ĐẠI HỌC NGÂN HÀNG THÀNH PHỐ HỒ CHÍ MINH

BLOCKCHAIN

THÀNH PHỐ HỒ CHÍ MINH, 2022

OUTLINE

1. Introduction to Cryptographic Digital Money, Ledger, Bitcoin
2. Cryptography and cryptocurrency
3. Consensus protocol and mining
4. Transactions and Transaction processing in blockchain
5. Contract and Smart contract
6. The future of blockchain technology
7. Writing very first blockchain in JAVA

Chapter 1

INTRODUCTION TO CRYPTOGRAPHIC DIGITAL MONEY, LEDGER, BITCOIN

WHAT YOU WISH TO LEARN?

1. Technological Understanding

- Understand Blockchain Technology
- Understand the blockchain ecosystem (ICOs, currencies, etc.)
- Benefits, risks, challenges and next steps of blockchain

2. Application

- Understand blockchain applications
- Learn to apply blockchain to areas of interest
- Think about new applications of blockchain

WHAT YOU WISH TO LEARN?

3. Impact

- Understand blockchain impacts on internet, business, and finance
- Implications in people's lives

4. Regulation

- How will regulation and public policy change and need to change
- Learning about regulations

5. Market & Money

- Make money
- Investment
- Trends and top influencers in the market

SURVEY

- Assess how realistic it is for blockchain to traditional systems
- Specific blockchain startup success/failure stories and why
- Get a startup idea
- Application to international trade supply chains
- When to use and when not to use
- How blockchain can improve financial system
- Assets tokenization

Study Questions

- What is a blockchain as an overview?
- What is money? Role of money? Characteristics of money?
- What is ledgers? Characteristics of good ledgers?
- What is a payment system? Its entities? Potential issues?
- Group of 3 or 4 students:
  - self-study and take notes: 45 minutes
  - discussion: 45 minutes

NON-METAL MONEY

Salt Bars - Ethiopia

Cowrie Shells - Nigeria

Tally Sticks - England

Rai Stones - Yap

METAL MONEY

Bronze Aes Rude - Rome

Bronze Spade - China

Cooper Plate - Sweden

MINTED MONEY

Bronze Yuan - China

Silver Dekadrachm - Greece

Gold Aureus - Rome

PAPER MONEY

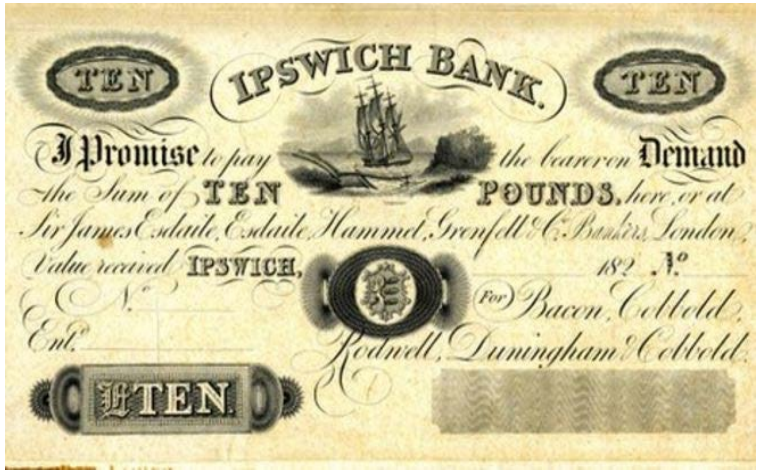
Jiaozi Promissory Note - China

5 Pound Note - England

Continental Note – U.S.

PRIVATE BANK NOTES

Australia



USA

Canada

England

What is money?

- Money is any substance that serves as a medium of exchange, store of value, or unit of account
- It must be accepted by everyone in a society
- Fiat money - money issued by government decree

What is the role of money?

- **Medium of exchange**: an item that can be traded for another good or service
- **Store of value**: allows purchasing power to be used over time
- **Unit of account**: a common denominator that can be used to express worth

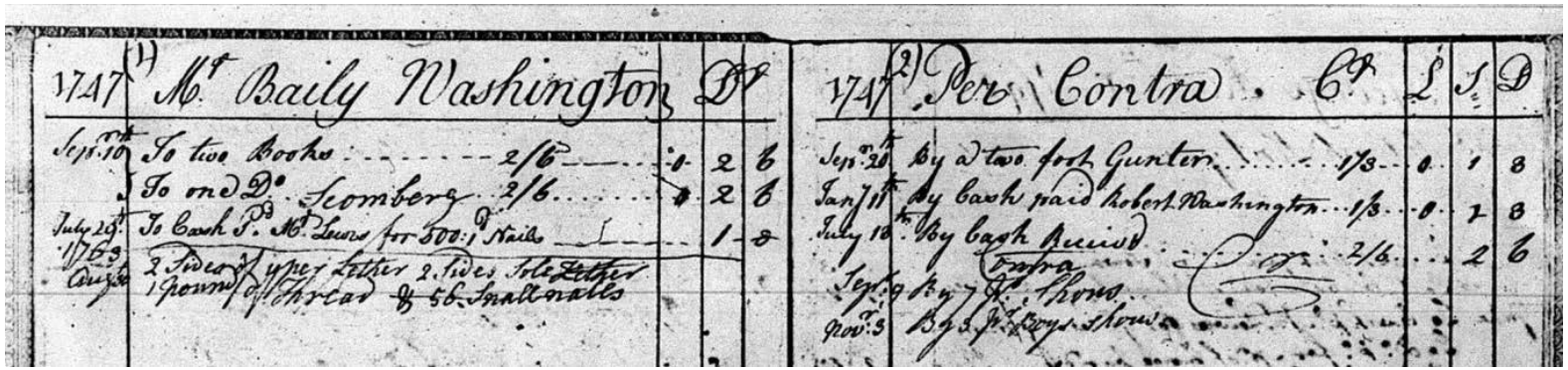
Characteristics of money?

To be a successful medium of exchange, money must be:

- Portability: easily transferred from one to one
- Durability: does not deteriorate when handled often
- Divisibility: easily split/merge into smaller/larger denominations
- Limited supply: money loses value if there is too much

LEDGERS

Proto Cuneiform
Uruk, ca 3000 B.C



Personal Ledger
George Washington
1747

Principal Recordings of Accounts:

- Economic Activities
- Financial Relationships

CHARACTERISTICS OF GOOD LEDGERS

- Immutable, Consistency
- Timestamped
- Ownership
- Accuracy
- Description of Transaction
- Comprehensive

What is a payment system?

- A method to amend & record changes in ledgers for money
- Any system used to settle financial transactions through the transfer of monetary value [wikipedia]
- Potential issues in online payment systems?

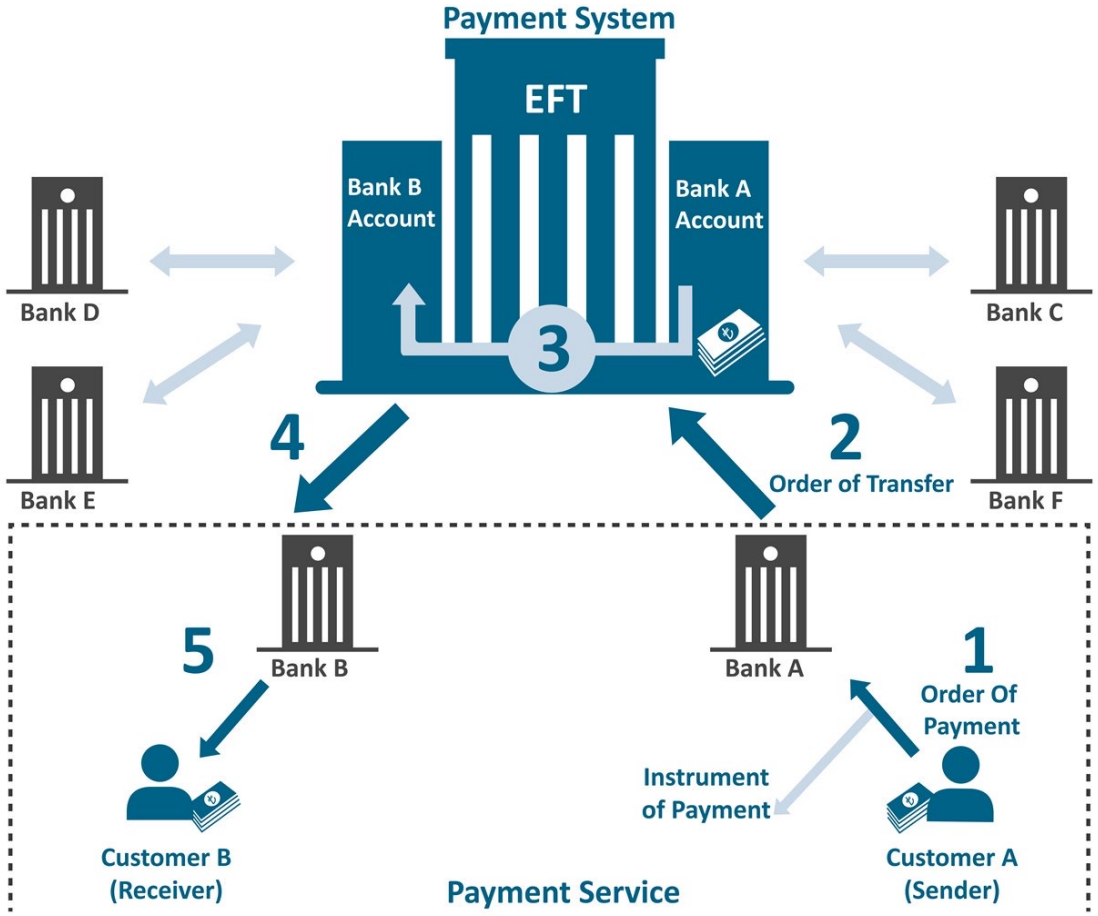


Image from https://www.tcmb.gov.tr

EARLY CRYPTOGRAPHIC DIGITAL CURRENCIES

- DigiCash (David Chaum) – 1989
- Mondex (National Westminster Bank) – 1993
- CyberCash (Lynch, Melton, Crocker & Wilson) – 1994
- E-gold (Gold & Silver Reserve) – 1996
- Hashcash (Adam Back) – 1997
- Bit Gold (Nick Szabo) – 1998
- B-Money (Wei Dai) – 1998
- Lucre (Ben Laurie) – 1999

FAILED

WHY DID EARLY DIGITAL CURRENCIES FAIL?

- Merchant adoption
- Centralization
- Double spending
- Consensus

DIGITAL & MOBILE PAYMENTS

PayPal — 2007

ERICSSON telenor — 1999

支付宝 ALIPAY — 2003

M-PESA Safaricom — 2007

2011

Google Wallet — 2011

微信支付 WeChat Pay — 2013

Pay — 2014

👉 Have you ever used one of the above payment method?

THE RIDDLE REMAINED

- P2P transactions
- Without trusted central intermediary

Bitcoin: A Peer-to-Peer Electronic Cash System (2008)
Satoshi Nakamoto: “I've been working on a new electronic cash system that's fully peer-to-peer, with no trusted third party”

DISTRIBUTED DATABASES vs DISTRIBUTED LEDGER

Centralized relational databases:

- (Multiple) clients talk to central server
- Server manages competing requests, assigns priority, prevents conflicts
- Examples: web server

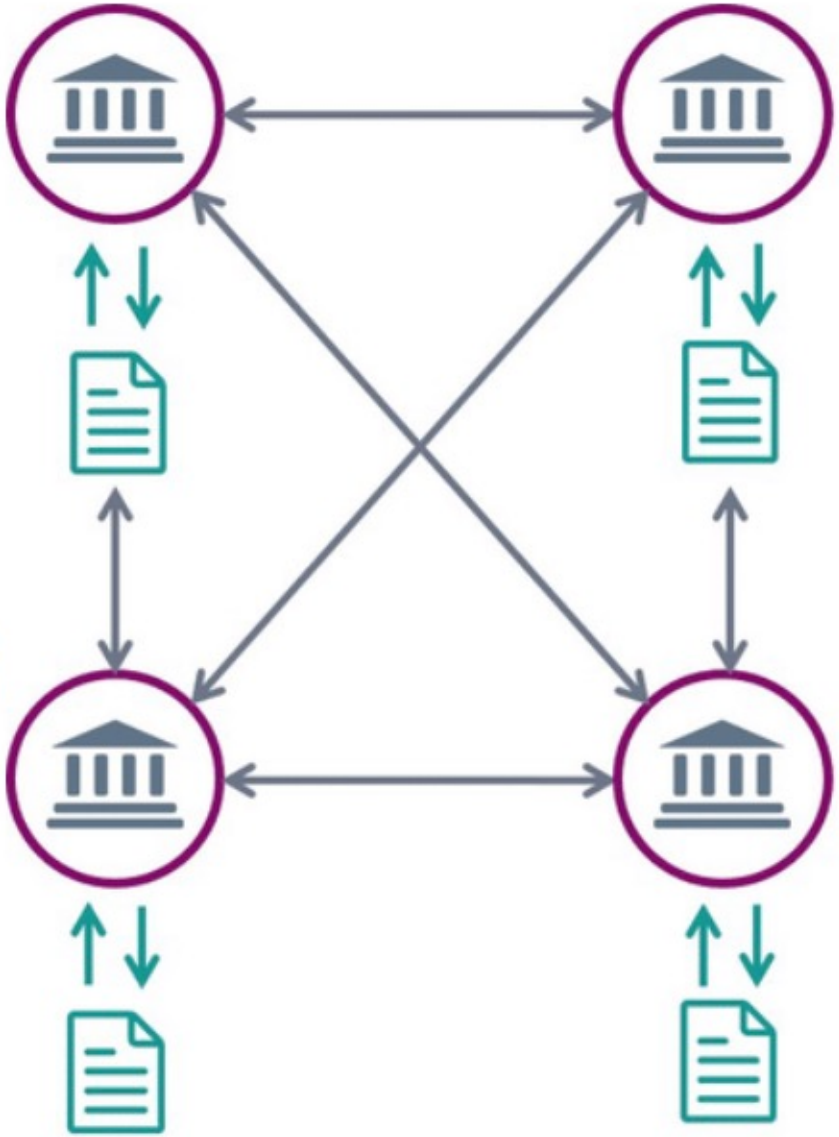
Distributed databases:

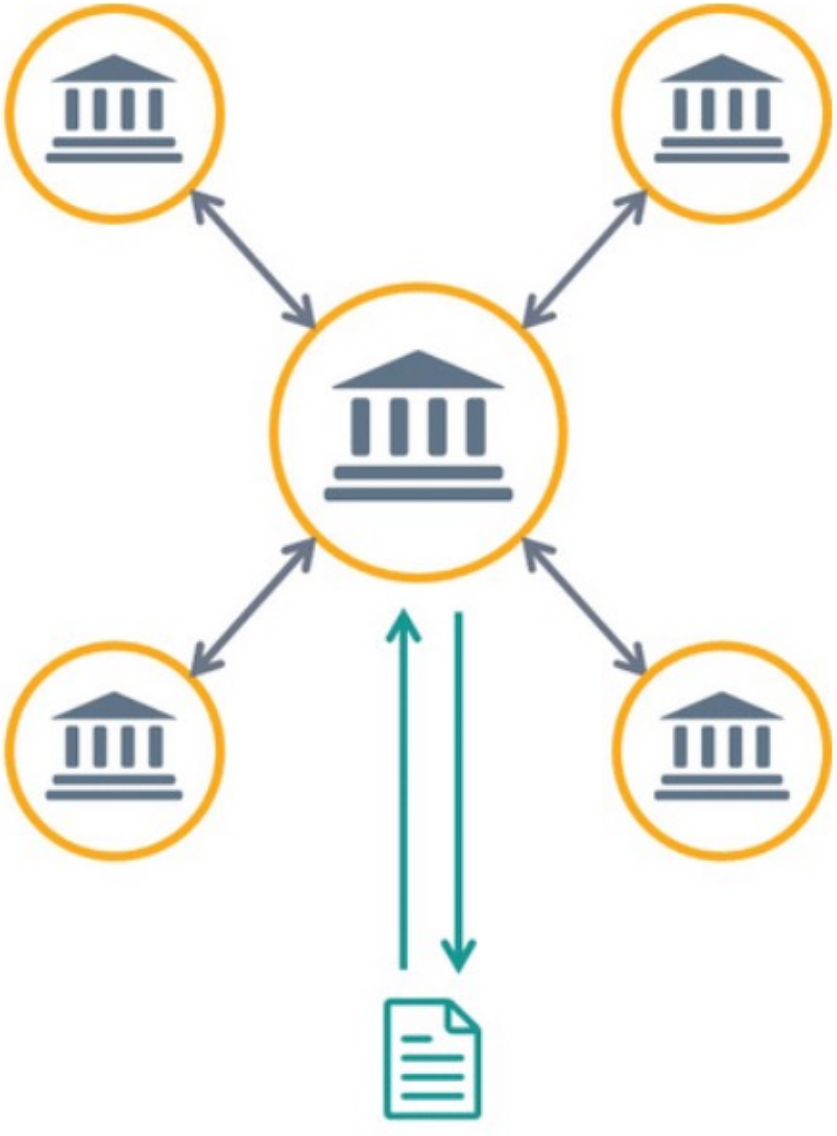
- Distribute storage of information across multiple locations
- Distributed consensus algorithm is used to ensure consistency
- Examples: 2PC, 3PC, Paxos

Distributed ledgers: adds additional features

- Complete (unalterable) history of transactions
- Protection against (Byzantine) attack

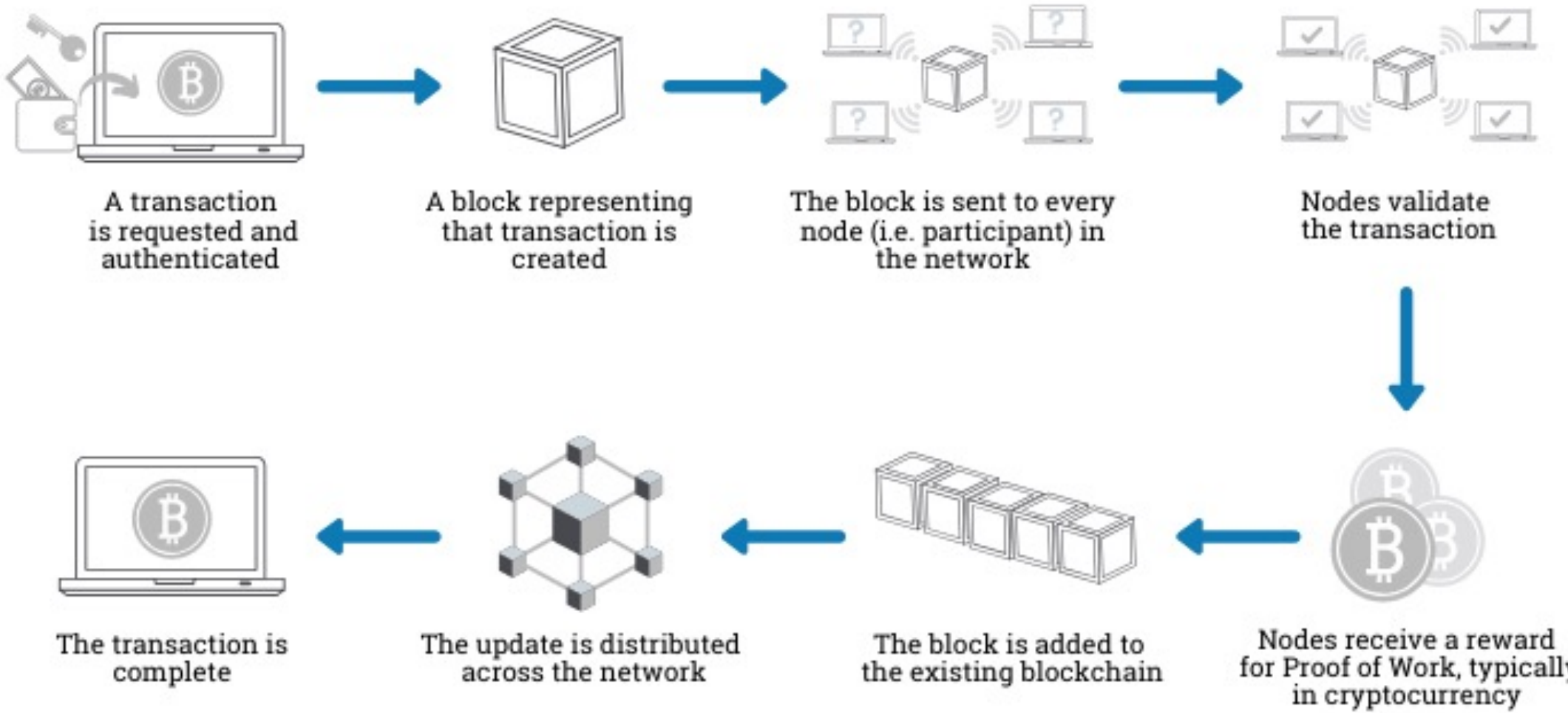
DISTRIBUTED DATABASES vs DISTRIBUTED LEDGER





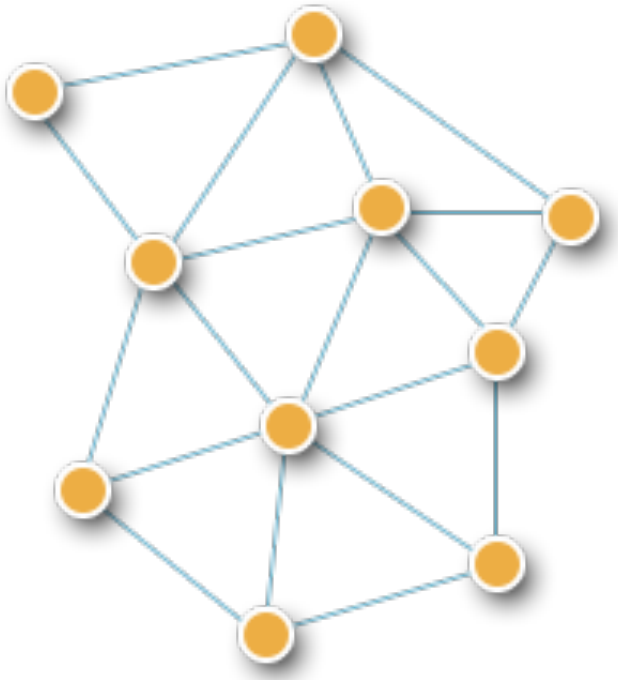
BITCOIN

Bitcoin = mechanism for maintaining a distributed ledger of payment transactions



DATA STORING

Distributed



Centralized

Decentralized

Distributed vs Centrialized vs Decentrialized

- Centrialized:
  - client/server architecture: client nodes are directly connected to a central server.
  - characteristics:
    - ✓Presence of a global clock
    - ✓One single central unit
    - ✓Dependent failure of components. Components: node, server, communication link
  - Example: Wikipedia server

Distributed vs Centrialized vs Decentrialized

- Decentrialized:
  - every node makes its own decision.
  - aggregate of the decisions of the individual nodes.
  - no single entity that receives and responds to the request.
  - characteristics:
    - ✓Lack of a global clock
    - ✓Multiple central units
    - ✓Dependent failure of components: not the whole but part of the system
  - Example: Bitcoin

Distributed vs Centrialized vs Decentrialized

- Distributed:
  - a collection of computer programs that utilize computational resources across multiple, separate computation nodes to achieve a common, shared goal
  - characteristics:
    - ✓Resource sharing
    - ✓Simultaneous processing
    - ✓Scalability
    - ✓Error detection
    - ✓Transparency
  - Example: Google search system

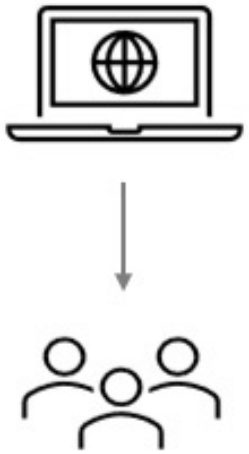
BLOCKCHAIN - A NEW LAYER?

Blockchain	2009
SSL/TLS	1996
HTTP	1990
TCP/IP	1974
Ethernet	1974

BLOCKCHAIN – WEB 3.0?

Web 1.0

Static read-only webpages
(1900s-2000)

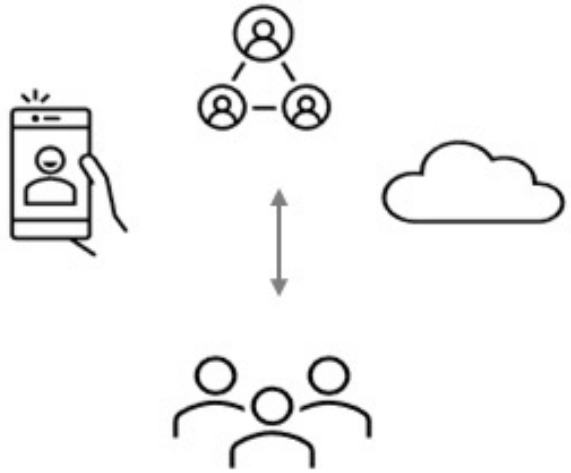


LiveJournal

HTML Pages

Web 2.0

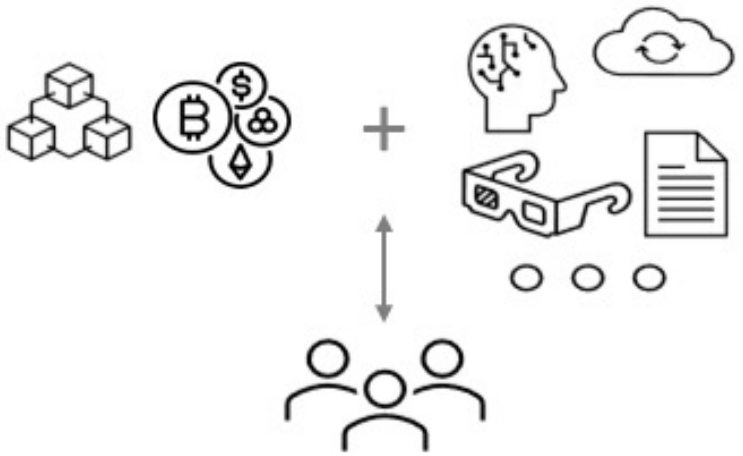
Information-centric and interactive
(2000-2020s)



Meta YouTube Spotify aws NETFLIX

Web 3.0

User-centric, decentralized, private,
and secure (2020s and beyond)



WolframAlpha

Demonstrates semantic search capabilities
as one of the key features

DISCUSSION