THE UNIVERSITY OF HONG KONG

DEPARTMENT OF COMPUTER SCIENCE

HKU-SCF FinTech Academy Workshop Series

Digital Currency - Technology, Challenges and Opportunities

History and Recent Advances in Blockchain-Enabled Cryptocurrencies

DR. ALLEN AU

THE UNIVERSITY OF HONG KONG

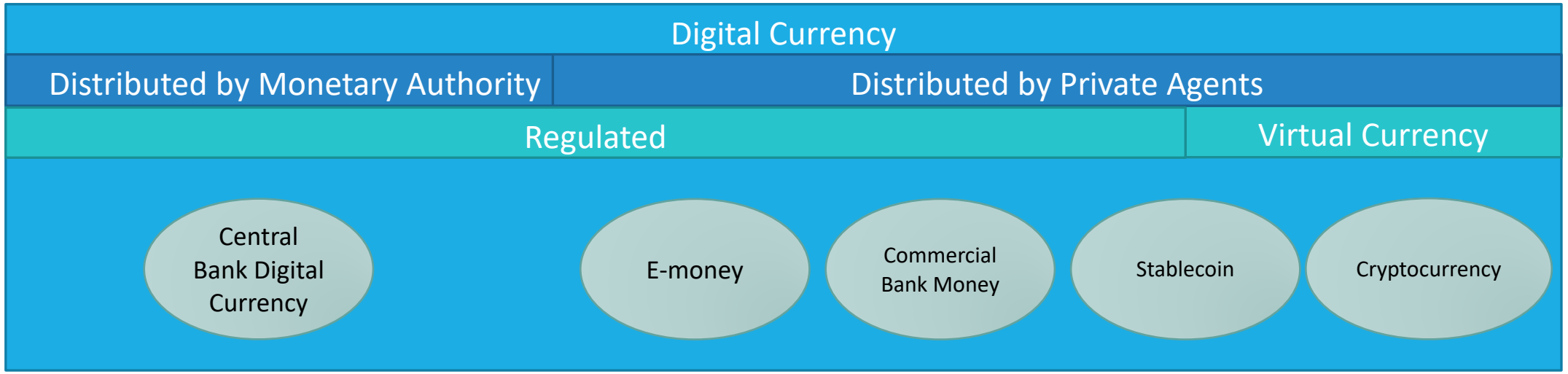
Outline

- Digital, Virtual and Cryptocurrency
- Blockchain-Based Cryptocurrencies
- Challenges
- Recent Advances
- Conclusions

A Money Taxonomy

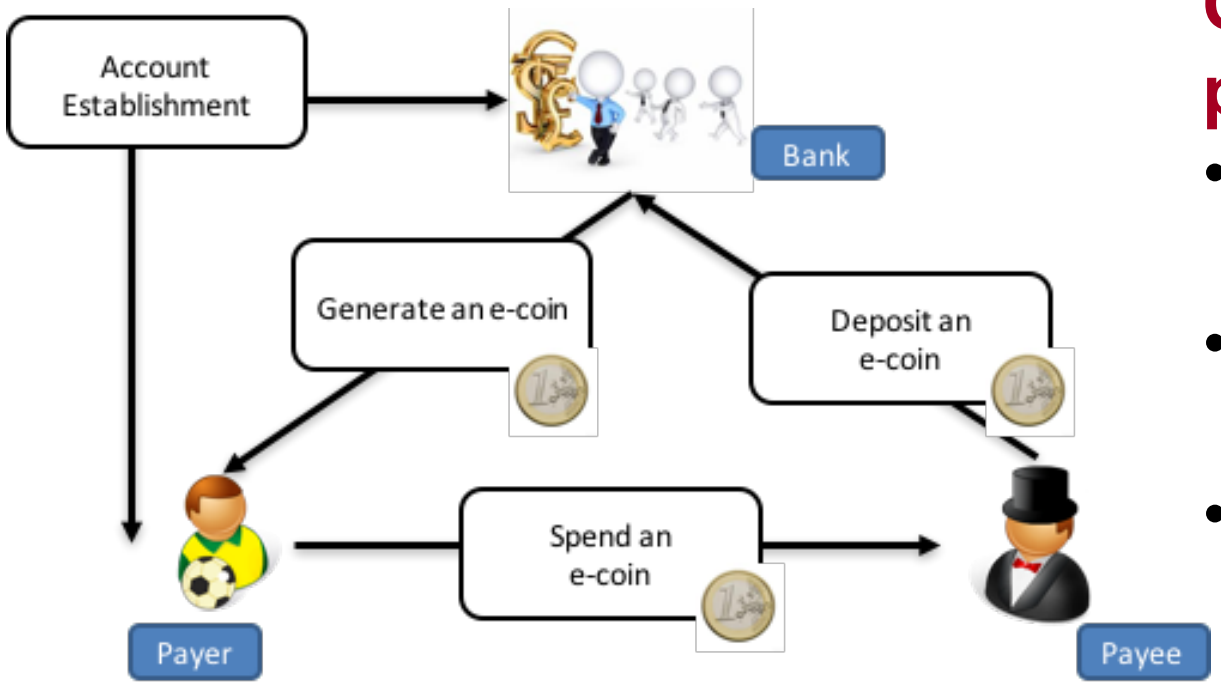
Legal Status		Some local currencies	Virtual currency
	Unregulated		
	Regulated	Banknotes / coins	E-money, CBDC
		Physical	Digital
		Format	

Virtual Currency Schemes
ECB 2012



Taxonomy and definition of terms for digital fiat currency ITU 2019

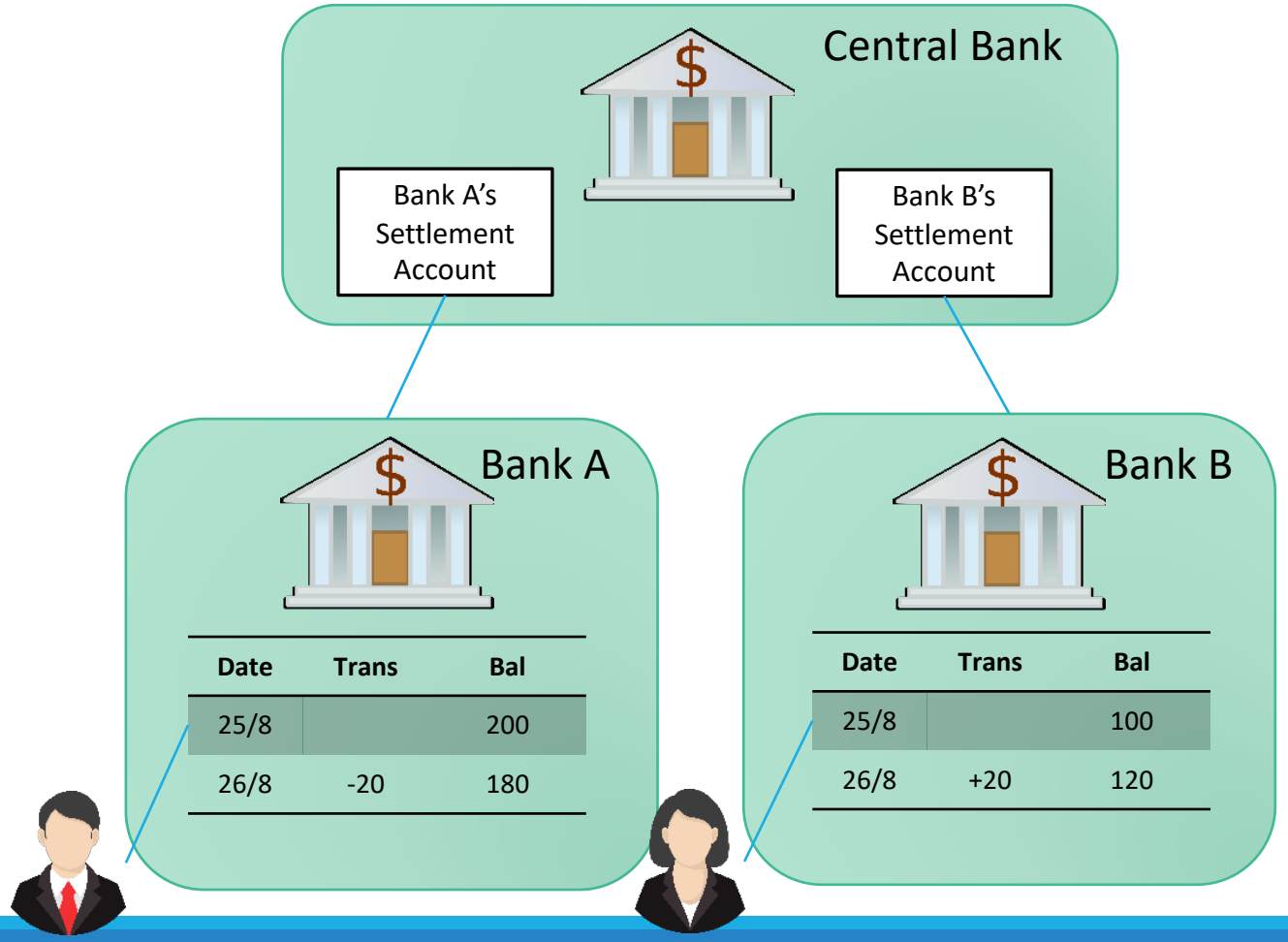
Electronic Cash



One crucial difference between paper money and digital money

- Paper money protected by anti-counterfeit technology
- Digital money can be copied electronically
- The Problem of double-spending

The Payment System



Central Bank's Ledger: Settlement accounts

Clearing Bank's Ledger: Customer accounts

Payments are made by reducing the balance in the sender's account and increasing the balance in the recipient's account. Note that the central ledger takes a crucial role in the transaction.

- One ledger per user
- Trust the bank

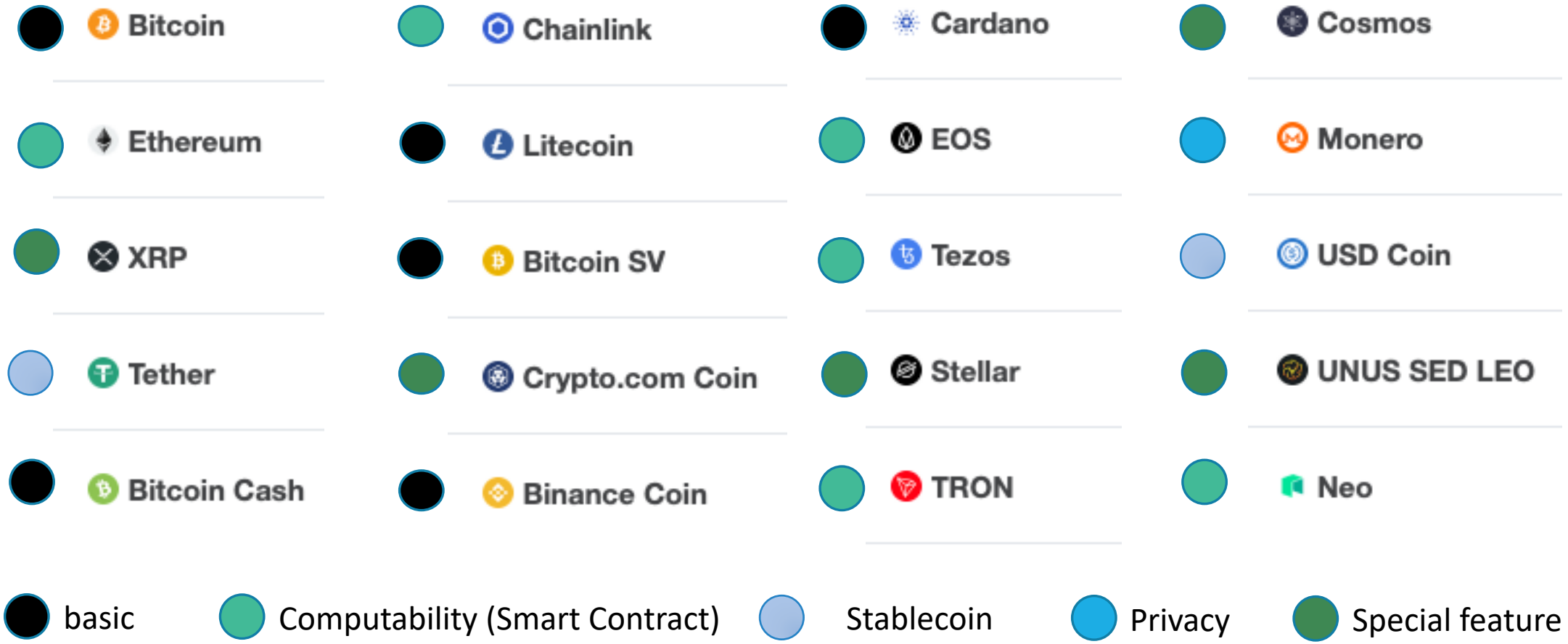
Towards Blockchain-Based Cryptocurrencies

Date	Transatcion	Consent
25/8	Bob -> Alice : 10	Bob's digital signature
26/8	Bob -> Alice : 50	Bob's digital signature
26/8	Alice -> Bob : -20	Alice's digital signature

Who maintain this ledger?

- One single, shared ledger
- Of all users
- Consent represented by digital signatures
- Trust the technology

Cryptocurrencies with various features



Blockchain 101

Applications (Ledger)

Data Structure

Consensus

Date	Trans	Consent
12/3	Bob -> Alice : 10	Bob's digital signature
13/3	Bob -> Alice : 50	Bob's digital signature
14/3	Alice -> Bob : -20	Alice's digital signature

Transaction

Each block contains data

Block 1

Block 2

Block 3

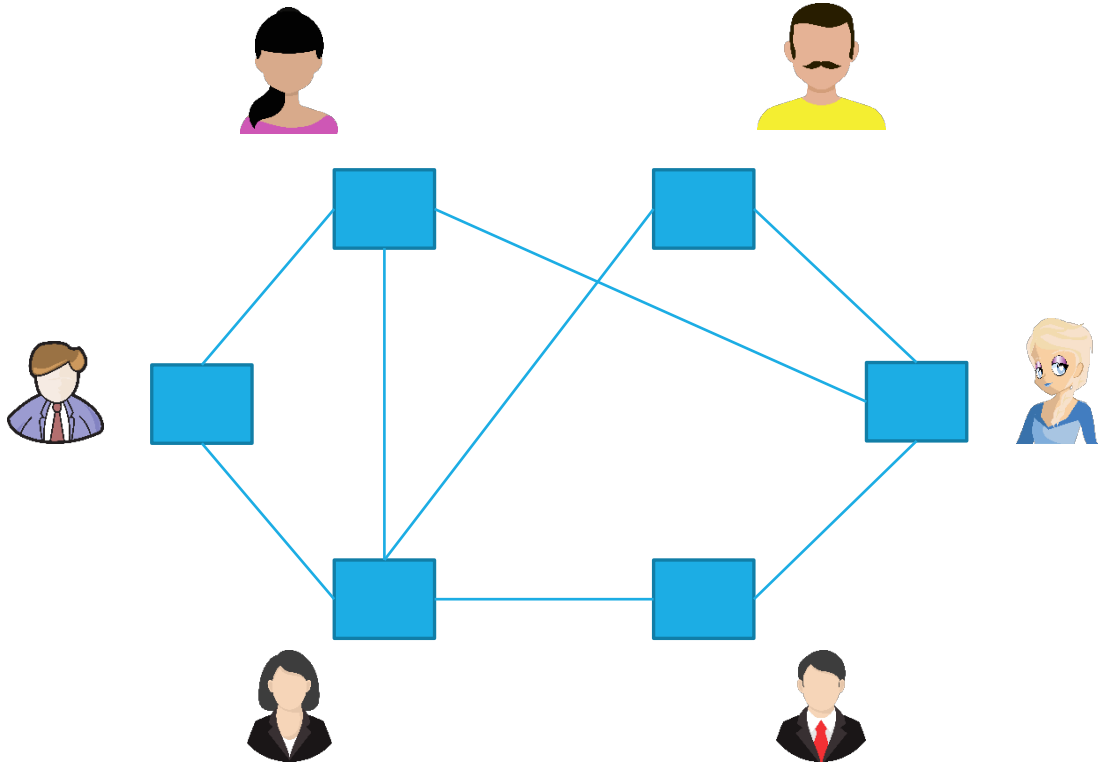
Block 4

A block is tied to previous block

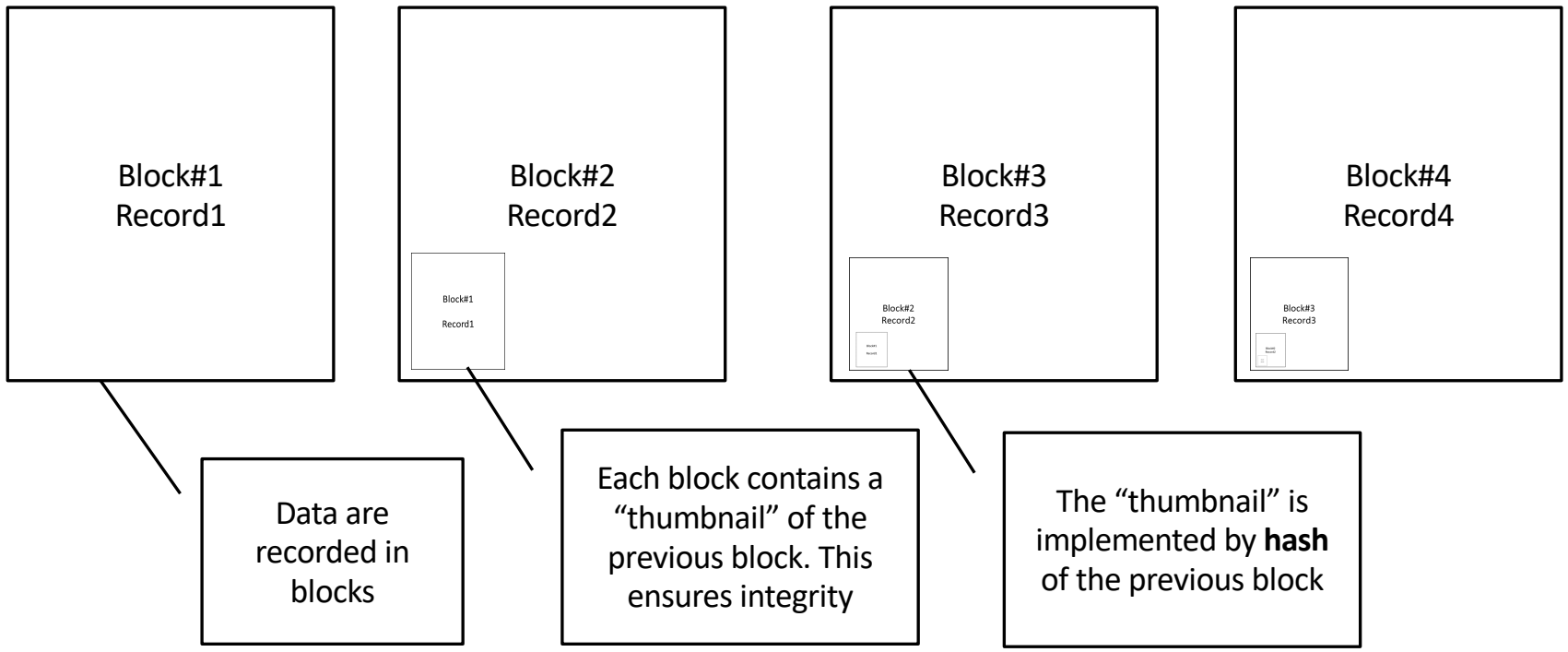
Network nodes

Blockchain: A Distributed Ledger

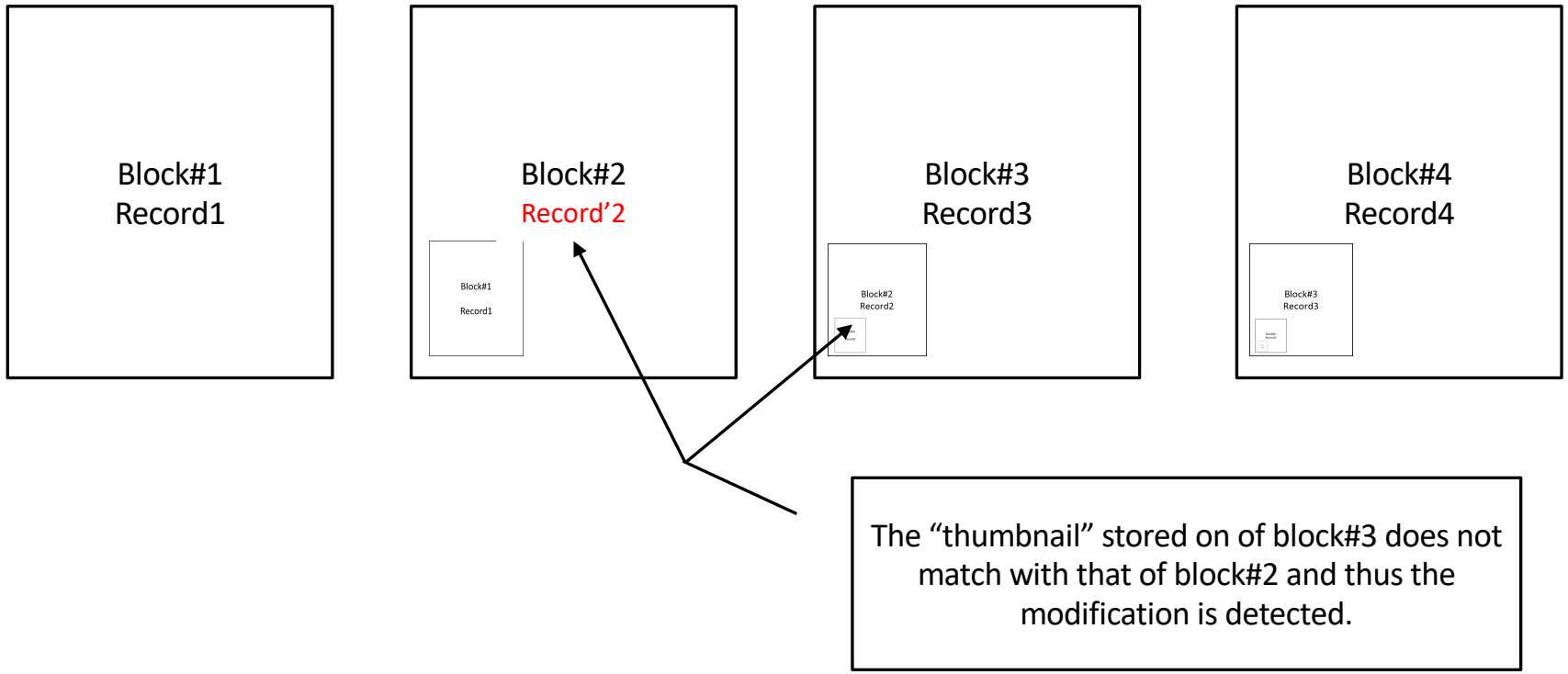
- Blockchain is the technology that built distributed ledger
- Each node in the network maintains a consistent view of the ledger
- Secure even if some of the nodes are malicious



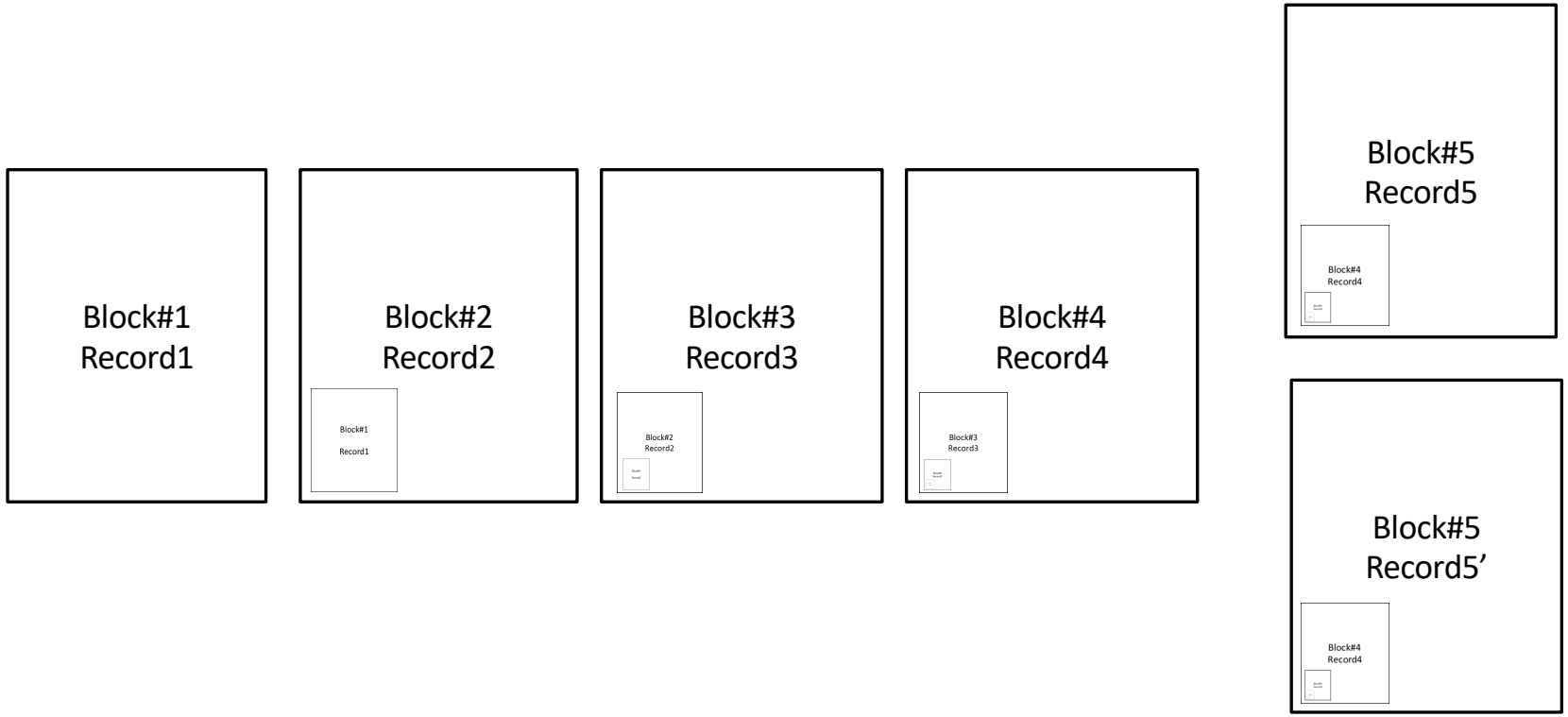
Blockchain: An Append-Only Ledger



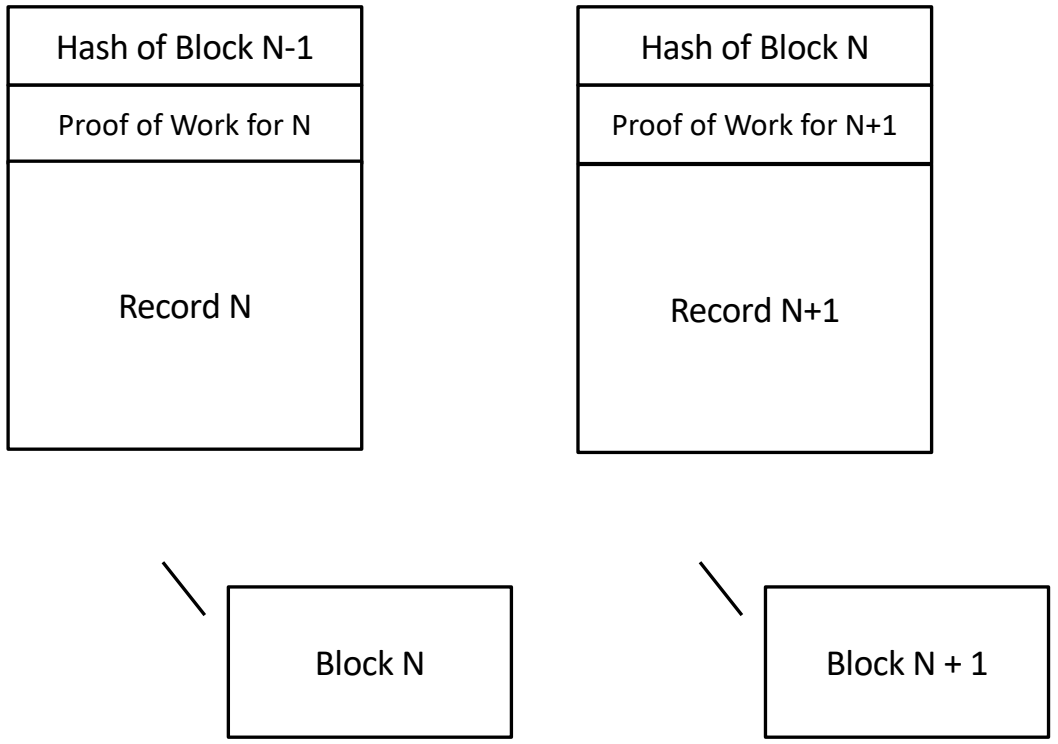
Blockchain: An Immutable Ledger?



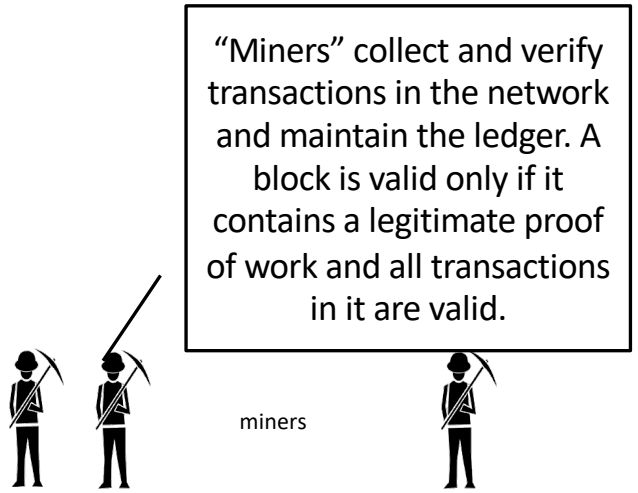
Appending new records



Mining: The competition for the next block



$$H(\boxed{\text{Block N+1}}) < 2^{186}$$



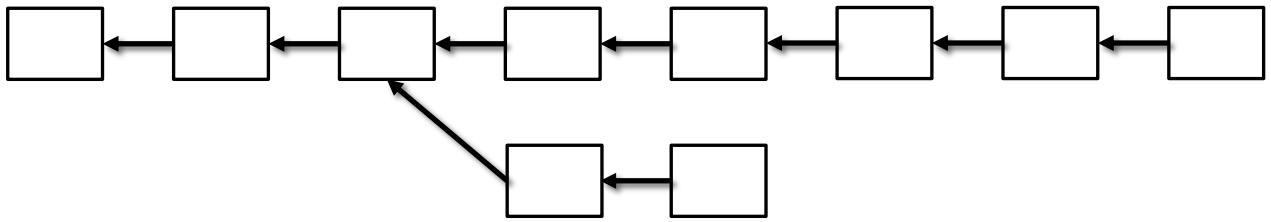
Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008

Consensus Protocol

What happen if two blocks are broadcasted more or less the same time?

- A node should follow the longest chain rule
- Pick one in case there are chain of the same length

Eventually, one chain will be longer



PC

FPGA

field-programmable gate array

Mining rigs inside a mining center

ASIC

application-specific integrated circuit

Blockchain-Based Cryptocurrency

Block 18	
Account	Balance
PK_{Alice}	10
PK_{Bob}	0
PK_{Tom}	0
Transactions	
∅ -> Alice, 10	

Block 19	
Account	Balance
PK_{Alice}	10
PK_{Bob}	10
PK_{Tom}	0
Transactions	
∅ -> Bob, 10	

Block 20	
Account	Balance
PK_{Alice}	0
PK_{Bob}	20
PK_{Tom}	10
Transactions	
∅ -> Tom, 10 Alice -> Bob, 10, Alice's Signature	

Block reward

Smart Contract: Support of Complex Transactions

Block 21	
Account	Balance
PK_{Alice}	2.5
PK_{Bob}	12.5
PK_{Tom}	12.5
Contract code **P**, Contract owned by PK_{Bob}	10
Transactions	
Add new contract from PK_{Bob} with 10 dollar, Code of the contract P	

Smart Contract (aka Distributed Applications DAPP):
The code stored and synchronized in blockchain, which is triggered by user initialized special transaction, and executed concurrently by consensus nodes. It can update the data stored in blockchain and the modified data remains synchronized among all nodes.

```
contract P
{
  uint storedData;
  function init() public {
        storedData = 59;
  }
  function get() public constant returns (uint) {
        return storedData;
  }
  function withdraw(uint w) {
        if (w*w + 10*w + 3 == storedData) {
          msg.sender.transfer(1);
        }
}
```

It can response to input automatically

It is not easy, if not impossible, to write a smart contract that connect to any external system

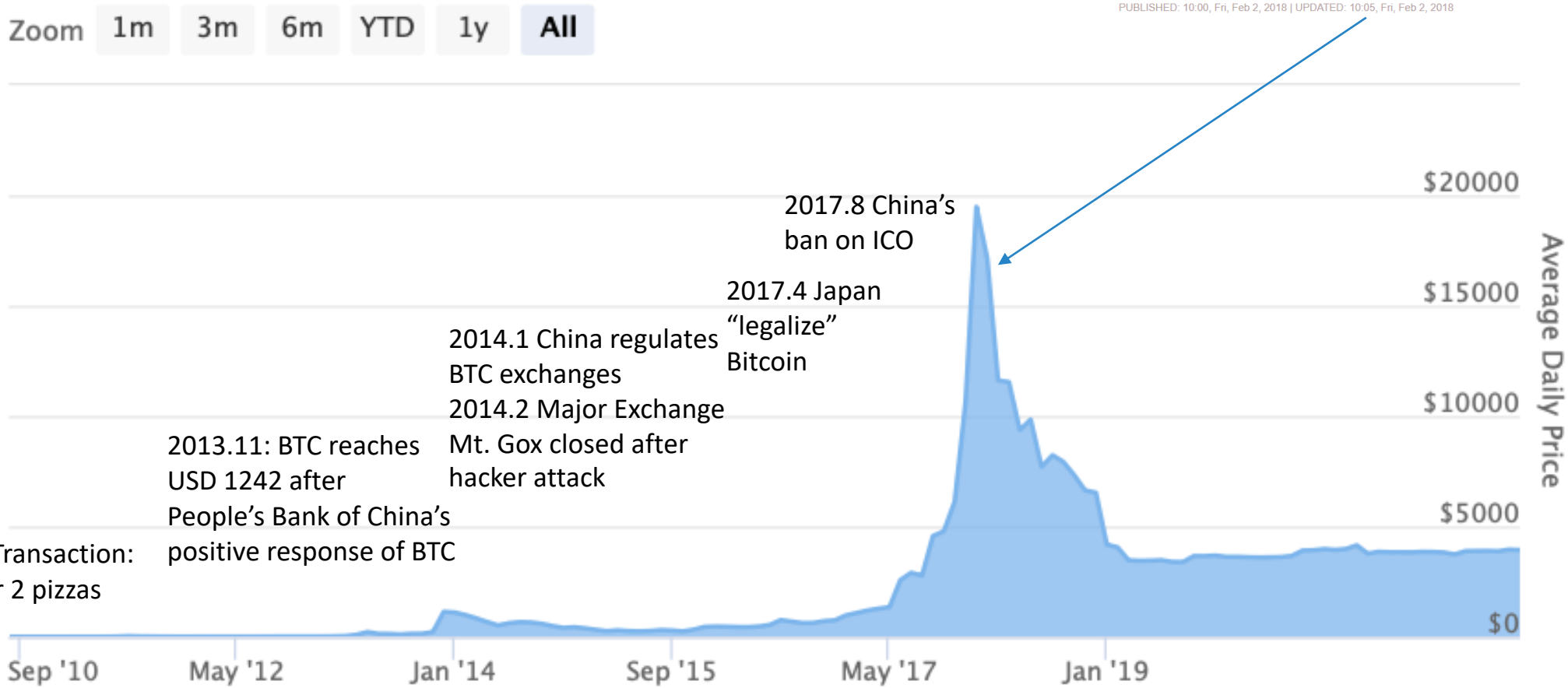
A Brief History of Bitcoin

City & Business News

Bitcoin price: Why is Bitcoin BTC falling today? Will it continue to fall?

BITCOIN's price has plunged by about $25billion in the past 24 hours and the cryptocurrency looks set to suffer another disappointing day on the markets. But why is bitcoin (BTC) falling today?

By JOE TAMBINI
PUBLISHED: 10:00, Fri, Feb 2, 2018 | UPDATED: 10:05, Fri, Feb 2, 2018



2010.5 First Transaction: BTC10000 for 2 pizzas

2013.11: BTC reaches USD 1242 after People's Bank of China's positive response of BTC

2014.1 China regulates BTC exchanges
2014.2 Major Exchange Mt. Gox closed after hacker attack

2017.4 Japan "legalize" Bitcoin

2017.8 China's ban on ICO

Challenges in Adoptions

Business obstacles

Cryptocurrency Bubble

- Promising applications are overwhelmed by unrealistic projects due to speculative investments

Auditing

- Difficult to find out the real user identity under pseudonym

Regulation

- Lack of law for cryptocurrency, smart contract and Fintech use cases (e.g. ICO, P2P lending, etc.)

Technical obstacles

Efficiency

- Bitcoin:7 transactions per second (tps)
- Most blockchain system: <10,000 tps
  - Cf. Visa with peak capacity 56,000 tps, Alibaba with max. 256,000 tps on 2017.11.11

Privacy

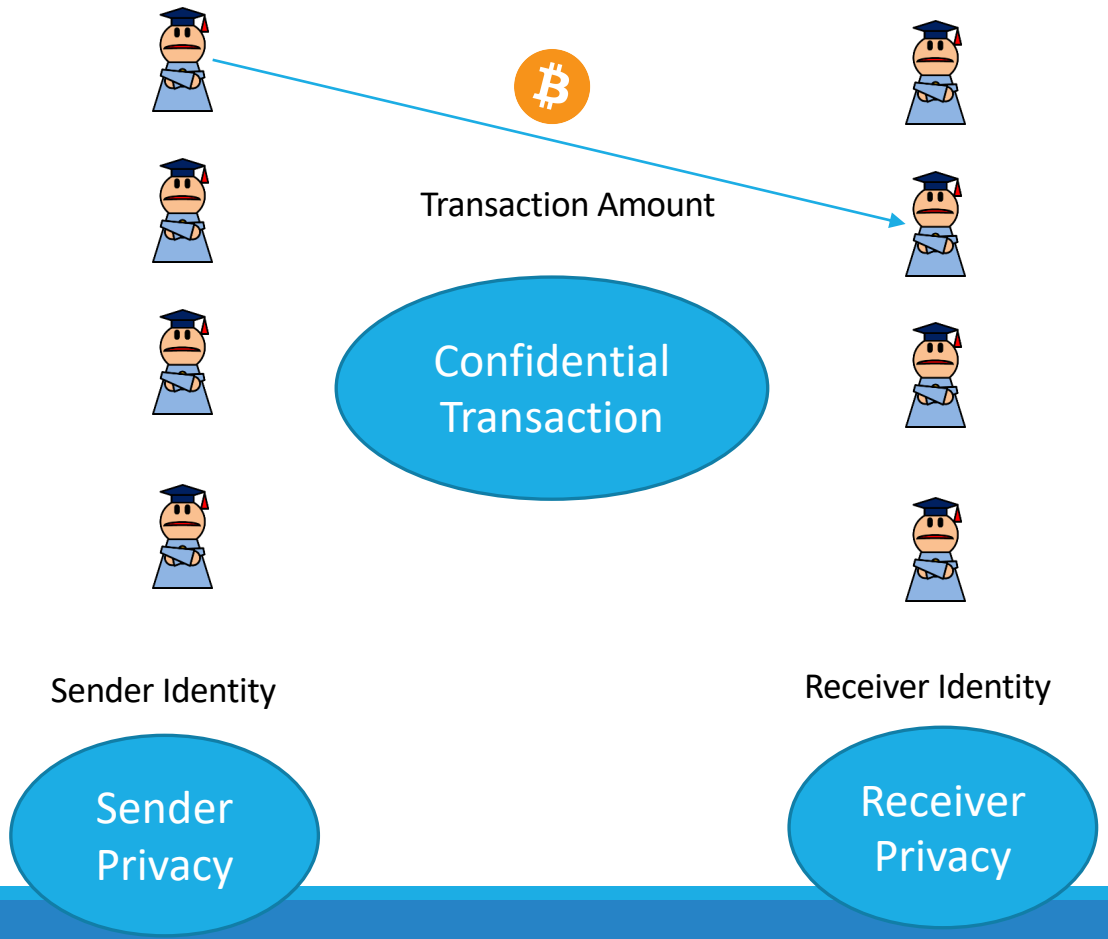
- Public transaction history → no privacy of transaction amount/address
- Use cryptography → Tradeoff between privacy and efficiency

Security

- Software security of user's wallet and exchange
  - Major exchange Mt. Gox was bankrupted after USD$450M bitcoin was stolen

This slide is taken from Dr. John Yuen's presentation

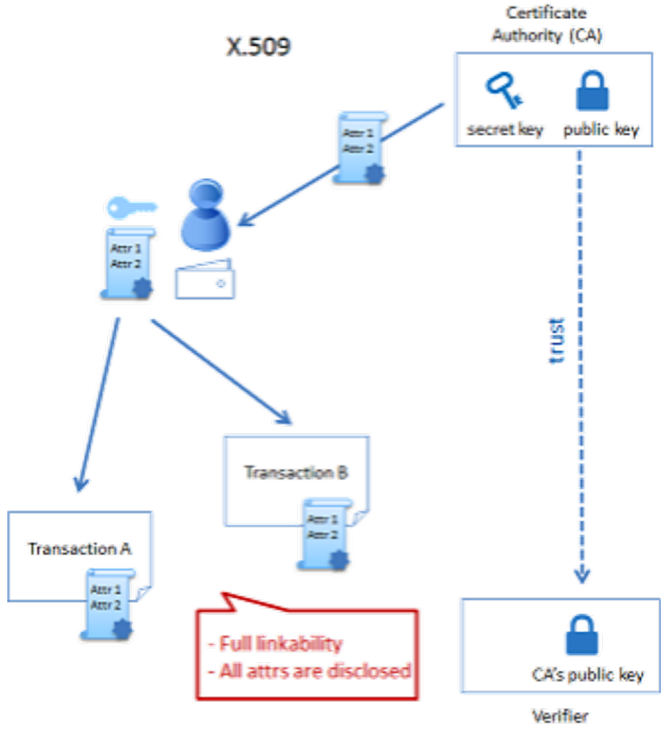
Recent Advances on Privacy Protection



Solution	Description
Advanced Crypto Primitives	Tailor-made crypto solutions - Homomorphic Encryption - Homomorphic Commitment - Linkable Ring Signatures
Zero-Knowledge Proofs	Include proofs, not information in plain for miner to verify
Trusted Execution Environment	Trusted hardware such as Intel SGX

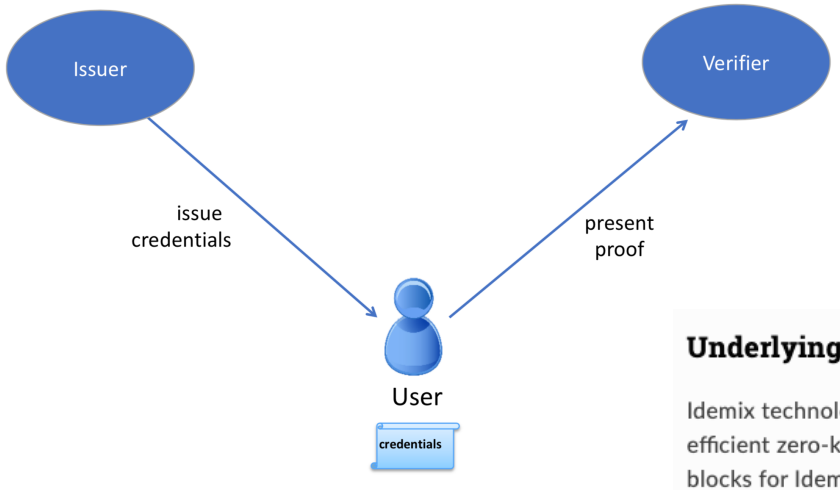
Identity Mixer in Hyperledger Fabric

Normal Authentication



Privacy-Preserving Authentication

Identity Mixer Overview



HYPERLEDGER FABRIC

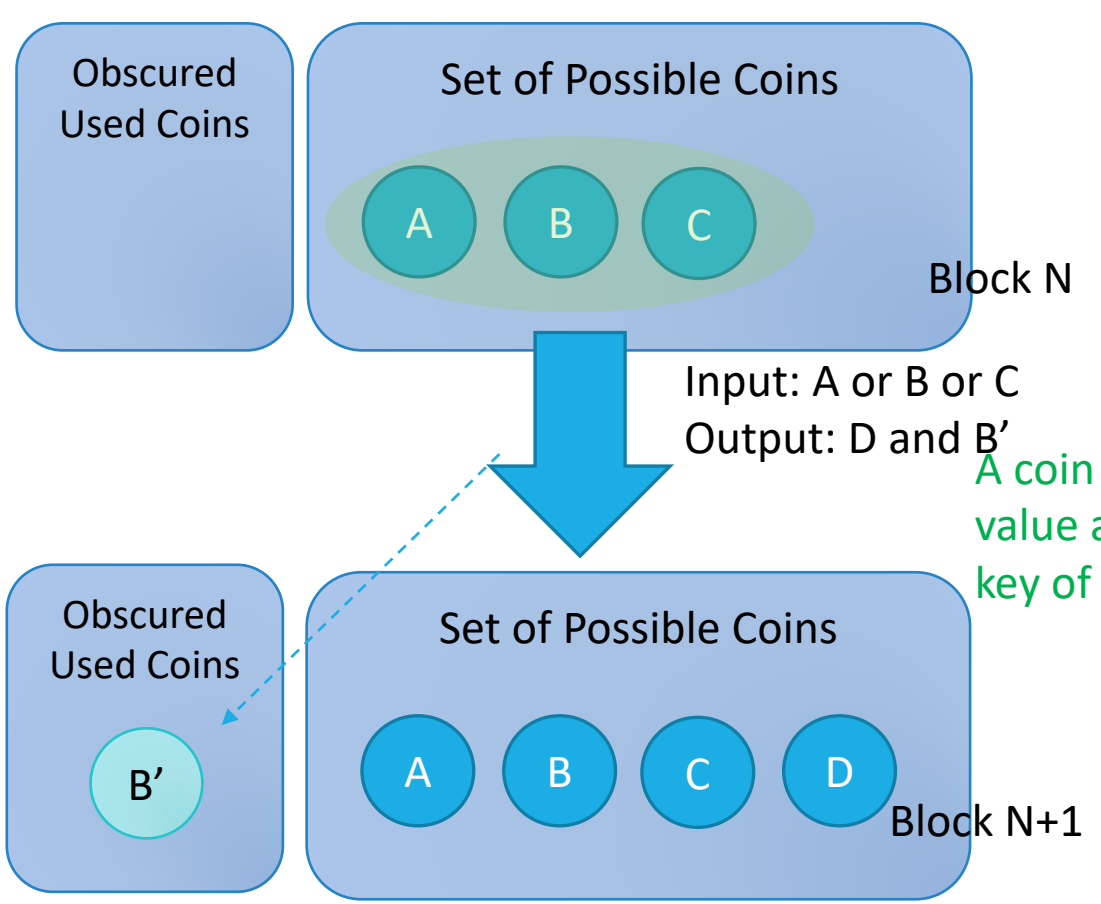
Underlying cryptographic protocols

Idemix technology is built from a blind signature scheme that supports multiple messages and efficient zero-knowledge proofs of signature possession. All of the cryptographic building blocks for Idemix were published at the top conferences and journals and verified by the scientific community.

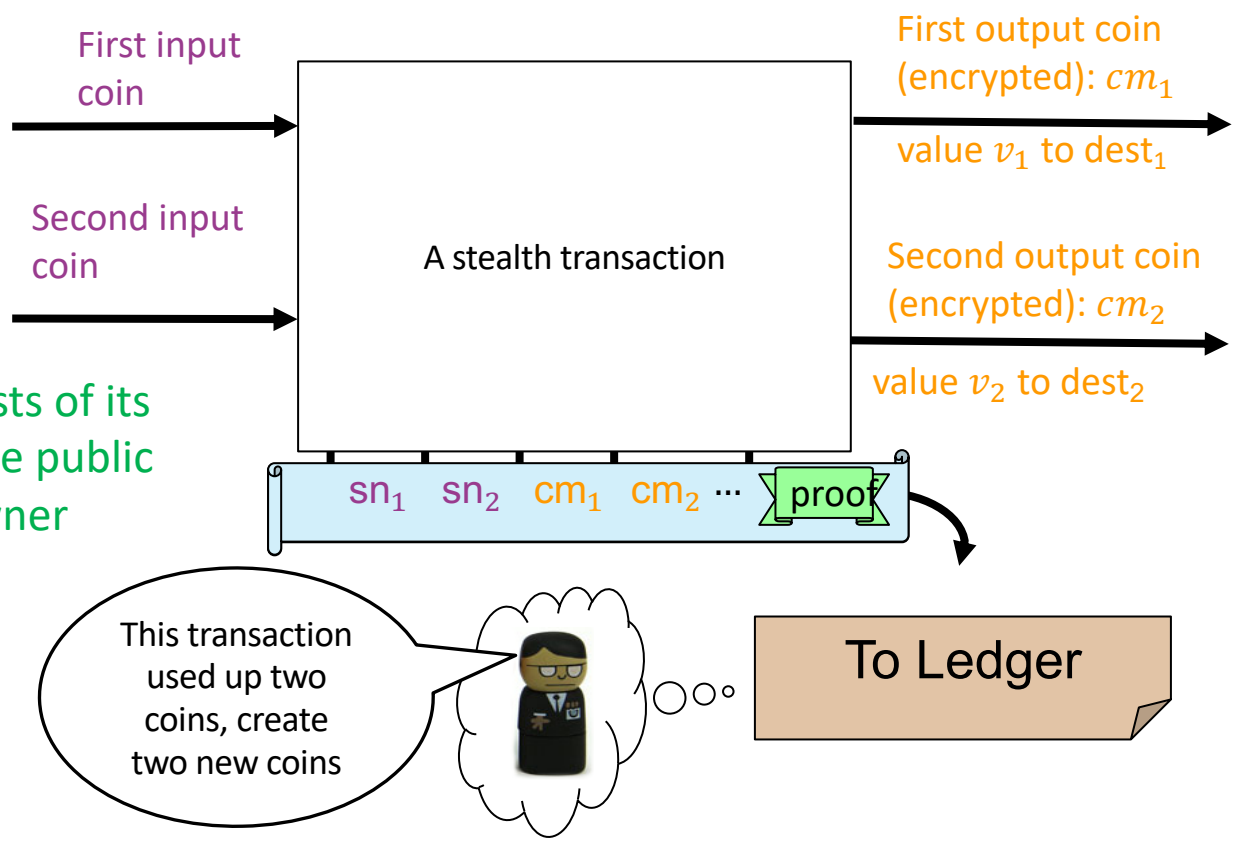
This particular Idemix implementation for Fabric uses a pairing-based signature scheme that was briefly proposed by Camenisch and Lysyanskaya and described in detail by Au et al.. The ability to prove knowledge of a signature in a zero-knowledge proof Camenisch et al. was used.

https://hyperledger-fabric.readthedocs.io/en/release-2.2/idemix.html

Ring Confidential Transaction (Monero)
Stealth transactions (Zcash)



A coin consists of its value and the public key of its owner



Privacy vs. Accountability

Is bitcoin truly anonymous?

- No! it is only pseudonymous
- It is vulnerable to transaction graph analysis
- If people uses a bitcoin to buy things in the physical world, it is possible to reveal the real identity

Some cryptocurrencies aim to maximize user privacy

- Monero's ring confidentiality transaction
- Zcash's stealth transaction
- Mixing approach such as coinjoin

On the other extreme, with blockchain, one could build cryptocurrency that allows designated entity to track all transactions

- Recent work: impose rules without sacrificing privacy

Security

In centralized payment system, authentication and authorization are more mature

- Password + biometric/ OTP/ Token, …
- Risk-based analysis

In blockchain-based cryptocurrency, we rely on digital signature where the assumption is that the signing key is properly protected

- Worse still, sometimes the key is stored on the server…

Possible directions

- Threshold cryptography
- Education!

Quantum threat and post-quantum security!

Scalability

Blockchain Trilemma?

Trade decentralization for scalability?

Better consensus protocol?

- PoW, PoS, PBFT, etc…

Parallelization? Off-chain solutions?

Recent directions

- Do we need total order (consensus) to ensure no double-pending?
  - Recent results shows that Byzantine broadcast is sufficient in the permissioned setting
- Architecture improvement (separation of nodes' role)

	TPS	Consensus	Smart-Contract	Smart Contract Language	Type	Currency	Launch Date
Bitcoin	7	POW	Limited	The Script	Public	BTC	9 Jan 2009
Ethereum	15	PoW/PoS	Turing-complete	Solidity	Public	ETH	30 July 2015
EOS	1200	DPoS	Turing-complete	C/C++	Public	EOS	31 Jan 2018
Wanchain	20	PoS	Turing-complete	Solidity	Public	WAN	18 Jan 2018
NEO	400	dBFT	Turing-complete	C#/Java/Python	Public	NEO	Founded in 2014 under the name AntShares), rebranded as NEO in June 2017
Hyperledger Fabric	200 - 250	Various	Turing-complete	Go/ Java	Consortium	N/A	11 July 2017 (v1.0) 11 Jan 2019 (v1.4 LTS)
Corda	1000-1800	Notary	Turing-complete	Kotlin	Consortium	N/A	30 Nov 2016

	Bitcoin	Ethereum	EOS	Wanchain	NEO	Hyperledger Fabric	Corda
Decentralised	☑	☑	○	☑	○	×	×
Consistent	☑	☑	☑	☑	☑	☑	☑
Scalable	×	×	☑	×	○	☑	☑

What makes it special?

How can the public trust the output of some social function?

Computation by responsible party

Trust someone

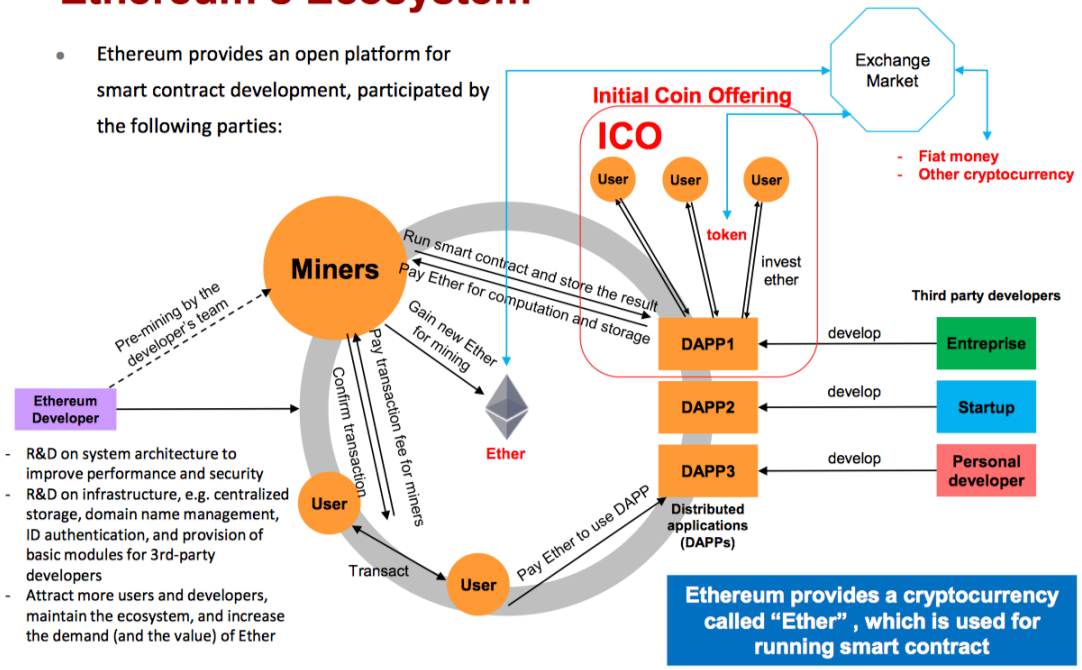
Blockchain-based applications represent a paradigm shift!

Verification by Re-Execution

Trust the technology

Ethereum's Ecosystem

- Ethereum provides an open platform for smart contract development, participated by the following parties:



Concluding Remarks

A blockchain is an immutable (unchangeable), decentralized open ledger. It is the basis of many cryptocurrencies. As a technology, it can also be used for other types of asset or fiat currency

Cryptocurrency has a currency aspect as well as a payment system aspect.

6 challenges & recent trends

Obstacles	Recent Trends
Cryptocurrency Bubble	Stablecoin, CBDC
Auditability	Semi-centralization, tracking mechanisms
Regulations	Regulatory developements
Efficiency	Trade-offs, side-chains, improved consensus, broadcast-based
Privacy	Privacy-preserving techniques
Security	Cybersecurity, wallet security, post-quantum security

Questions and comments are welcome!

Allen Au <allenau@cs.hku.hk>