Application of Blockchain in Asset Management and Transfer

Dr Allen AU
Assistant Professor & Director of MonashU-PolyU-CC Joint Lab on Blockchain
Department of Computing
The Hong Kong Polytechnic University

THE HONG KONG POLYTECHNIC UNIVERSITY
香港理工大學

Department of Computing
電子計算學系

Outline

- What is Blockchain?
- Blockchain & Cryptocurrency
- Applications of blockchain for asset management
- Challenges

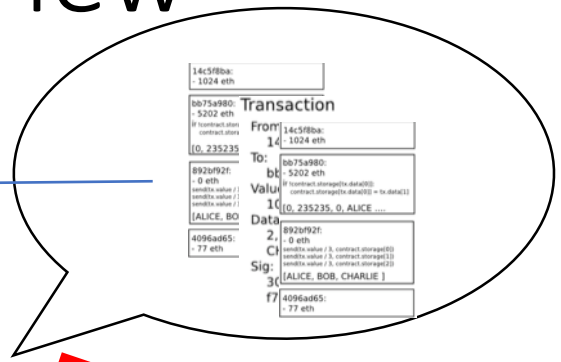
Blockchain – A High-level View

Applications (Ledger)

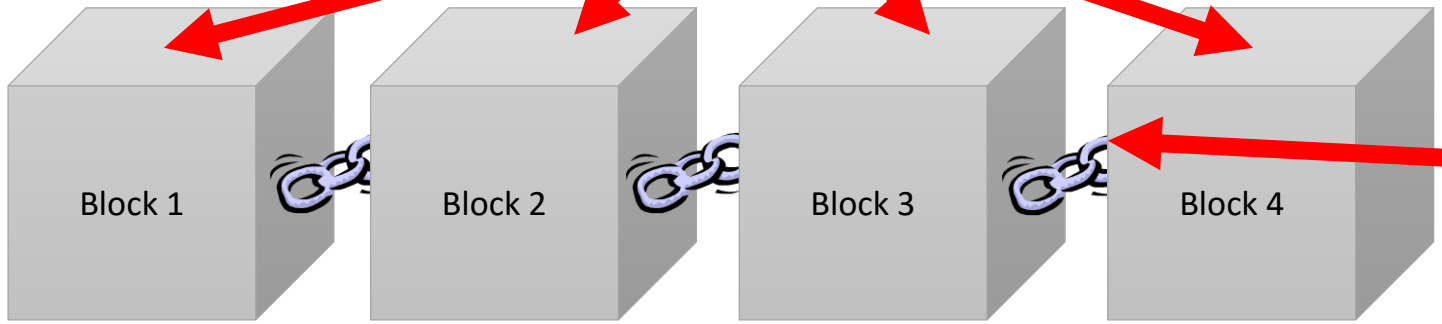
Data Structure

Consensus

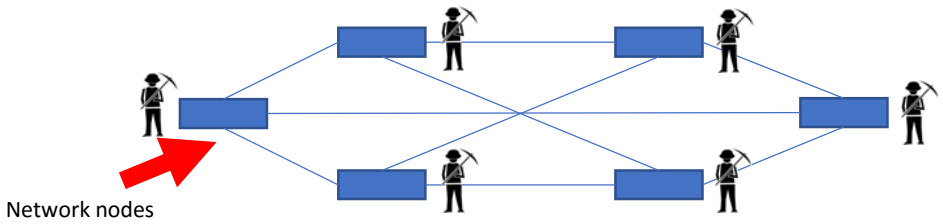
Date	Trans	Consent
12/3	Bob -> Alice : 10	Bob's digital signature
13/3	Bob -> Alice : 50	Bob's digital signature
14/3	Alice -> Bob : -20	Alice's digital signature

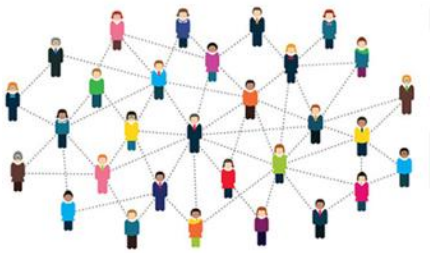


Each block contains data



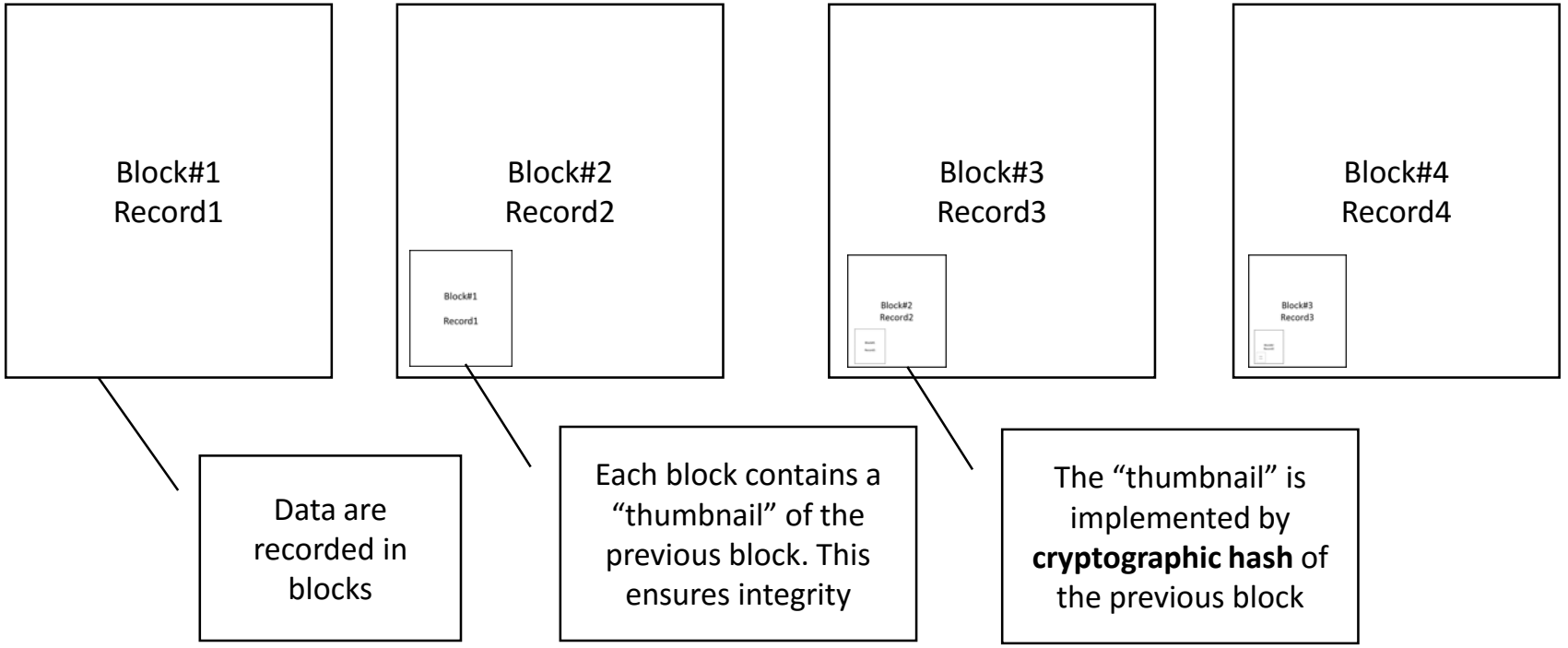
A block is tied to previous block



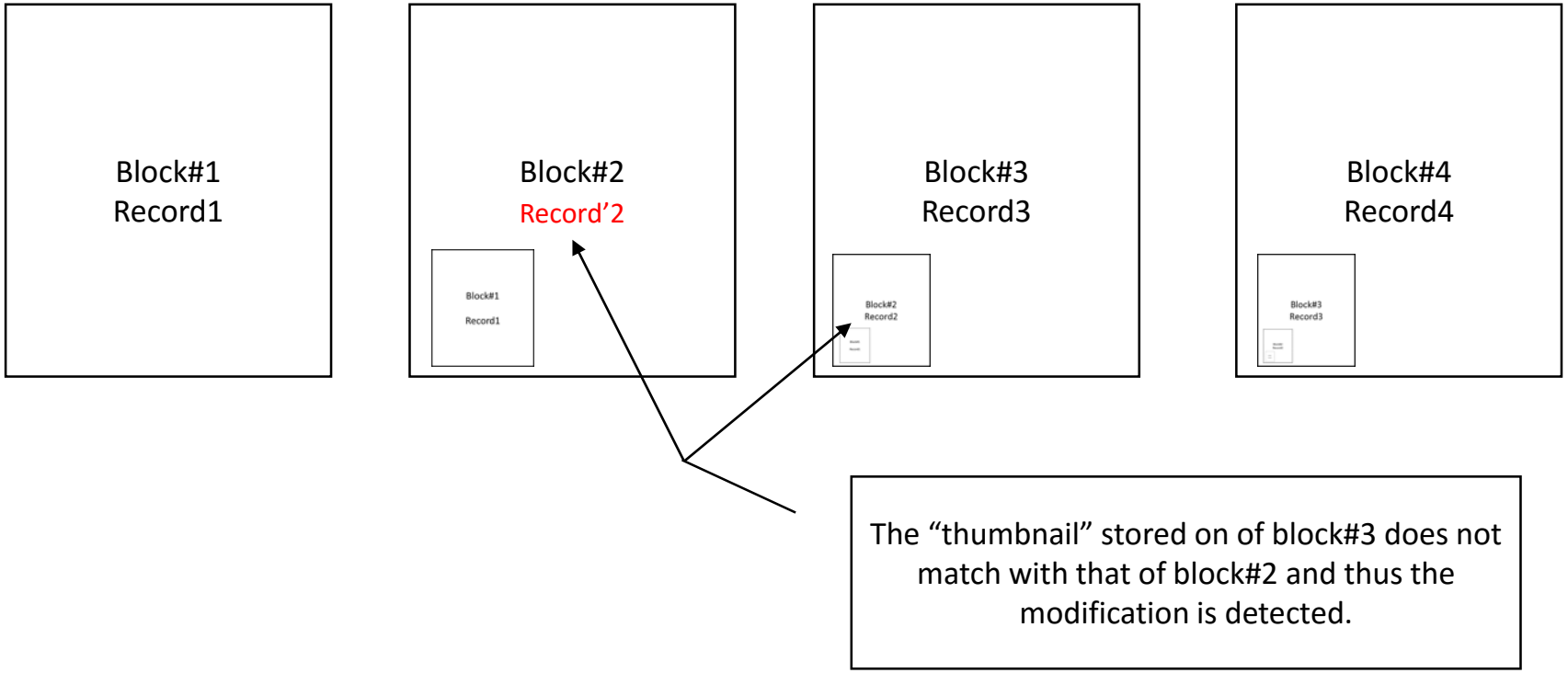


Blockchain: An Append-Only Ledger

Data Structure



What if someone tries to modify an existing record?



Hash Functions

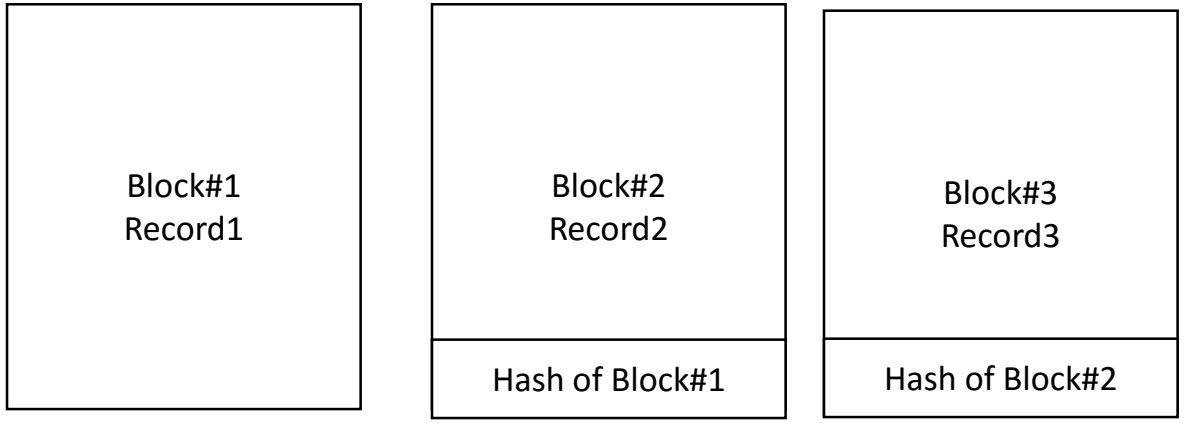
Hash

```
b2f346b4f964918934684dd
d9d0c6f0527c62cd99bdc01
88cd5471be63b68fdb
```

Hash

```
8088ebdcb32b796dc76722
6fa84c621097f1ec1d2f70
7ffda5c8e9ce69398e75
```

The SHA256 hash function produces a unique 256-bit fingerprint for each data item

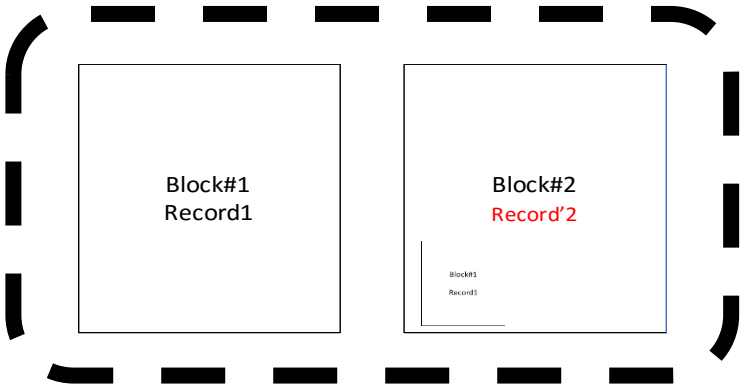


Blockchain: Decentralization

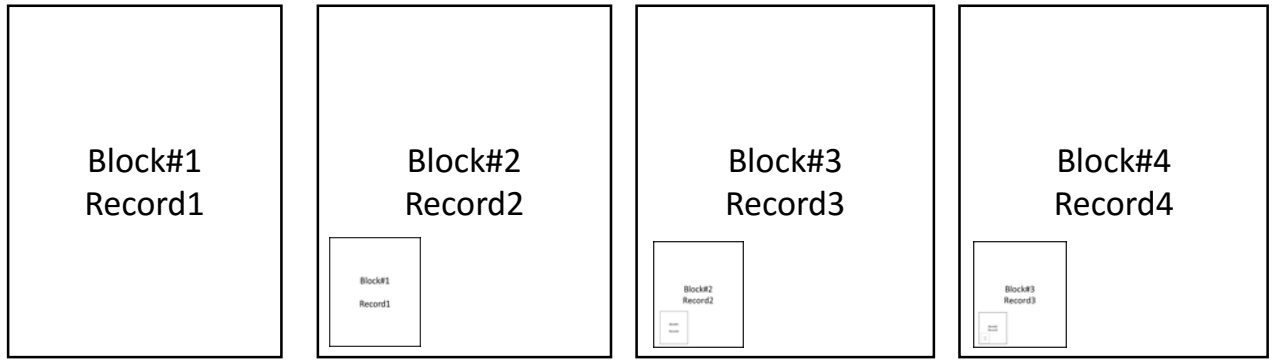
Consensus (1)

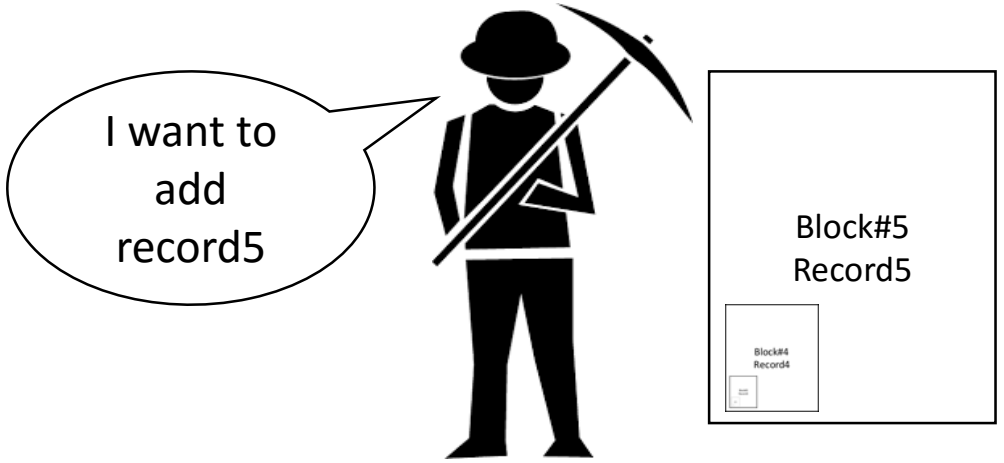
Longest chain rule:
When different versions are received, the longer one is real

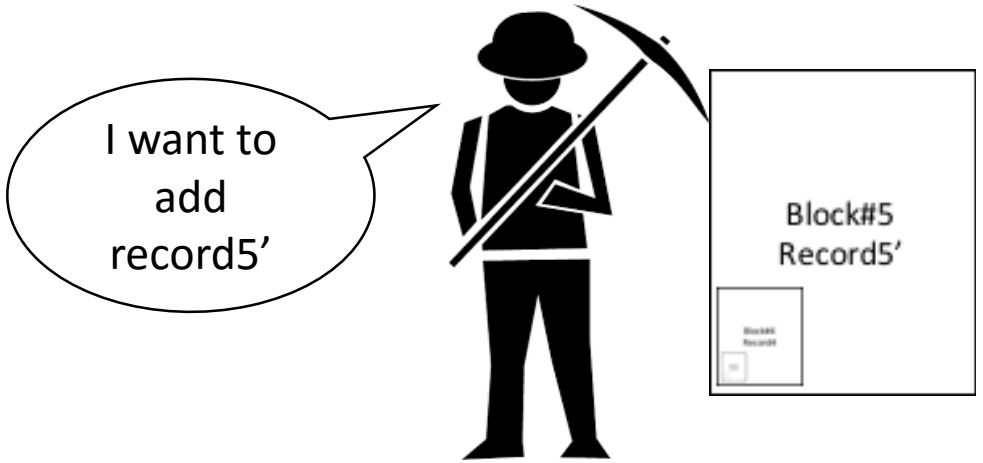
This is real



Blockchain: The Right to Append Consensus (2)





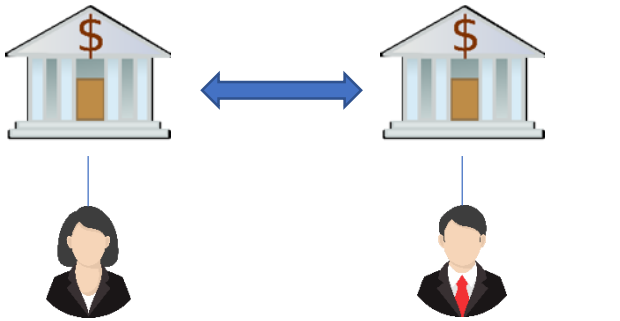


Blockchain: The Right to Append Consensus (3)

- Proof-of-Work (e.g. Nakamoto Consensus)
  - Proof that you have done some computation to earn the right to publish the next block
- Proof-of-Stake
  - The one with more stake (more coins, for example) in the system has the right to publish the next block
- Discussion (e.g. PBFT, voting)
  - The stakeholder discuss and agree on the content of the next block

Blockchain: Decentralized Cryptocurrency

Applications



Date	Trans	Bal
12/3	+10	200
13/3	+50	250
14/3	-20	230

Date	Trans	Bal
12/3	-10	300
13/3	-50	250
14/3	+20	270

Traditional banking system
- One ledger per user
- Trust the bank to verify consent

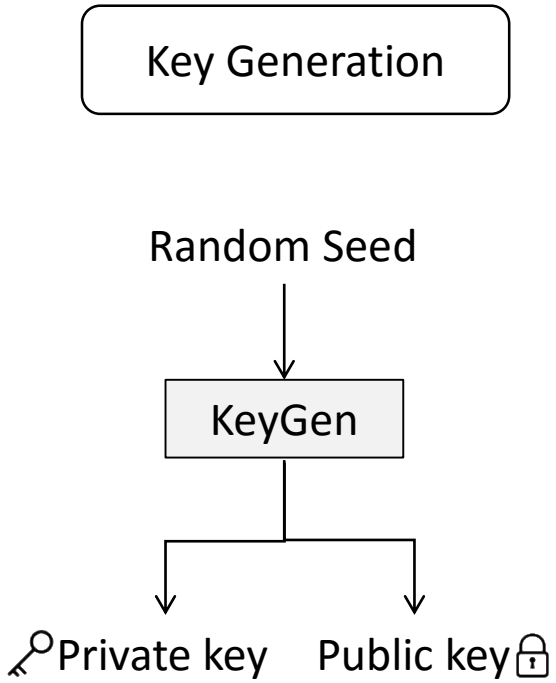
Block N	
Account	Balance
PK_{Alice}	12.5
PK_{Bob}	12.5
Block N+1	
Account	Balance
PK_{Alice}	2.5
PK_{Bob}	22.5
Transactions	
[Alice sends to Bob 10 dollars], instruction signed by Alice	

Decentralised Cryptocurrency
- One shared ledger for all users
- Consent represented by digital signatures
- Trust the technology

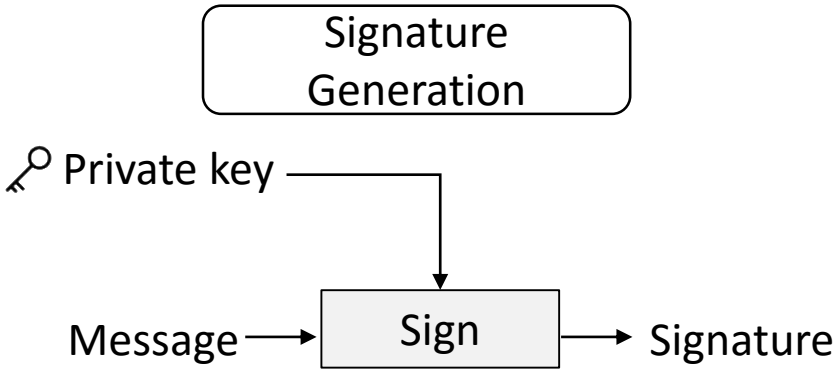
Digital Signatures

- In a traditional banking system, signature is used as a mean to represent consent and authorization
- A digital signature is a functional equivalence to a handwritten signature
  - Easy for Alice to sign on the document
  - Hard for anyone else to forge
  - Easy for anyone to verify

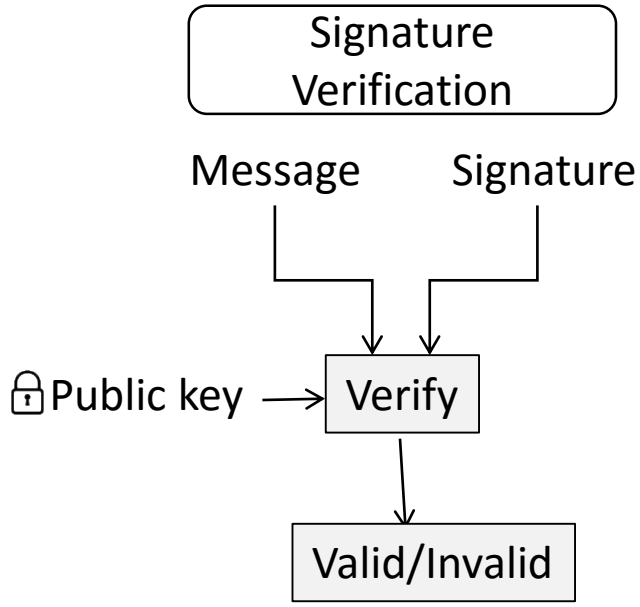
Digital Signatures



Given a public key, it is hard to compute to corresponding private key



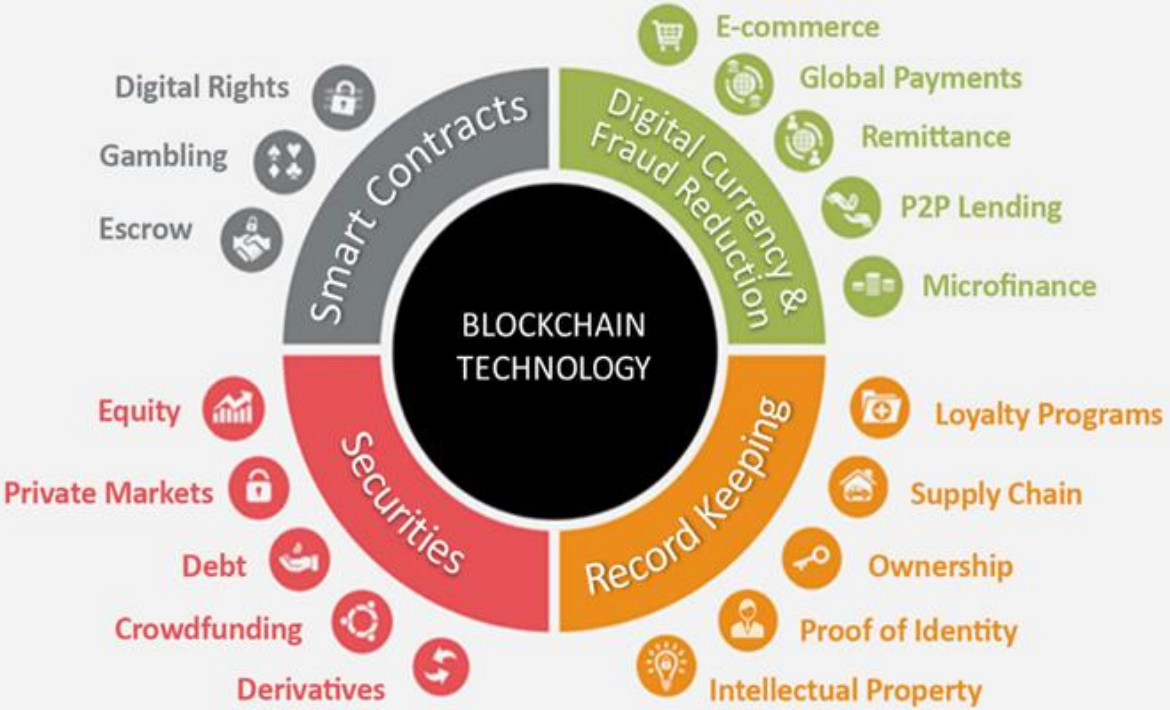
A private key is needed to create a signature on any message



Anyone can verify a digital signature using the public key and the message

Potential Use Cases for Blockchain

- No trusted Party
- Immutable Global History
- Data Transparency
- System Self-Management



https://www.aciworldwide.com/insights/expert-view/2017/march/blockchain-for-retailers-producing-real-business-benefits

Asset Ownership Management

- One could use blockchain to record ownership of an asset
- Potential Advantages
  - An immutable record of events
  - Easier audits
  - Simplified process of due diligence
  - Simplified trading and exchange
  - Tokenization

Anti-counterfeiting & Supply chain management

- One could use blockchain to record the whole supply chain process
- Provide another way to allow consumers to validate a genuine product by checking who owns what
- This is straightforward if the asset is also “virtual”
  - Cryptocurrency
  - Virtual asset in online game
- Need to combine with other technology when the asset is physical
  - RIFD tags? Tamperproof seals?

Example – Blockchain Chicken

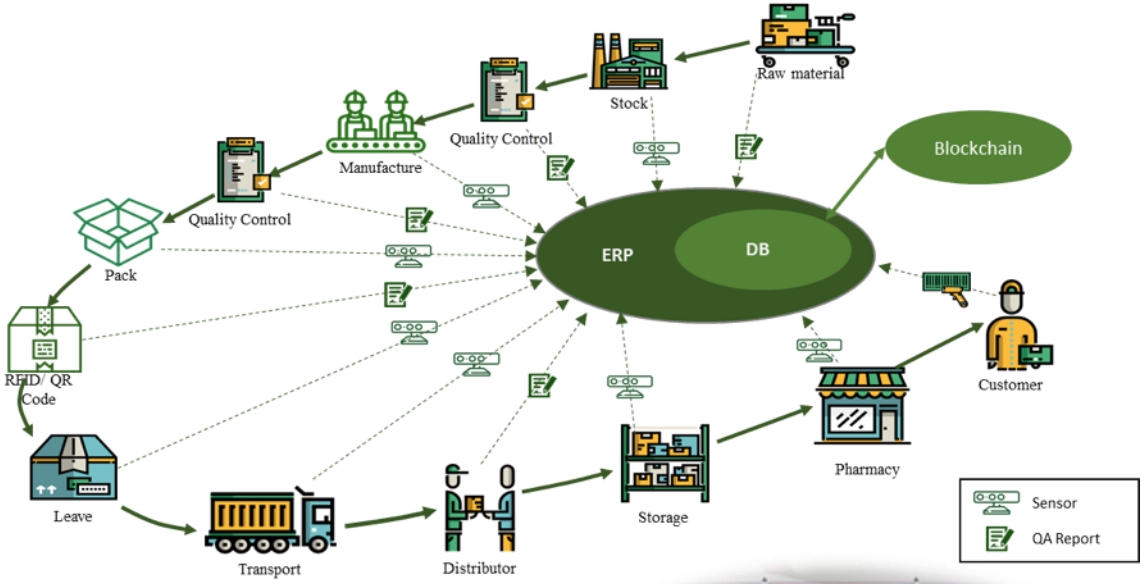
- A Chinese Mainland company launches the first blockchain poultry
- Every chicken's identity can be verified, with raising conditions (movement, location, soil temperature, etc.), transportation and sales information logged
- Blockchain technology enables counterfeit detection and traceability by all parties, including customers

Source: HK01, 2017-12-22

Enhanced data transparency

Example - Blockchain-Based Food and Drug Counterfeit Detection and Regulatory System

- **Counterfeit Detection**
  - allow customers to effectively detect any fake drugs
- **Ease of Quality Control and Audit**
  - allow auditor to monitor the manufacturing procedures
- **Accountability and Tracing**
  - allow manufacturer / government to trace the cause and identify responsible parties



Challenges for Blockchain Technologies

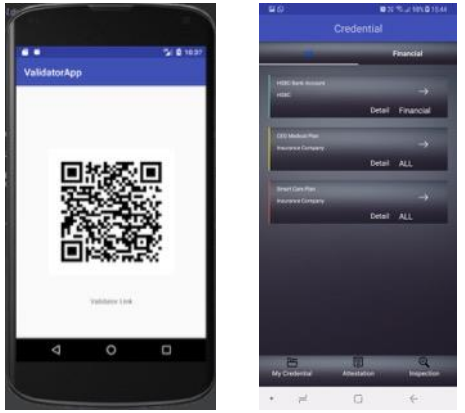
- Efficiency
  - Bitcoin platform can only handle 7 transactions per second (TPS);
  - Hyperledger Fabric can handle 1,000 TPS
  - Existing electronic payment systems can handle much more (e.g. VISA has a peak capacity of 56,000 TPS)
- Security
  - Blockchain and crypto-currencies can be mis-used, e.g. money laundering
  - Target of many hackers
  - Future threats from quantum computers … … …
- Privacy
  - Sensitive information is stored on blockchain (account details, balance, transaction history) but data on blockchain are public

Challenges and Potential Directions for Applications of Blockchain in Asset Management

- Lack of identity management
- Connection between physical asset and its virtual identity
- Legal issues

https://www.e123.hk/ElderlyPro/details/276503/77

http://www.eenewsanalog.com/news/printed-nfc-tags-detect-opened-goods



Blockchain-based ID management system

Thank You

Web: www.comp.polyu.edu.hk/~csallen
Email: mhaau@polyu.edu.hk

Scan QR code and enter Allen's personal homepage

The Hong Kong Polytechnic University
香港理工大學
Department of Computing
電子計算學系

“Smart contracts” conceptualized by Szabo in 1994

A smart contract is a computerized transaction protocol that executes the terms of a contract. The general objectives are to satisfy common contractual conditions (such as payment terms, liens, confidentiality, and even enforcement), minimize exceptions both malicious and accidental, and minimize the need for trusted intermediaries. Related economic goals include lowering fraud loss, arbitrations and enforcement costs, and other transaction costs.

-Nick Szabo “The Idea of Smart Contracts”

A Note on Smart Contract

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 set(uint x) public {
          storedData = x;
  }
  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 possible at all, to write a smart contract that connect to any external system