COMP4137 Blockchain Technology and Applications
COMP7200 Blockchain Technology

Lecturer: Dr. Hong-Ning Dai (Henry)

Lecture 1

Introduction to Blockchain

Outline

- Cryptocurrency
- Blockchain
- Blockchain Applications

Cryptocurrency

Bitcoin

Ethereum

Satoshi Nakamoto
中本聰

Vitalik Buterin

https://vitalik.ca/index.html

Bitcoin: A Peer-to-Peer Electronic Cash System

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

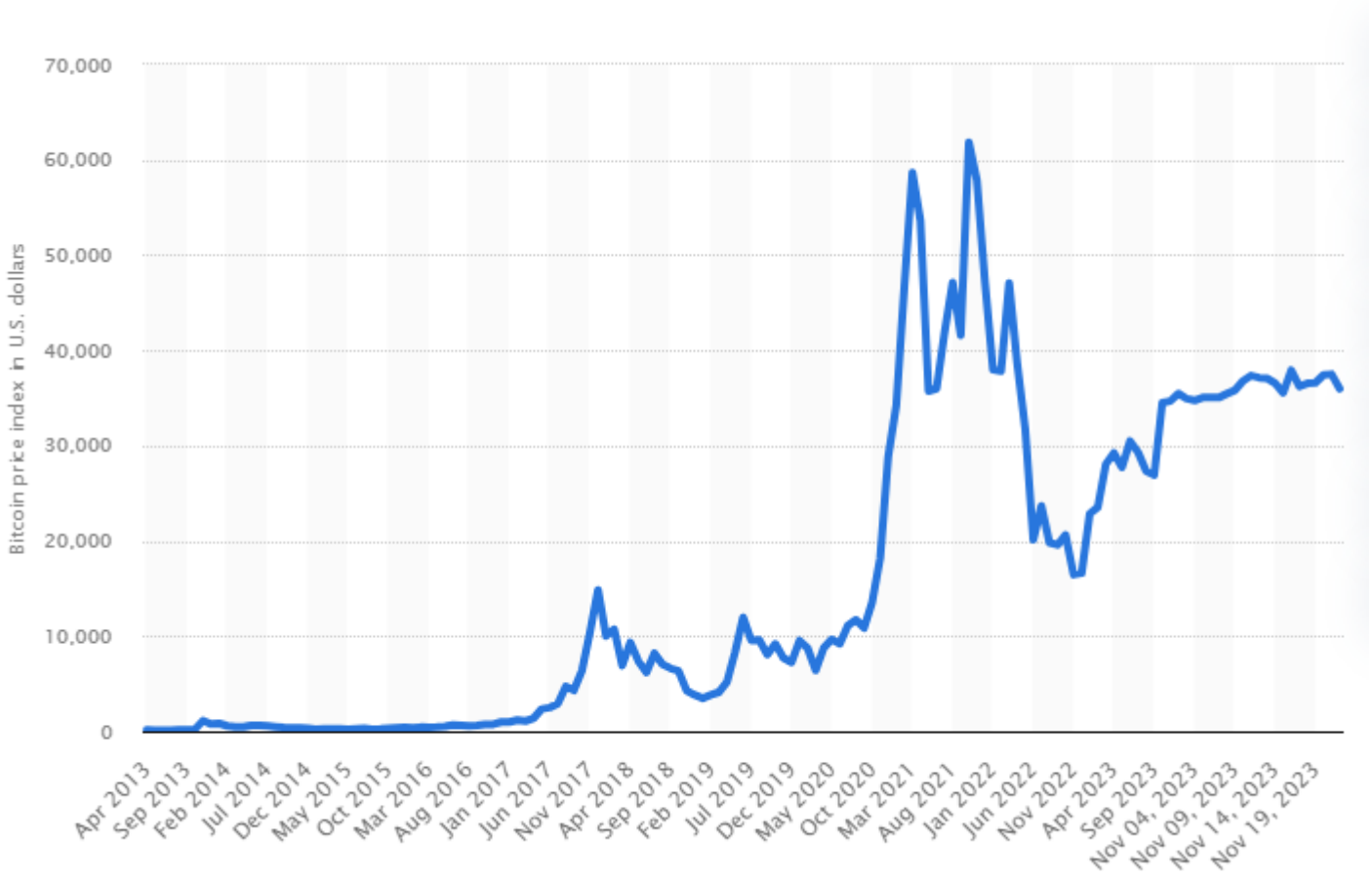
Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required 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.

1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-

Cryptocurrency

- Historical price of Bitcoin



https://www.statista.com/statistics/326707/bitcoin-price-index/

Cryptocurrency

- Over 2000 cryptocurrencies at this moment

#	Name	Price	1h %	24h %	7d %	Market Cap	Volume(24h)	Circulating Supply	Last 7 Days
1	Bitcoin BTC	$16,548.55	0.15%	0.10%	1.82%	$318,509,031,371	$14,072,750,370 850,380 BTC	19,246,943 BTC	
2	Ethereum ETH	$1,193.86	0.10%	0.03%	2.33%	$146,097,300,026	$3,924,639,802 3,287,236 ETH	122,373,866 ETH	
3	Tether USDT	$0.9997	0.00%	0.00%	0.04%	$66,242,049,307	$18,204,631,186 18,210,808,169 USDT	66,263,713,461 USDT	
4	USD Coin USDC	$1.00	0.00%	0.00%	0.02%	$44,418,526,764	$1,911,644,643 1,911,650,421 USDC	44,417,953,798 USDC	
5	BNB BNB	$244.23	0.34%	0.15%	1.00%	$39,068,018,516	$333,823,839 1,366,927 BNB	159,965,012 BNB	
6	XRP XRP	$0.3375	0.27%	2.45%	3.54%	$16,991,559,763	$773,054,475 2,287,497,371 XRP	50,343,500,506 XRP	
7	Binance USD BUSD	$0.9999	0.04%	0.02%	0.03%	$16,874,072,993	$4,444,906,244 4,444,314,970 BUSD	16,875,827,752 BUSD	
8	Dogecoin DOGE	$0.06965	0.57%	1.16%	11.25%	$9,240,250,237	$285,725,288 4,102,712,672 DOGE	132,670,764,300 DOGE	
9	Cardano ADA	$0.2421	0.33%	1.38%	6.61%	$8,355,124,379	$185,021,878 763,200,272 ADA	34,513,553,899 ADA	
10	Polygon MATIC	$0.7615	0.03%	2.41%	4.85%	$6,651,258,197	$193,536,301 254,040,670 MATIC	8,734,317,475 MATIC	
11	Dai DAI	$0.9997	0.02%	0.00%	0.05%	$5,774,087,747	$154,837,083 154,874,872 DAI	5,775,736,311 DAI	

Cryptocurrency

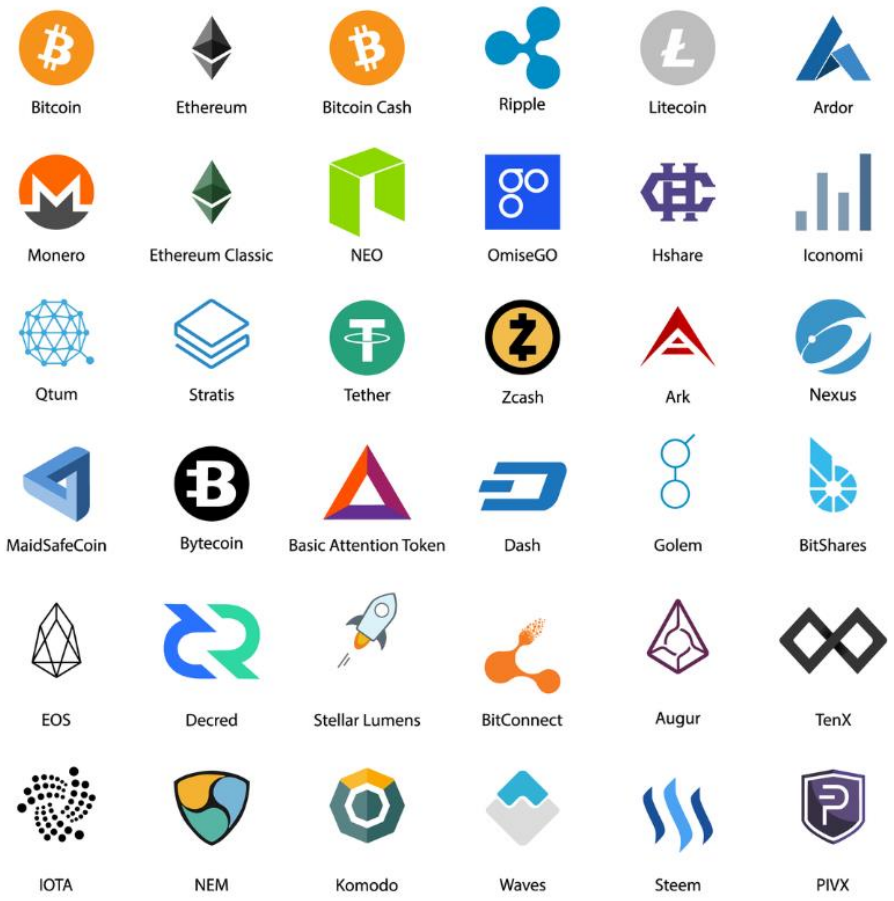
- Cryptocurrencies have different features.

	Bitcoin (BTC)	Zcash (ZEC)
System	Homology Difference: Zcash code is modified based on Bitcoin V.0.11.2 code	
Concept	Digital currency	Private digital currency
Tx details	Publicly viewable	Hidden (readable with key)
Tx example	addr. X sent 1 BTC to addr. Y	? sent ? ZEC to ?
Market cap	~ $800 billion	~ $2 billion
Release date	Jan. 2009	Oct. 2016
Release method	Mining	Mining / founders' reward
Mining algorithm	SHA256	Equihash
Support	Web-based wallet	Zcash: only linux, command line without GUI
Total Amount	21 million	21 million
Time	10 mins	2.5 mins
Block size	1 M	2 M

Cryptocurrency

Advantages

- Fast, safe and cheap
- Ease of use and high portable
- Pseudonymity
- Decentralization
- Active involvement of users
- Transparent and neutral



Cryptocurrency

Disadvantages

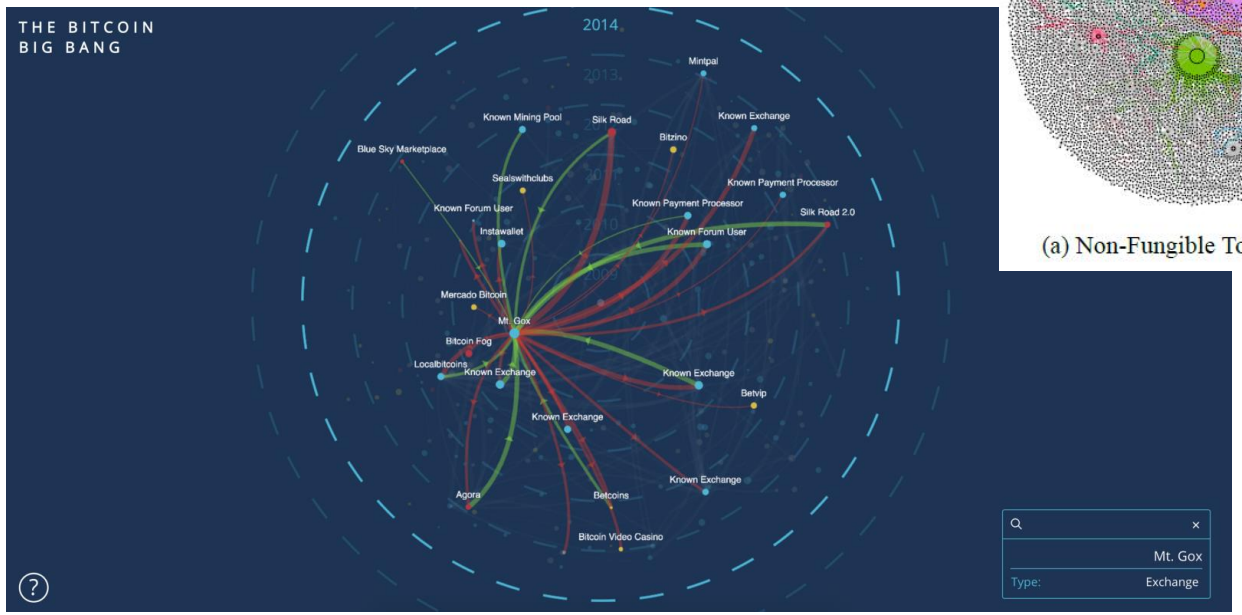
- Unrecoverable once lost
- High market volatility
- Malicious activities (money laundering, scam)

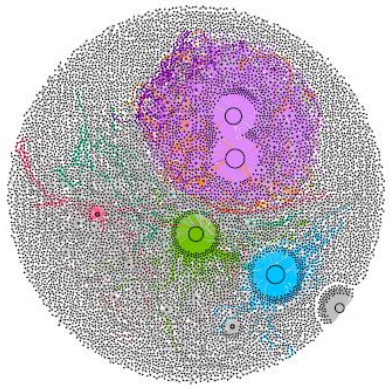
Challenges

- Lack of auditability
- Complex mathematical calculations
- Data privacy
- Performance (high latency, low throughput)
- Communication between different blockchains

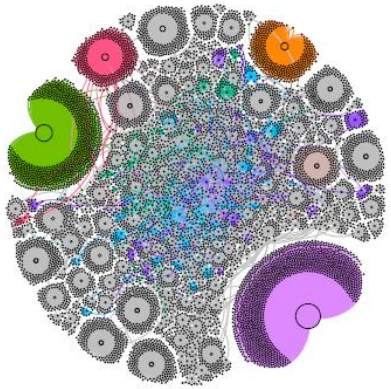
Data analysis on Cryptocurrency

- Software (such as Chainalysis, Elliptic) can infer your address if you have transacted with other addresses that are not anonymous.

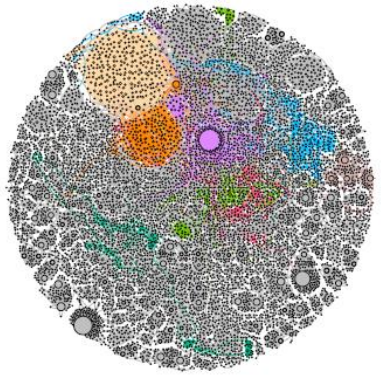




(a) Non-Fungible Token (NFT)



(b) Ethereum



(c) Blockchain

Visualization of blockchain networks

Non-Fungible Token (NFT)

- NFT is a unit of data stored on blockchain to represent the ownership of an object (a virtual asset)
  - Each NFT represents something unique, not interchangeable, and not divisible
  - Can be photos, videos, audio, and other types of digital files
- Platforms and Standards
  - Ethereum
    - ERC-721
    - ERC-1155
  - FLOW
  - Tezos
  - Solana

Community: Projects and Brands

NFT

- NFTs are unique and non-interchangeable assets (data) stored on blockchains
- Fungibility – the ability of an asset to be exchanged or substituted with similar assets of the same value.

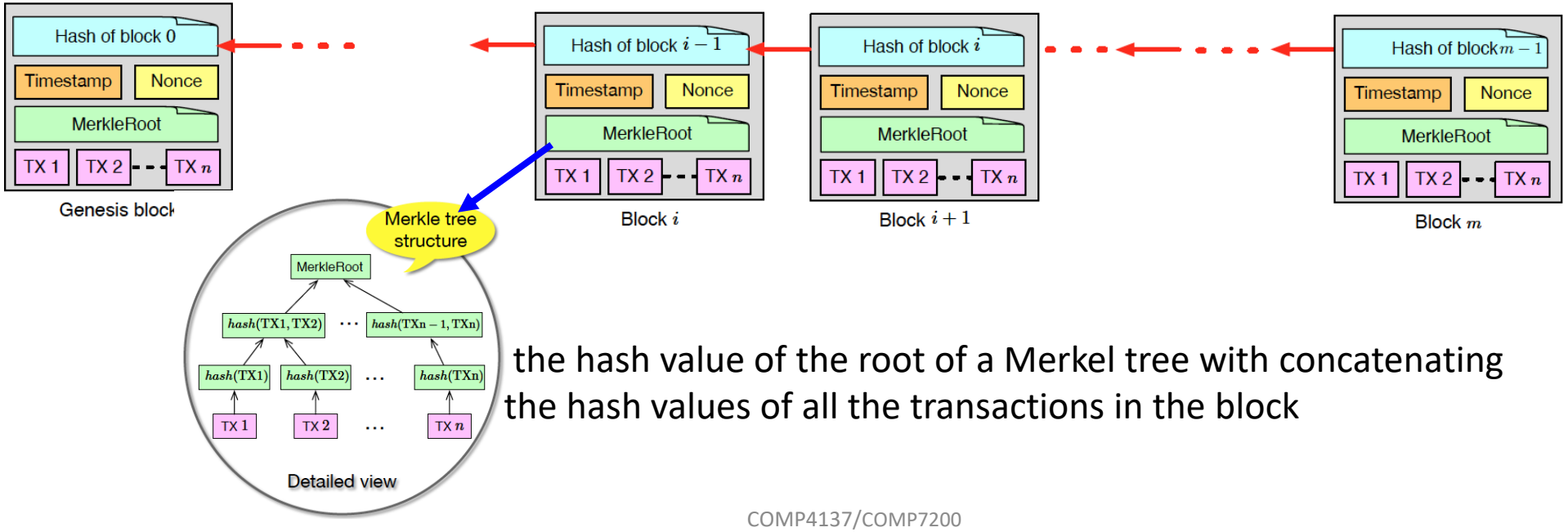
The lack of interchangeability (fungibility) distinguishes NFTs from blockchain cryptocurrencies.

Outline

- Cryptocurrency
- Blockchain
- Blockchain Applications

Blockchain - A High-level View

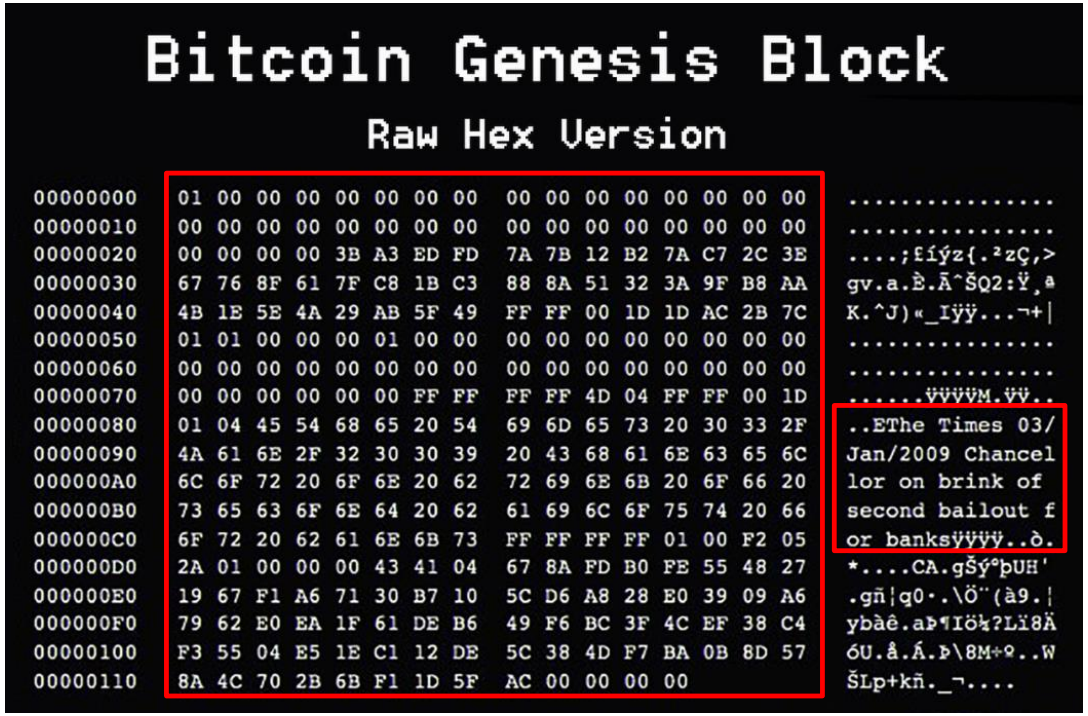
- Cryptocurrency != Blockchain
- Blockchain: a kind of data structure
- A blockchain consists of a number of consecutively-connected blocks.
  - Each block points to its immediately-previous block (called parent block) via an inverse reference that is essentially the hash value of the parent block.



the hash value of the root of a Merkel tree with concatenating the hash values of all the transactions in the block

Blockchain

- Bitcoin Genesis Block



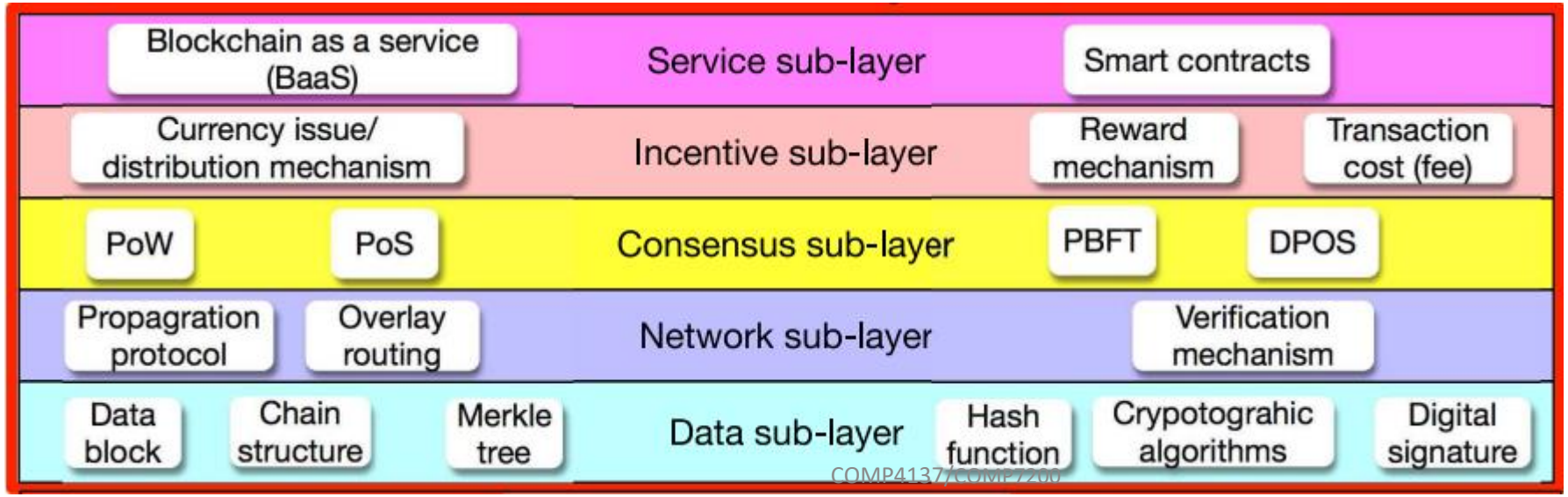
"The Times 03/Jan/2009 Chancellor on brink of second bailout for banks"

*hypotheses…

https://btc.com/4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b

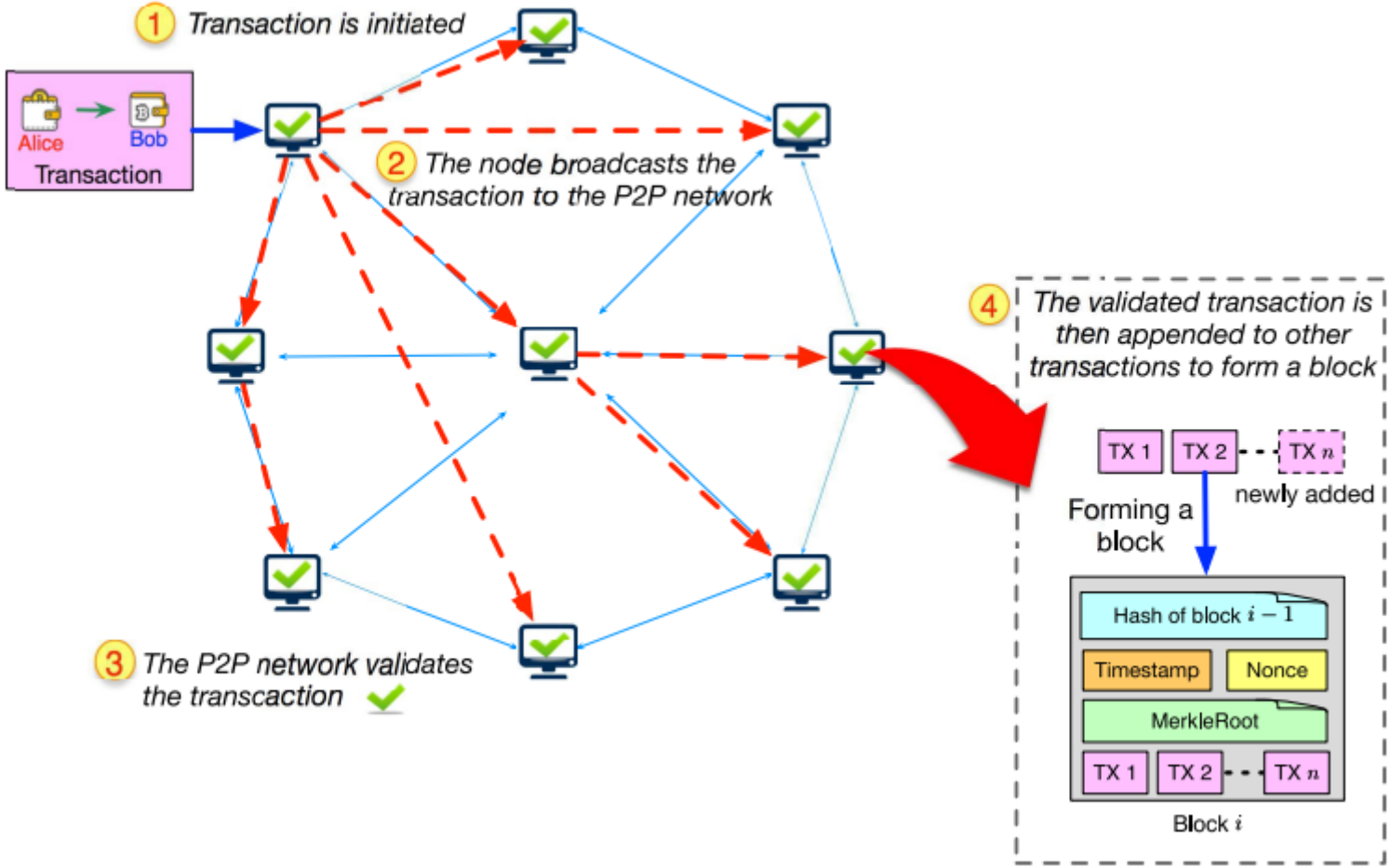
Blockchain - A High-level View

- Blockchain System: a decentralized system
- The construction of a blockchain system requires diverse ICT technologies:
  - Cryptographic algorithms
  - Computer networks
  - Distributed systems and consensus
  - Smart contracts (software technology)
  - Reward and transaction cost (economics)



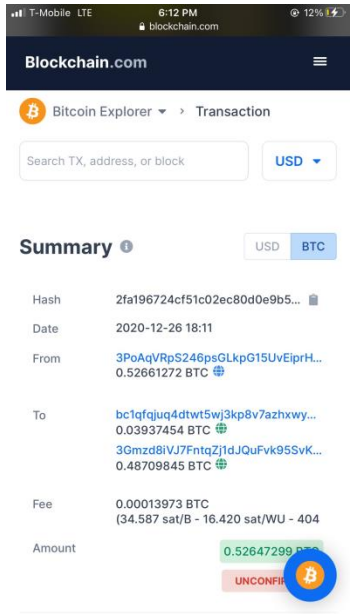
Working flow of blockchain

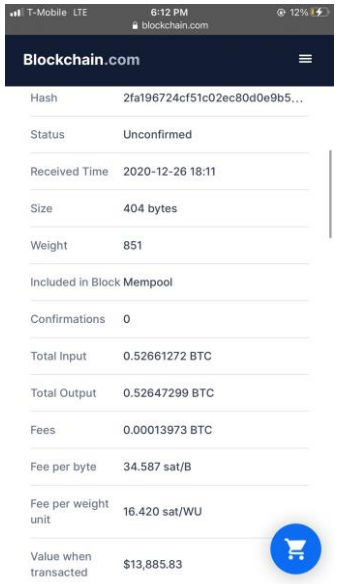
- Consider a single transaction



Blockchain Transactions

- Smallest element
- Record every decision and action taken
- Proof of history, provides **provenance**





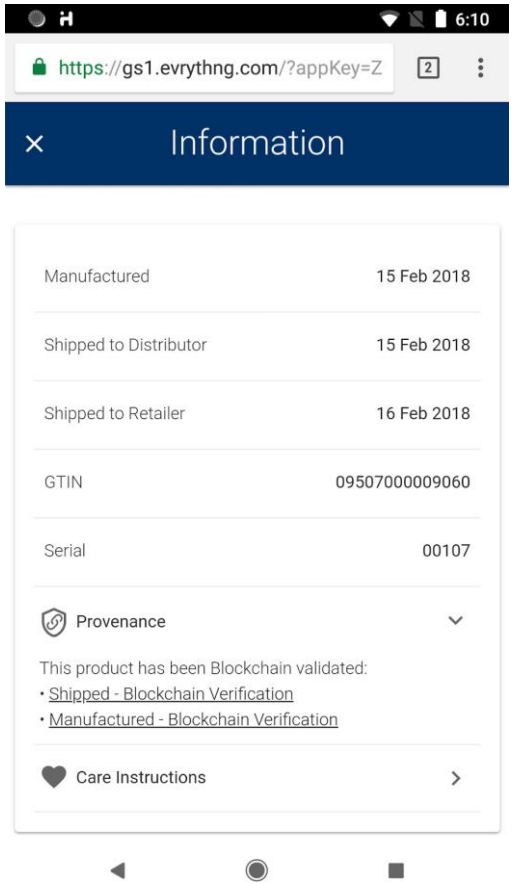
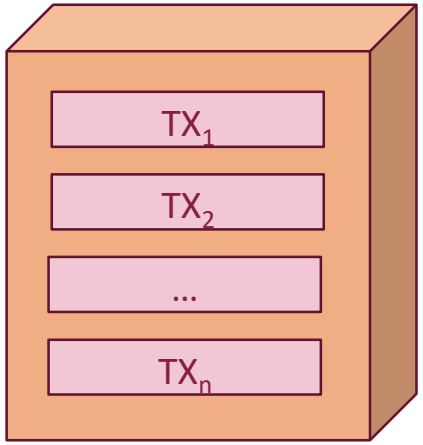


Image from https://evrythng.com/

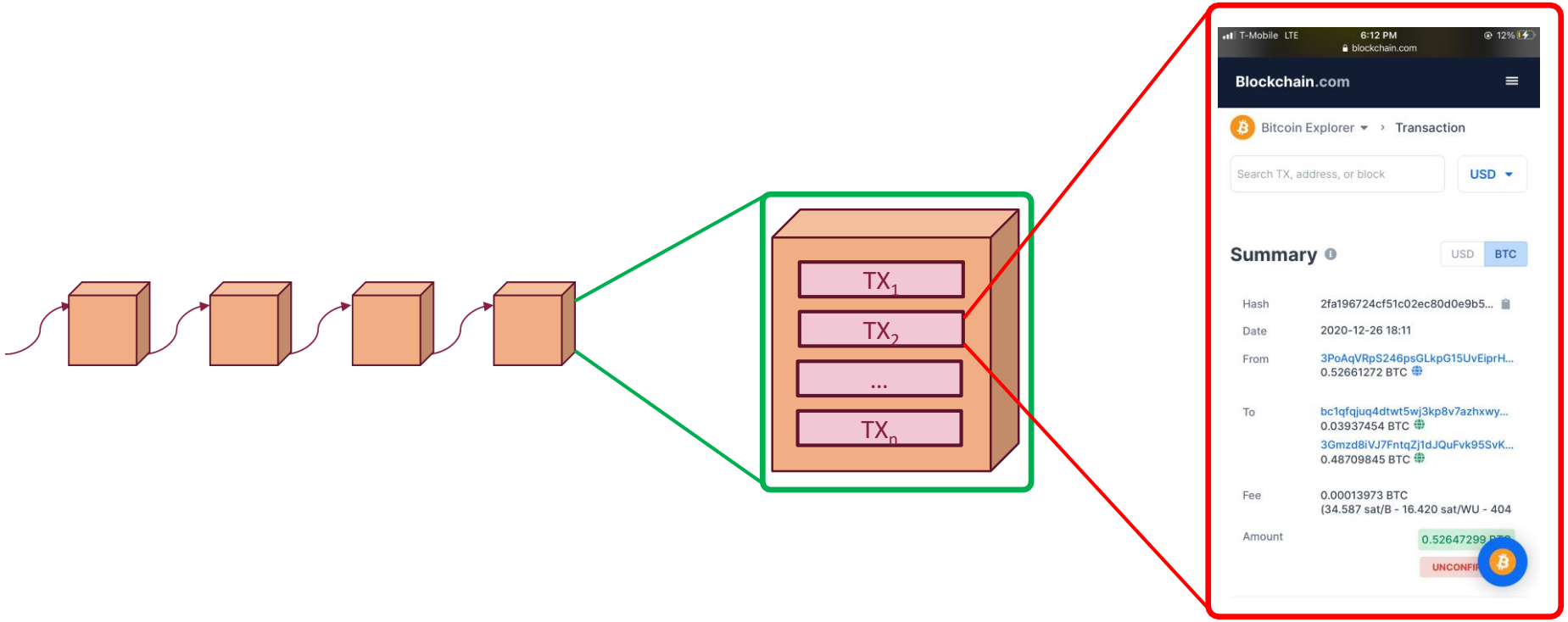
Blockchain "Block"

- Contain multiple transactions
  - The transaction is <u>immutable/indelible</u>
- Write and Read-Only
- Once a block is chained, it is extremely difficult to change
  - Modification possible
  - Rework on all the subsequent blocks and consensus for each block



Chain of Blocks

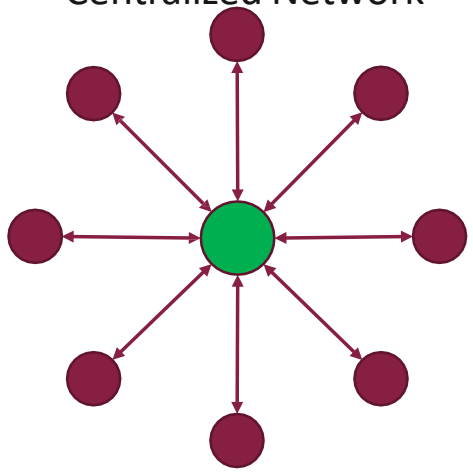
- Contain multiple blocks
- Blocks linked using cryptography
- An instance of distributed ledger



Distributed Network

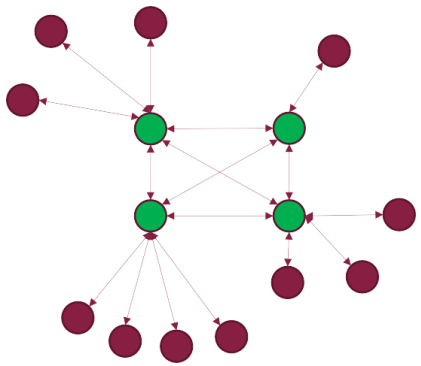
- Blockchain operates on a decentralized/distributed P2P network
- Each node stores a copy of the ledger
  - Distributed Ledger

Centralized Network



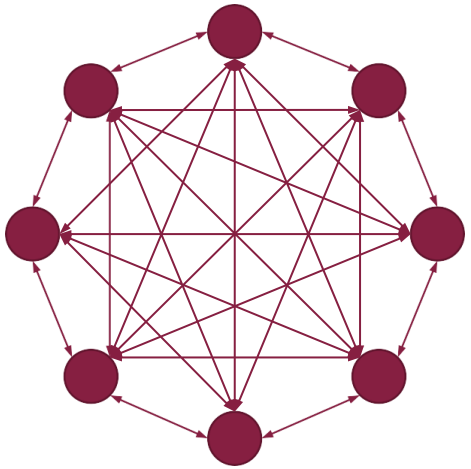
nodes interact with a single central node

Distributed Network



nodes interact with some central nodes

Decentralized Network



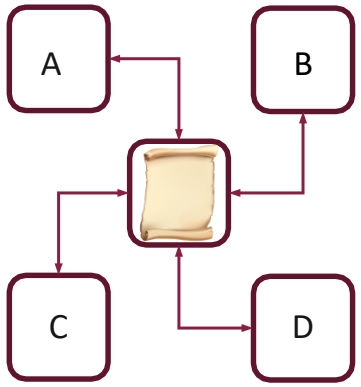
Nodes interact with each other directly

Distributed Ledger

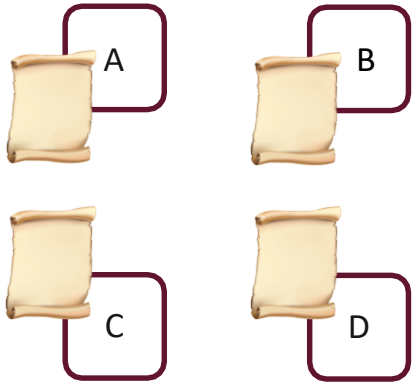
Blockchain is a distributed ledger

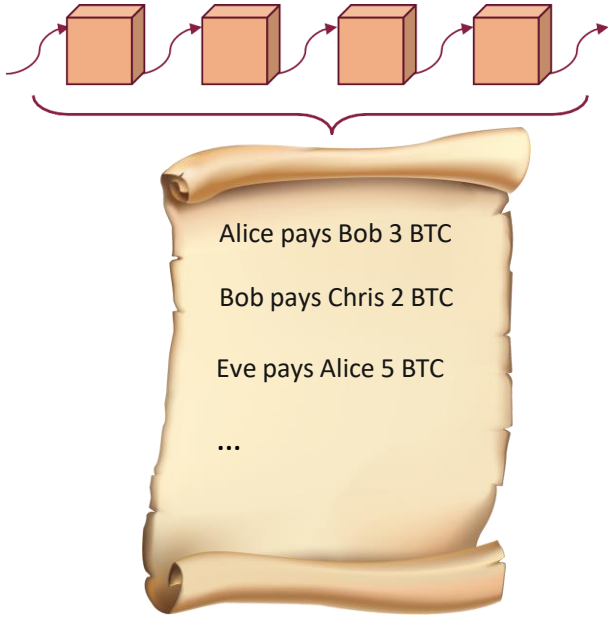
- **Centralized ledger:** stored by a central node
- **Distributed ledger**: stored in every node
  - All nodes agree on the true state of the ledger (via a consensus protocol)

Centralized ledger



Distributed ledger





Distributed Ledger

- Keep track of <u>all</u> transactions performed in the network
- Can be encrypted for confidentiality
- Can be used without by individuals without a central authority
- **Immutable:** Ledger records are very difficult to be altered
  - Changing a record in the ledger requires a consensus from <u>all</u> participants
  - Rework on all subsequent records

Demo of blockchain

- https://andersbrownworth.com/blockchain/

Distributed Consensus

- Ensure the blocks in blockchain are <u>valid</u> and <u>truthful</u>
- Prevent malicious adversaries from system compromise and chain-forking
- Many consensus protocols, each with different pros and cons
  - Proof of Work (PoW), Proof of Stake (PoS), Proof of Elapsed Time (PoET), Proof of Activity (PoA), Proof of Burn (PoB)
  - Paxos, BFT, Streamlet
- We will explore many of blockchain consensus protocols later

Smart Contract

- A program running in a secure environment that controls the transfer of digital assets between parties under certain conditions
- Contract encoded into blockchain
- Enable broader blockchain applications beyond cryptocurrencies

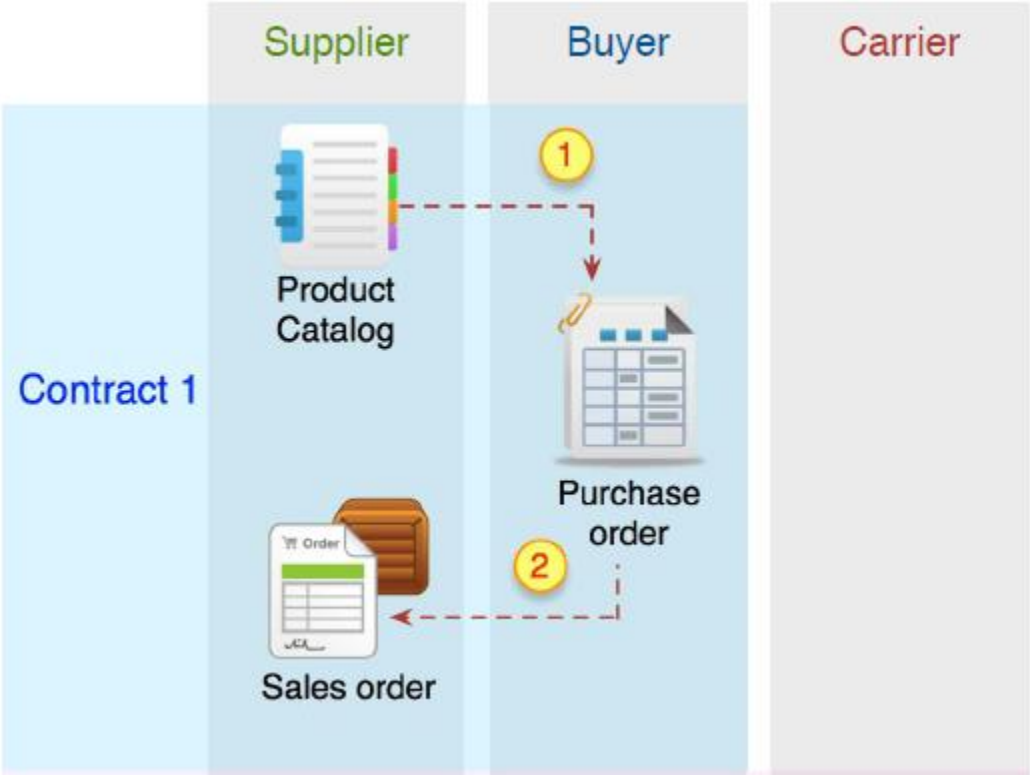
```
pragma solidity 0.5.8;

contract SimpleBank {

   mapping(address => uint) balances;

     function deposit(uint amount) payable public {
     balances[msg.sender] += amount;
   }

     function withdraw() public {
     msg.sender.transfer(balances[msg.sender]);
     balances[msg.sender] = 0;
   }
}
```

Smart Contract

- Smart contract is a computer program that
  - **Defines** rules
  - **Enforces** obligations and penalties
  - **Executes** actions required by clauses
  - **Autonomous** without ownership
  - **Secure**
- Written in a high-level programming language (e.g., Solidity)

Blockchain Techniques	Smart Contracts?	Language
Bitcoin	✗	C++
Ethereum	✓	**Solidity**
Hyperledger	✓	GoLang, C++, etc

Smart contract



Smart contract

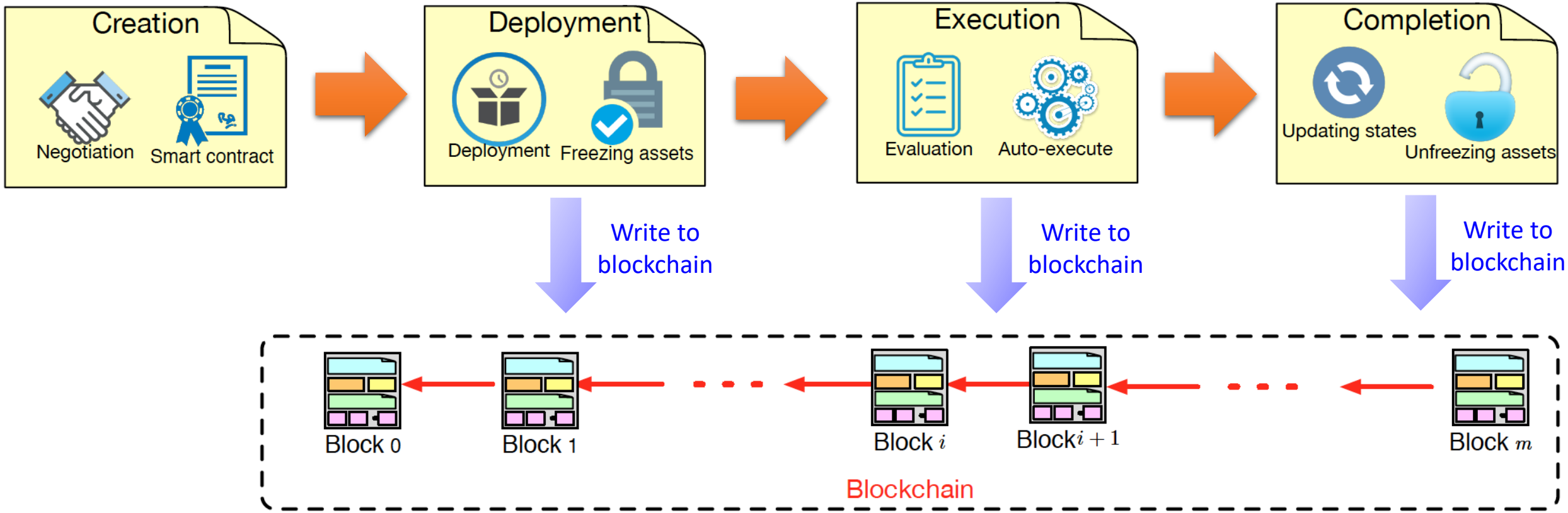
Smart contract

Merits of smart contract

- **Reducing risks**. Due to the immutability, traceability and auditability of blockchain data
- **Cutting down administration and service costs**. Blockchains assure the trust without going through a central broker or a mediator. Smart contracts can be automatically triggered in a decentralized way.
- **Improving the efficiency of business processes**. The elimination of the dependence on the intermediary can significantly improve the efficiency of business process.

Smart Contract

- Blockchains are enabling smart contracts.
  - Essentially, smart contracts are implemented on top of blockchains.
- Life cycle of smart contracts



Outline

- Cryptocurrency
- Blockchain
- Blockchain Applications

Development of Blockchain

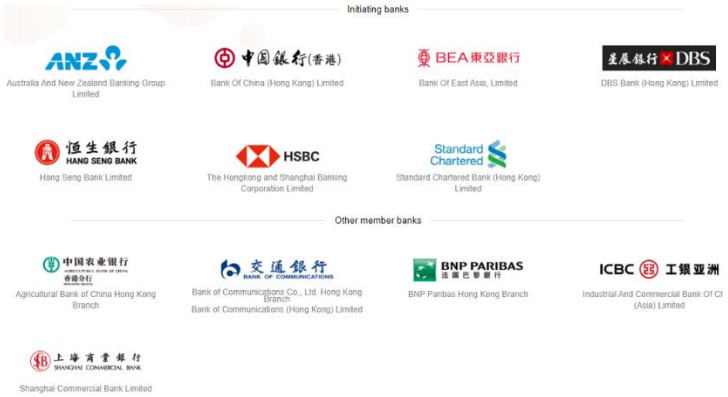
- Blockchain 1.0
  - Bitcoin
  - Programmable Money
- Blockchain 2.0
  - Ethereum
  - Smart Contract
- Blockchain 3.0
  - Fix problems in current blockchain industry
  - Scalability
  - Inter-operability
  - Privacy
  - …

Blockchain Applications

- Key industries with blockchain
  - Banking and investment
    - improve decades old operations and processes
  - Gaming and artwork
    - trade of virtual goods with token
  - Retail
    - track & trace, counterfeit prevention, inventory management and auditing

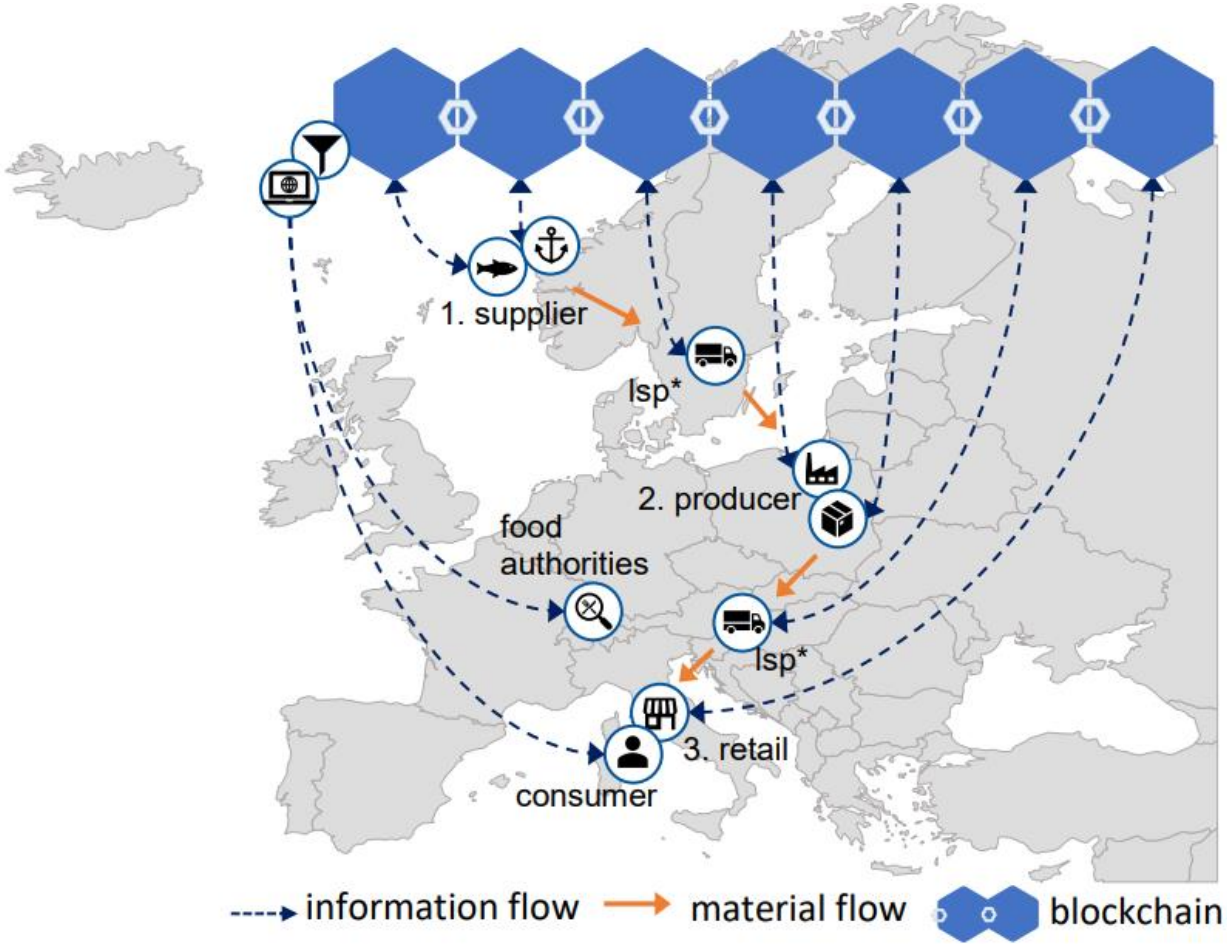
HONG KONG MONETARY AUTHORITY
香港金融管理局

貿易聯動
eTradeConnect



Blockchain network in food industry

- Blockchain can be used in food industry to achieve the traceability of food supply chain
- Information in each procedure will be stored in the blockchain



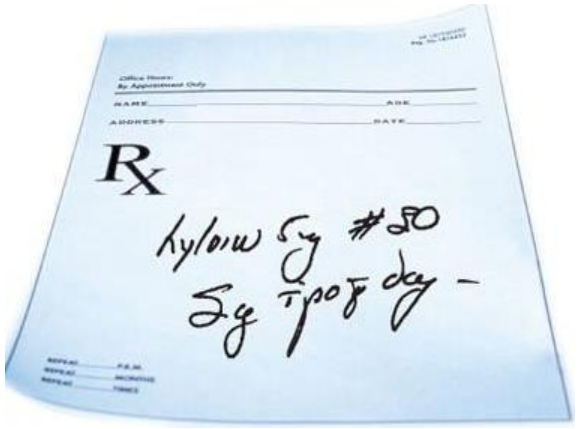
Source: Thume et al., "Blockchain-based traceability in the food industry: requirements analysis along the food supply chain", DOI: 10.31219/osf.io/uyb64

Blockchain in Medical records

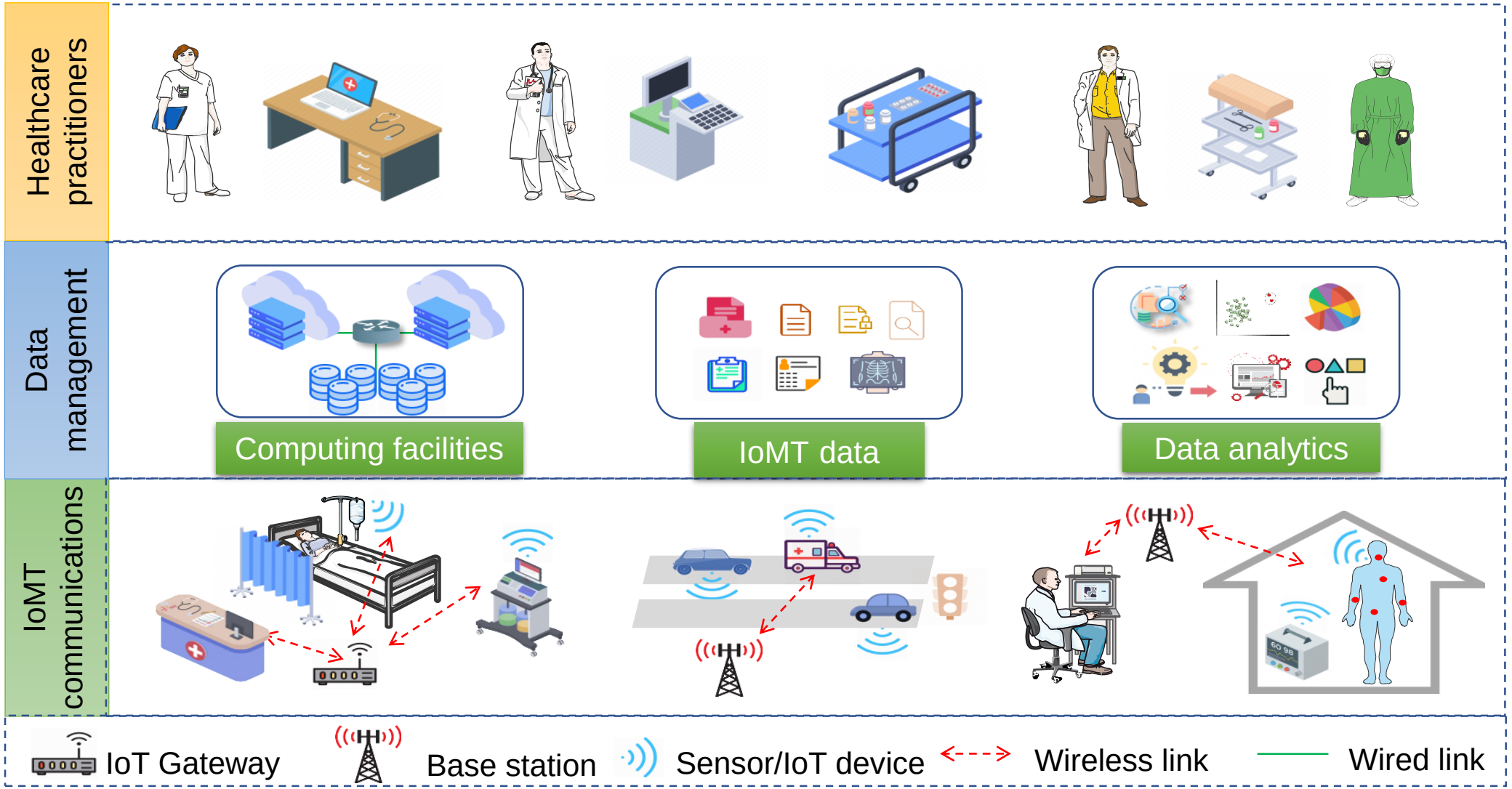
- You enter a health facility (not your home facility)
- You provide proof of identity verified with a blockchain
- Your “private key” unlocks encrypted data related only your health records
- Also provides a much stronger privacy protection
  - Instead of a medical database being encrypted with one key (which might be lost or discovered), each patient’s record has its own key. Hence, to compromise the database you would need to guess potentially millions of keys

Blockchain in Medical Prescriptions

- Widespread fraud
- Blank scripts are stolen from doctors' offices or forged
- Some doctors abuse the system
- Token issued to patient: it cannot be resold and has an expiration
- Patient presents token to pharamacist and blockchain is checked to make sure patient owns the token (and has not already spent it)



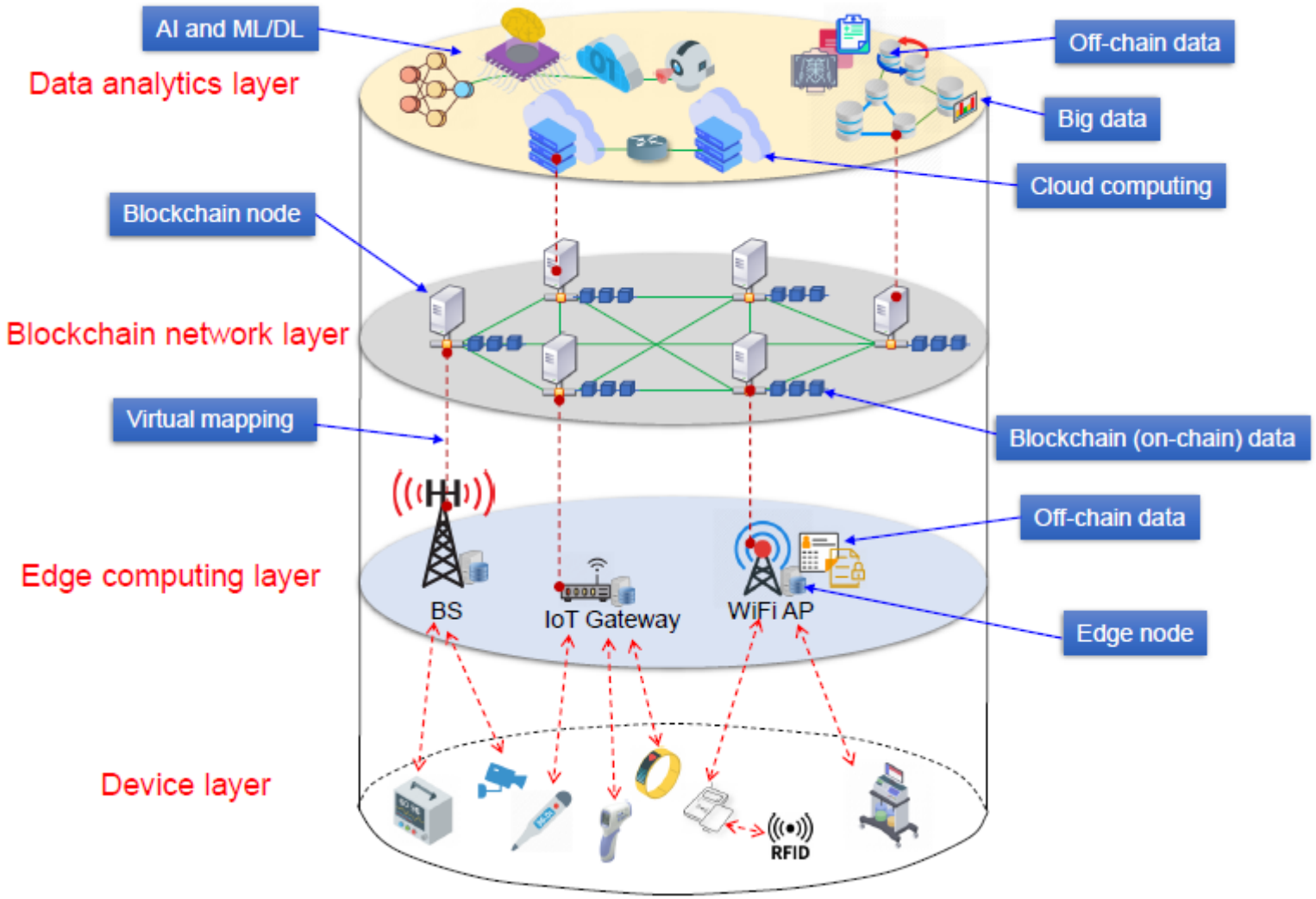
Internet of Medical Things



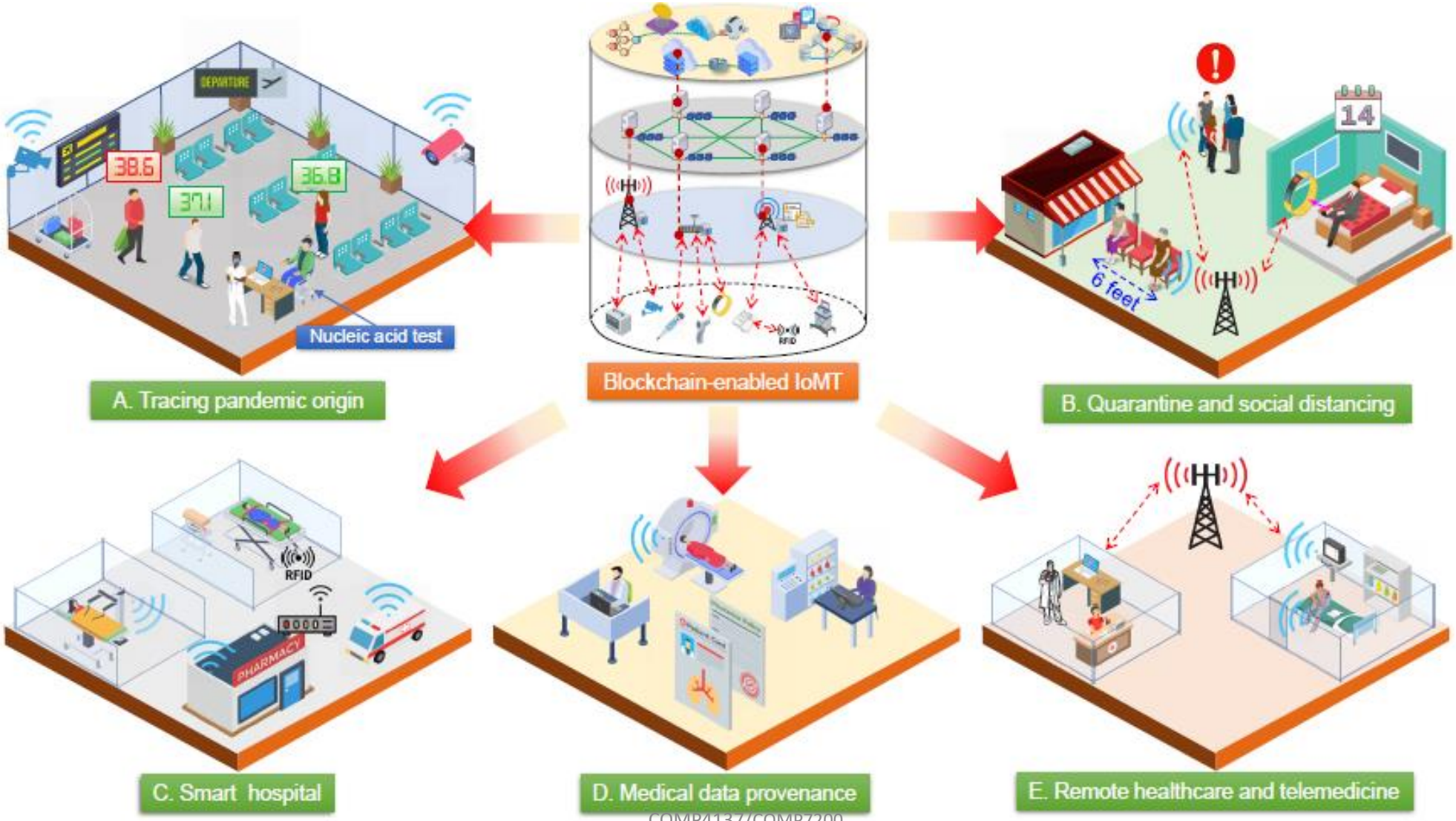
Challenges of IoMT

- Absence of interoperability across different IoMT sectors
  - Different IoMT devices (body sensors, medical devices)
  - Diverse IoMT protocols
- Privacy and security vulnerabilities of IoMT devices and systems
  - Difficult to deploy cryptographic algorithms
  - Outsourcing data to clouds (untrusted, e.g., icloud instrusion)

Architecture of blockchain-enabled IoMT



Solutions of Blockchain-enabled IoMT to COVID-19



Summary

- Blockchain is <u>interdisciplinary</u>
- Cryptography and Distributed Systems are fundamental building blocks

Operation	Crypto Techniques
Init & Broadcast Transactions	• Digital Signature • Private/Public Keys
Transaction Validation	• Proof-of-Work
Chaining blocks	• Hash Function