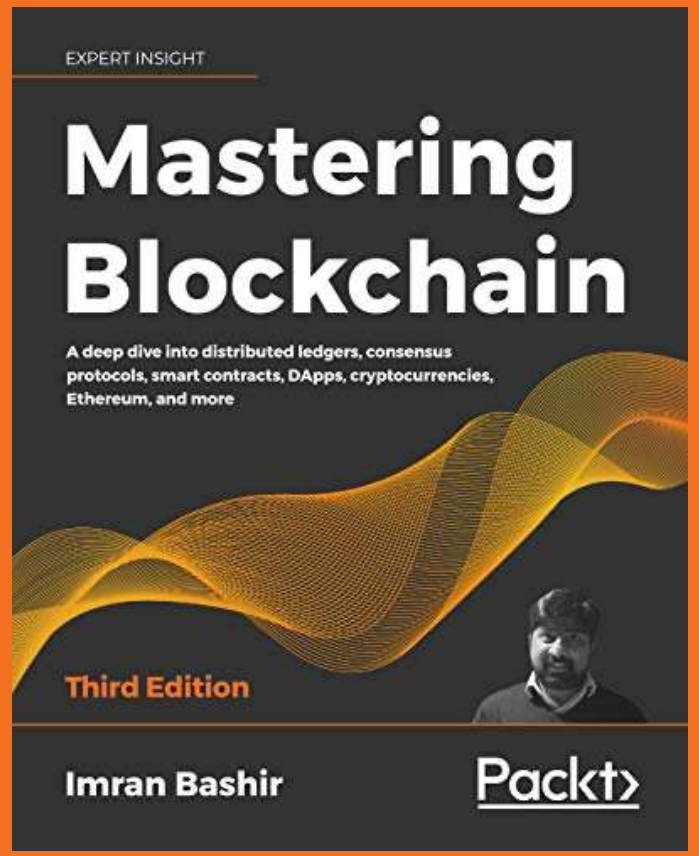


Blockchain 101

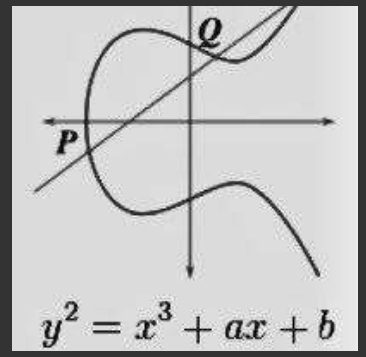
with Imran Bashir

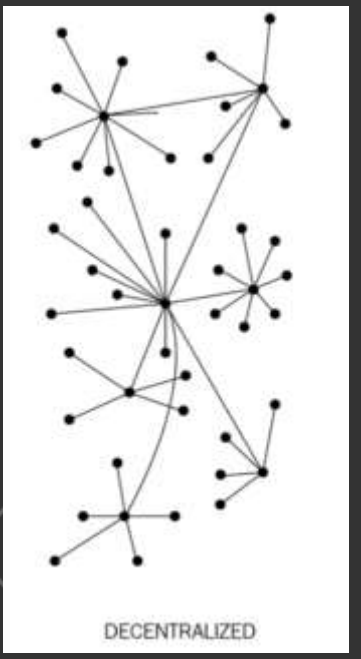
Outline

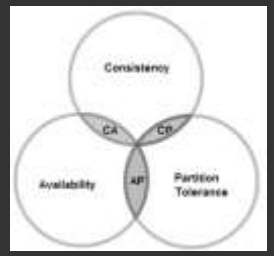
- Describing the fundamentals of distributed systems
- Defining blockchain technology
- Understanding how blockchain technology was developed
- Detailing the elements of a blockchain
- Identifying the benefits and limitations of blockchain technology

Introduction

Blockchain is a new revolutionary technology that will change our lives. In this chapter we will cover the theory of blockchain technology, and its technical foundations.



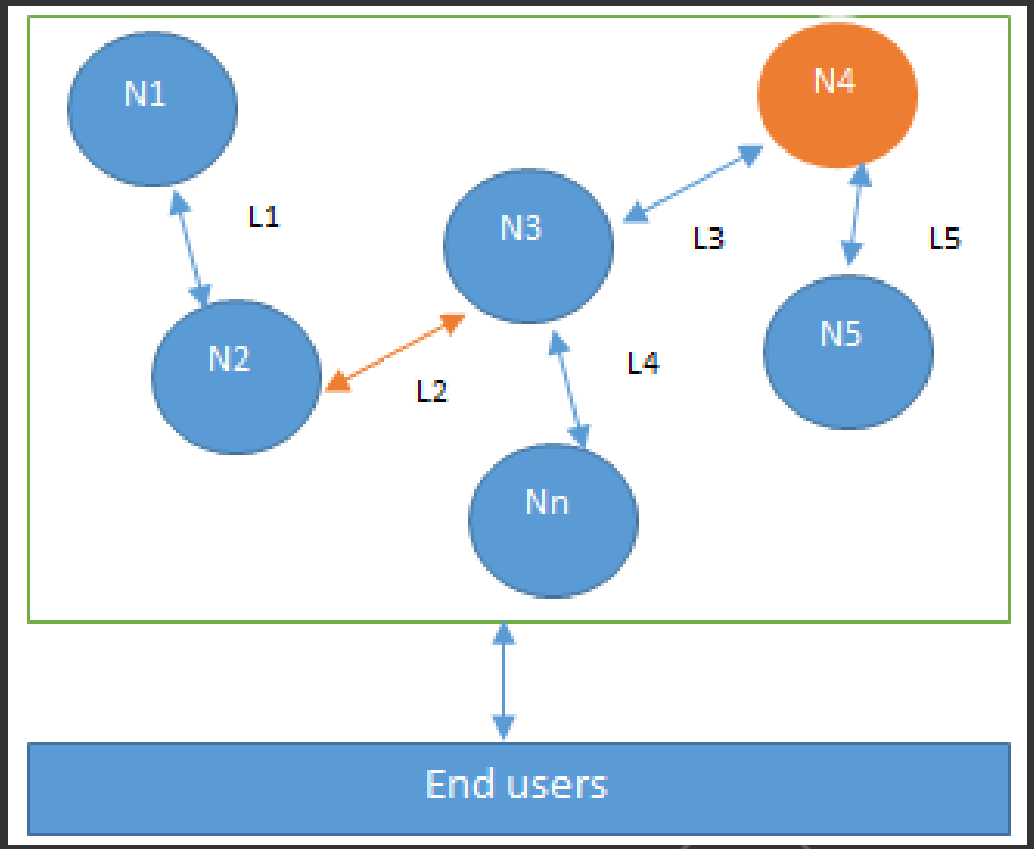




Introducing distributed computing

- A distributed system is a computing paradigm whereby two or more nodes work with one another, in a coordinated fashion, to achieve a common outcome.
- A distributed system is modeled in such a way that end users see it as a single logical platform.
- Examples include clusters and clouds.

Design of a distributed system

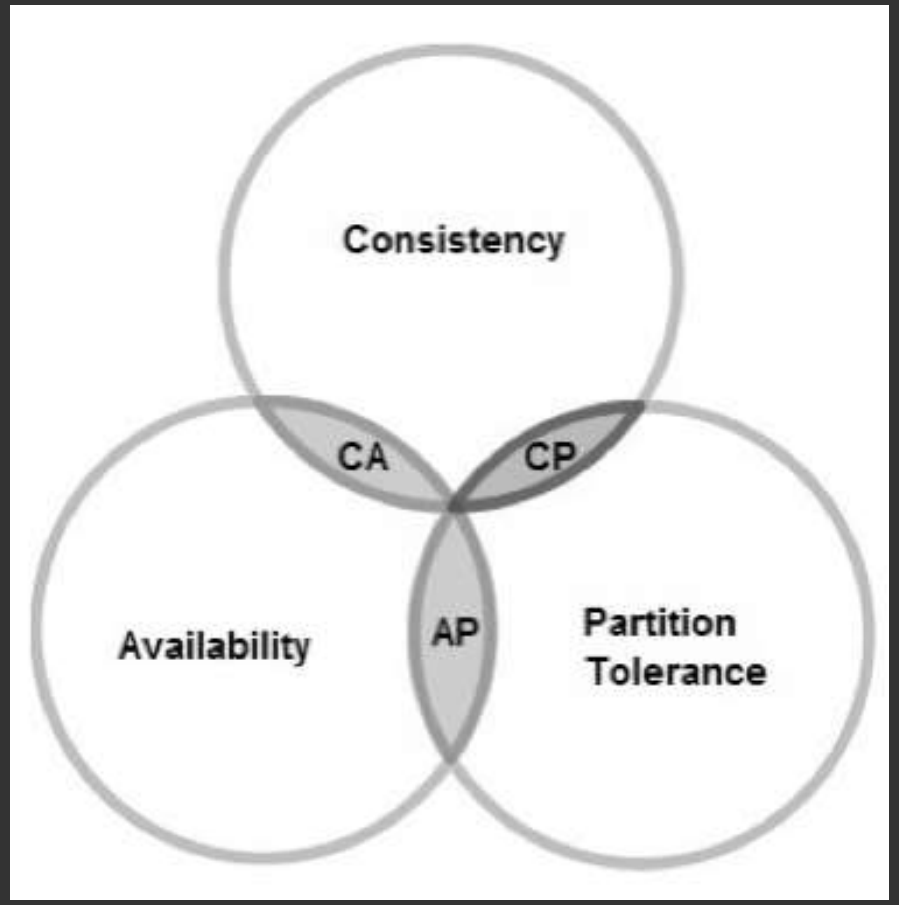


N4 is a Byzantine node, L2 is broken or a slow network link

CAP theorem

This states that a distributed system cannot have all three of the desired properties simultaneously; that is:

- Consistency
- Availability
- Partition tolerance



Types of faults in distributed systems

Fail-stop faults (crash faults)

- Where components crash or cease to operate
- Simpler to deal with

Byzantine faults

- Where components are potentially untrustworthy or malicious
- Difficult to deal with

Defining ‘Blockchain’

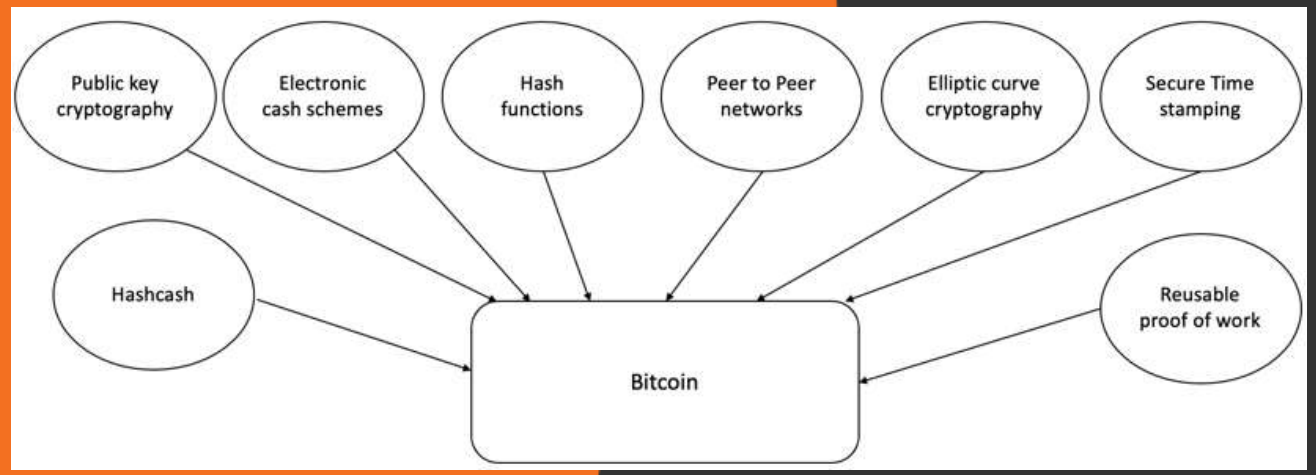
Layman's definition: Blockchain is an ever-growing, secure, shared recordkeeping system in which each user of the data holds a copy of the records, which can only be updated if all parties involved in a transaction agree to update.

Technical definition: Blockchain is a peer-to-peer distributed ledger that is cryptographically-secure, append-only, immutable (extremely hard to change), and updateable only via consensus or agreement among peers.

Blockchain definition

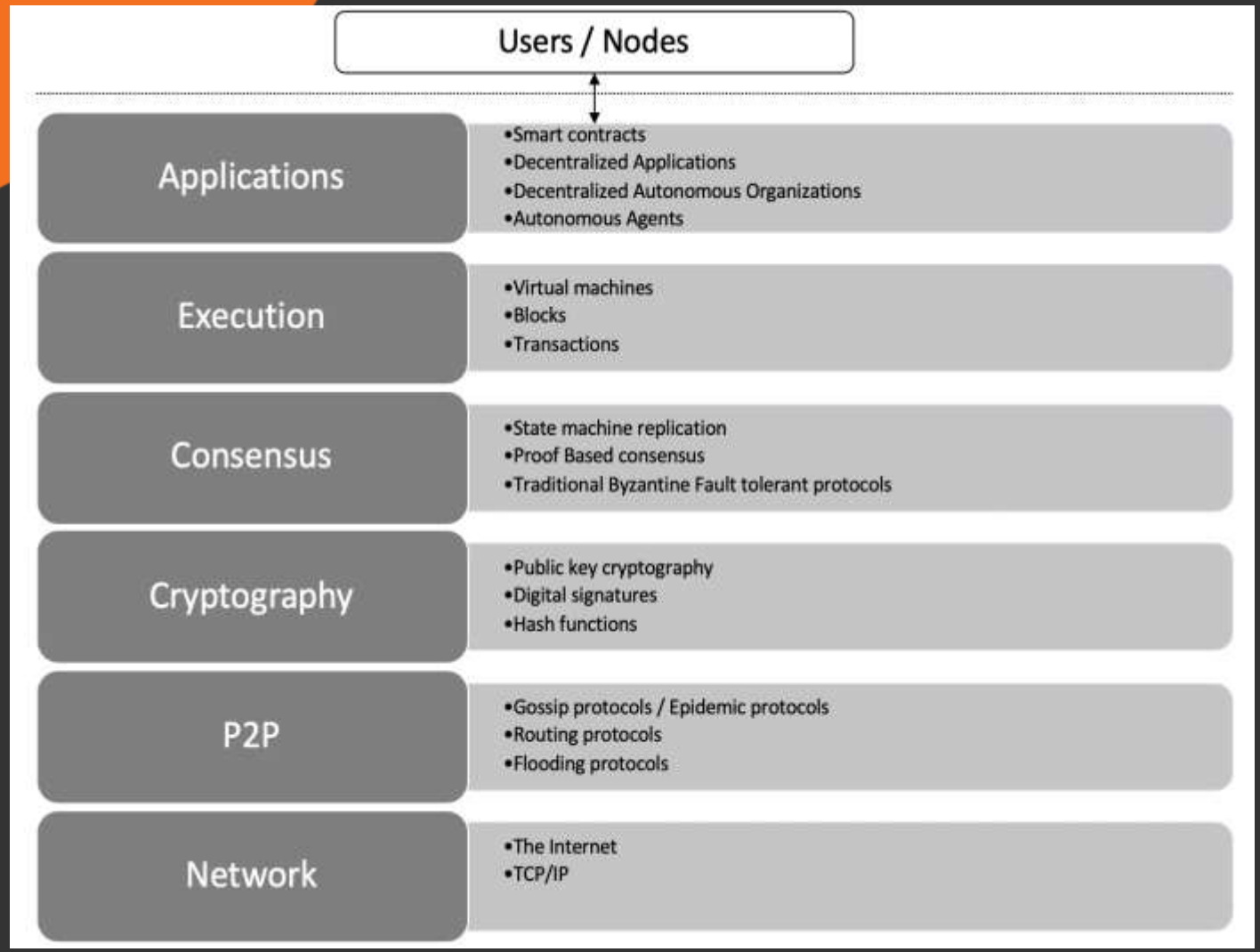
- Peer-to-peer
- Distributed ledger
- Cryptographically secure
- Append only
- Updateable via consensus (consensus-driven)

How did blockchain technology develop?

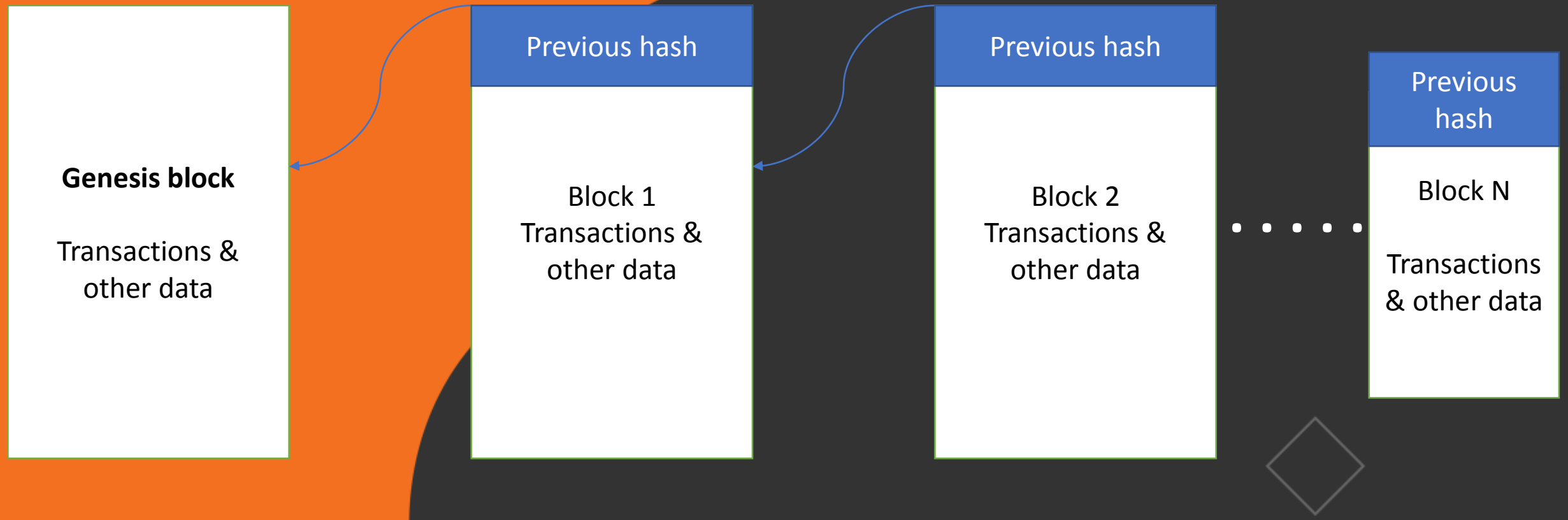


- 1991 – Secure timestamping of digital documents.
- 1992 – Hashcash idea to combat junk emails
- 1994 – S/KEY application for Unix login.
- 1997/2002 – Hashcash
- 2008/2009 – Bitcoin (the first blockchain)
- 1950s – Hash functions
- 1970s – Merkle trees - hashes in a tree structure
- 1970s continued – Research in distributed systems, consensus, state machine replication
- 1980s – Hash chains for secure logins
- 1990s – e-Cash for e-payments

Architectural view of Blockchain



Generic structure of a blockchain



Generic elements of a blockchain

- Addresses
- Accounts
- Transactions
- Blocks
- Peer-to-peer network
- Scripting or programming language
- Virtual machine
- State machine
- Nodes
- Smart contracts

How a blockchain works

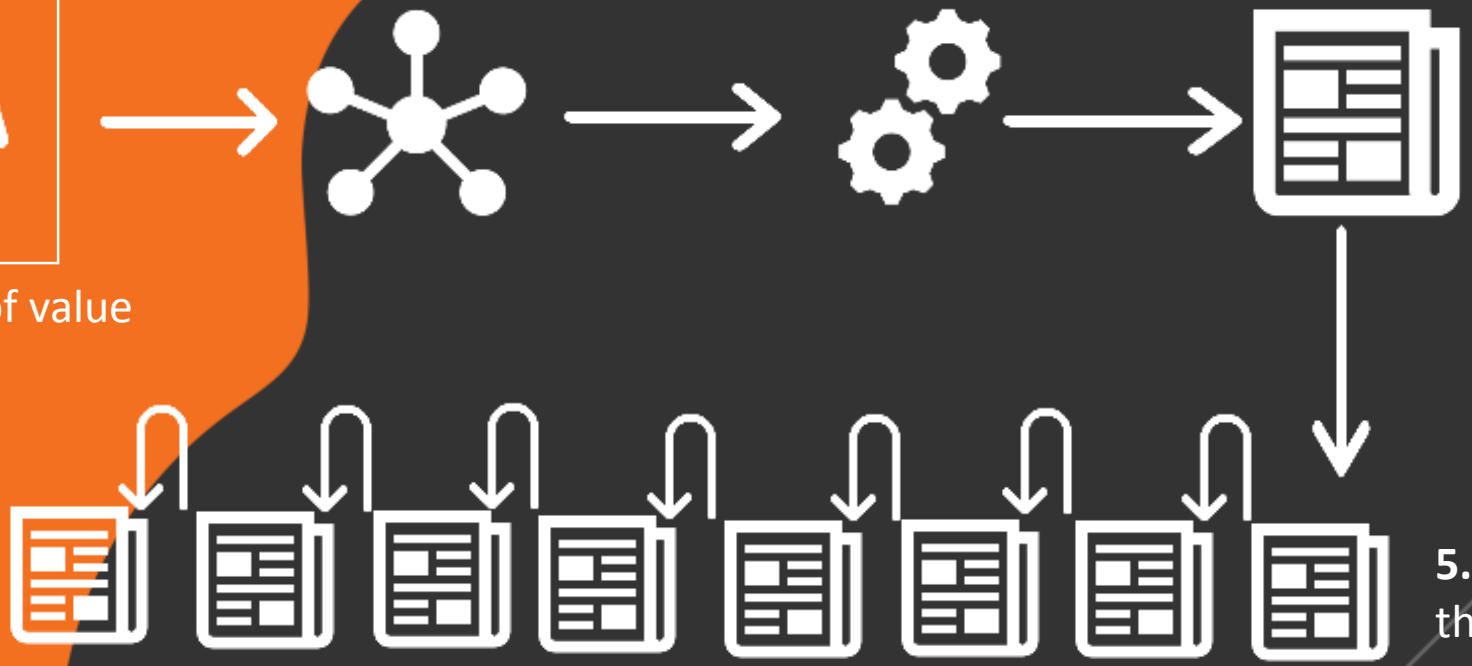
1. User X transacts with User Y

Smart contract or transfer of value

2. Transaction broadcast

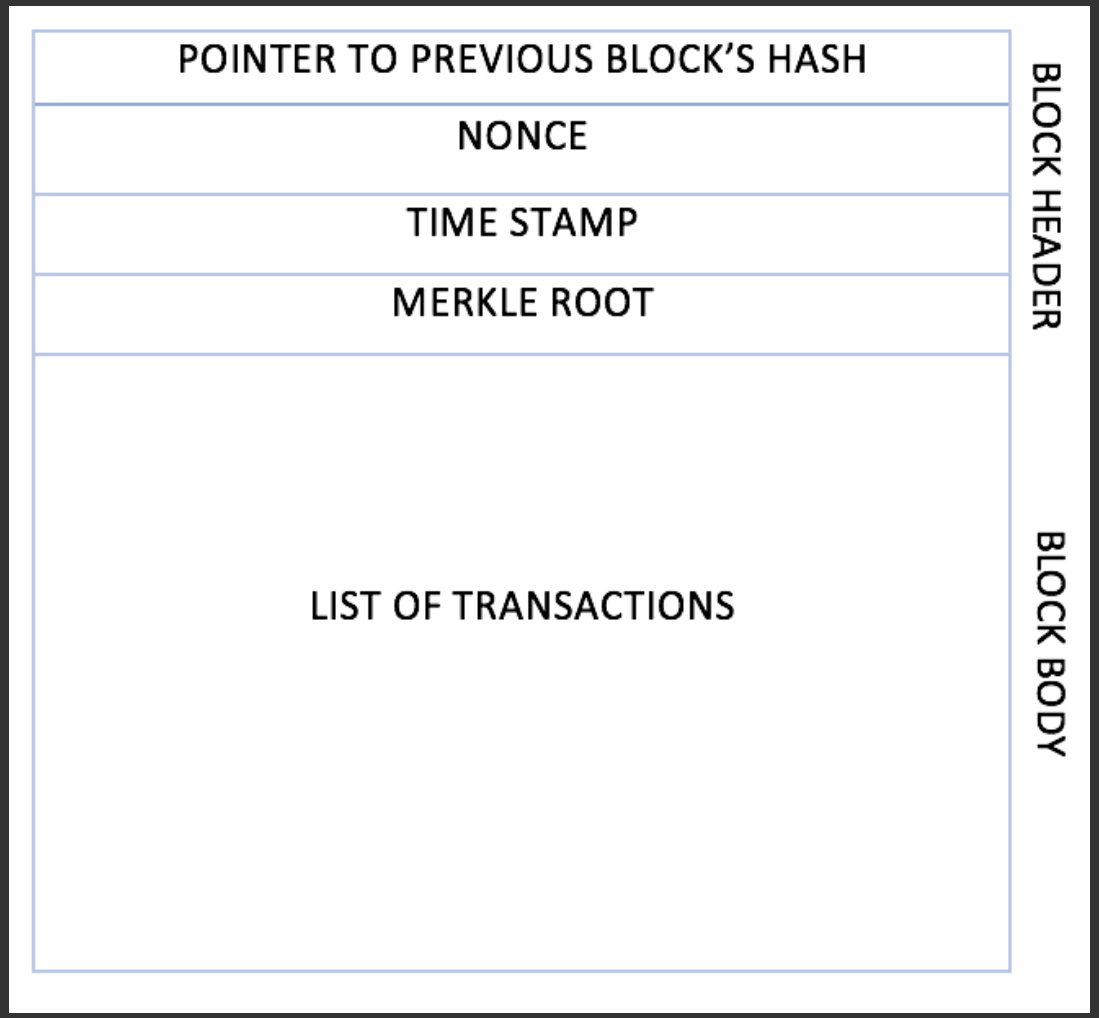
3. Find new block (mining)

4. New block found (mined)



5. Add new block to the blockchain

Generic block structure



Benefits of Blockchain

- Decentralization
- Transparency
- Trust
- Immutability
- High availability
- Highly secure
- Simplification of current paradigms
- Faster transactions
- Cost saving

Limitations of blockchain

- Scalability
- Adaptability
- Regulation
- Relatively immature technology
- Privacy

Features of a blockchain

- Distributed consensus
- Transaction verification
- Platform for smart contracts
- Transferring value between peers
- Generation of cryptocurrency
- Provider of security
- Immutability
- Uniqueness

Exercise

- Think about a scenario where blockchain can solve a challenge at your place of work or education, or in your community.
- Read the Bitcoin paper at https://bitcoin.org/bitcoin.pdf

Summary

In this presentation, we:

- Covered the design of a distributed system and faults in distributed systems.
- Defined blockchain as a distributed ledger—a replicated digital ledger which is immutable and updateable only via consensus.
- Introduced precursors to blockchain technology such as hash functions, consensus mechanisms, Hashcash, and e-cash schemes.
- Explored various elements of a blockchain, such as addresses, peer-to-peer networks, blocks, and transactions.
- Considered the benefits and limitations of blockchain technology.

Book Links

Amazon:

https://www.amazon.com/Mastering-Blockchain-distributed-consensus-cryptocurrencies/dp/1839213191

Packt:

https://www.packtpub.com/product/mastering-blockchain-third-edition/9781839213199