edbd6759a2b2
- https://www.skalex.io/support/blockchain/blockchain-technology/
- https://www.forbes.com/sites/forbestechcouncil/2018/09/06/what-does-the-future-of-blockchain-hold-10-predictions-from-tech-experts/#4aa9322d301a