KARABÜK UNIVERSITY

Blockchain from Hype to Reality

ADIB HABBAL, Ph.D.
Computer Engineering Department, Karabuk University
adibhabbal@karabuk.edu.tr



ICATCES 2019
Alanya, TURKEY, April 26-28, 2019

Disclaimer

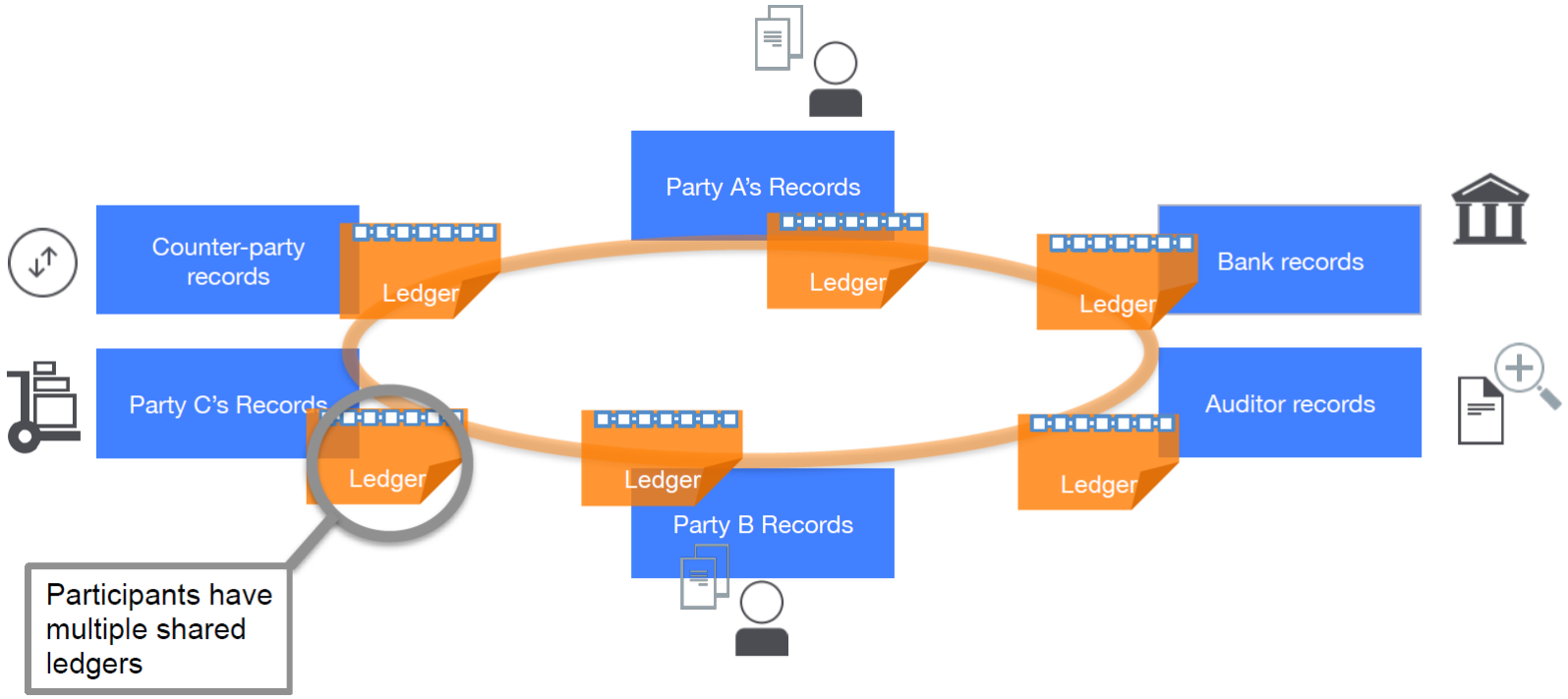
- This is not a Bitcoin introduction.
- Today there are various *flavors* of Blockchain.
- Lastly, no single Blockchain solution will fulfill all needs.

Agenda

- Blockchain Overview
- Benefits of Blockchain
- How Blockchain Works
- Types of Blockchain
- Blockchain Use Cases
- Blockchain Challenges
- Future Direction

Blockchain Overview

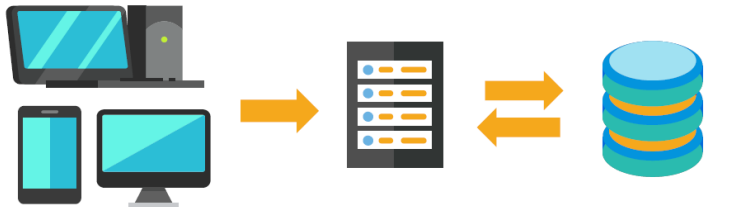
- A distributed, shared ledger



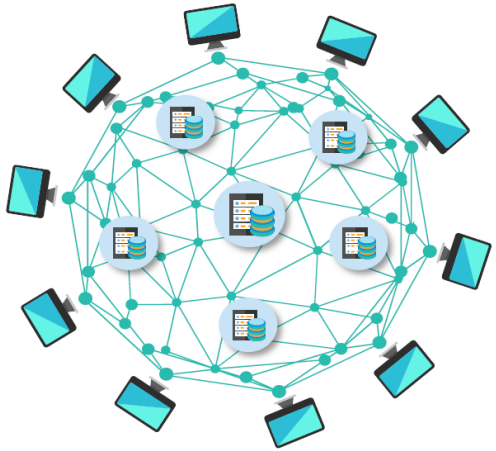
2016 IBM Corporation

Blockchain Overview

A distributed ledger that is secure & encrypted, hack-proof, tamperproof (immutable), scalable and low cost to deploy and thereby creating a trusted network for any transaction to go through.



Conventional Centralized Database



- Distributed Ledger
- Scalable
- Immutable
- Hackproof
- Encrypted
- Low cost

2018 nem Foundation

Blockchain Overview



Technical Definition	Economical-semi-technical Definition	Financial-accounting Definition
A blockchain is a linked list that is built with hash pointers instead of regular pointers	A blockchain is an open*, borderless, decentralized, public, permissionless, immutable record of transactions	A blockchain is a public, distributed ledger of peer-to-peer transactions

* All terms in **red** are open to debate

Benefits of Blockchain Technology

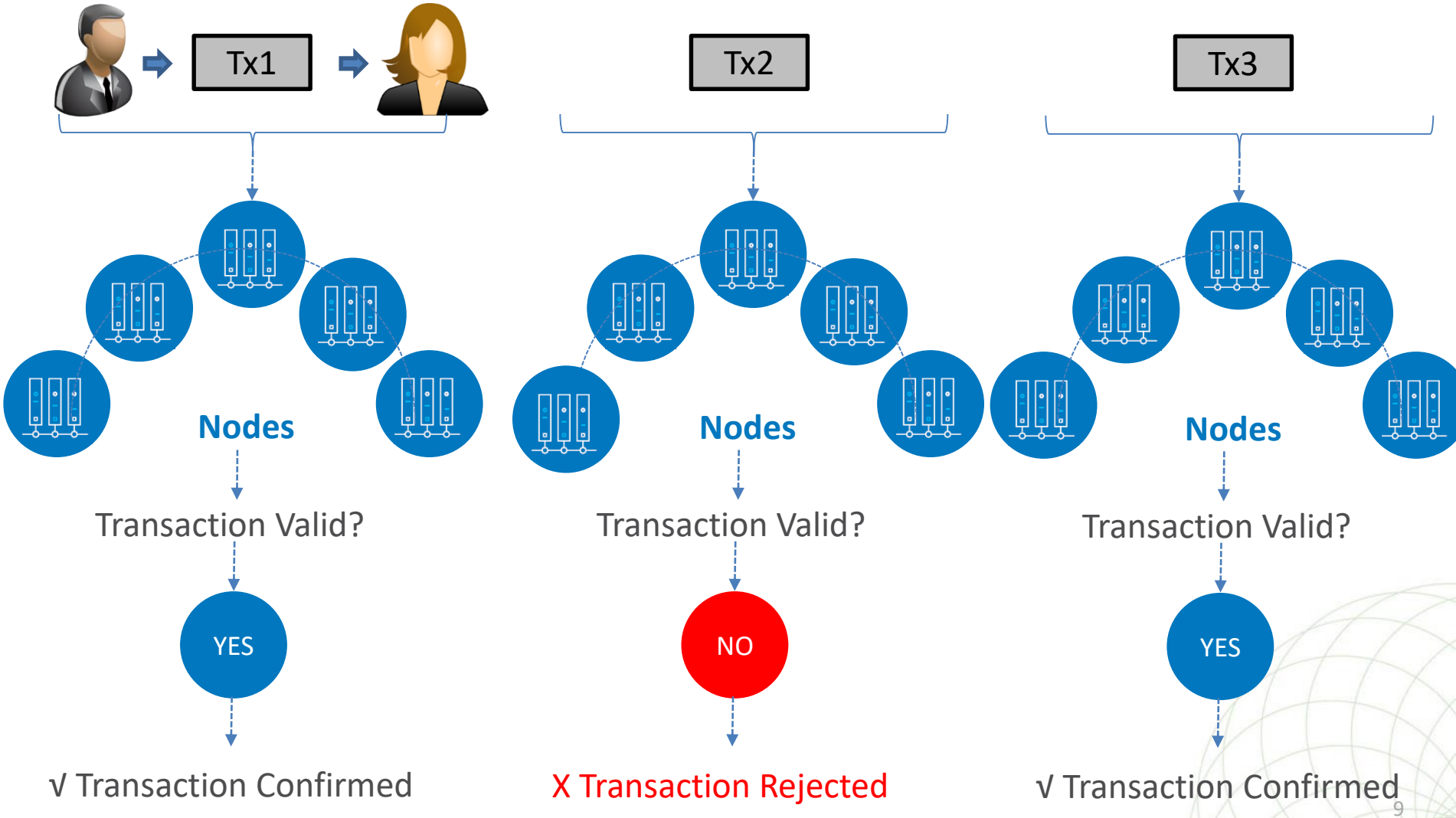
Increases Trust	Limits Risk	Reduces Cost	Saves Time	Increases Security
An immutable record can be relied and trusted by everyone, as it cannot be tampered.	Transparent records prevents tampering, fraud or cyber crime Distributed ledger without central point of failure	An autonomous system without middlemen reduces overheads	Transactions are quicker without middlemen	Each transaction is securely encrypted

2018 nem Foundation

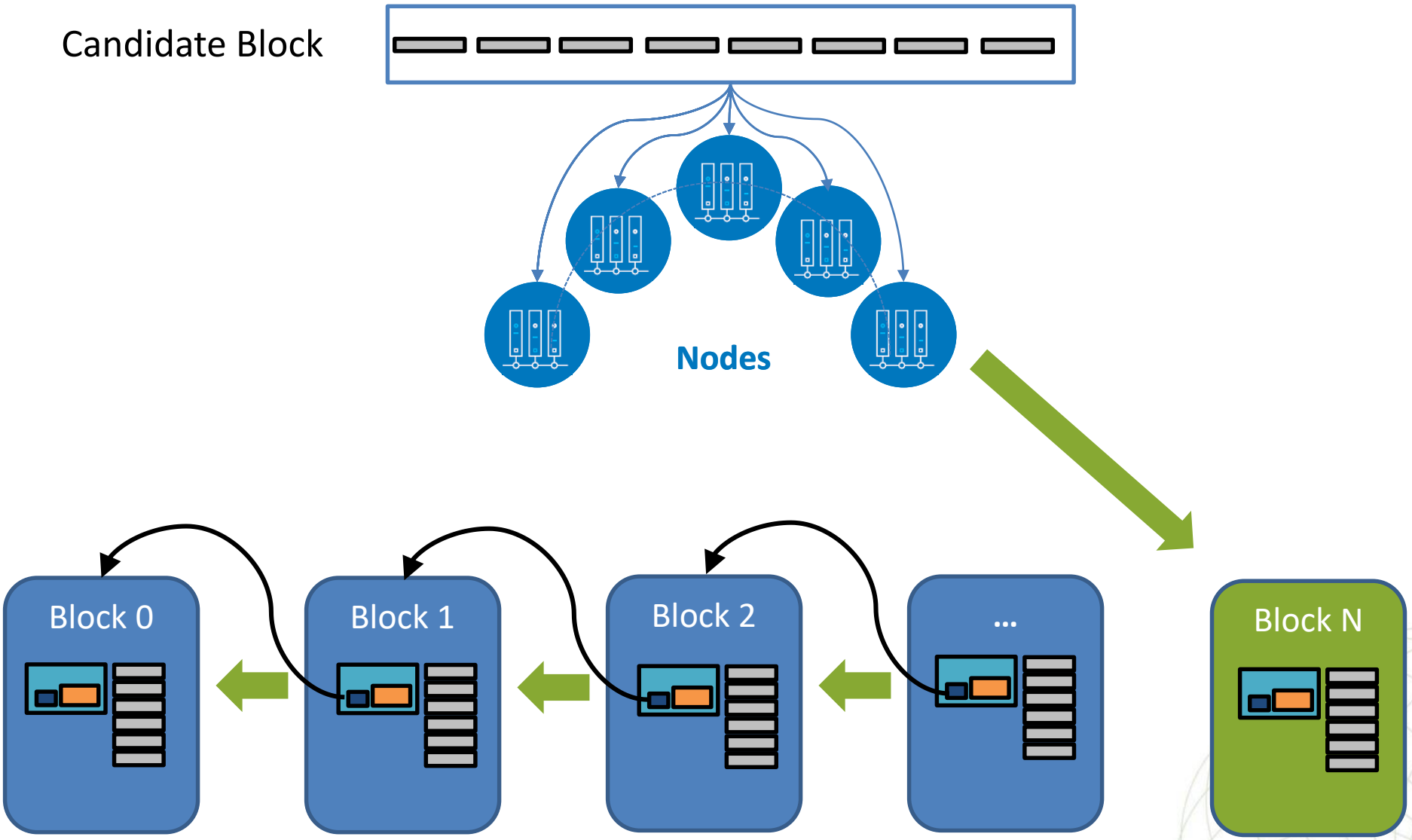
How Blockchain works

- It is decentralized
- Nodes on the network hold copies of the ledger
- All nodes abide by the same consensus rules that govern the creation and validation of transactions/blocks.
- When a new block is relayed, the other nodes validate it and add it to their blockchain
- Any attempt to tamper with the history of database will be evident to all other nodes to reject the change

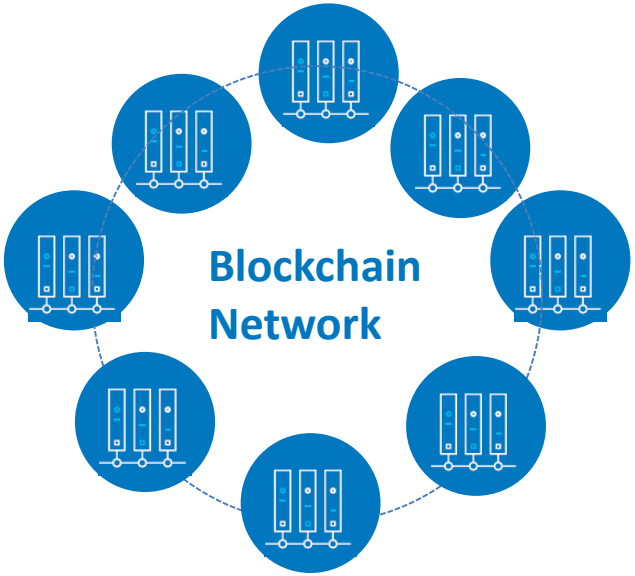
How Blockchain Works

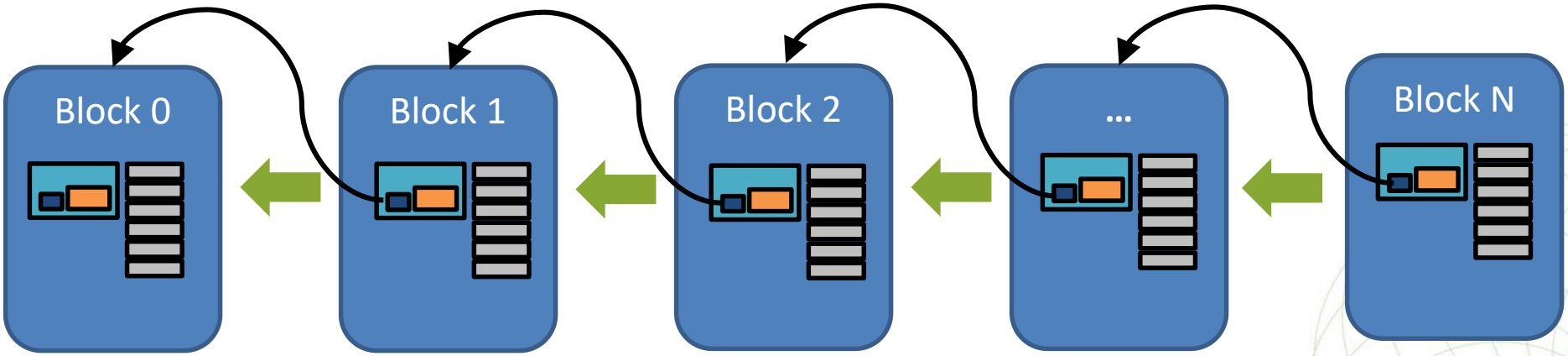


How Blockchain Works

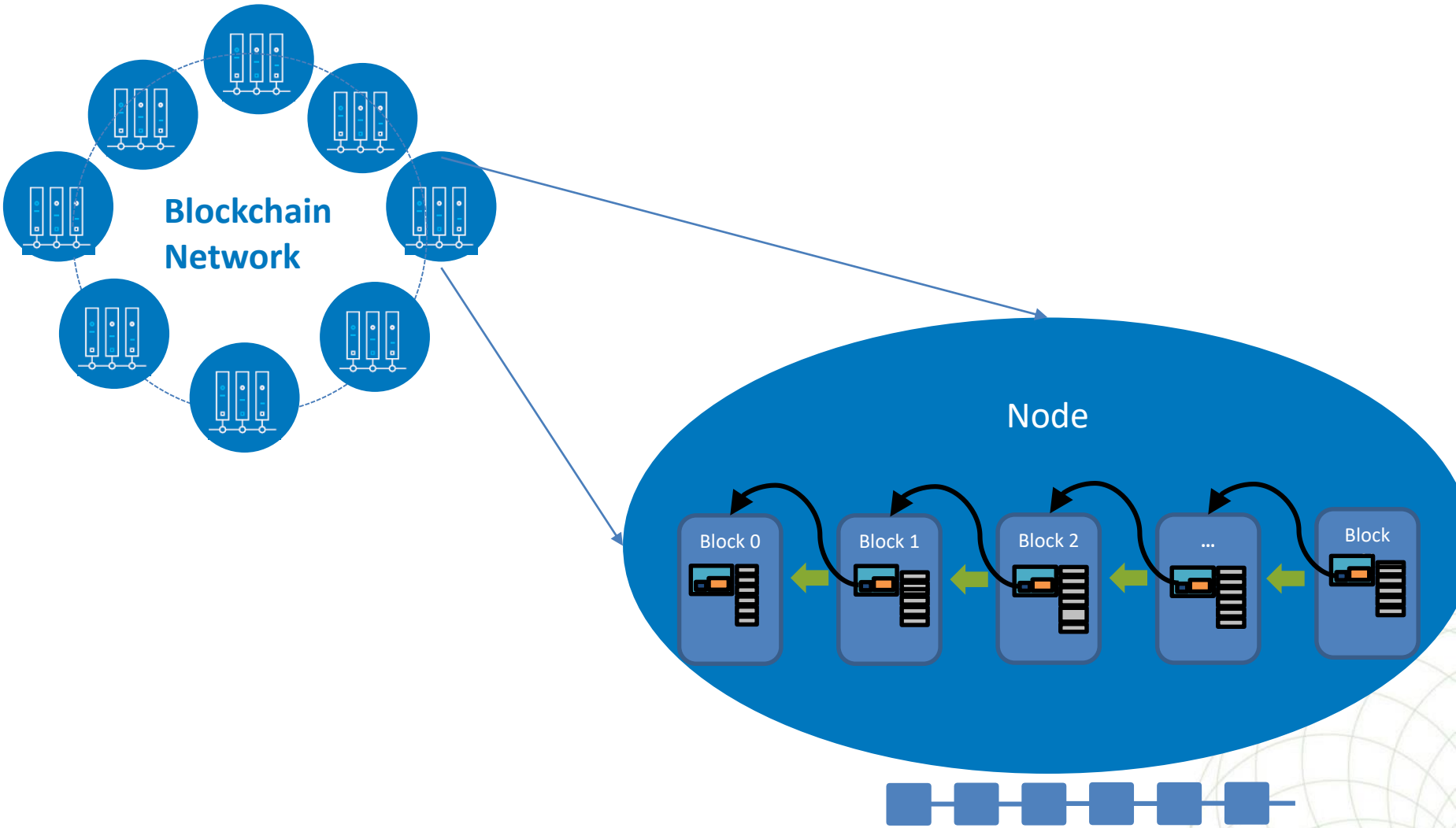


How Blockchain Works





How Blockchain Works



Types of Blockchain

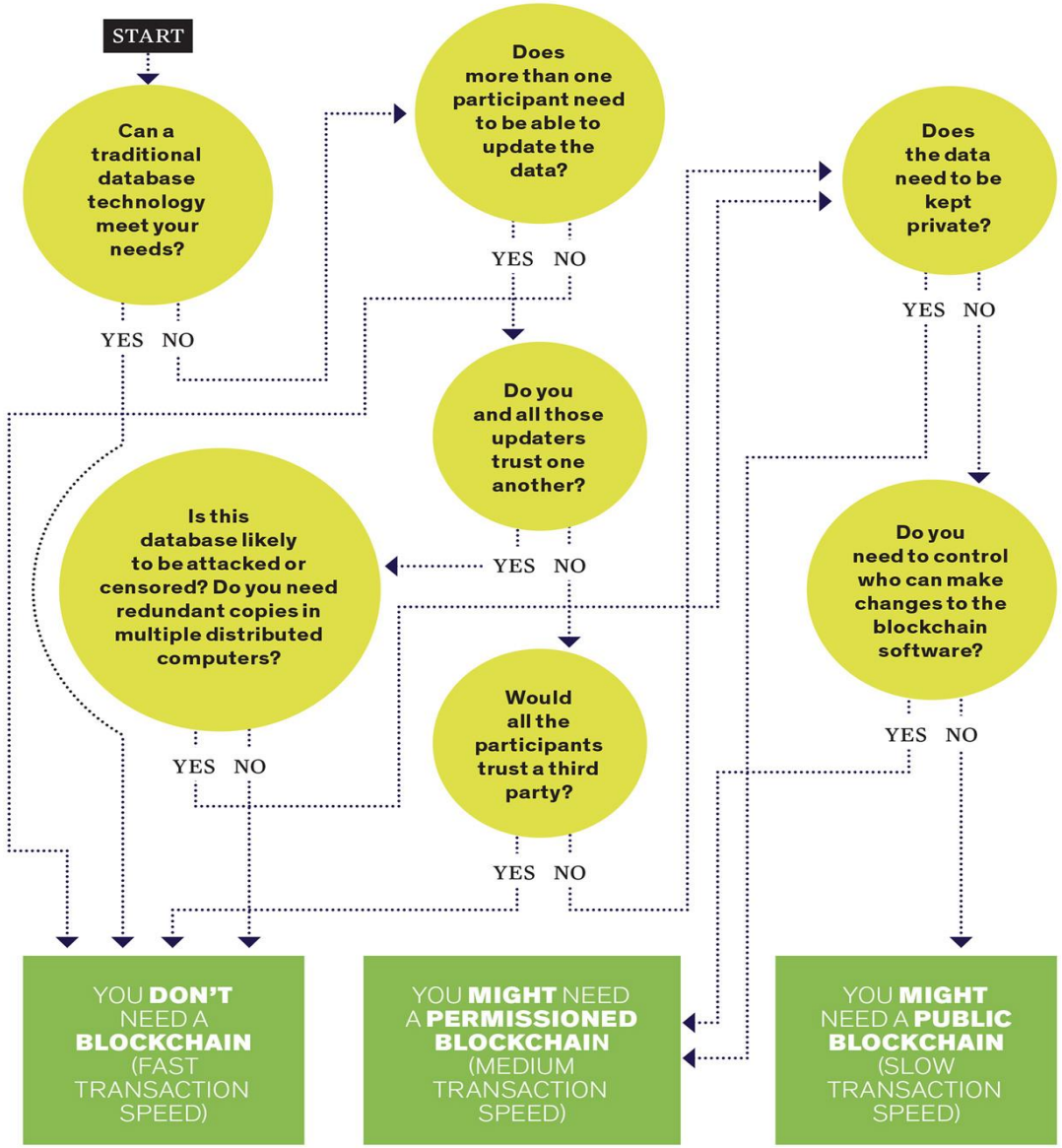
- Blockchain architectures:
  - Private
  - Consortium
  - Open



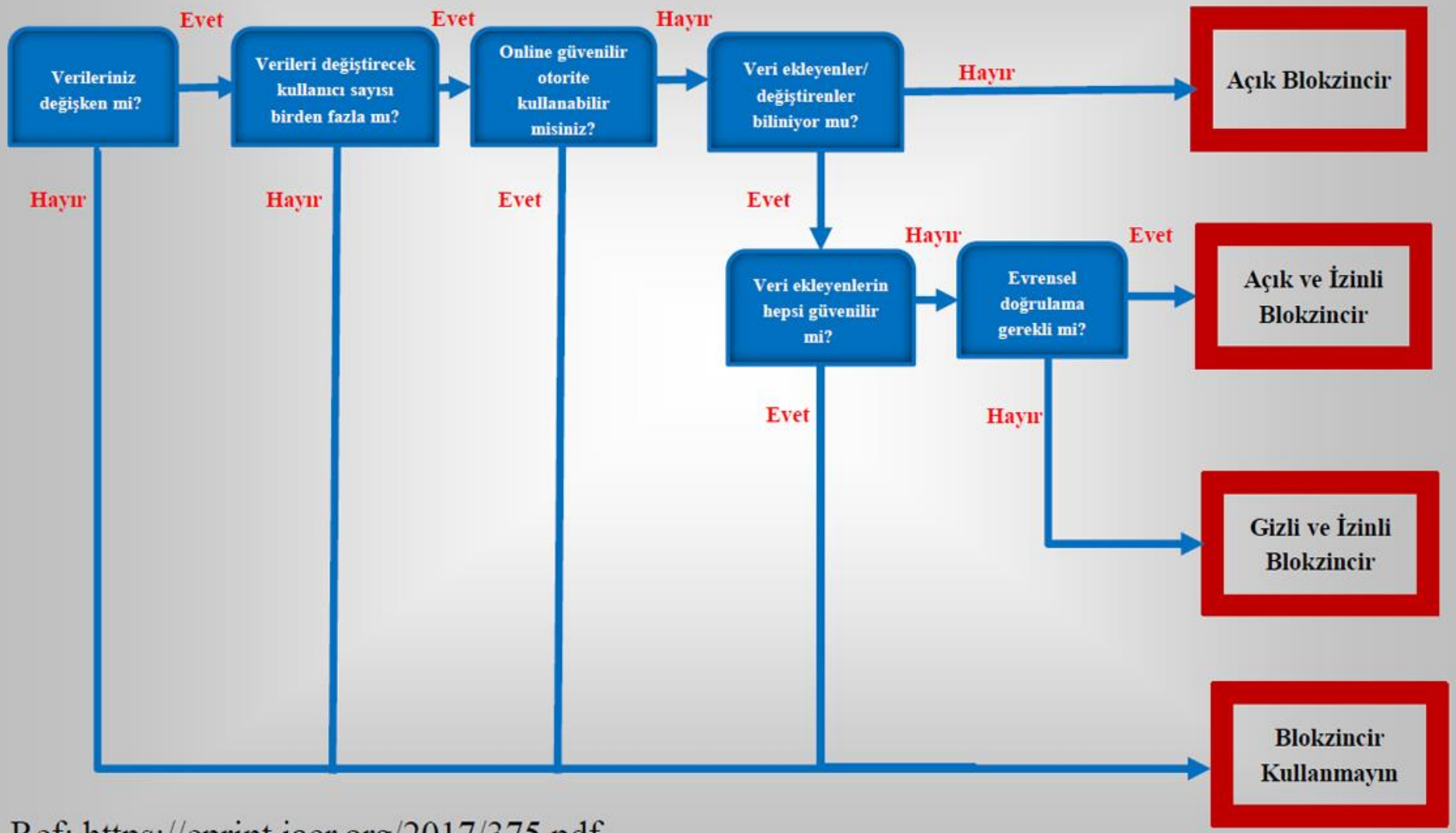




Do you need a blockchain?

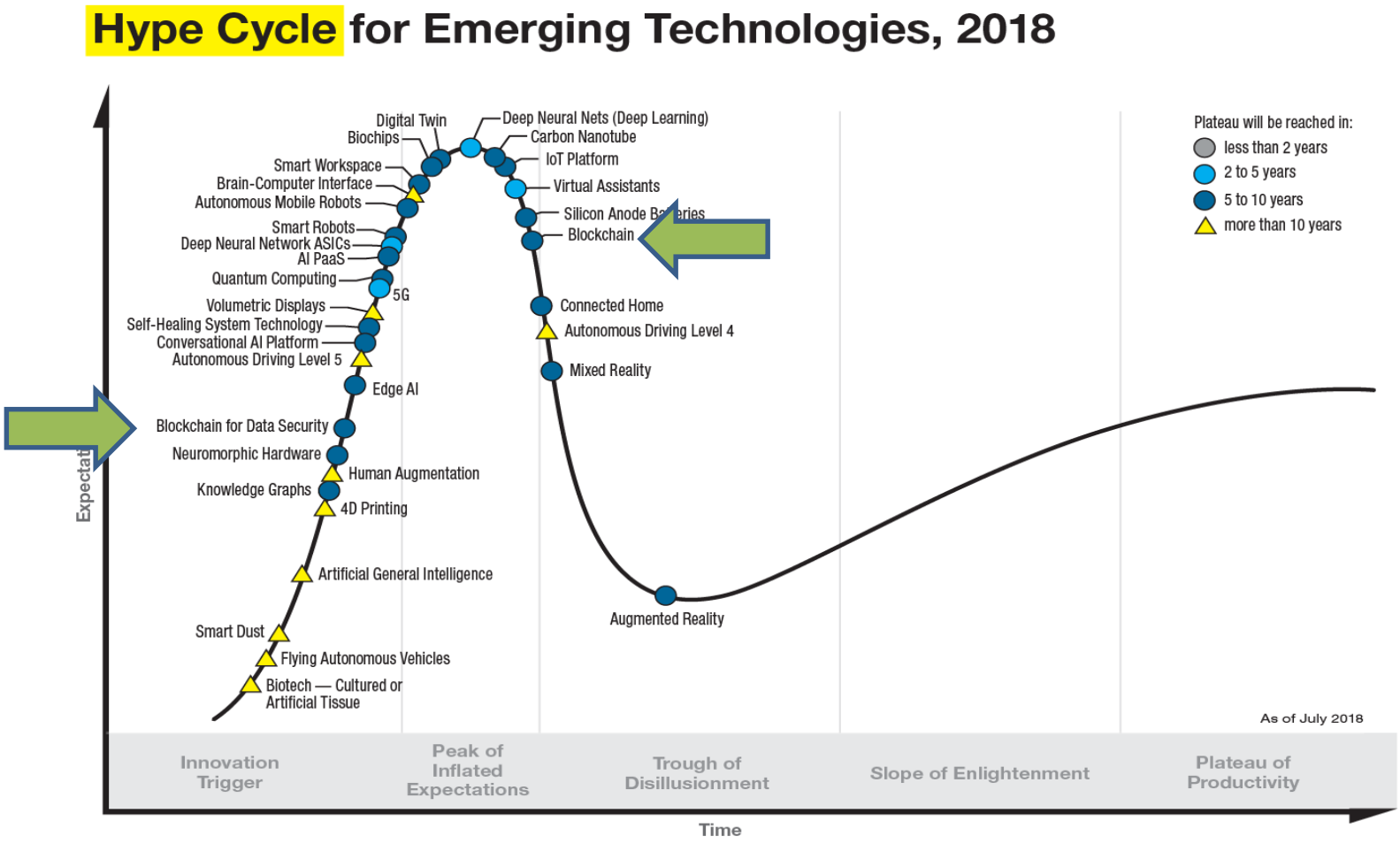


İş Modelinizde Blokzincire İhtiyacınız Var mı?



Ref: https://eprint.iacr.org/2017/375.pdf

Hype Cycle for Emerging Technologies, 2018



gartner.com/SmarterWithGartner

Source: Gartner (August 2018)

© 2018 Gartner, Inc. and/or its affiliates. All rights reserved.

Blockchain Use Cases

Data Provenance

- Keeping track of origin and history of movement of data among the databases or documents
- Traditional solution: Logging and auditing
- In a distributed cloud environment, centralized logging is required and is difficult
- Blockchain can be used to log the changes
- Miners verify the changes
  - ProvChain
  - SMARTDATA

Blockchain Use Cases

Data Privacy

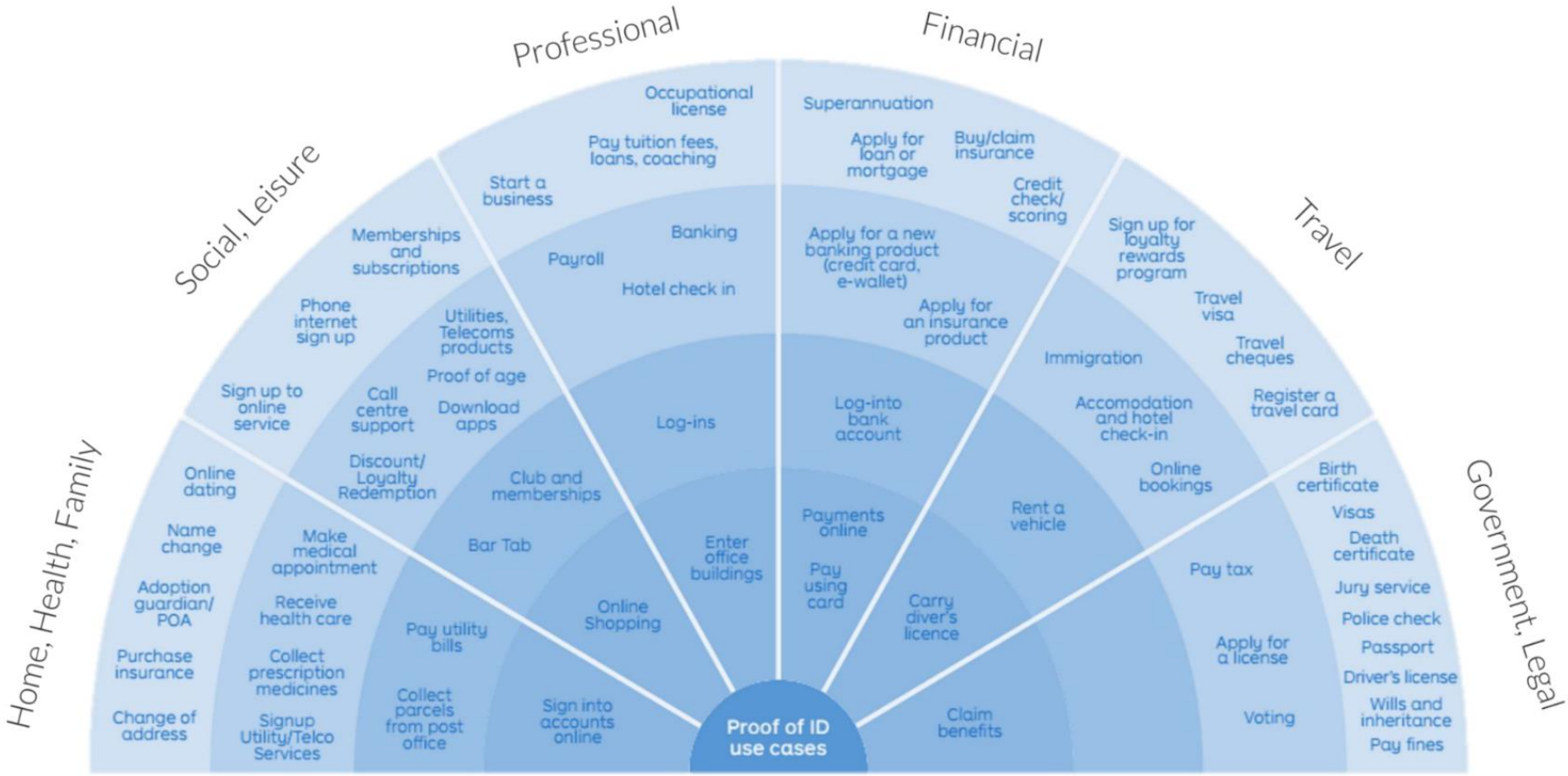
- Facebook and Google have massive amounts of personal information
- Who can access this information?
- Can someone do statistics on the database without having rights to personal information of all?
- Can the user hide its identity?
- Traditional Method: Access Control Lists (ACL) managed centrally (by Facebook and Google)
- Blockchain can be used to keep ACL and data stored in a distributed manner with no central control

Blockchain Use Cases

Data Integrity

- Data has not been corrupted
- Traditional techniques: Digital Signatures and PKI, Replication
- In blockchain, data can not be tempered once committed to a block.
- Ericson provides a blockchain based integrity assurance service

Blockchain Use Cases



Blockchain Challenges

- **Performance** issues:
  - deficiency of existing consensus mechanisms
  - chain size and speed of access
  - transaction speed
- **Security** issues:
  - selfish miners
  - sybil attacks
  - privacy leakage
- **Legal** issues:
  - is data on a blockchain “property”?
  - Smart contract implementation related issues

Consensus Mechanisms
Proof of Work (PoW)
Proof of Stake (PoS)
PBFT
Proof of Activity
Proof of Burn
Proof of Capacity
Proof of Importance
And others….

Will Blockchain Success?

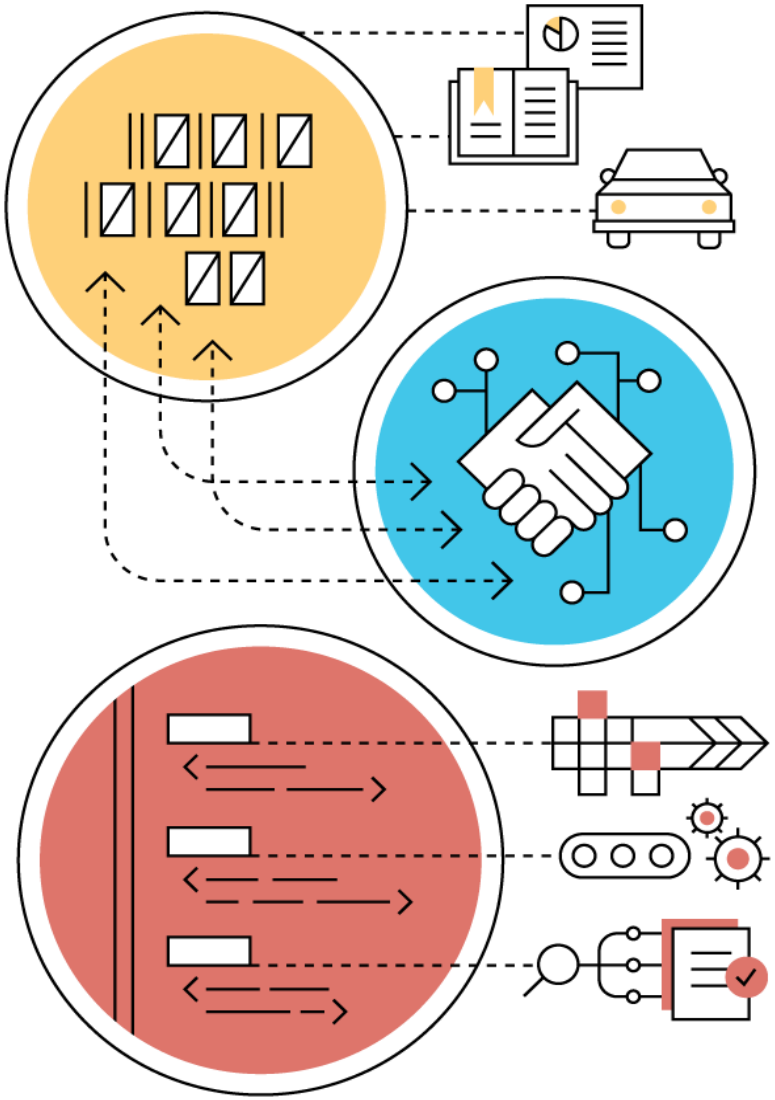
- Blockchain is near the top of hype
- Other examples of hype:
  - Personal Computer 1981
  - Internet 1994
  - Y2K 1999
  - Bitcoin 2014
- Ignoring hype can lead to failure
  - DEC ignored the PC market
- Being a leader can change your future if the hype succeeds
  - IBM
- Betting on false hype can lead to wastage
  - Y2K

Requirements for Technology Success

1. Low Cost:
   - → Each customer must save.
   - 2x cost → 10x performance
2. Killer Application (Crypto)
3. Coexistence with legacy
   Existing infrastructure is more important than new technology → Evolution
4. Timely completion
5. Promised Performance (PoW)
6. Manageability
7. Interoperability

©2017 Raj Jain

Future Direction



1 Storing digital records

Blockchain allows unprecedented control of information through secure, auditable, and immutable records of not only transactions but digital representations of physical assets.

---

2 Exchanging digital assets

Users can issue new assets and transfer ownership in real time without banks, stock exchanges, or payment processors.

---

3 Executing smart contracts

Self-governing contracts simplify and automate lengthy and inefficient business processes.

Ground rules Terms and conditions are recorded in the contract's code.

Implementation The shared network automatically executes the contract and monitors compliance.

Verification Outcomes are validated instantaneously without a third party.

Future Direction

4th Generation Blockchain

- A blockchain that provides knowledge
  - Moving the chain from data to knowledge
  - Moving the chain from information to decision making

Blockchain Initiatives in Turkey

- **BLOKZİNCİR ARAŞTIRMA LABORATUVARININ**
  https://blockchain.bilgem.tubitak.gov.tr/

- **Blockchain Turkey Platform (BCTR)**
  https://bctr.org/en/

- **BlockchainIST *Center***
  https://www.blockchainist.center/

Learn More

- Project to watch:
  - Hyperledger: www.hyperledger.org
  - Ethereum: www.ethereum.org
  - Nem: www.nem.io
  -
- Paper to read:
  - Bitcoin: A Peer-to-Peer Electronic Cash System, Satoshi Nakamoto
- Books to read:
  - Mastering Bitcoin : Unlocking Digital Cryptocurrencies, Andreas Antonopoulos
  - Mastering Blockchain: Distributed ledger, decentralization and smart contracts explained, Imran Bashir
- MOOCS and Courses to attend:
  - IBM online course
  - MIT course
  - Coursera course

Thank You
Q & A

Adib Habbal, Ph.D.,
Department of Computer Engineering
Faculty of Engineering, Karabuk University

Email: adibhabbal@karabuk.edu.tr
Phone: 0090535 74 16217