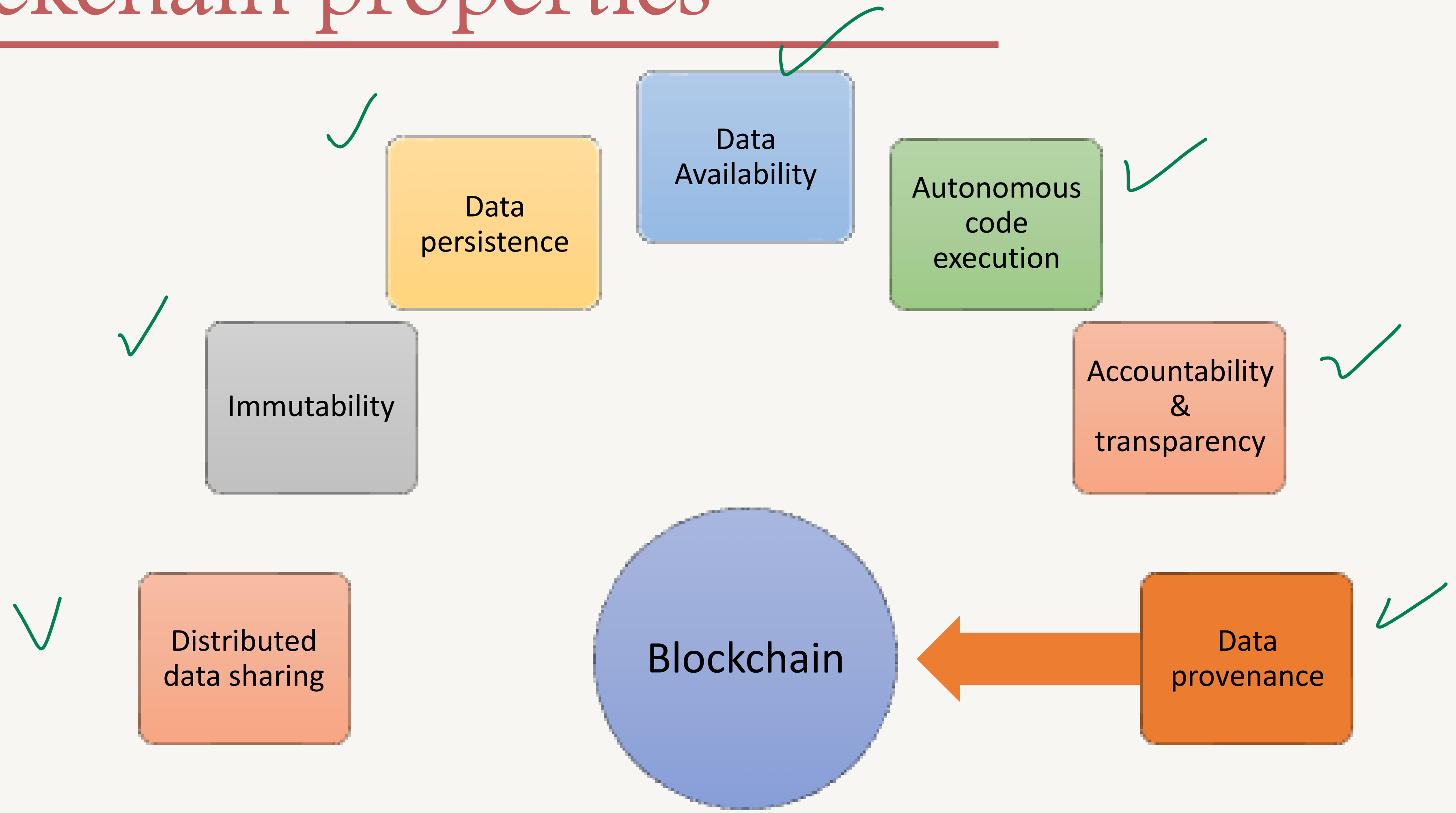
CSE446: Blockchain & Cryptocurrencies

Lecture – 17: Blockchain Properties, Misconception, Limitations and Feasibility

BRAC UNIVERSITY

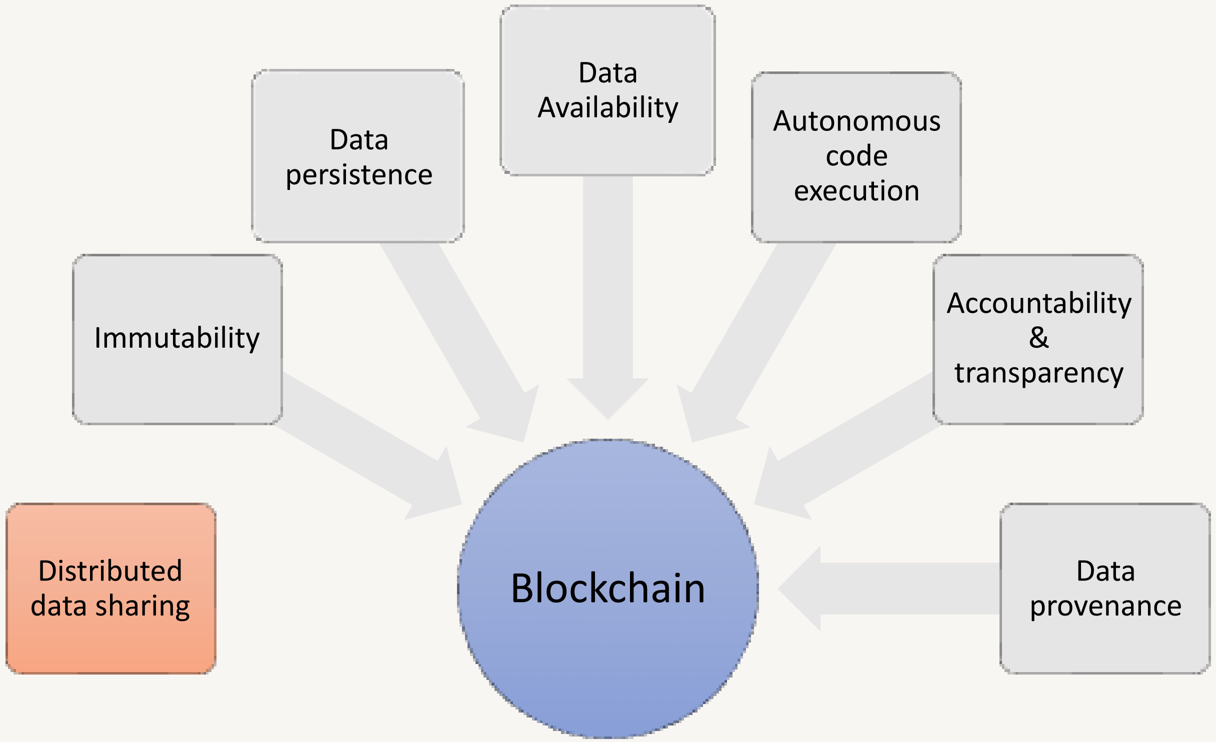
Inspiring Excellence

Blockchain properties



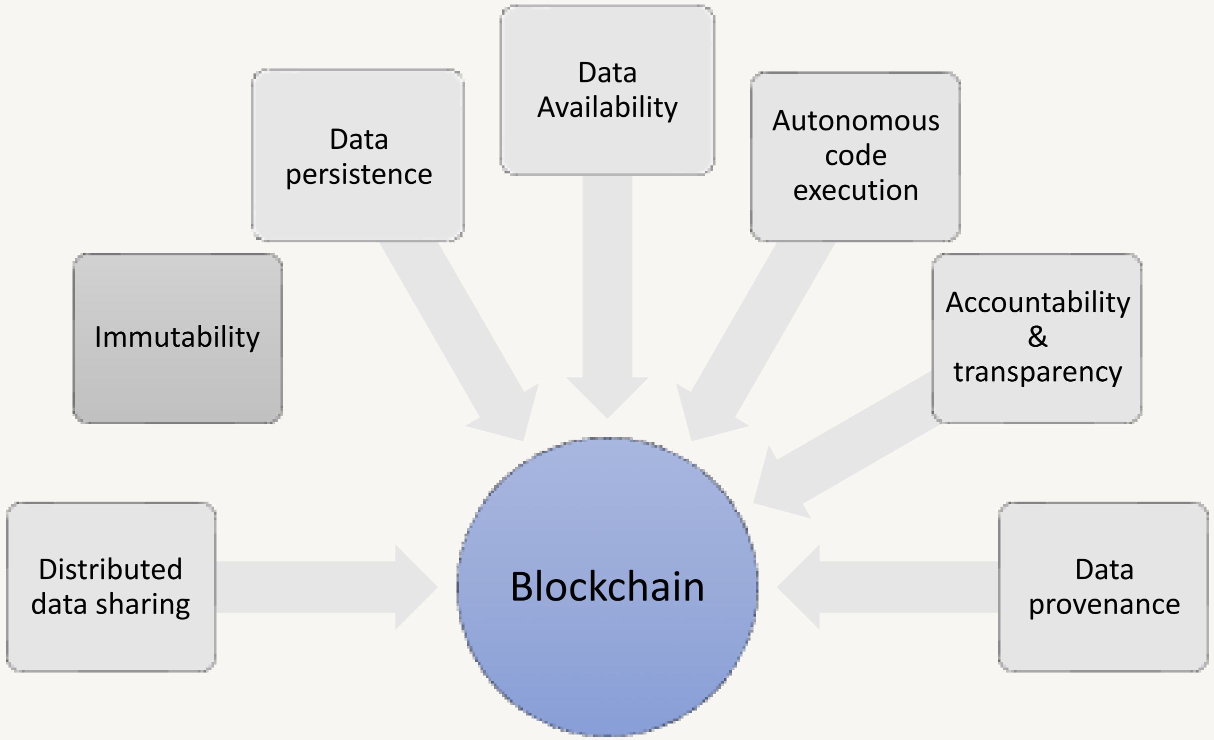
Distributed Data Sharing

- Blockchain data is distributed across multiple nodes
- The protocol ensures that data inserted in a particular node gets synced across all nodes in a timely fashion



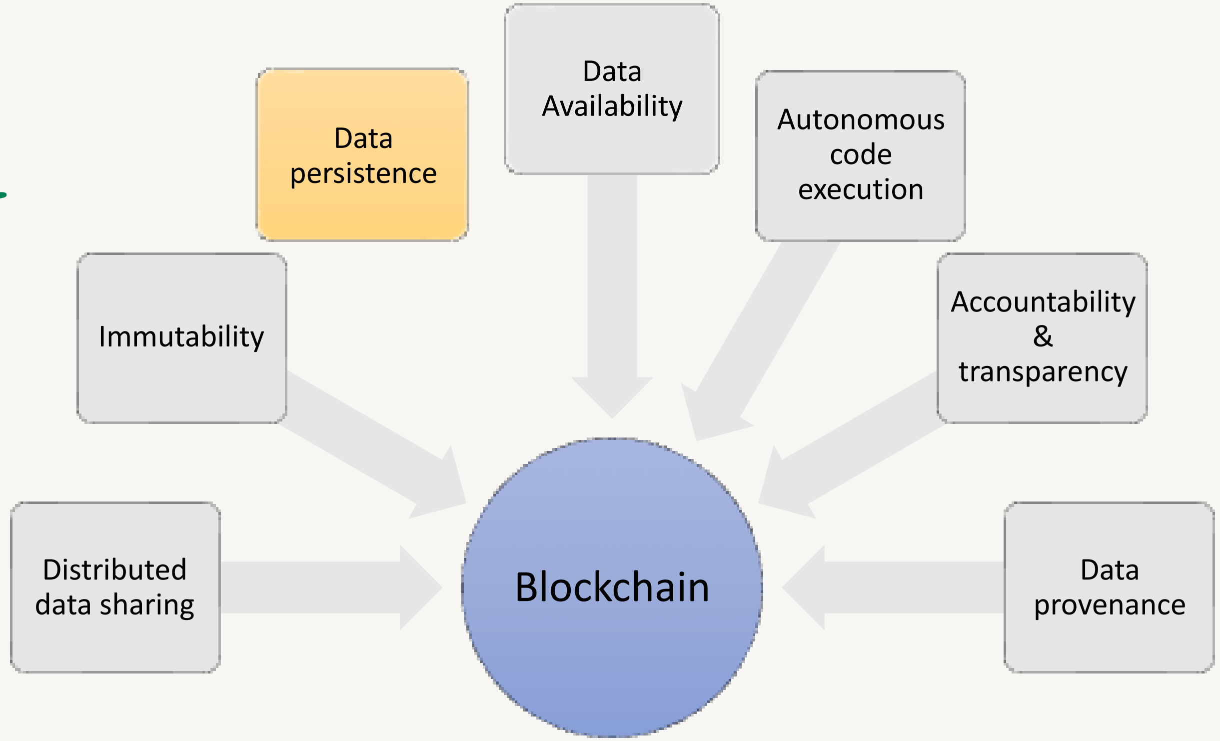
Immutability

- Data and code immutability in blockchain emerges from the fact that to change data/code inserted in a previous block, an attacker must posses either
  - significant computational power, in case of a public blockhain
  - or compromise the majority of nodes in any type of blockchain



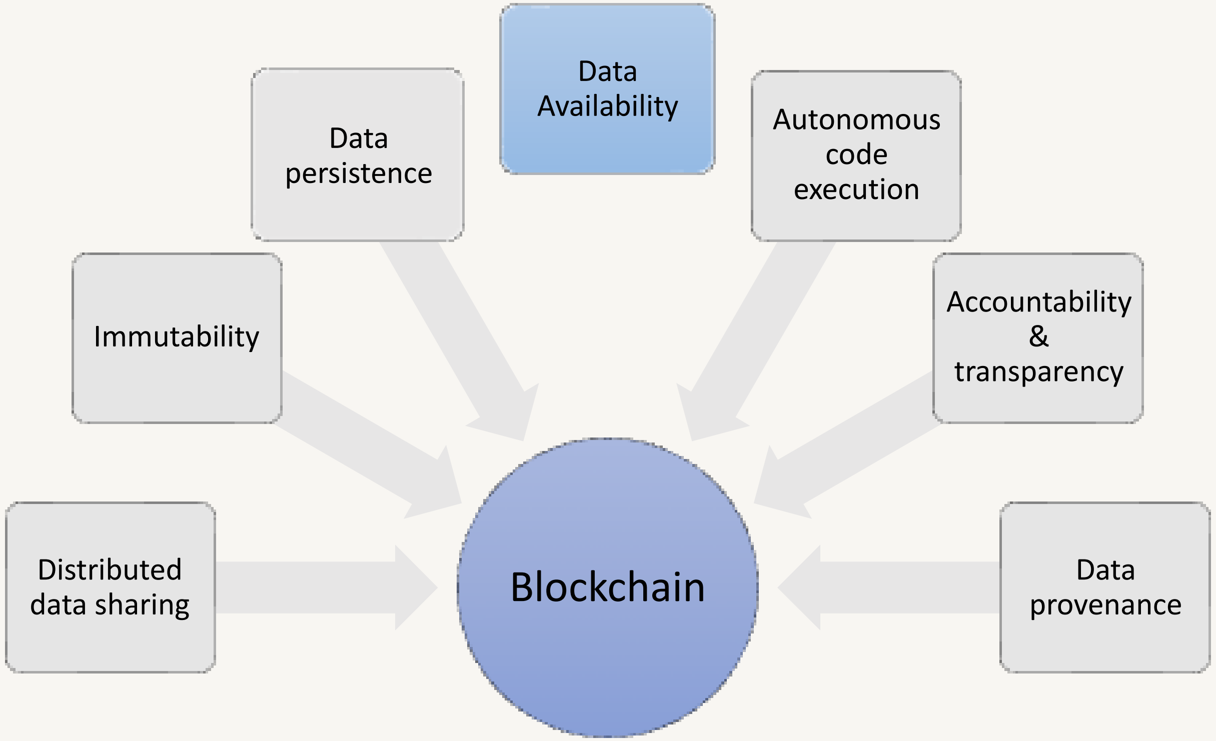
Data persistence

- Being a distributed system implies that data in a blockchain will persist as long as there are enough nodes to execute the protocol in a secure way



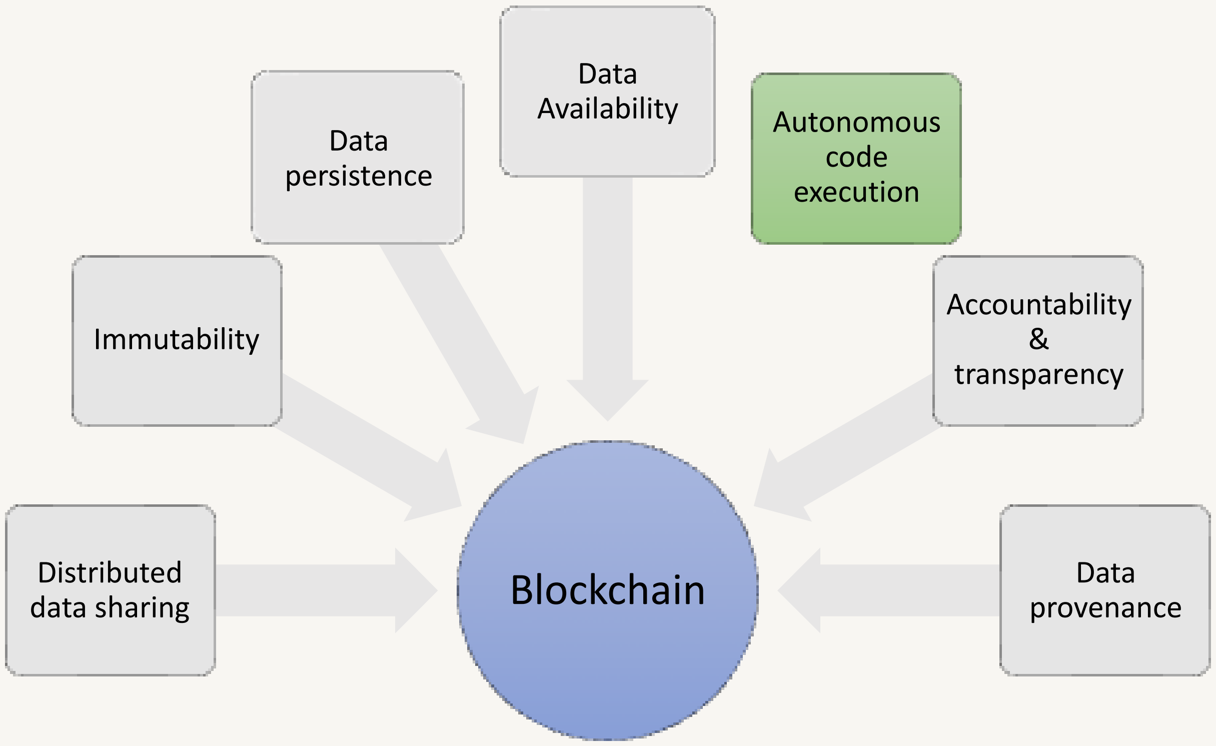
Data availability

- Data in blockchain are always available
- Even when a particular node is offline, data can be retrieved from another node in the blockchain



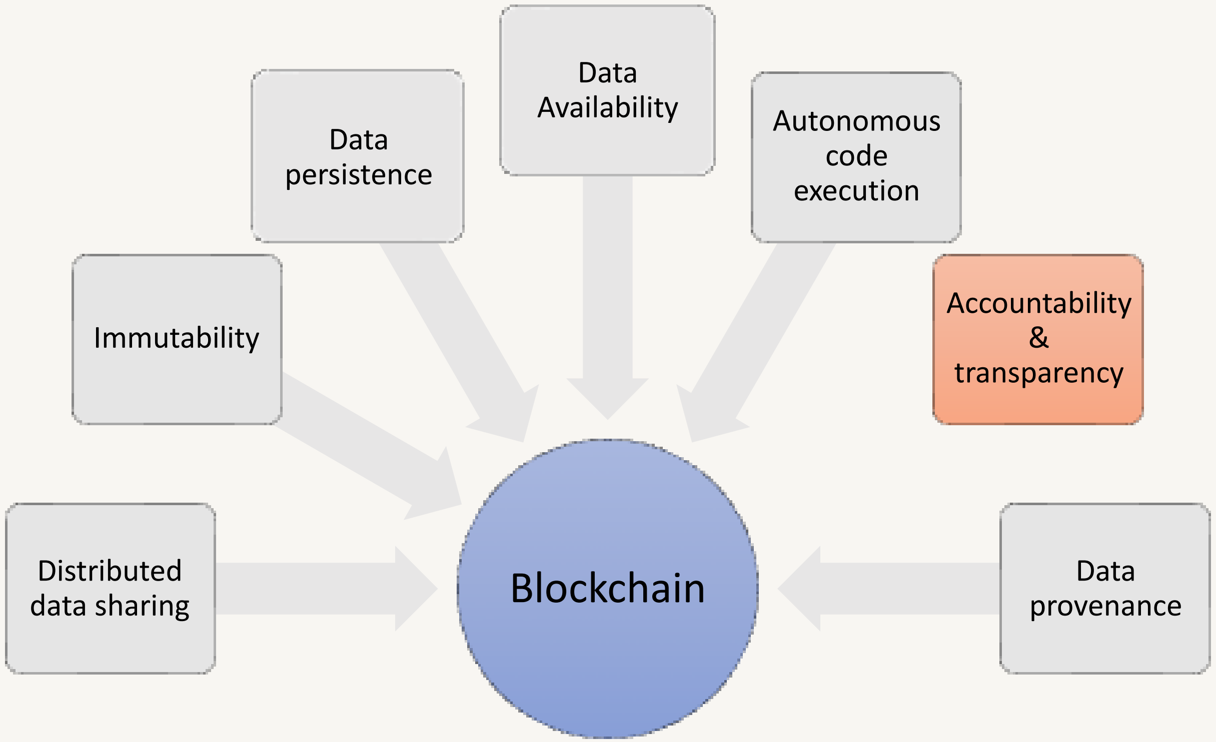
Autonomous code execution

- A smart-contract will facilitate autonomous code execution without a single point of failure
- It does not require any human intervention
  - anyone can submit a transaction to execute a code
- For any private blockchain system, anyone authorised can execute a code



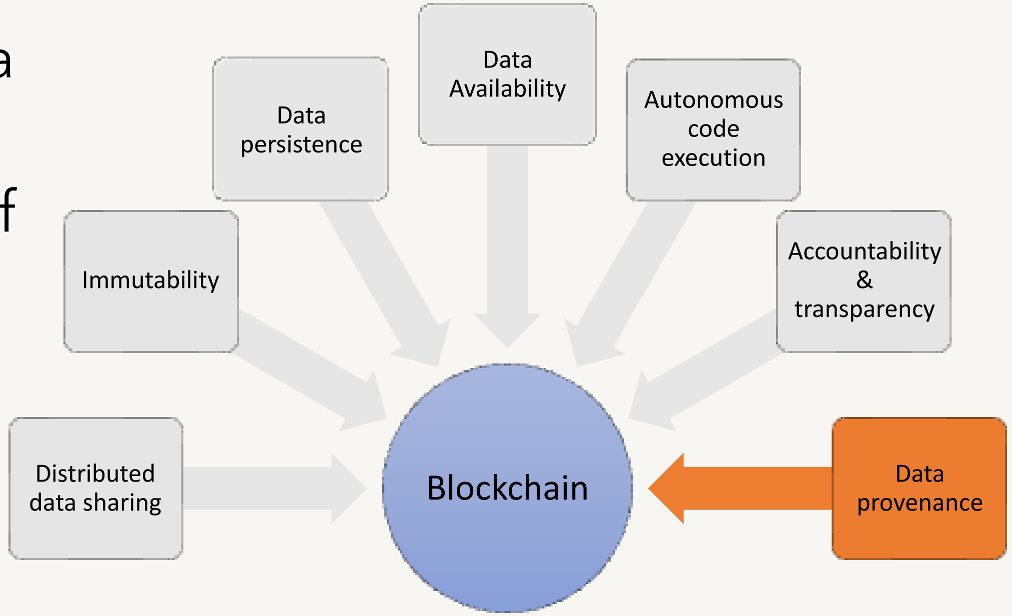
Accountability and transparency

- All authorised entities can verify each single transaction which can ensure accountability and transparency



Data provenance

- The term "data provenance" refers to a record trail that accounts for the origin of a piece of data (in a database, document or repository) together with an explanation of how and why it got to the present place
- Data in a blockchain can only be stored with a signed transaction
- Blockchain also stores the transactions which might have changed the data
- Both of these ensure data provenance



Blockchain misconception

DATA IMMUTABILITY

LARGE-SCALE DATA STORAGE

DATA INTEGRITY

DATA ENCRYPTION

POWER CONSUMPTION

Data immutability misconception

- Blockchain data can be never be changed
- This is true for transaction/blockchain data which are immutable
- However, smart-contract data can be changed as required
  - Remember we could change different variable values in the smart-contract
  - However, how such data is changed is recorded in the blockchain and hence, is immutable

DATA IMMUTABILITY

Large-scale data storage misconception

- Blockchain provides integrity of data and hence, users are tempted to store large amount of data in blockchain to ensure integrity
- Performance of any database in terms of data access rate is much better than that of any blockchain system
- Also storing a large amount of data in a public blockchain is costly
- Thus, it is advisable to store as minimum data as possible in the blockchain

LARGE-SCALE DATA STORAGE

Data integrity misconception

- People think blockchain can support data integrity for any type of data
- However, it must be remembered that a blockchain system is essentially a "*Garbage-in-garbage-out*" system
- A corrupted data will be stored and remain as corrupted
- It can guarantee the integrity of data only after it is stored in the blockchain

DATA INTEGRITY

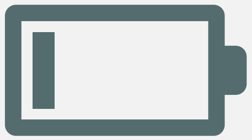
Data encryption misconception

- Many believe that a blockchain provides data encryption by default
- A blockchain system strongly depends on cryptographic mechanisms, such as digital signature and cryptographic hash, to function
- Digital signature is used for data provenance while a cryptographic hash is used to ensure data integrity
- In a blockchain system, data encryption is not provided

DATA ENCRYPTION

Power consumption misconception

- Many believe that every blockchain system consumes a huge amount of power
- However, the reality is that only public blockchain systems which utilise PoW or similar consensus algorithms consume huge electricity
- Public blockchain systems with PoS or DPoS consume significantly less electricity
- The power consumption of any private blockchain system will be comparable to any existing system



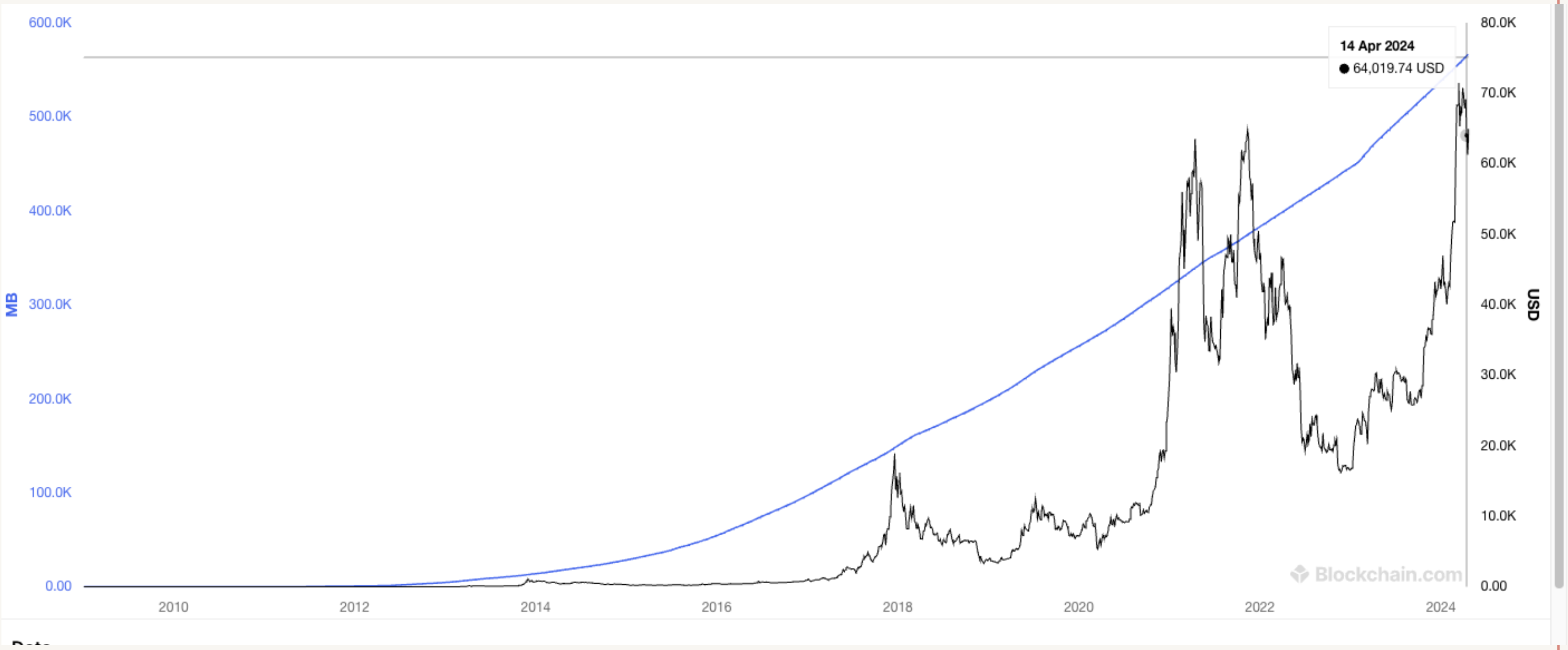
POWER CONSUMPTION

Blockchain limitations

- Blockchain bloating
- Blockchain scaling
- Code immutability
- Associated expense

Blockchain bloating

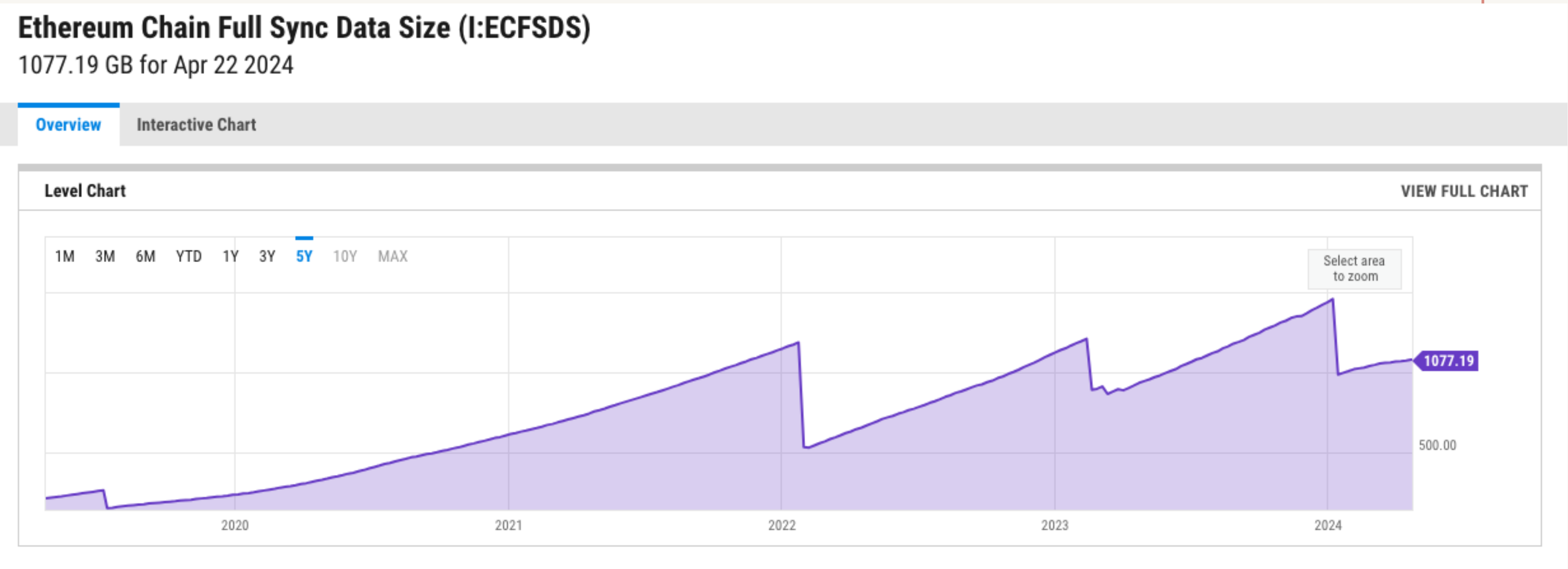
- Blockchain being an add-only distributed database, its size keeps increasing
- Bitcoin size is currently more than 500 GB and increasing



https://www.blockchain.com/explorer/charts/blocks-size

Blockchain bloating

- Ethereum size is currently >1TB and increasing
- What will happen in 20/30/50 years?
- Blockchain bloating would also increase data processing time
  - Finding a particular UTXO and so on



https://ycharts.com/indicators/ethereum_chain_full_sync_data_size

Blockchain scaling

- The blockchain scalability problem refers to the limited capability of the blockchain network to handle large amounts of transactions on its platform in a short span of time
- This limited capability is due to two reasons:
  - Limitations in block size: some blockchains have fixed block size
  - Limited TPS (transaction per second)
    - Fixed block size implies that the respective blockchain accommodate fewer transaction, resulting in lower TPS

Code immutability

- Once a smart-contract is deployed it becomes immutable
- This has huge advantage, however, it also introduces limitations
- If there is a bug in a smart-contract it cannot be rectified
- The error needs to be fixed off-chain and then re-deployed in the network
  - This will result in a new contract address
- The Dapp then needs to be updated with the new contract address

Associated expense

- It takes considerable investment to join the mining and staking process
- Storage and computation costs crypto-currency (eth)
- In a 2018 estimation:
  - When 1 ETH = 200 USD
  - 1 KB required 2 USD
  - 1 MB would cost around 2000 USD
- But now, 1 ETH ~3100 USD
  - It is very difficult to predict, how much it might cost
  - One option is to try via Ganache or in the test network

Blockchain feasibility

DECENTRALI
SATION

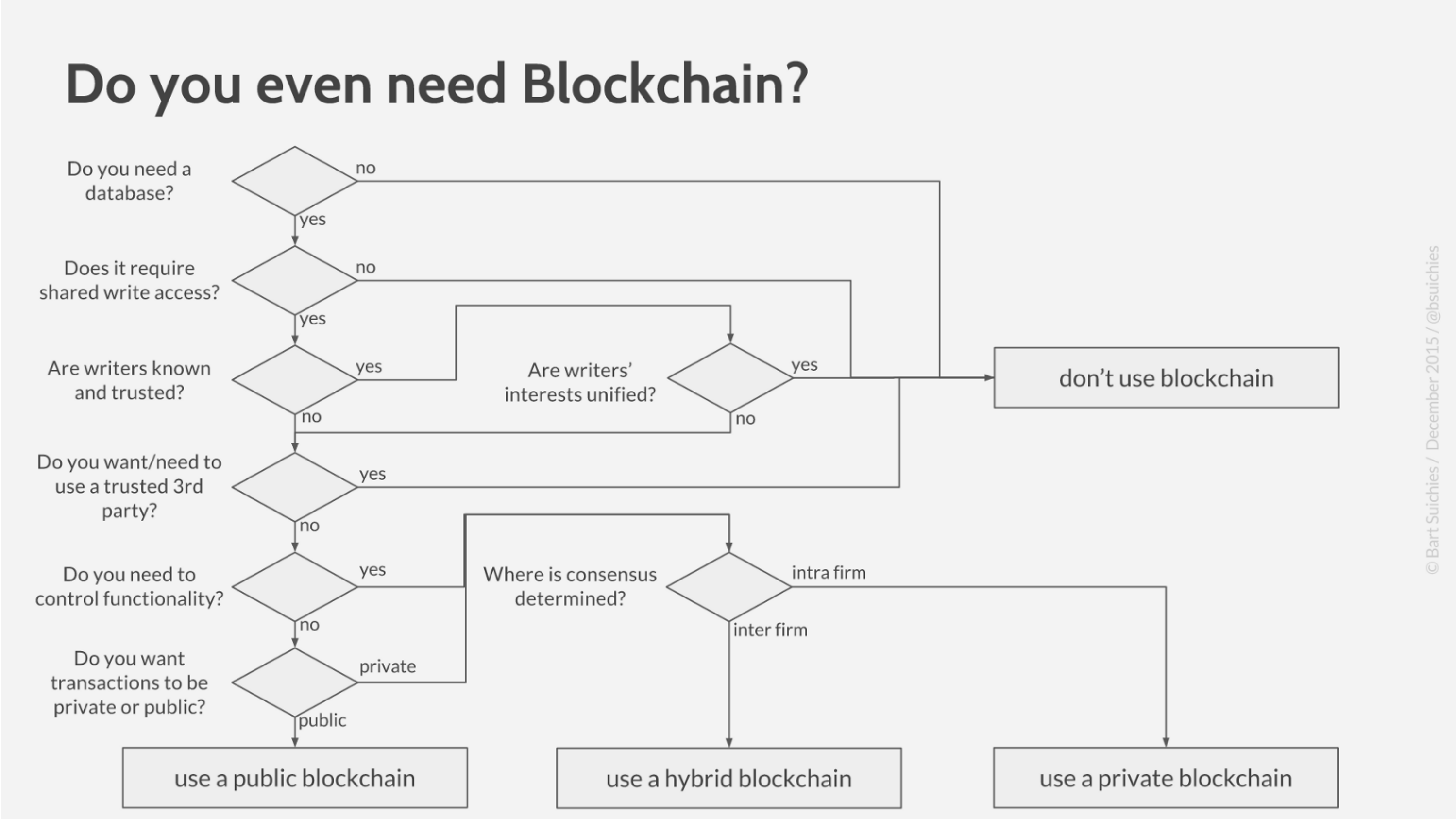
DISINTERME
DIATION

P2P VALUE
TRANSFER

DATA/CODE
IMMUTABILITY

DISTRIBUTED
DATA SHARING

Blockchain feasibility



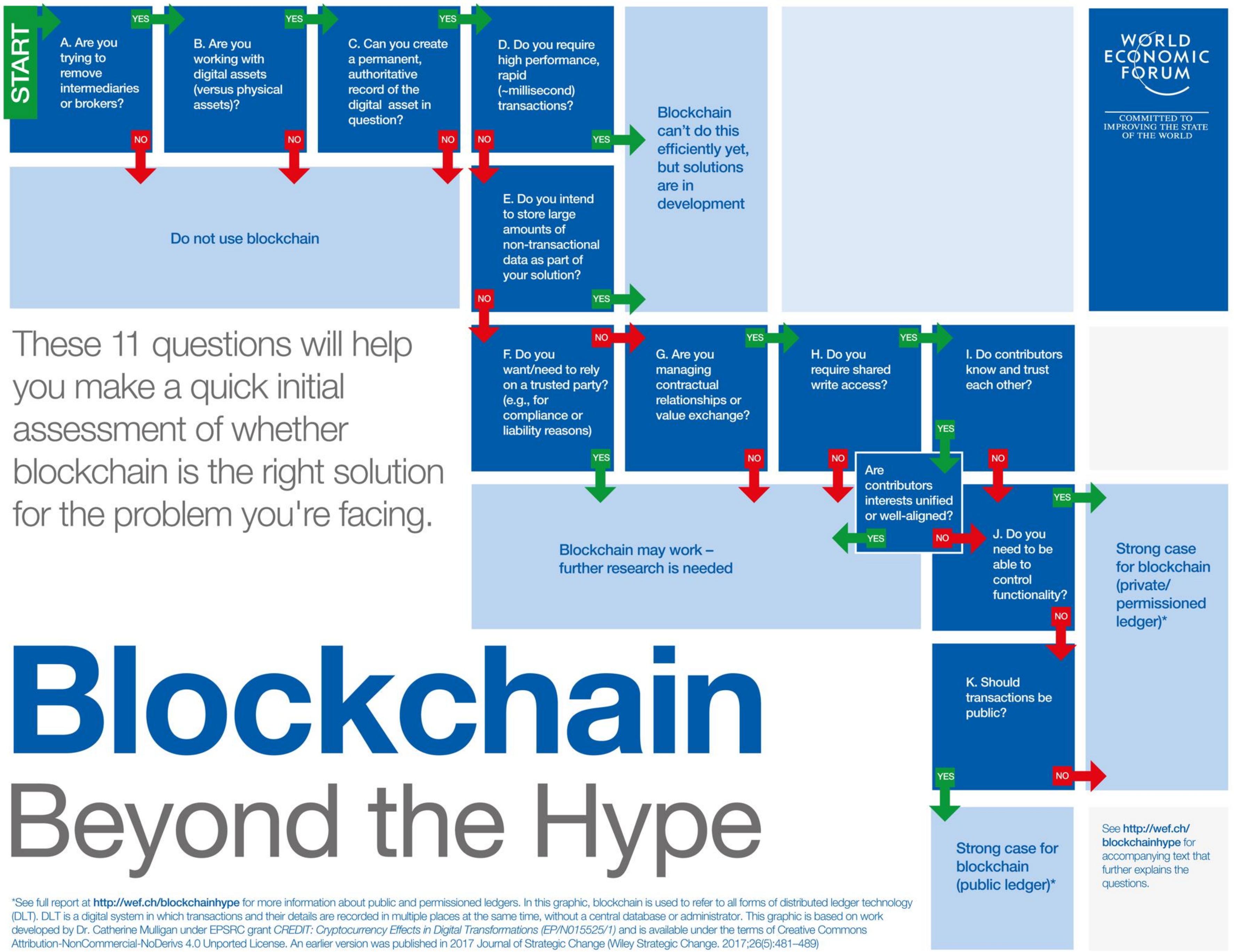
Bart Suichies model

https://medium.com/@bsuichies/why-blockchain-must-die-in-2016-e992774c03b4

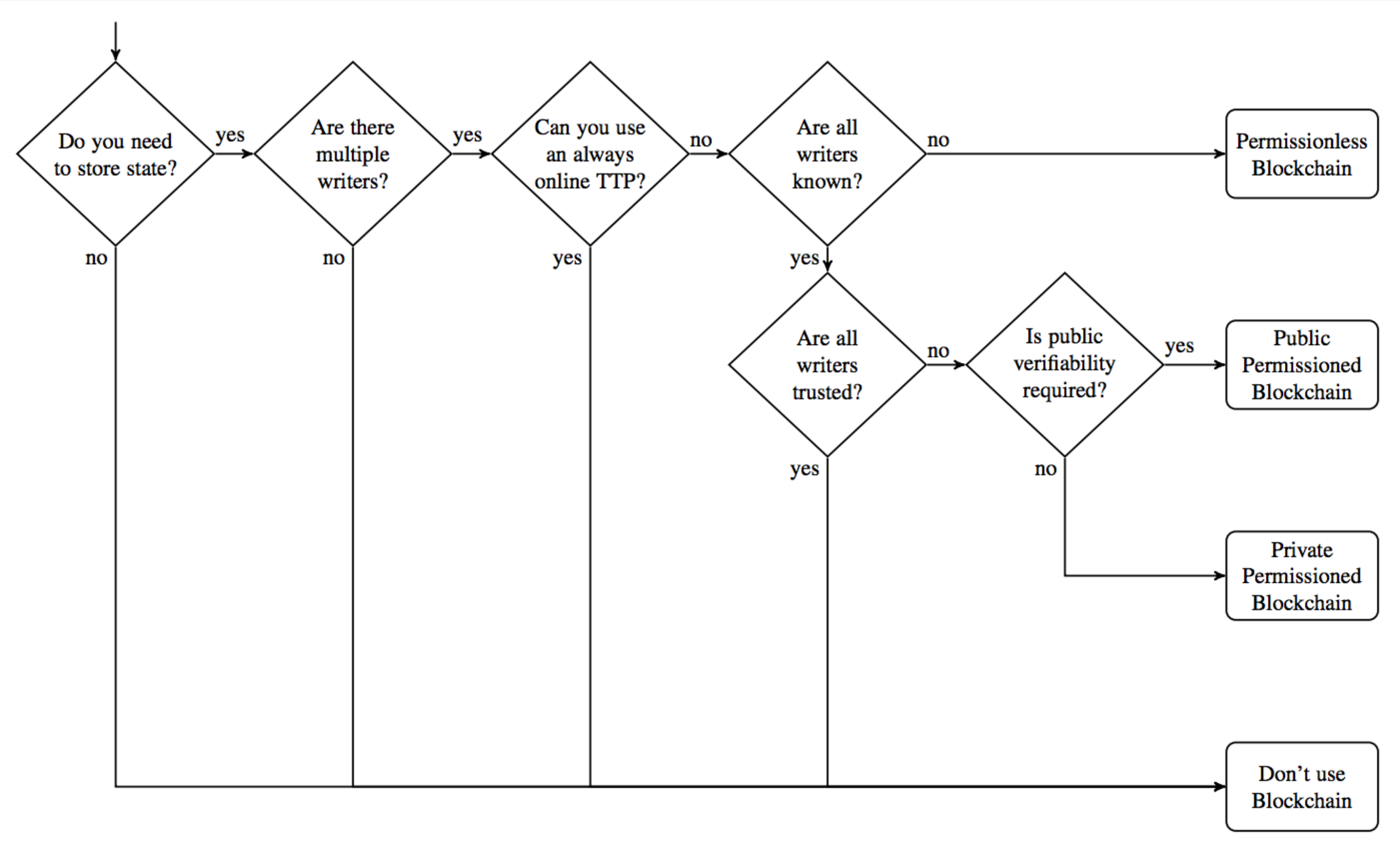
Blockchain

WEF Model

https://www.weforum.org/agenda/2018/04/questions-blockchain-toolkit-right-for-business

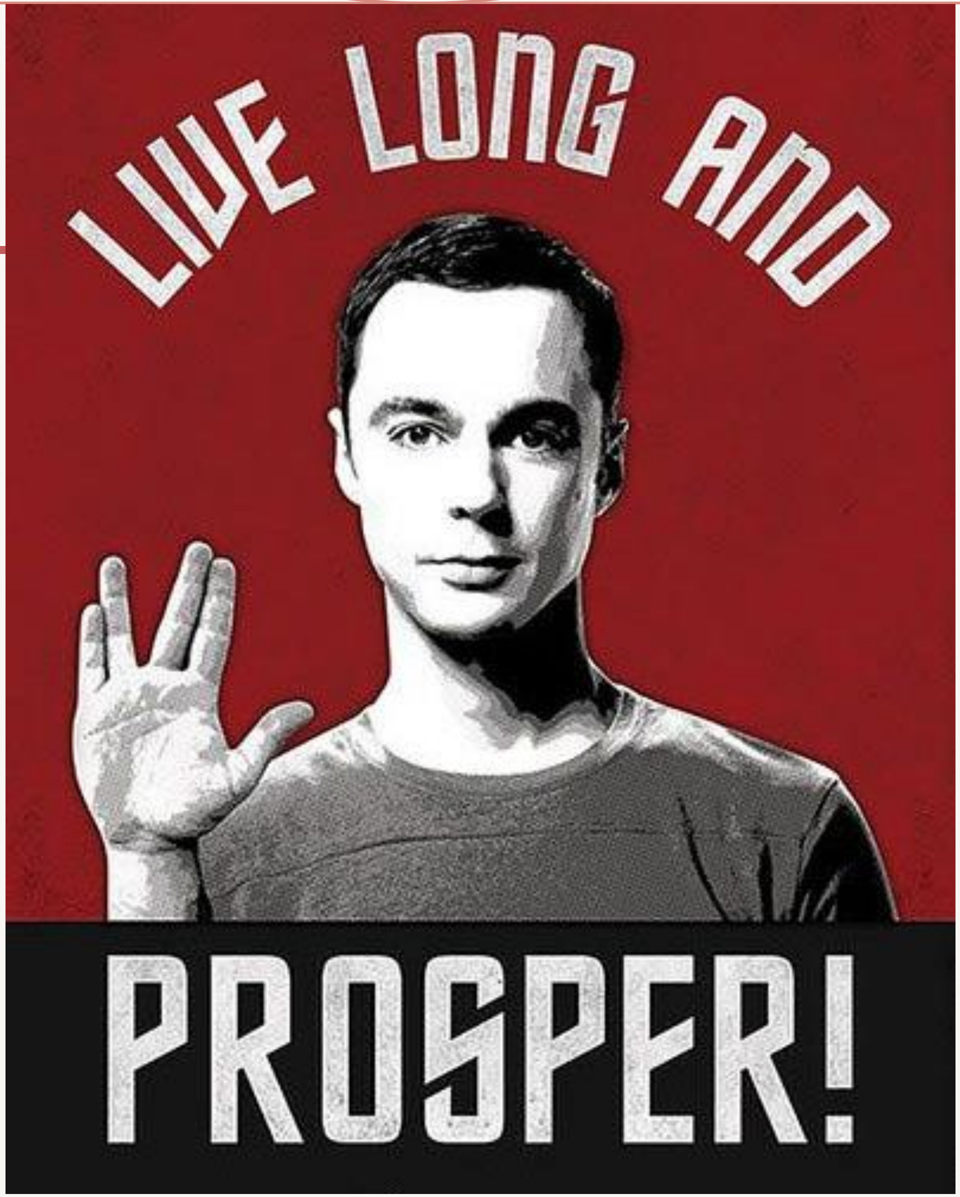


Blockchain feasibility



Model by Karl Wüst & Arthur Gervais

Wüst, Karl, and Arthur Gervais. "Do you need a Blockchain?." IACR Cryptology ePrint Archive 2017 (2017): 375.


LIVE LONG AND
PROSPER!