BLOCKCHAIN

Wanxing Dai

University of Illinois at Urbana-Champaign

INFORMATICS
BUSINESS
ANTHROPOLOGY

01

HISTORY

BITCOIN

02

STRUCTURE

HOW DOES IT WORK

03

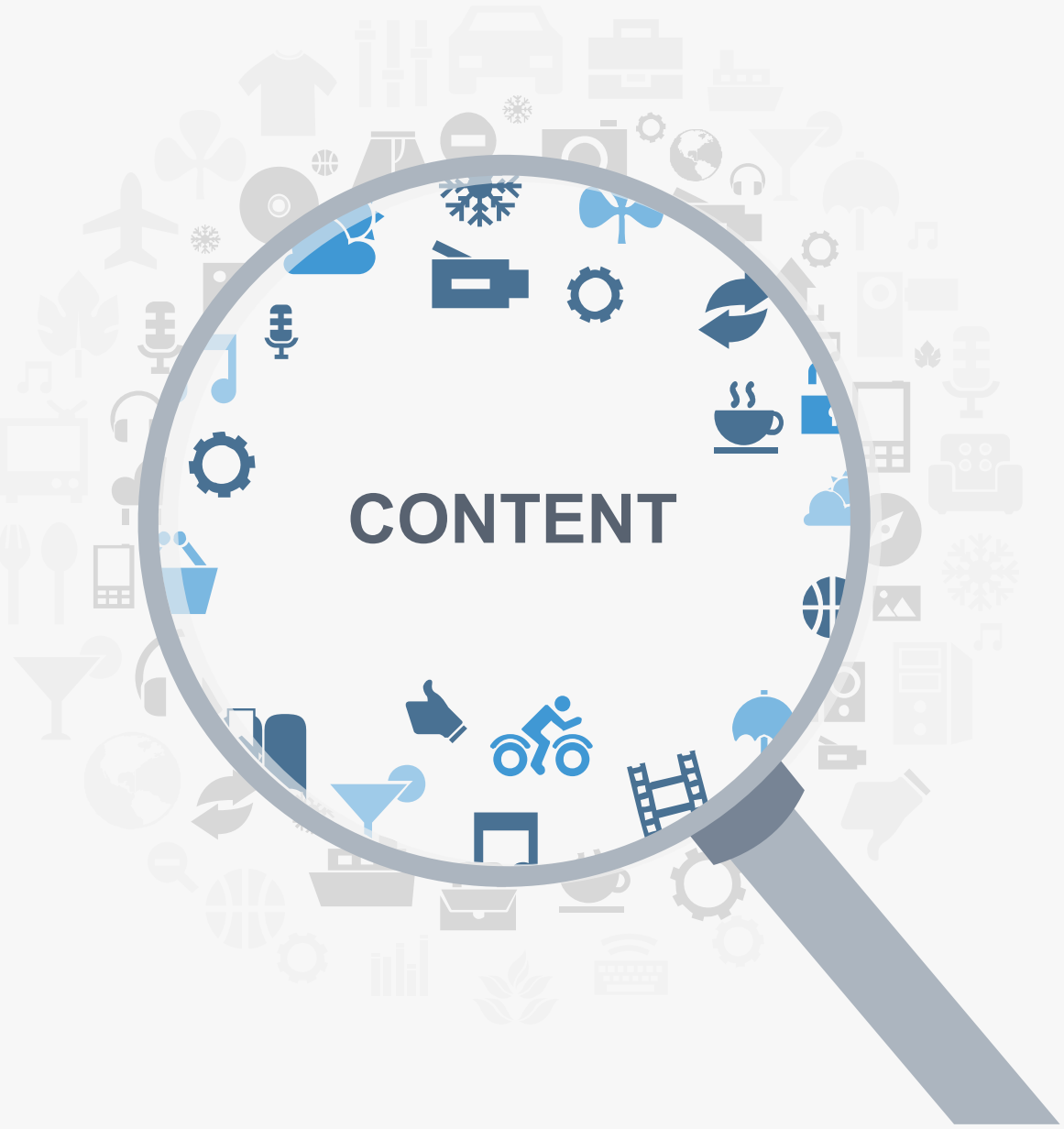
APPLICATION

FINANCIAL SERVICES

04

CHALLENGES

FUTURE USE



1 HISTORY

The shortcomings of current transaction systems

The birth of blockchain

HISTORY

Est. time	Circa 500 AD	Circa 700 AD	11th Century	21st Century	Future
Trust guarantor	Tribal chef/ headman of king	Central authority	State or bank	Central bank and commer-cial banks	Decentralised computer network
Collective ledger	Tribal chef's memory	Tallies	Balance sheet/paper register	Independent electronic ledgers	Distributed, shared public ledger
Issuer	Tribal chief	Central authority	Bank	Central bank	Digital currency algorithm
Token for money	Rai stone	Diamonds and precious metals	Fiat money	Fiat money + digital money as banks/credit cards	Digital currency

HISTORY

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

Satoshi Nakamoto

HISTORY

Cost-effectiv e

Bitcoin eliminates the need for intermediaries

Safe

The underlying ledger is tamper-evident.

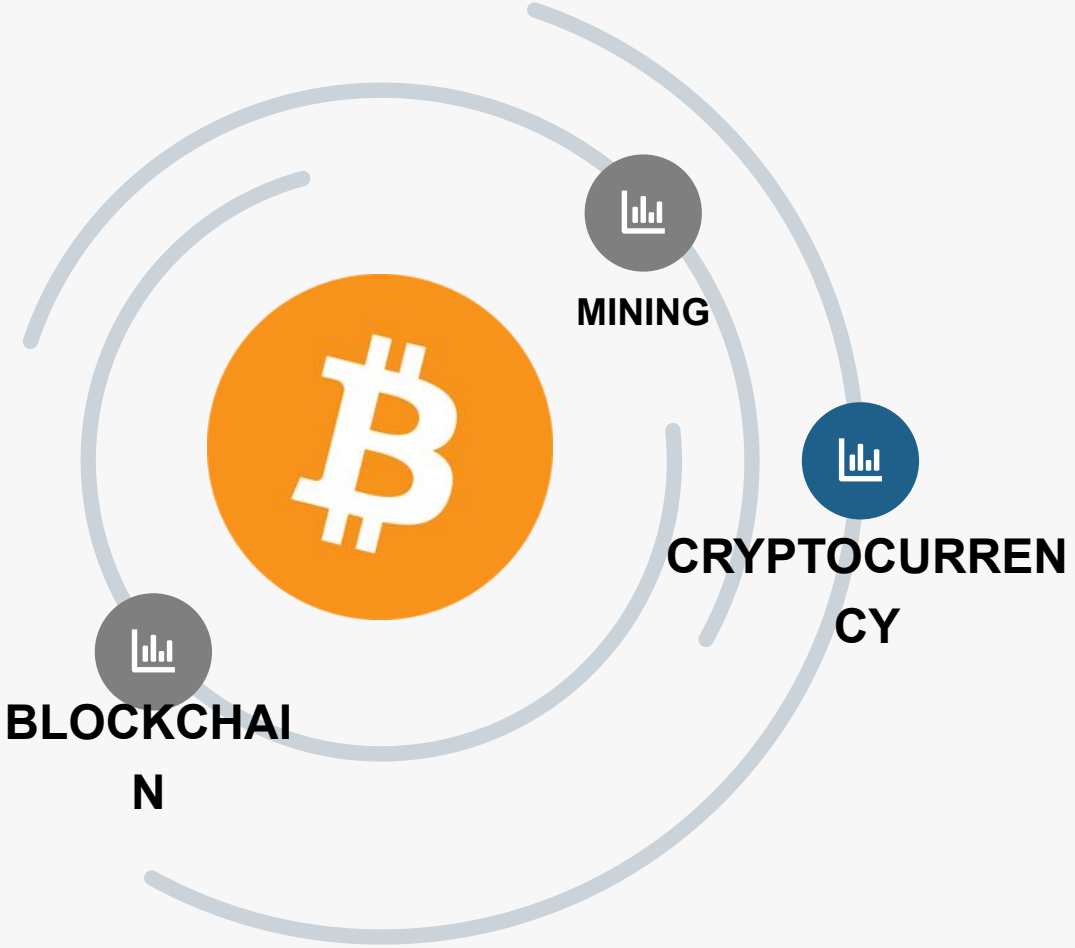
Efficient

Transaction information is recorded once and is available to all parties

Secure

A transaction can only be reversed with another transaction, in which case both transactions are visible.

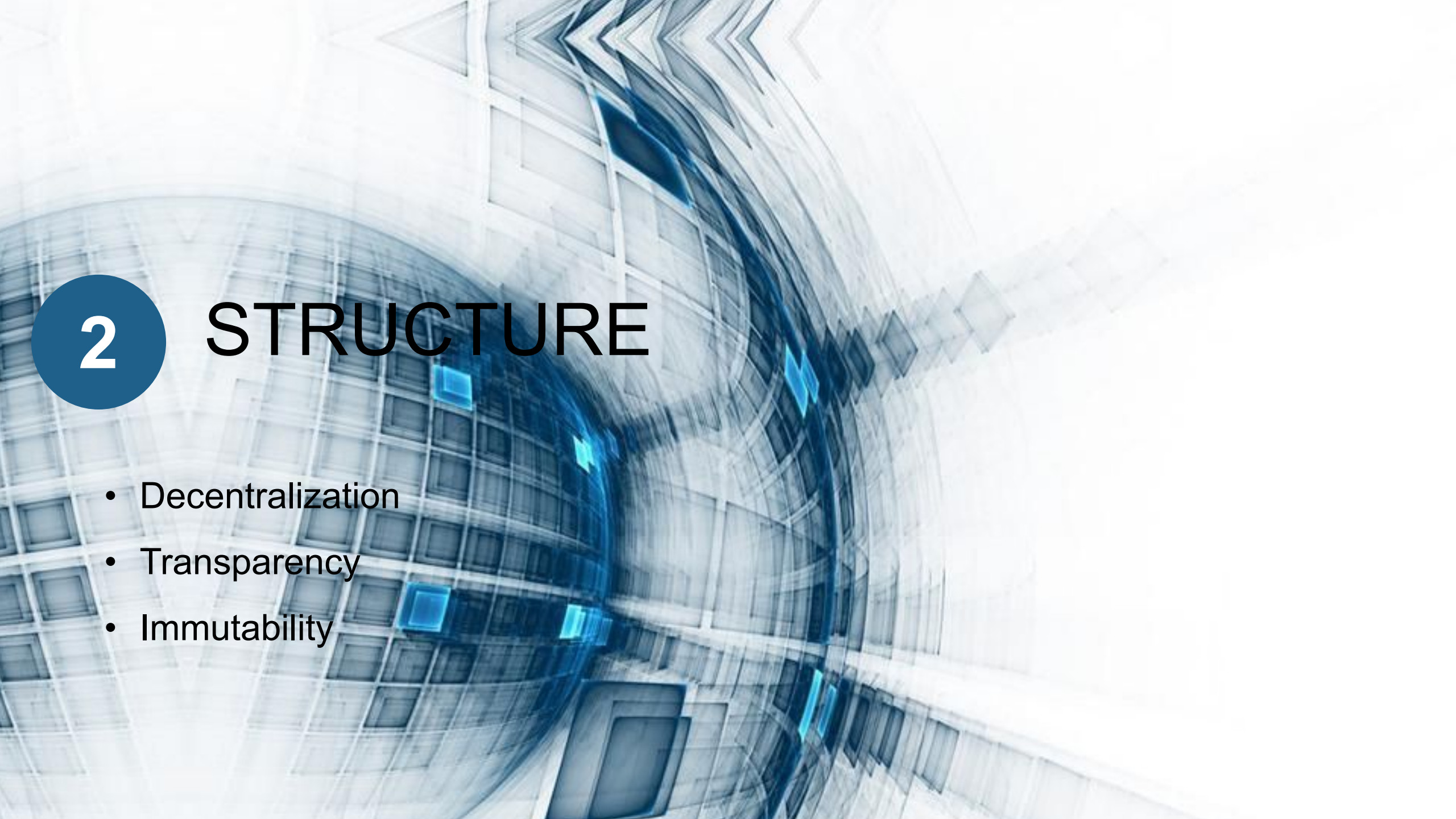
HISTORY



Bitcoin

≠

Blockchain



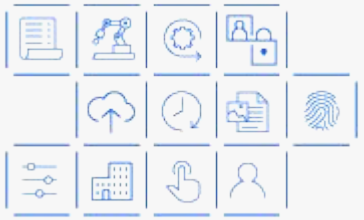
2 STRUCTURE

- Decentralization
- Transparency
- Immutability

STRUCTURE

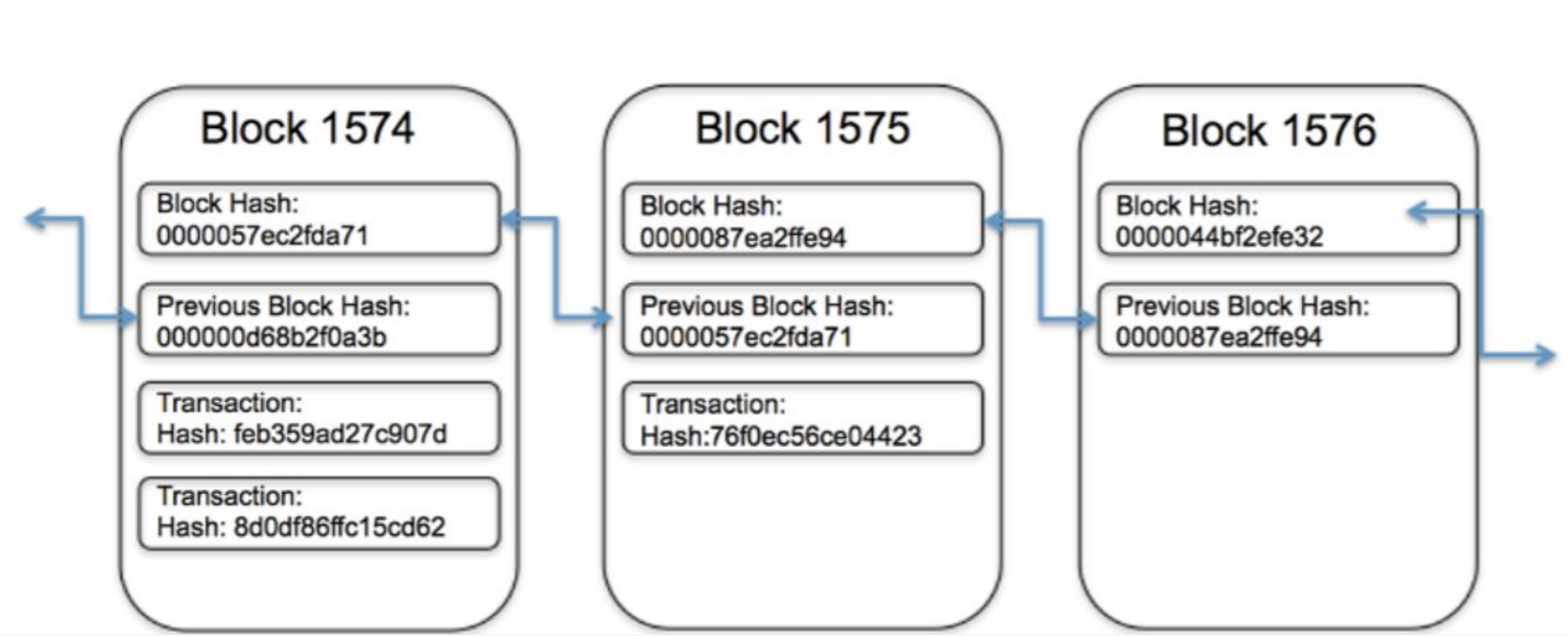
As each transaction occurs, it’s put into a block.

Each block is connected to the one before and after it.



Transactions are blocked together,
creating an irreversible chain.

STRUCTURE

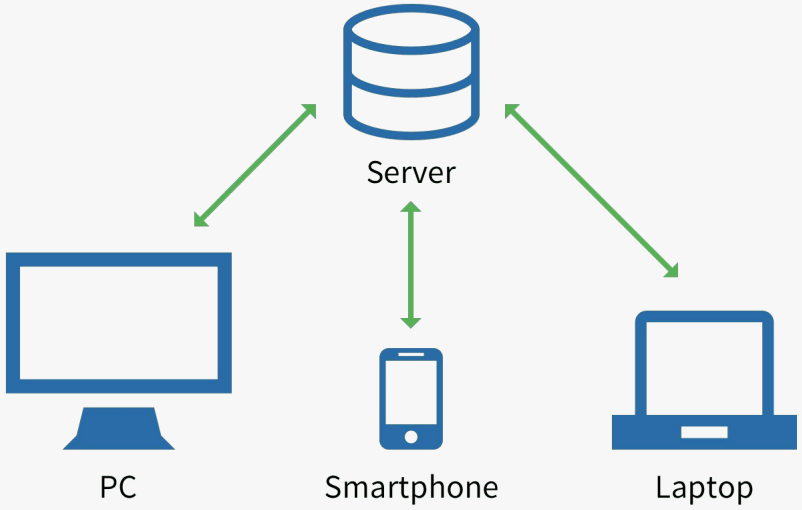

Block 1574
Block Hash:
0000057ec2fda71
Previous Block Hash:
000000d68b2f0a3b
Transaction:
Hash: feb359ad27c907d
Transaction:
Hash: 8d0df86ffc15cd62
Block 1575
Block Hash:
0000087ea2ffe94
Previous Block Hash:
0000057ec2fda71
Transaction:
Hash:76f0ec56ce04423
Block 1576
Block Hash:
0000044bf2efe32
Previous Block Hash:
0000087ea2ffe94

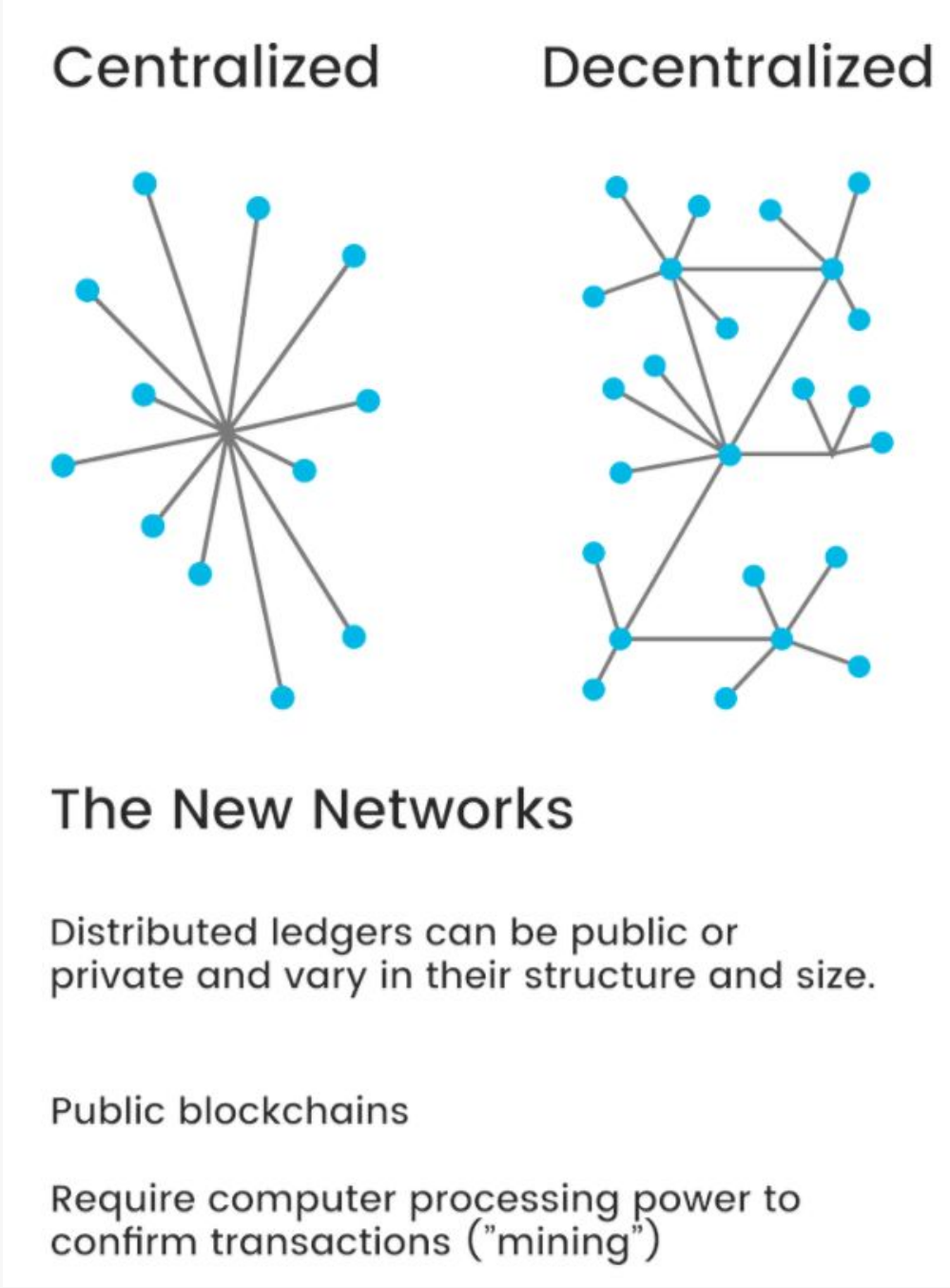
STRUCTURE

Decentr alization

TechTerms.com

Client-Server Model





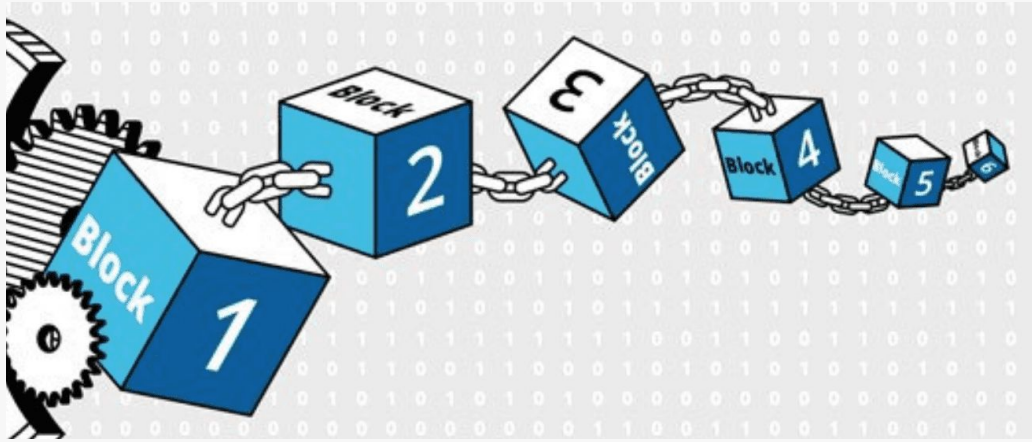
STRUCTURE

TRANSPARENCY

TxHash	Block	Age	From		To	Value	[TxFee]
0x2d055e4585ae2a...	5629306	16 secs ago	0x003e3655090890...		0x2bdc9191de5c1b...	0.004741591554641 Ether	0.000294
0xb4d37c791ff4cde...	5629306	16 secs ago	0x6c3b4faf413e0e4...		0xf14cb3acac7b230...	0.744767225 Ether	0.000294
0x9979410dcb5f4c...	5629306	16 secs ago	0x99bcd75abbac05...		0x2d42ee86390c59...	0.016294 Ether	0.000294
0x189c4d4aae09be...	5629306	16 secs ago	0x175cd602b2a1e7...		0xd39681bb0586fb...	0.01 Ether	0.000294
0xda0e9bbb11fb77...	5629306	16 secs ago	0x73a065367d111c...		0x01995786f14357...	0 Ether	0.00150007
0x6be498fafad9acb...	5629306	16 secs ago	0xa3eb206871124a...		0x8a91cac422e55e...	0.029594 Ether	0.000294

STRUCTURE

Immuta bility



INPUT	HASH
This is a test	C7BE1ED902FB8DD4D48997C6452F5D7E509FBCDBE2808B16BCF4EDCE4C07D14E
this is a test	2E99758548972A8E8822AD47FA1017FF72F06F3FF6A016851F45C398732BC50C

STRUCTURE

It is not owned by a single entity, hence it is decentralized

The data is cryptographically stored inside

The blockchain is immutable, so no one can tamper with the data

The blockchain is transparent so one can track the data if they want to

3 APPLICATION

APPLICATION

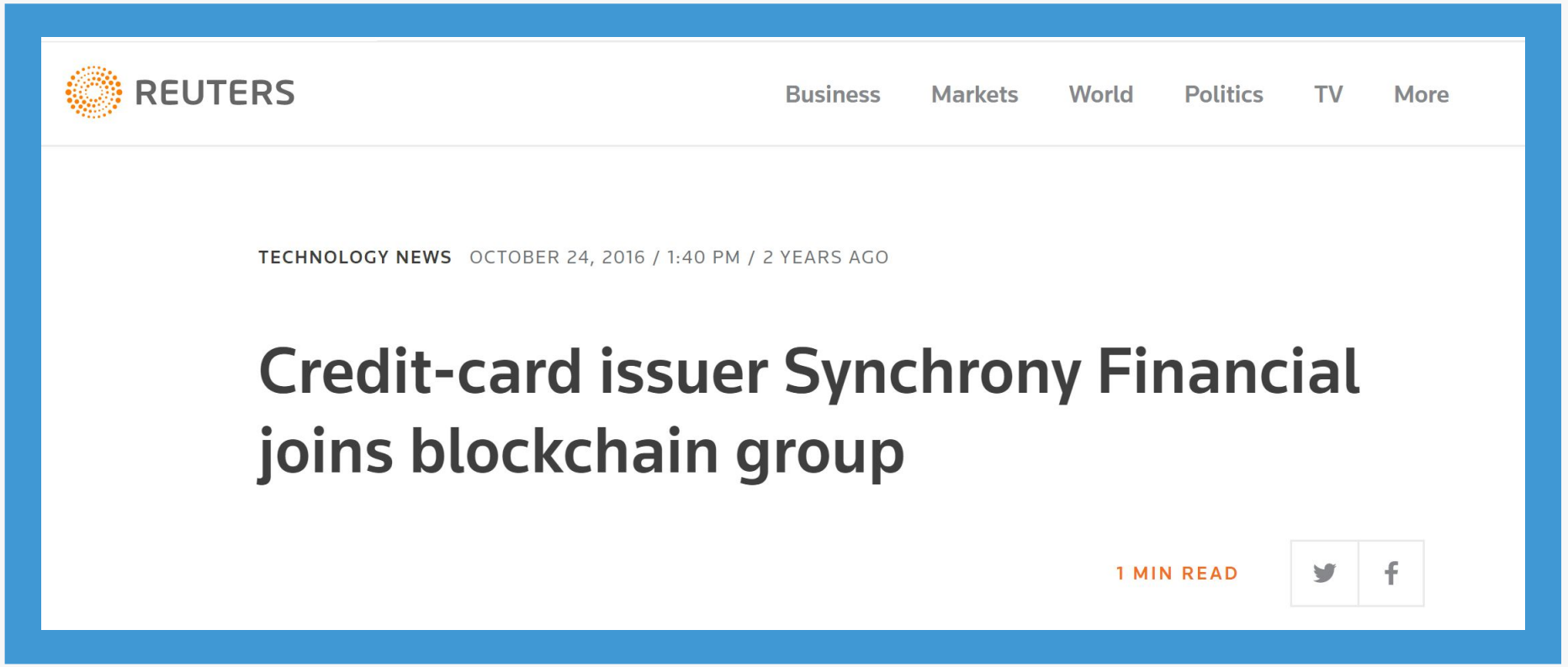
Supply Chain Management

- Secure
- Faster
- Publishing
- Sharing

APPLICATION

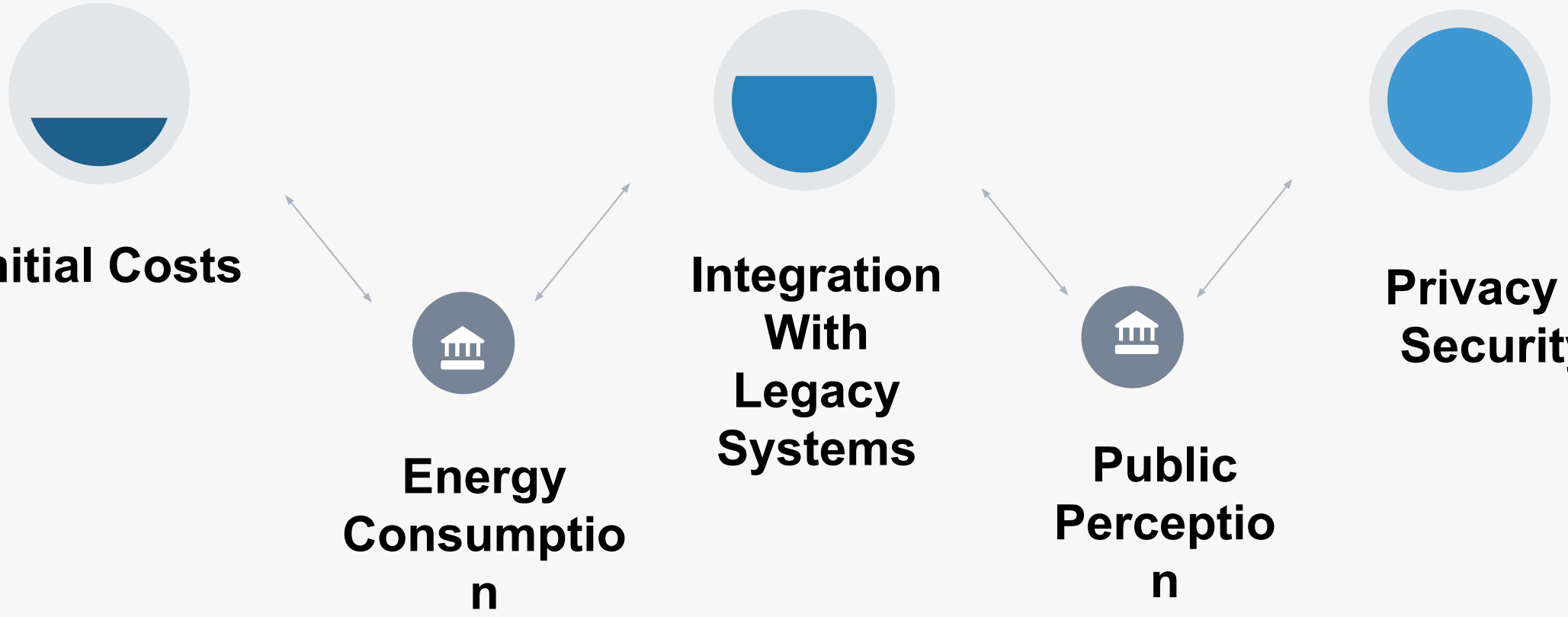
APPLICATION

DISTRIBUTED LEDGERS

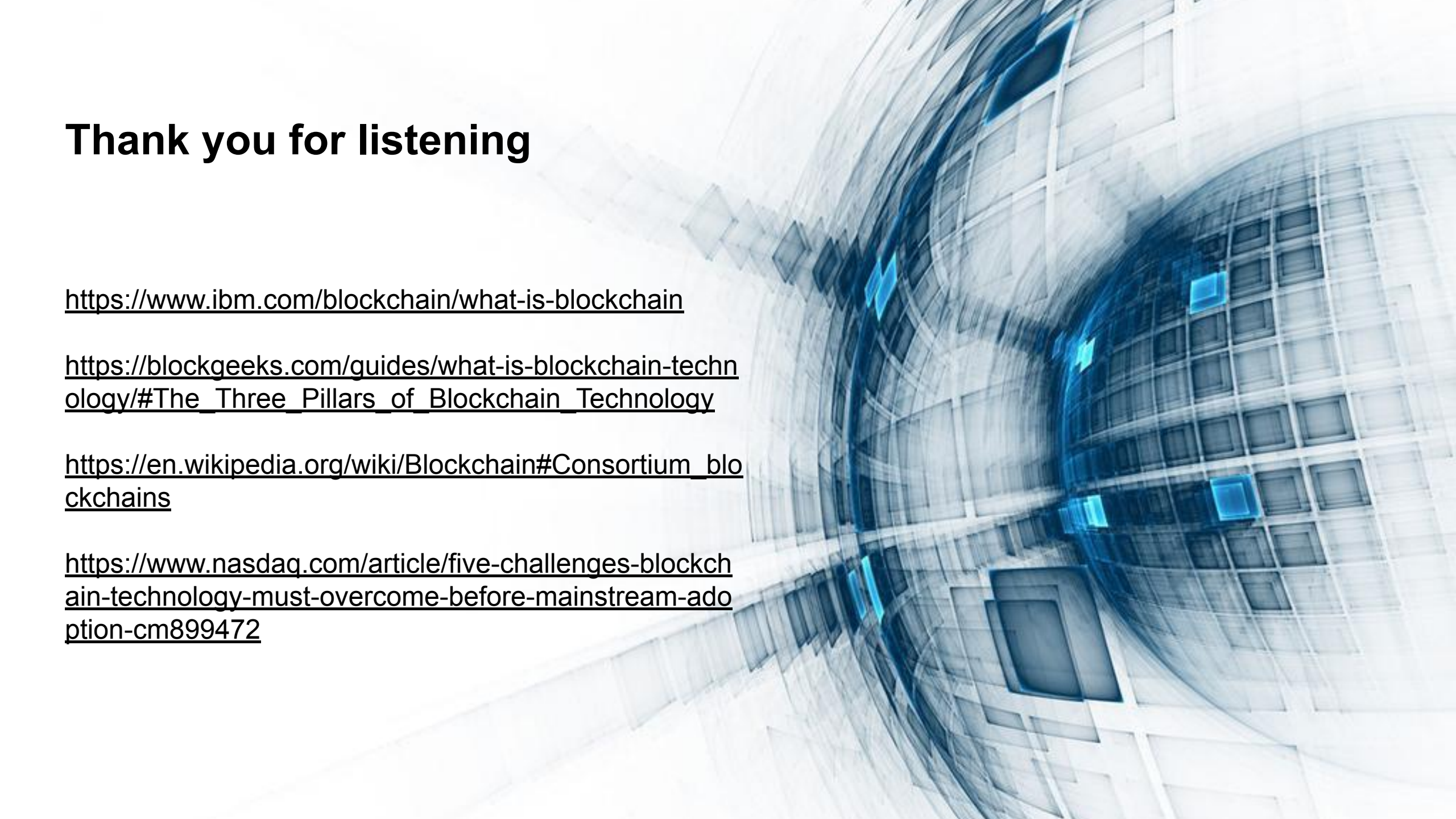


4 CHALLENGES

CHALLENGES


Initial Costs
Energy Consumption
Integration With Legacy Systems
Public Perception
Privacy & Security

Thank you for listening



https://www.ibm.com/blockchain/what-is-blockchain

https://blockgeeks.com/guides/what-is-blockchain-technology/#The_Three_Pillars_of_Blockchain_Technology

https://en.wikipedia.org/wiki/Blockchain#Consortium_blockchains

https://www.nasdaq.com/article/five-challenges-blockchain-technology-must-overcome-before-mainstream-adoption-cm899472


?
Q&A