Introduction to Blockchain (Part I)

Prof. James Won-Ki Hong

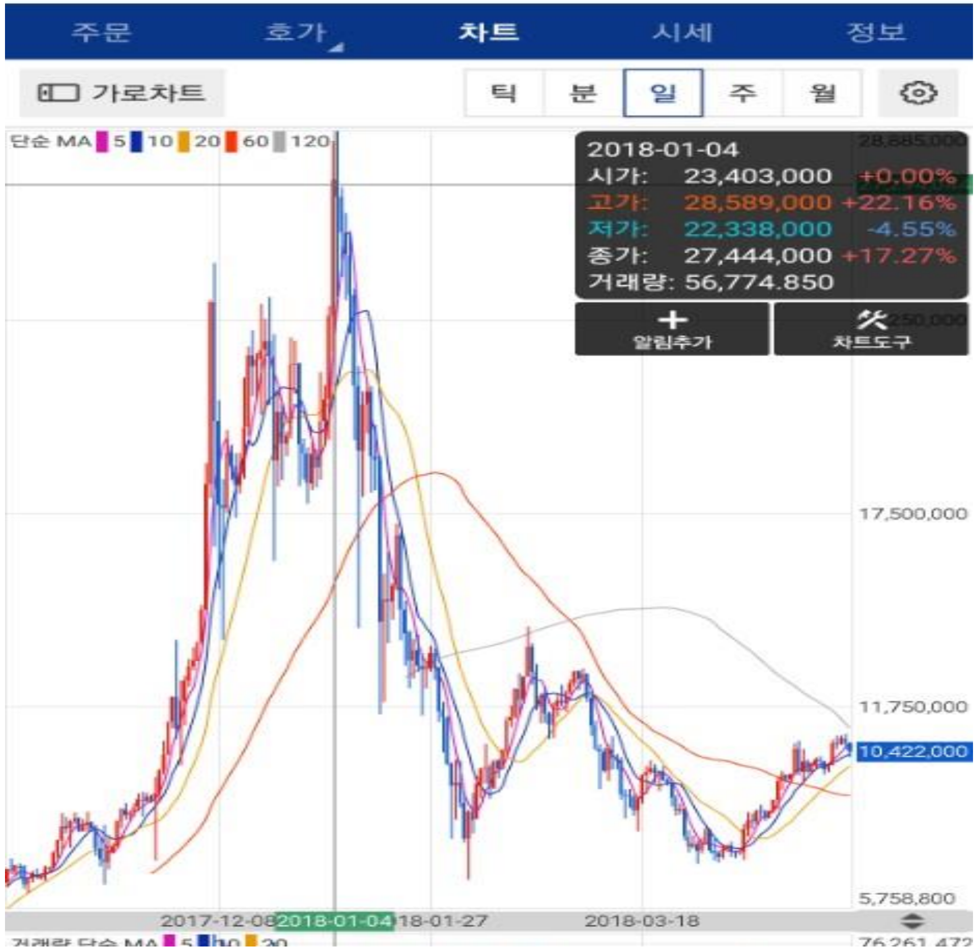
Distributed Processing & Network Management Lab.
Dept. of Computer Science and Engineering
POSTECH

http://dpnm.postech.ac.kr
jwkhong@postech.ac.kr

Table of Contents

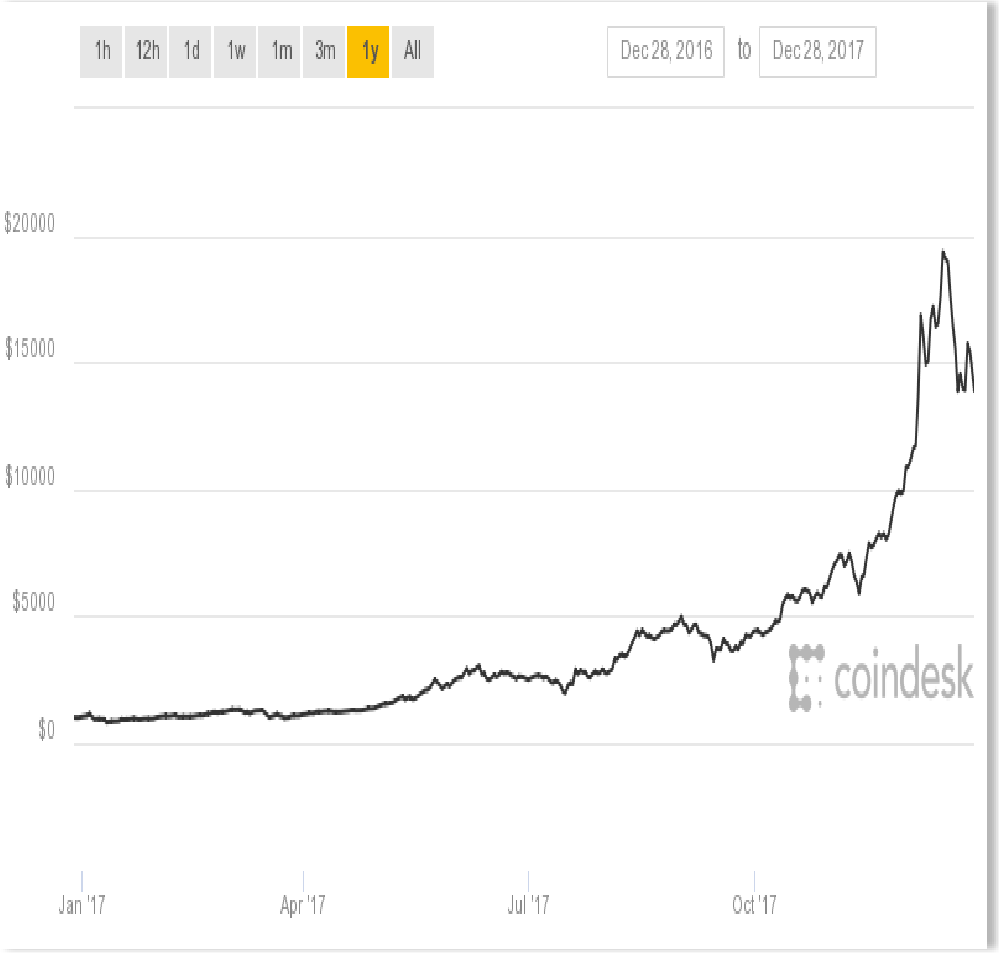
- Emergence of Cryptocurrency
- Blockchain Technology
- Limitations of Bitcoin
- AI vs. Blockchain
- Public vs. Private Blockchain
- Use Cases of Blockchain
- Concluding Remarks

Emergence of Cryptocurrency (1/6)



2018-01-04
시가: 23,403,000 +0.00%
고가: 28,589,000 +22.16%
저가: 22,338,000 -4.55%
종가: 27,444,000 +17.27%
거래량: 56,774.850

Bitcoin prices in Korea



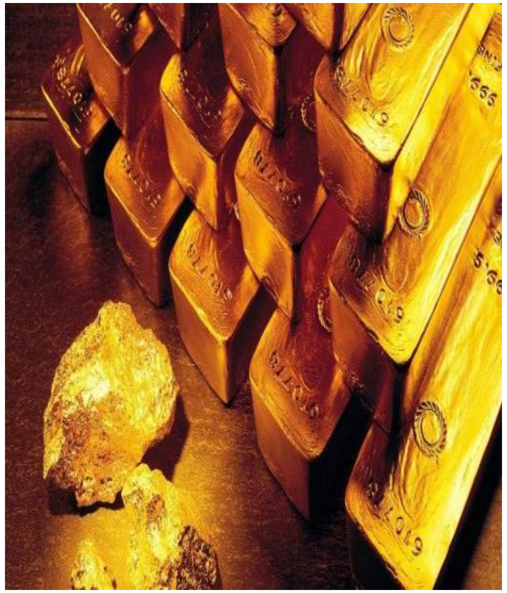
Dec 28, 2016 to Dec 28, 2017

Bitcoin prices in US

Emergence of Cryptocurrency (2/6)

- **History of transactions and payments**

① bartering



② commodity money

③ legal tender

Emergence of Cryptocurrency (3/6)

Problems of traditional currency (1)

- Production costs for currency issuance
- Need physical space to store currency (storage cost, worry of loss)
- Issued and controlled by central authority
  - Value of currency is always exposed to be manipulated by the interests of the government
- Different subjects and units in different countries

Korean currency

source: http://blog.ibk.co.kr/555

American currency

source: https://goobjoog.com/haddii-dakhliga-ku-soo-gala-maalintii-uu-gaarsiisan-yahay-qiimahan-ogow-inaad-ku-nooshahay-saboolnimo-baan/

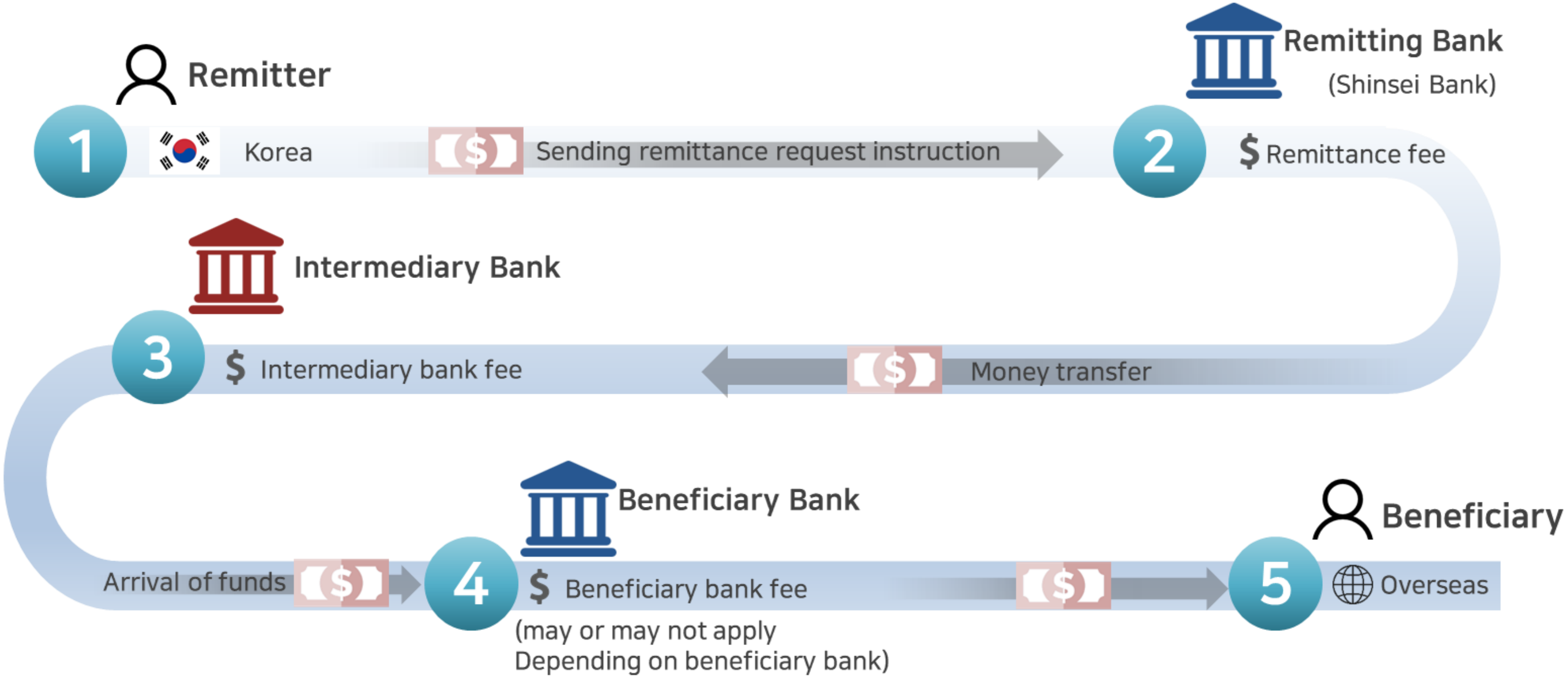
Japanese currency

source: https://commons.wikimedia.org/wiki/File:Series_D_1K_Yen_Bank_of_Japan_note_-_front.jpg

Emergence of Cryptocurrency (4/6)

Problems of traditional currency (2)

- Takes a long time to remittance abroad
- High cost to remittance abroad
- Very inconvenient



source: http://www.shinseibank.com/english/goremit/individuals/about.html

Emergence of Cryptocurrency (5/6)

- **What is Cryptocurrency?**
  - **A kind of digital currency**
  - **Very little production cost for currency issuance & significant reduction in transfer costs**
  - **No storage cost & no loss concerns**
  - **Most cryptocurrency follows the concept of decentralization**
  - Can be abused for drug trafficking, gambling, money laundering
  - Can be very risky for investments

source: http://bebop21.tistory.com/331

Emergence of Cryptocurrency (6/6)

▪ First cryptocurrency – Bitcoin

- In 2008, an anonymous developer or development group named "Satoshi Nakamoto" first proposed a cryptocurrency called Bitcoin
- No centralized management entity
- Distributed P2P-based digital cryptocurrency
- Total coins limited to 21 Million BTC (Bitcoins)
- Open transaction history
- No personal information required
- Low transaction fees
- Strong security (counterfeiting is impossible)

➔ Bitcoin is implemented based on Blockchain technology

What is Blockchain?

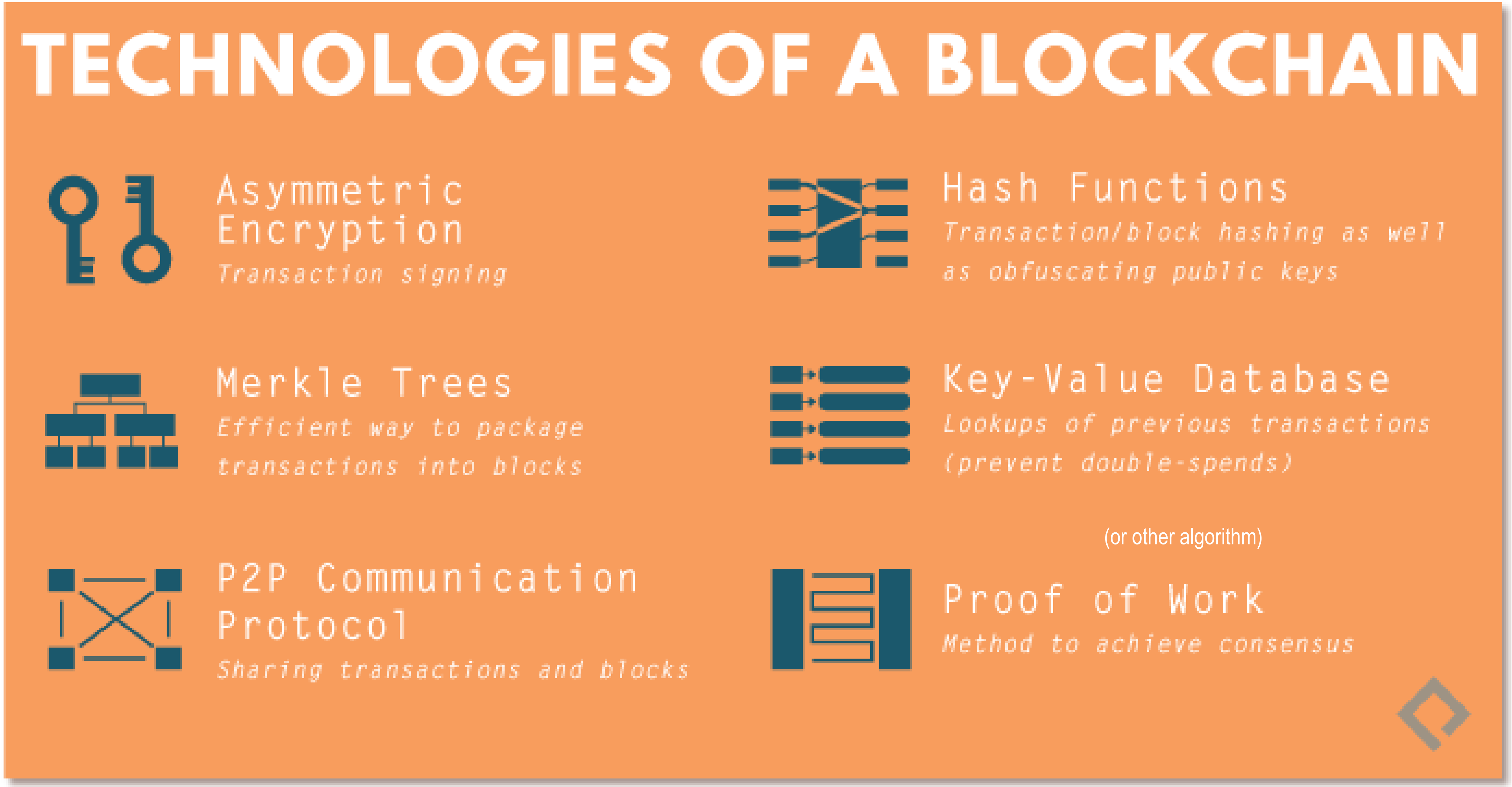
**“In the era of the Fourth Industrial Revolution,
a huge technology that goes beyond artificial intelligence”**

**“New technology that changes the sea of information
into the sea of value”**

“... It is considered another industrial revolution that reverses the existing paradigm and order. The World Economic Forum has projected that 80% of the world’s banks will adopt Blockchain technology. In addition, Blockchain will account for 10% of the world’s total production in 2025 ….”

『Blockchain revolution 2017』

Key Technologies of Blockchain



TECHNOLOGIES OF A BLOCKCHAIN

Asymmetric Encryption
Transaction signing

Hash Functions
Transaction/block hashing as well as obfuscating public keys

Merkle Trees
Efficient way to package transactions into blocks

Key-Value Database
Lookups of previous transactions (prevent double-spends)

P2P Communication Protocol
Sharing transactions and blocks

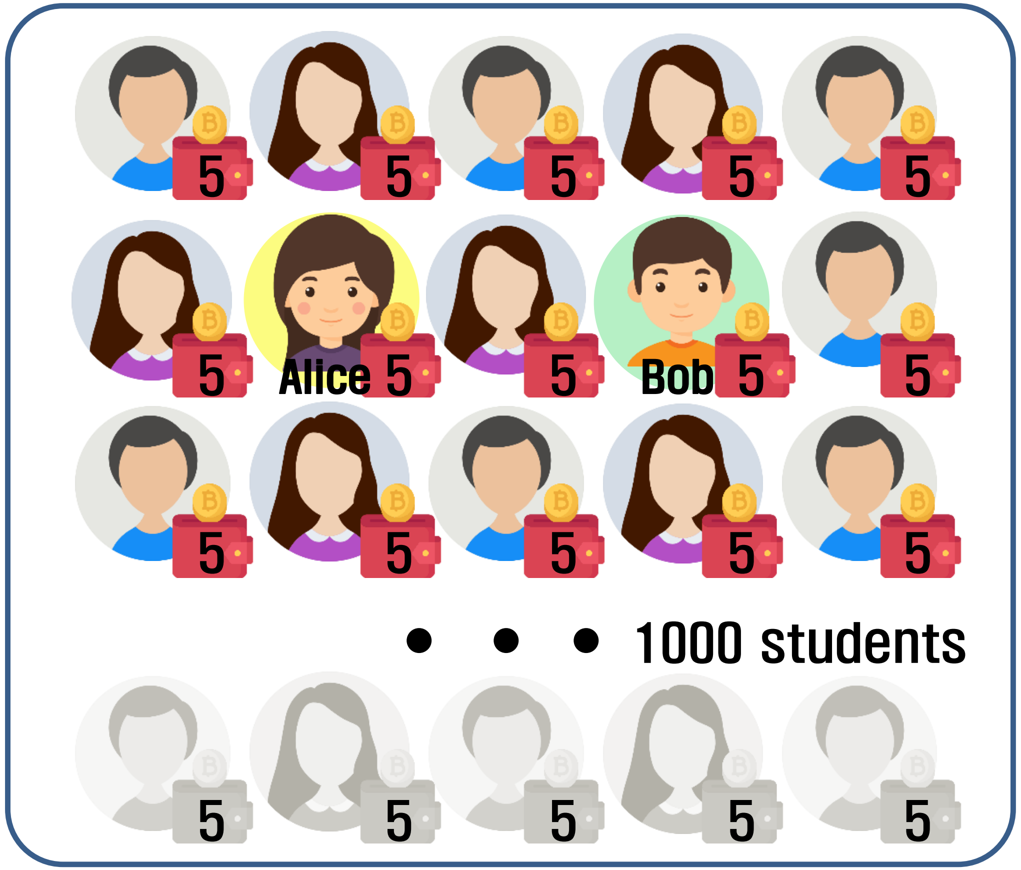
(or other algorithm)

Proof of Work
Method to achieve consensus

Source: https://eng.paxos.com/hs-fs/hubfs/_02_Paxos_Engineering/Technologies-of-a-Blockchain.png?t=1513284613258&width=700&name=Technologies-of-a-Blockchain.png.

Blockchain Technology (1/6)

- **Mechanism – Easy example**

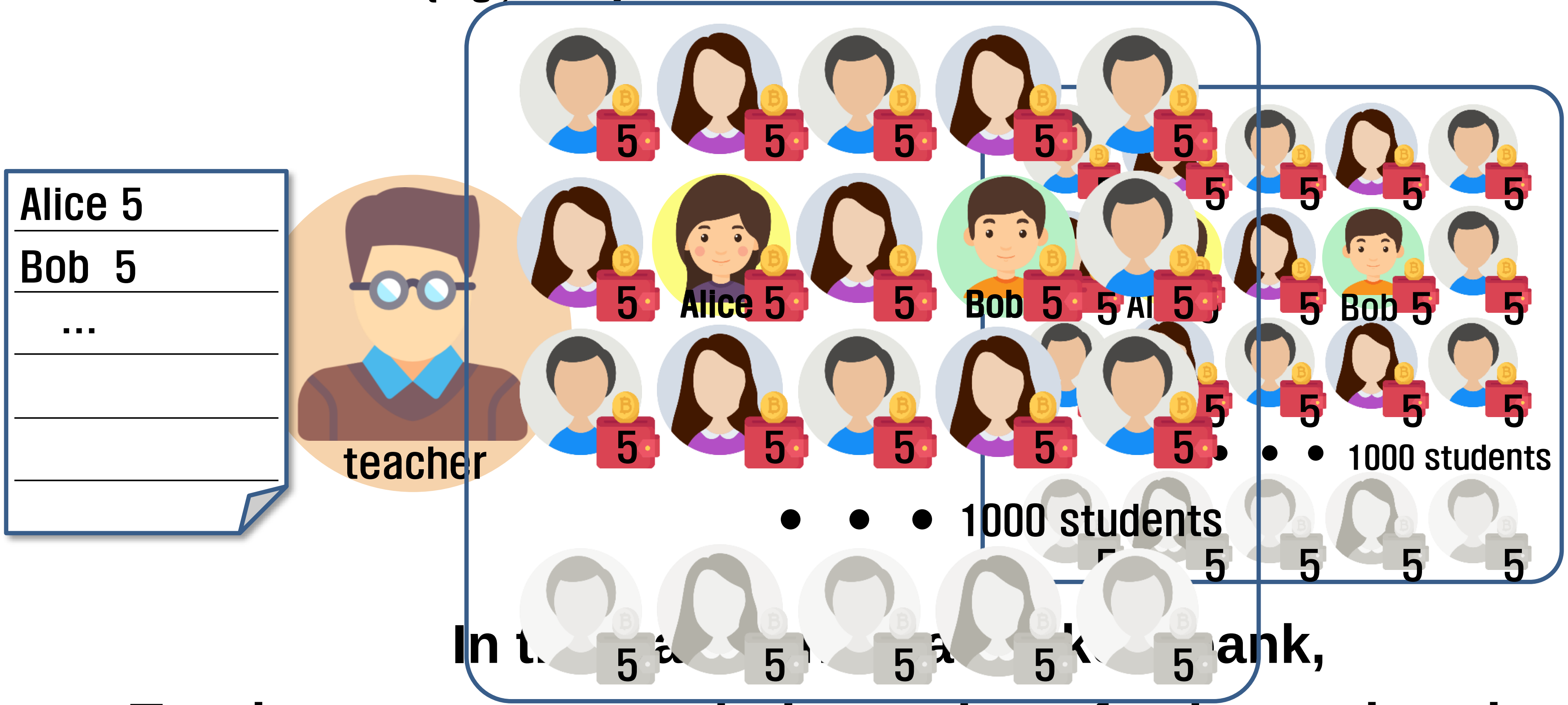


There are 1000 students in Alice & Bob's school

Each student has 5 coins which can be used in the cafeteria

Blockchain Technology (1/6)

- **Mechanism – Easy example**
  - traditional method (e.g., Bank)



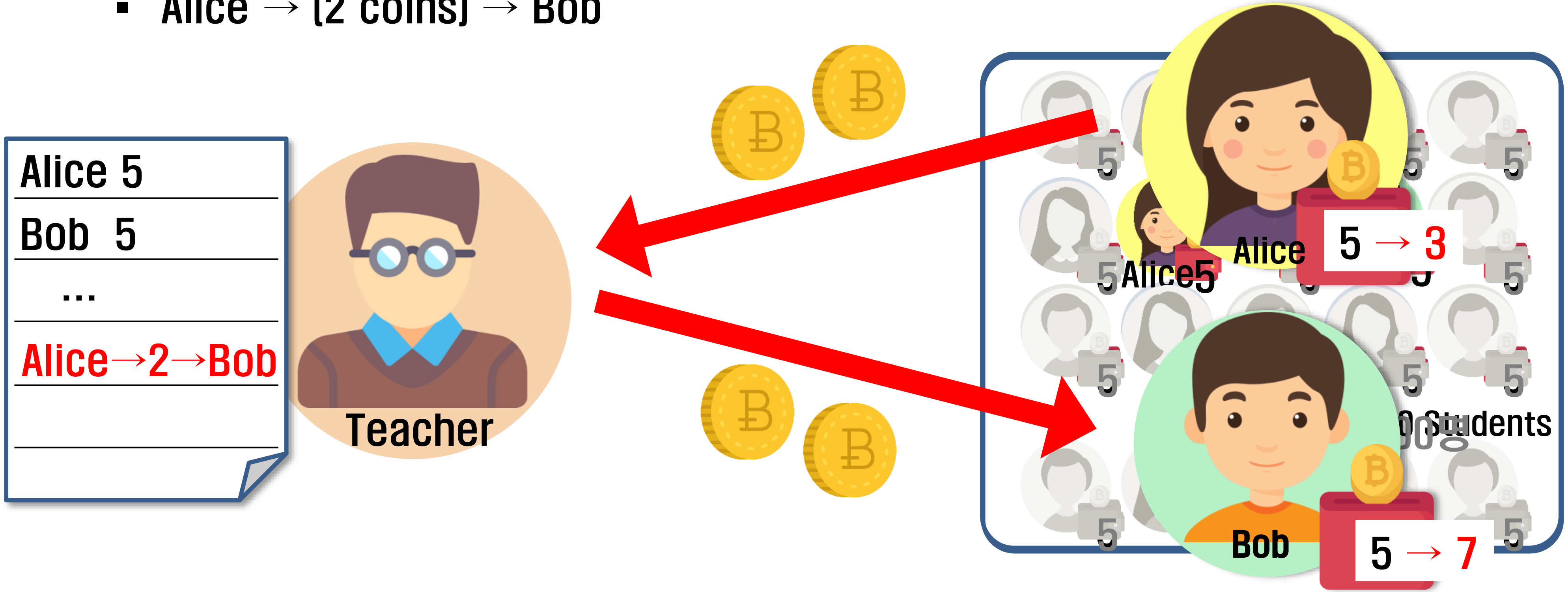
In t [illegible] ank,

Teacher manages to whole number of coins and each coin number to be included in each student.

Blockchain Technology (1/6)

Blockchain mechanism – Easy example

- traditional method (e.g., Bank)
    - Alice → (2 coins) → Bob

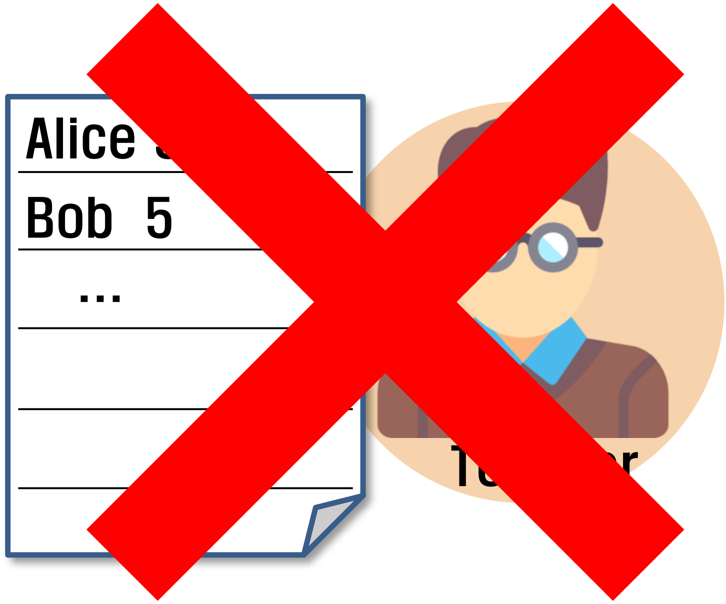


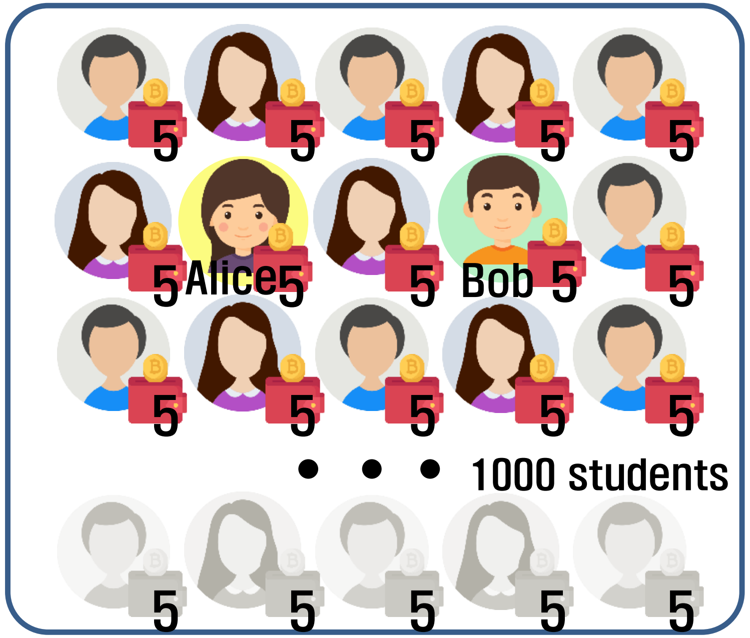
If Alice wants to transfer 2 coins to Bob,
The teacher must get involved to transfer 2 coins.

Blockchain Technology (1/6)

Blockchain mechanism – Easy example

- blockchain method



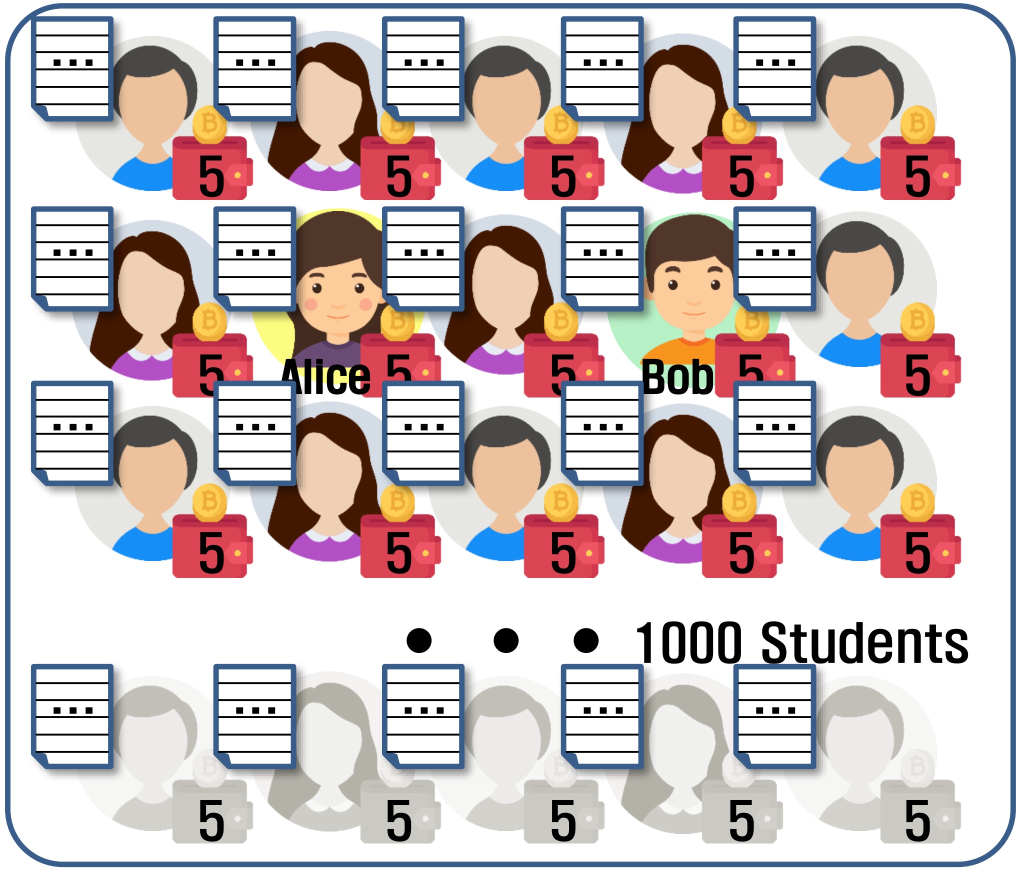


However, by using Blockchain,

the role of the teacher is not needed anymore.

Blockchain Technology (1/6)

- **Blockchain mechanism – Easy example**
  - blockchain method

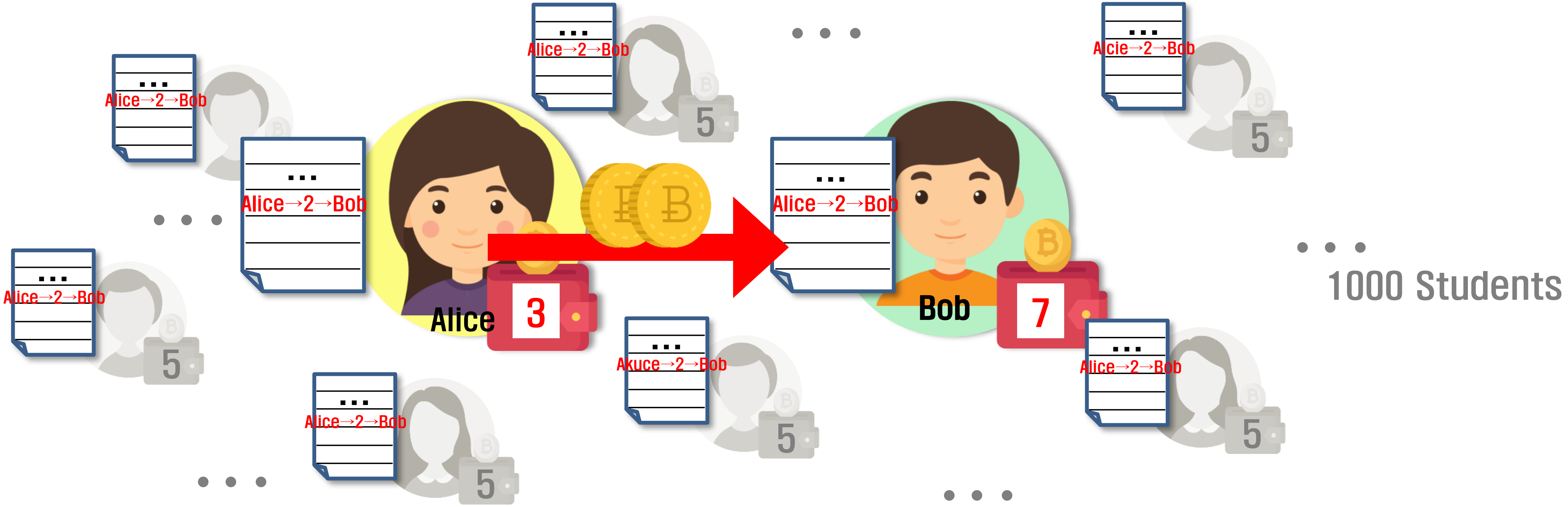


All students have their own copy of a ledger which has all coin transaction history and transactions are processed using these ledgers

Blockchain Technology (1/6)

▪ Blockchain mechanism – Easy example

- blockchain method
  - Alice → (2 coins) → Bob



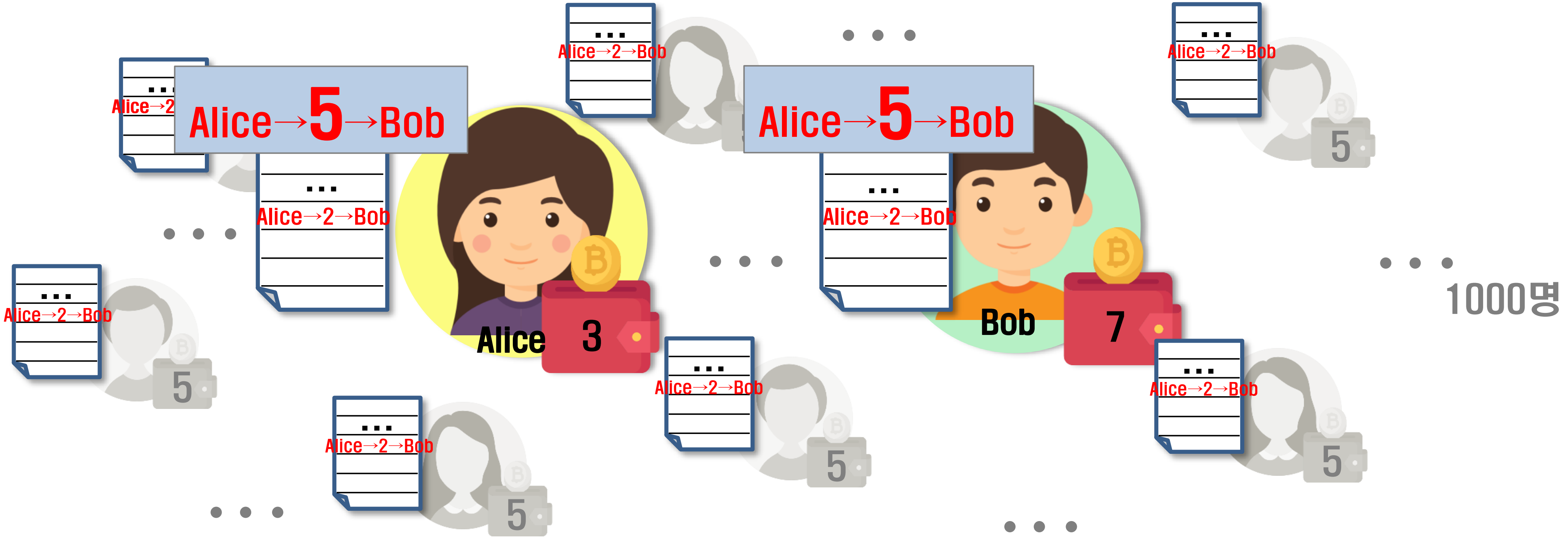
If Alice lend 2 coins to Bob,

This transaction is recorded in all ledgers.

Blockchain Technology (1/6)

Blockchain mechanism – Easy example

- blockchain method
  - Alice → (2 coins) → Bob

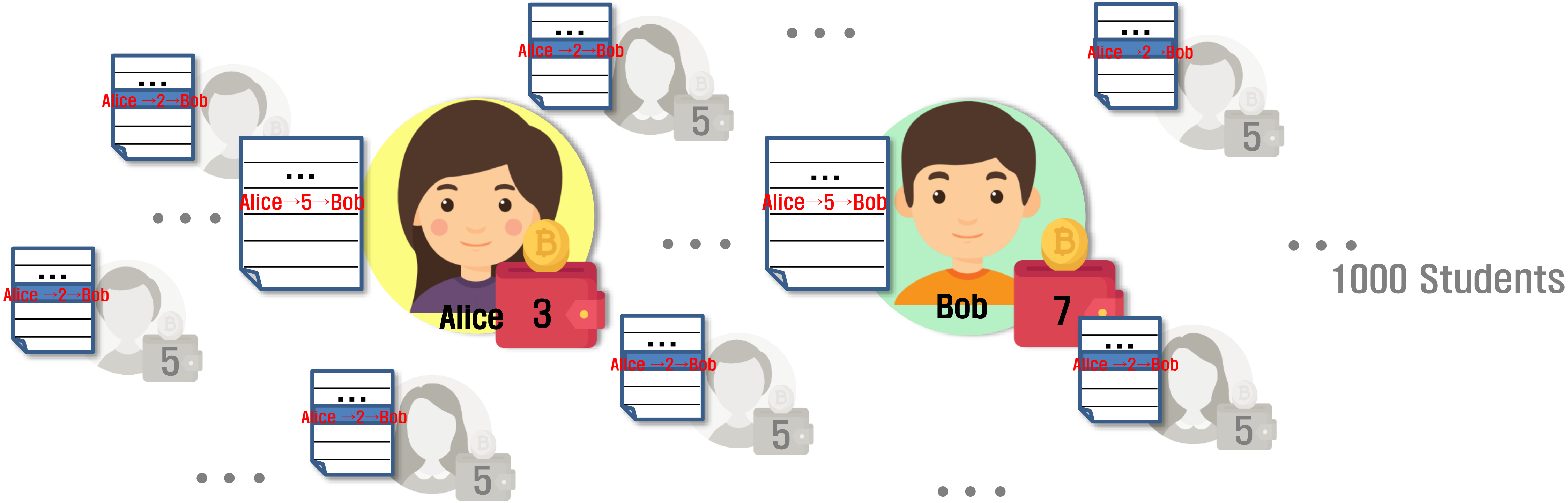


A few days later, Alice intentionally tries to manipulate Bob and her ledgers to get back more than 2 coins.

Blockchain Technology (1/6)

Blockchain mechanism – Easy example

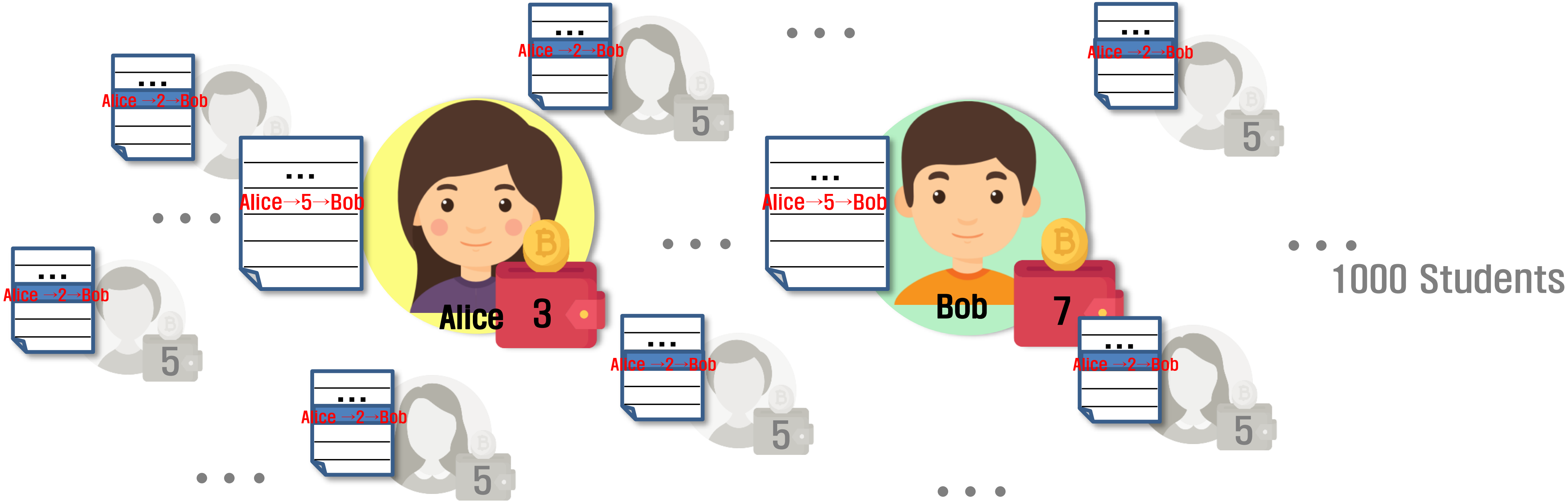
- blockchain method
  - Alice → (2 coins) → Bob



But for Alice to recover the coins,
More than 50% of other students must agree that she lent 5 coins to Bob.

Blockchain Technology (1/6)

- **Blockchain mechanism – Easy example**
  - blockchain method
    - Alice → [2 coins] → Bob

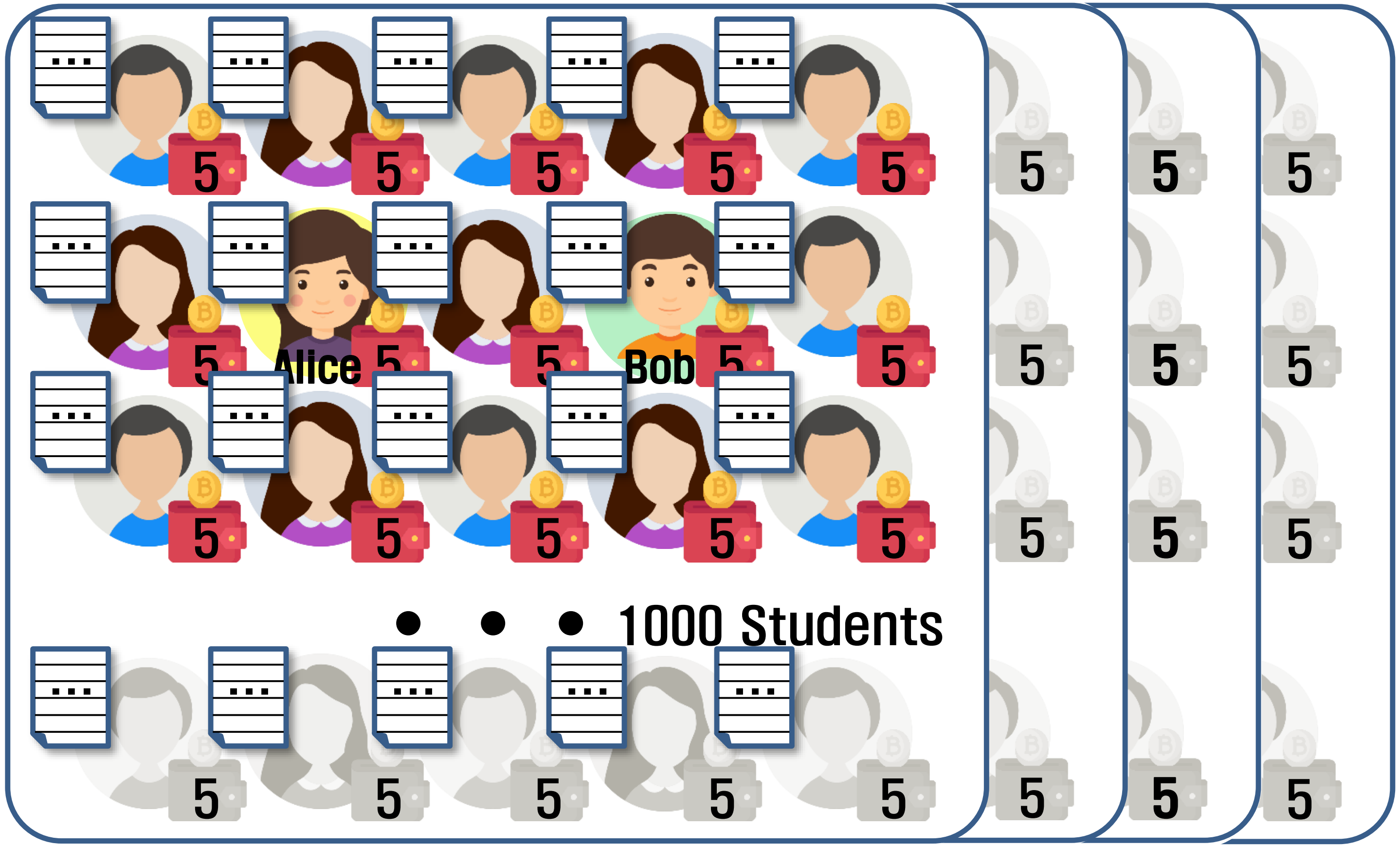


It means that at least 501 students' ledgers (> 50% of all students) must be modified for malicious manipulation.

Blockchain Technology (1/6)

Blockchain mechanism – Easy example

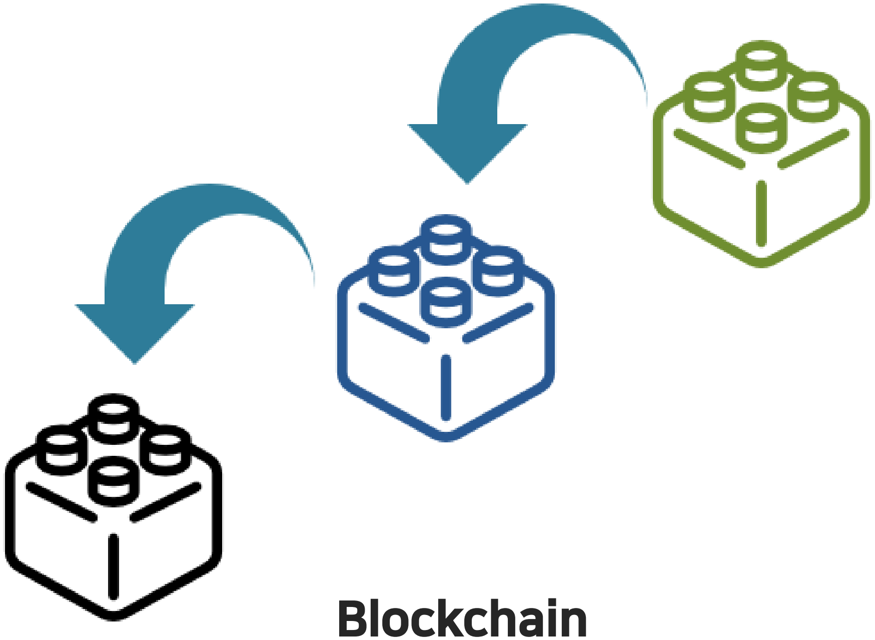
- blockchain method



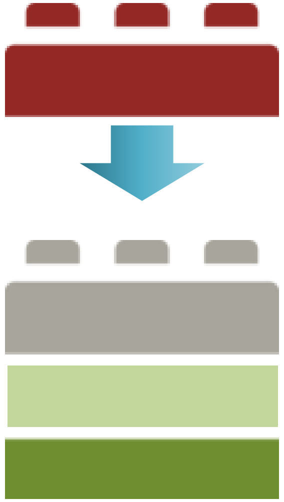
The bigger the size of group is, the harder manipulation is.

Blockchain Technology (2/6)

- **Blockchain (linked collection of blocks)**



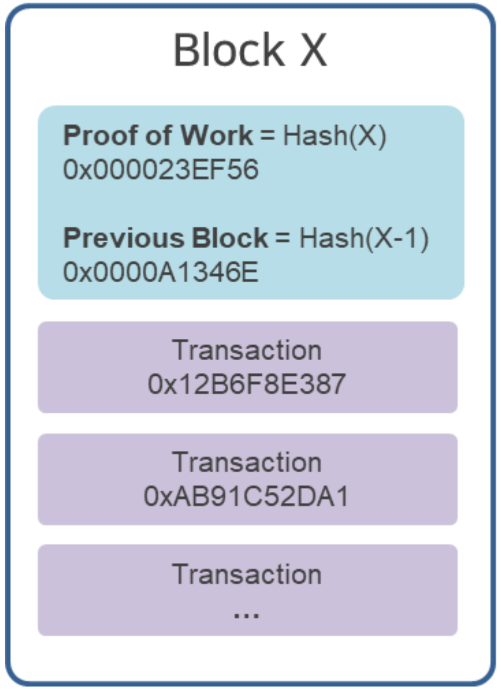
Blockchain



Add block

Blockchain Technology (2/6)

- **Blockchain (Block, Blockchain)**



Block X

Proof of Work = Hash(X)
0x000023EF56

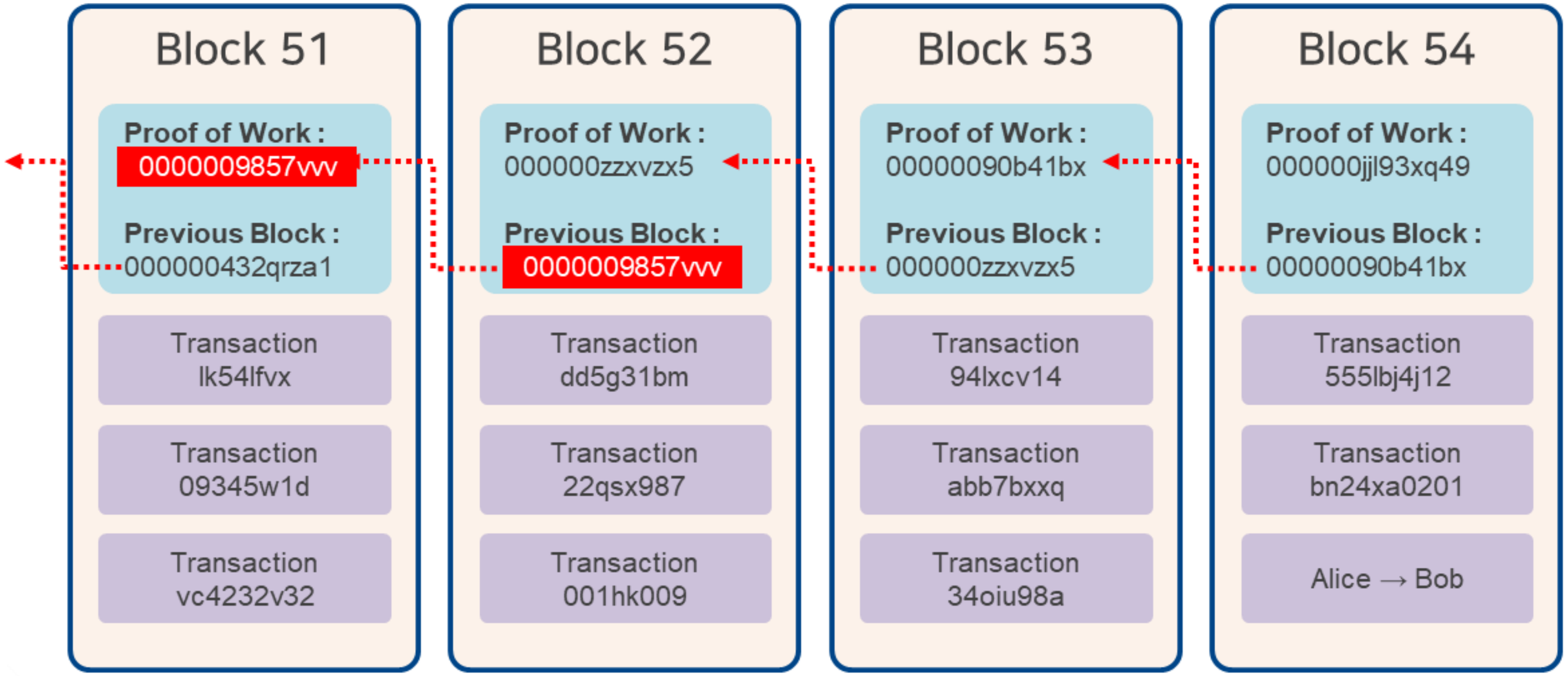
Previous Block = Hash(X-1)
0x0000A1346E

Transaction
0x12B6F8E387

Transaction
0xAB91C52DA1

Transaction
...

Block



Block 51

Proof of Work :
0000009857vvv

Previous Block :
000000432qrza1

Transaction
lk54lfvx

Transaction
09345w1d

Transaction
vc4232v32

Block 52

Proof of Work :
000000zzxvzx5

Previous Block :
0000009857vvv

Transaction
dd5g31bm

Transaction
22qsx987

Transaction
001hk009

Block 53

Proof of Work :
00000090b41bx

Previous Block :
000000zzxvzx5

Transaction
94lxcv14

Transaction
abb7bxxq

Transaction
34oiu98a

Block 54

Proof of Work :
000000jjl93xq49

Previous Block :
00000090b41bx

Transaction
555lbj4j12

Transaction
bn24xa0201

Alice → Bob

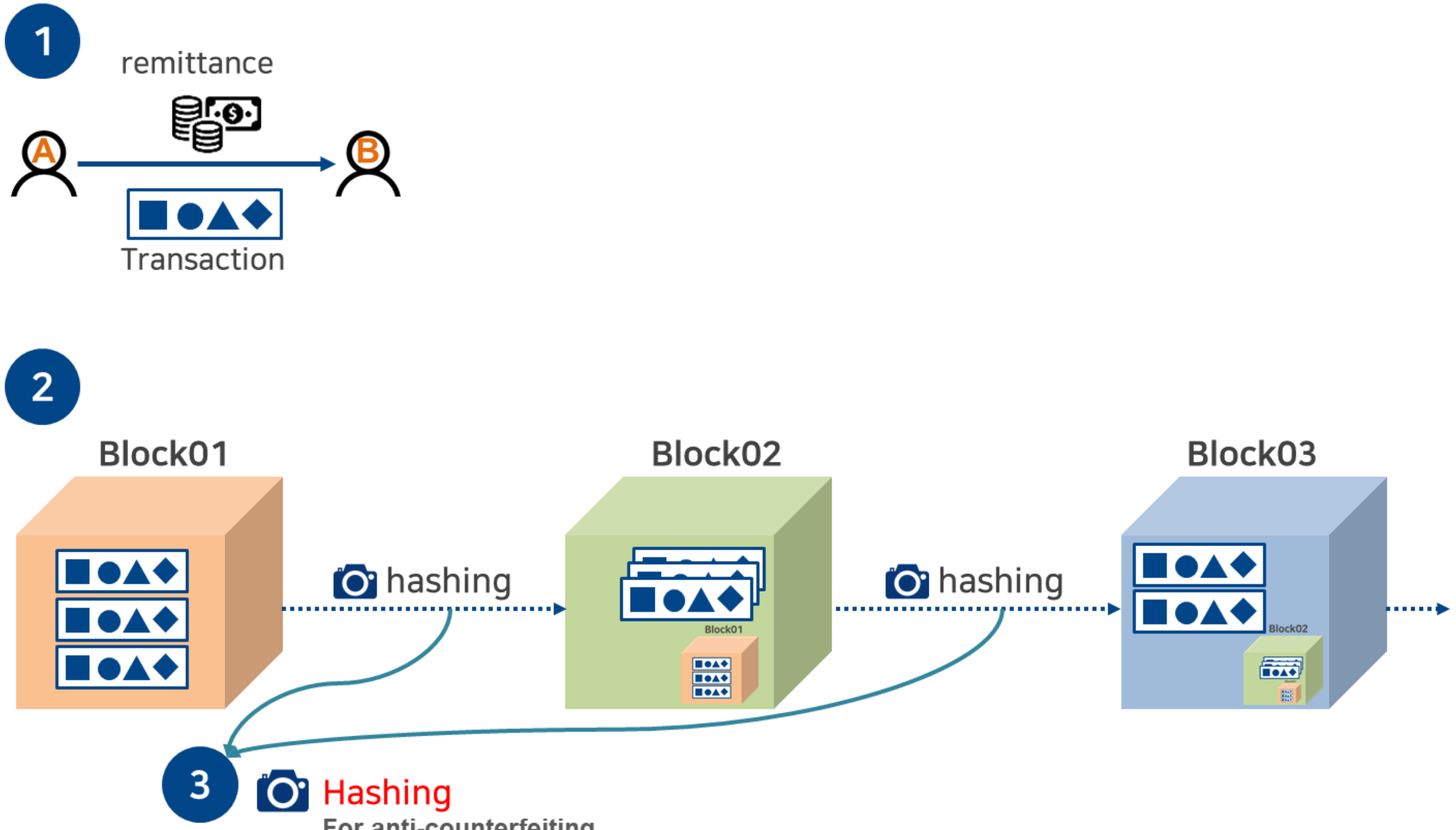
Blockchain

Source: https://www.netguardians.ch/news/2016/12/22/blockchain-explained-part-2

Source: https://fifthperson.com/how-the-blockchain-might-disrupt-the-banking-financial-industries/

Blockchain Technology (3/6)

- **Block creation, Linking Blocks by Hashing**



For anti-counterfeiting,
Take a picture of Block01 and put it into Block02

It is called Blockchain because the blocks are connected by a hash

Blockchain Technology (4/6)

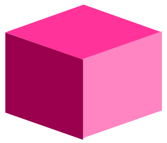
‘Transaction process’ in Blockchain

- **Transaction → Confirmation → Settlement**

1 **Transaction**

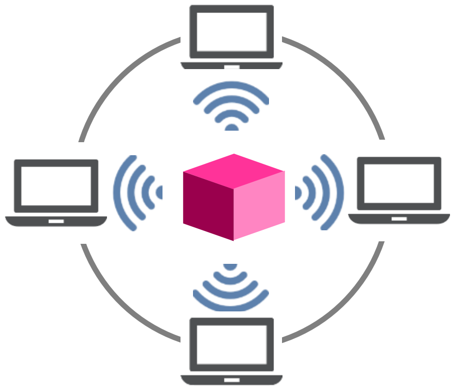
1. A wants to send money to B

2



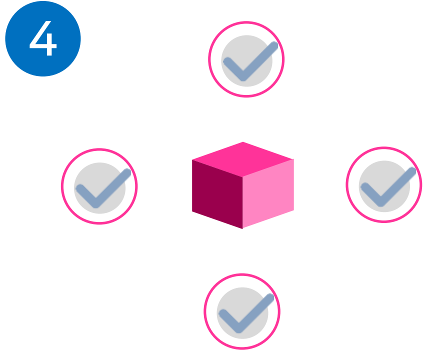
2. The transaction is represented online as a ‘block’

3



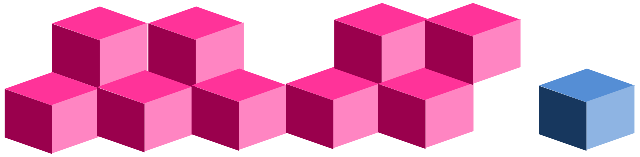
3. The Block is broadcast to every party in the network

4



4. Those in the network approve the transaction is valid

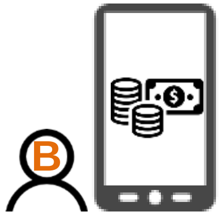
5



Confirmation

5. The block then can be added to the chain, which provides an indelible and transparent record of transactions

6



settlement

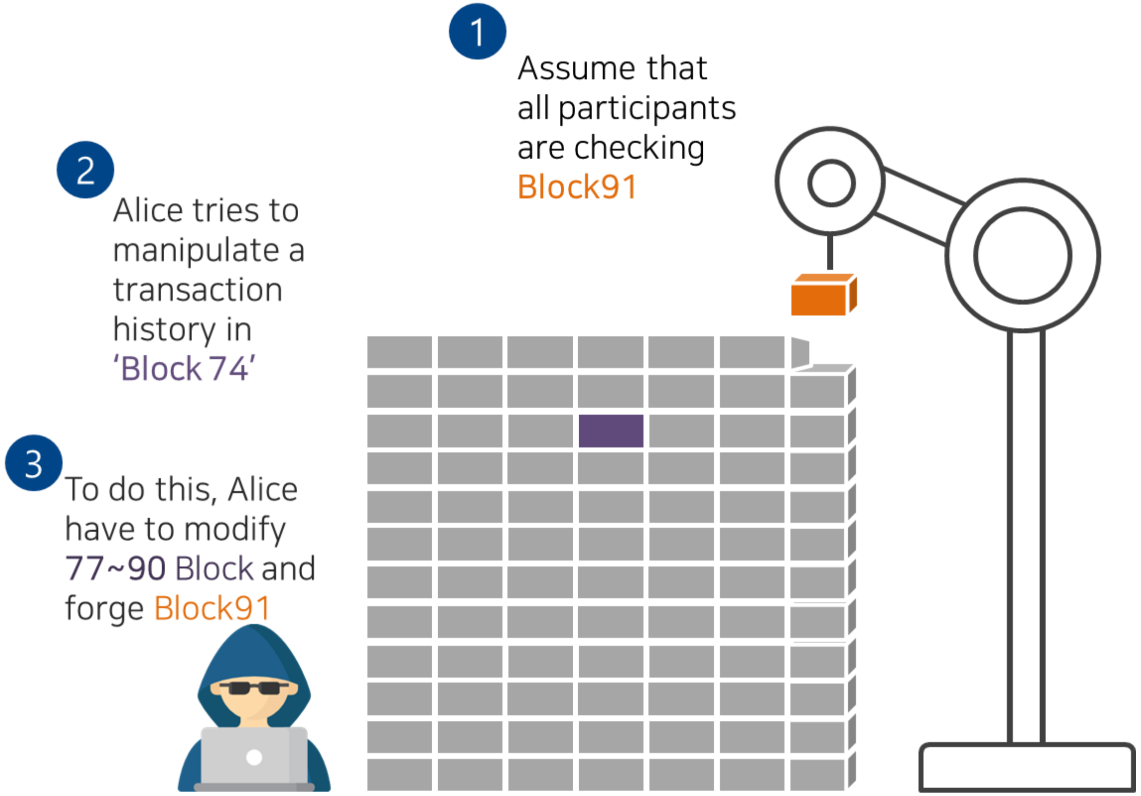
6. The money moves from A to B

Blockchain Technology (5/6)

▪ Reason why Blockchain is hard to forge

- **Unchangeable data**

Lego



1 Assume that all participants are checking Block91

2 Alice tries to manipulate a transaction history in 'Block 74'

3 To do this, Alice have to modify 77~90 Block and forge Block91

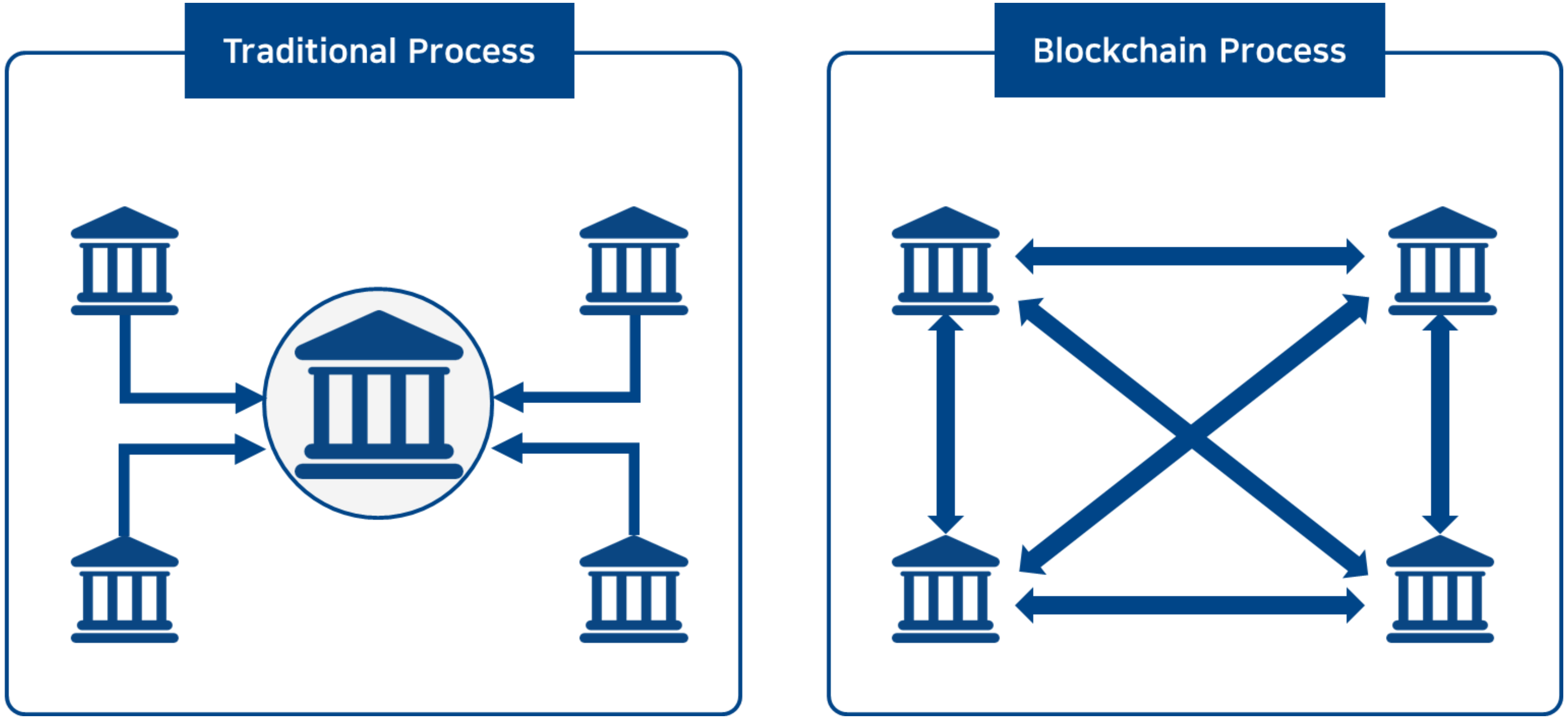
4 Alice must finish all work of 74~90 Block before other participants link Block91. It makes forge much harder

Block

source: http://blog.naver.com/PostView.nhn?blogId=with_msip&logNo=220933922730&parentCategoryNo=&categoryNo=56&viewDate=&isShowPopularPosts=true&from=search

Blockchain Technology (6/6)

- **Key Features of Blockchain**
  1) Decentralized Management
  2) Transparency and Chronology of Transaction Data
  3) Immutability of Transaction Data



source: https://cmp.smu.edu.sg/ami/article/20161208/smarter-banking

Limitations of Bitcoin (1/2)

- **Change in the means of payment**

source: https://www.flickr.com/photos/137346712@N07/27840875261

source: http://seattlekcr.com/Article/view.aspx?p=1&q=&page=1&aid=12125

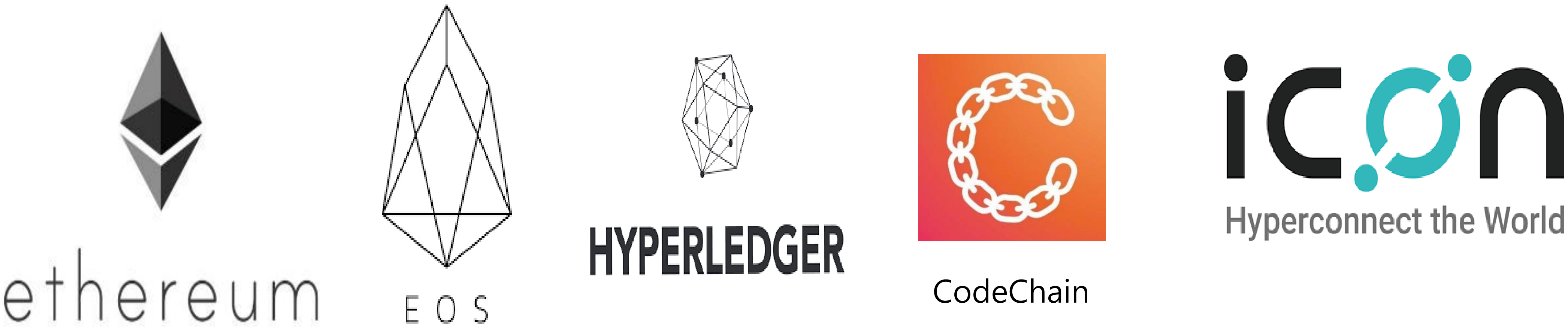
source: http://onboardfly.tistory.com/55

- **Problem of Bitcoin**

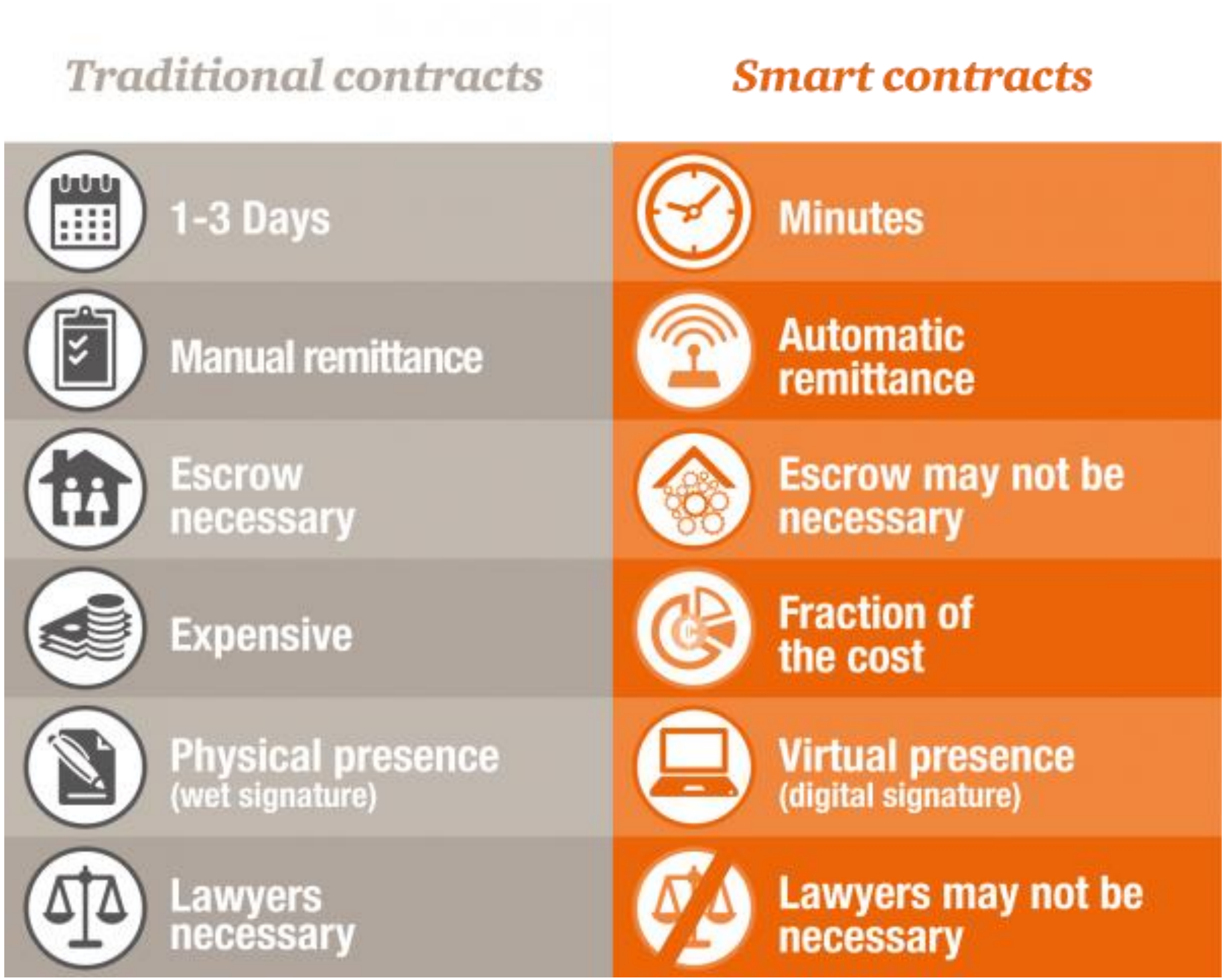
1. **Wastes huge resources**
2. **Long time to confirm transaction (a block is generated every 10 min)**
   - **Too small # of transactions generated per 1 second**
   - **Limit to the amount of transactions that can be included in one block**
3. **Only include payment information**
   - **No ‘Smart Contract’ function**

Limitations of Bitcoin (2/2)

- **Evolution of blockchain technology**
  - **To solve the problems of Bitcoin (as mentioned earlier), various new blockchains have been developed**
    - **Ethereum, EOS, Hyperledger, CodeChain, ICON, etc.**



Smart Contracts



Traditional contracts	Smart contracts
1-3 Days	Minutes
Manual remittance	Automatic remittance
Escrow necessary	Escrow may not be necessary
Expensive	Fraction of the cost
Physical presence (wet signature)	Virtual presence (digital signature)
Lawyers necessary	Lawyers may not be necessary

Source: http://www.thesundaily.my/sites/default/files/thesun/field/Property%203.png

AI vs. Blockchain (1/2)

- **Using AI (Artificial Intelligence)**

1. Can we solve existing hard, unsolved problems?
2. Can we reduce CAPEX/OPEX?
3. Can we provide better services to our customers?
4. Can we create new services in order to create generate new revenues?

AI vs. Blockchain (2/2)

- **Using Blockchain**

1. Can we solve existing hard, unsolved problems?
2. Can we reduce CAPEX/OPEX?
3. Can we provide better services to our customers?
4. Can we create new services in order to create generate new revenues?

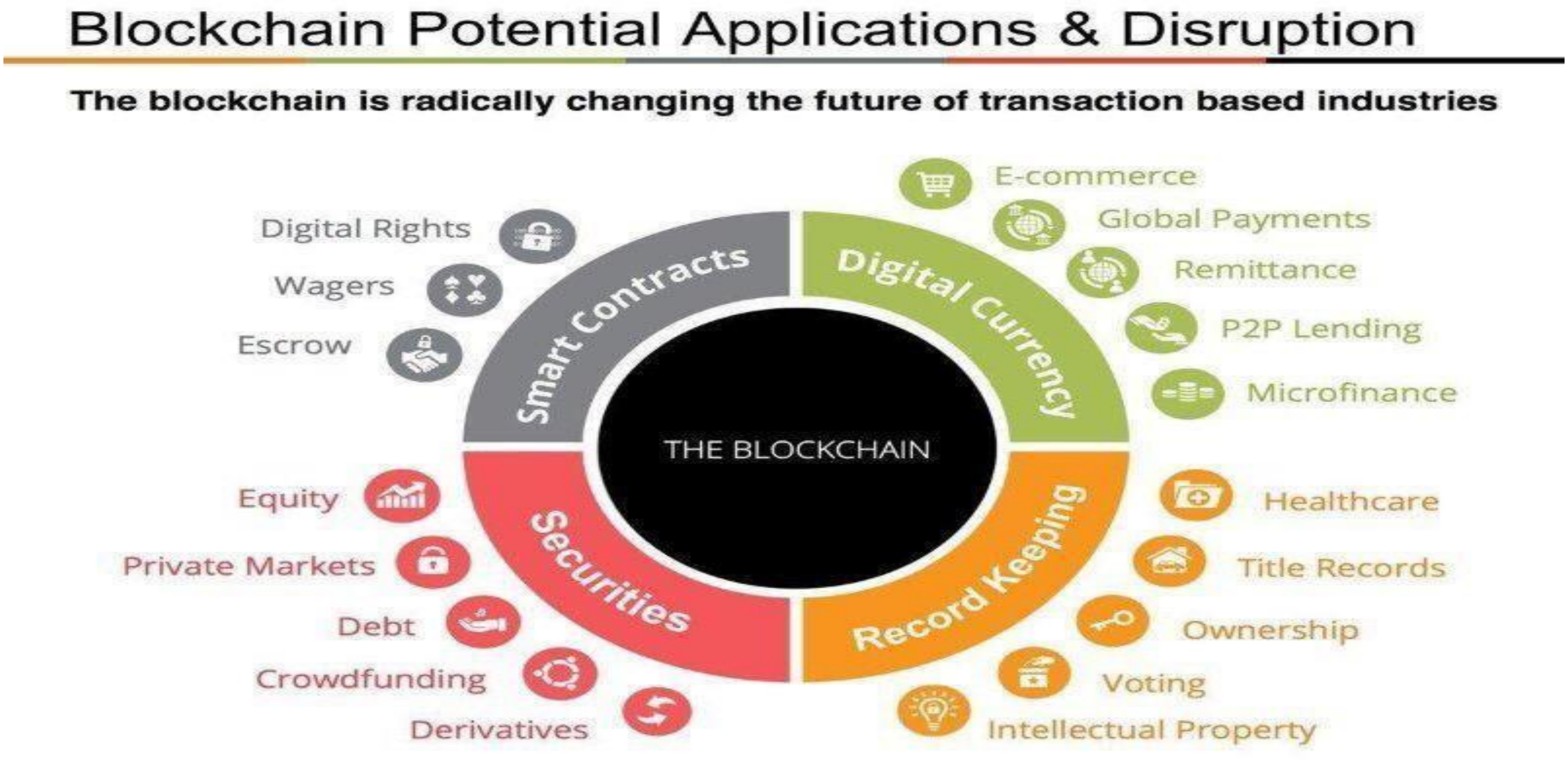
Blockchain Types

- **Public vs. Private**

Attribute	Permissioned	Non-Permissioned
Private	e.g. Hyperledger Fabric, MS BaaS	-
Public	e.g., Ripple	e.g., Bitcoin, Ethereum

MS BaaS = Microsoft Blockchain as a Service

Use Cases of Blockchain (1/5)



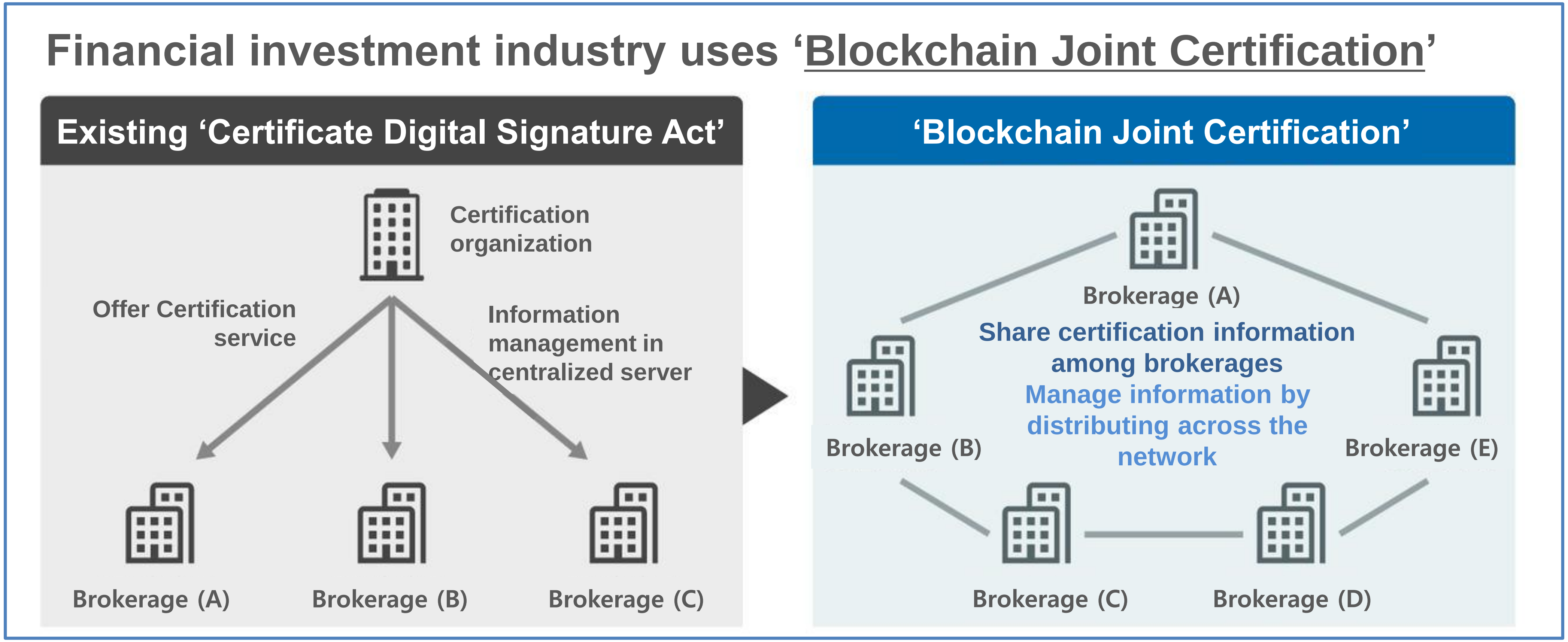
Blockchain Potential Applications & Disruption

The blockchain is radically changing the future of transaction based industries

Source: https://cdn-images-1.medium.com/max/1600/1*PLtFNY0JQPAPkjrQkbQtRw.jpeg

Use Cases of Blockchain (2/5)

- **Commercialization case – Financial security companies**
  - **CHAIN ID of theloop**



Financial investment industry uses ‘Blockchain Joint Certification’

Existing ‘Certificate Digital Signature Act’

Certification organization

Offer Certification service

Information management in centralized server

Brokerage (A)

Brokerage (B)

Brokerage (C)

‘Blockchain Joint Certification’

Share certification information among brokerages

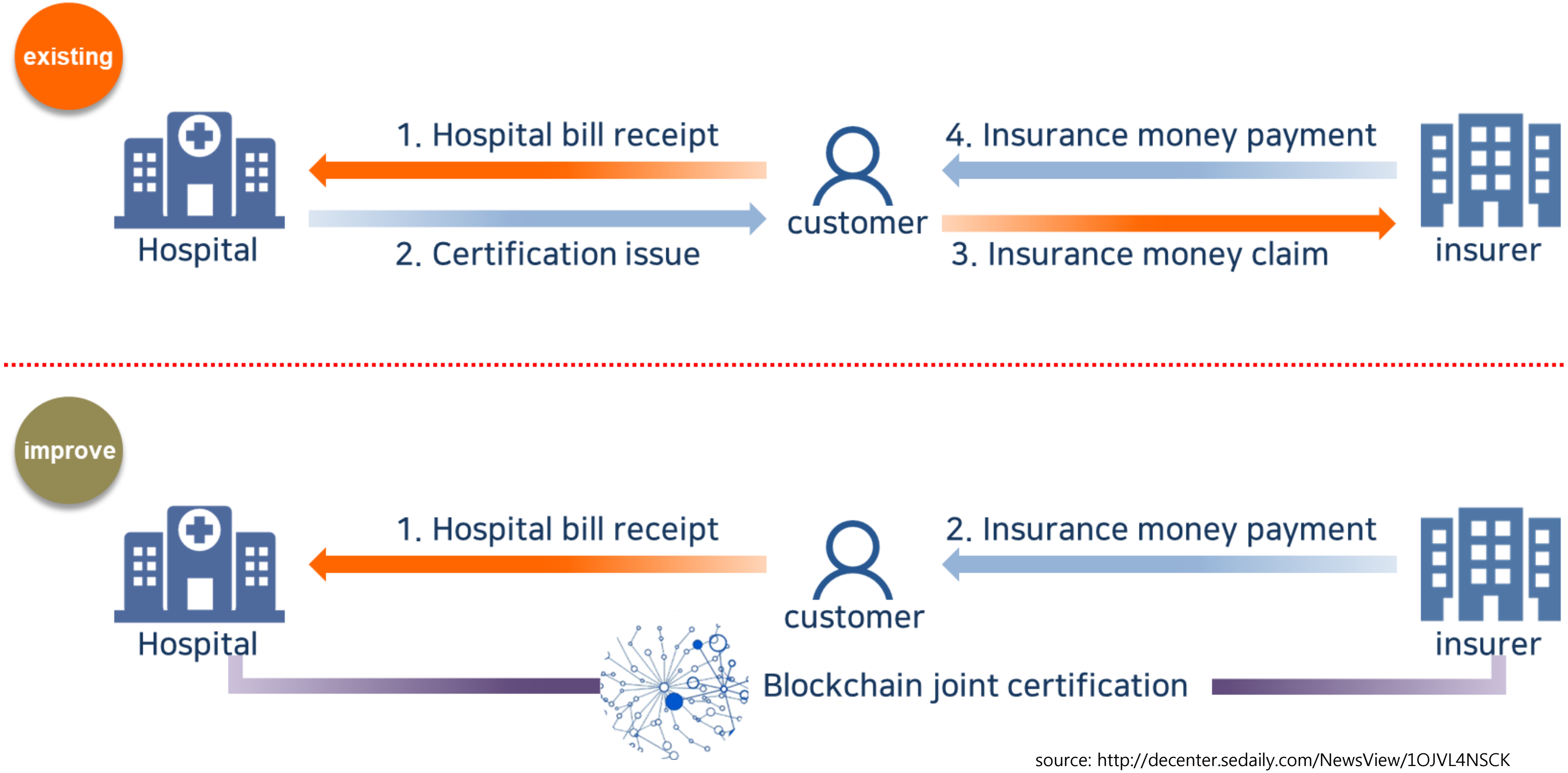
Manage information by distributing across the network

source: http://www.hani.co.kr/arti/economy/finance/816893.html

Use Cases of Blockchain (3/5)

Commercialization case – Insurance companies

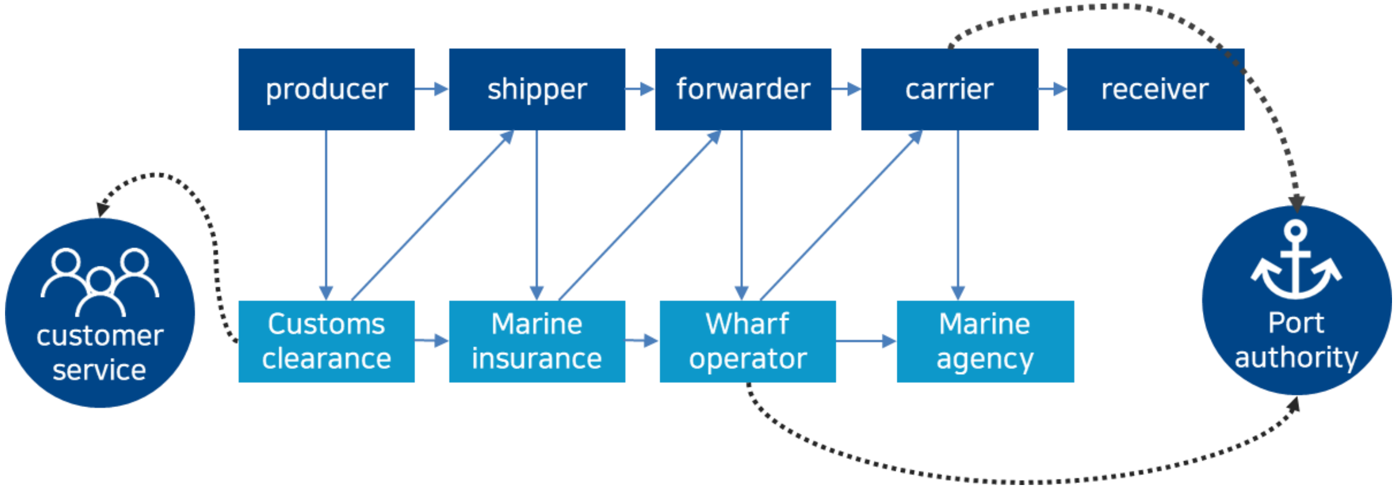
- Insurance money payment service



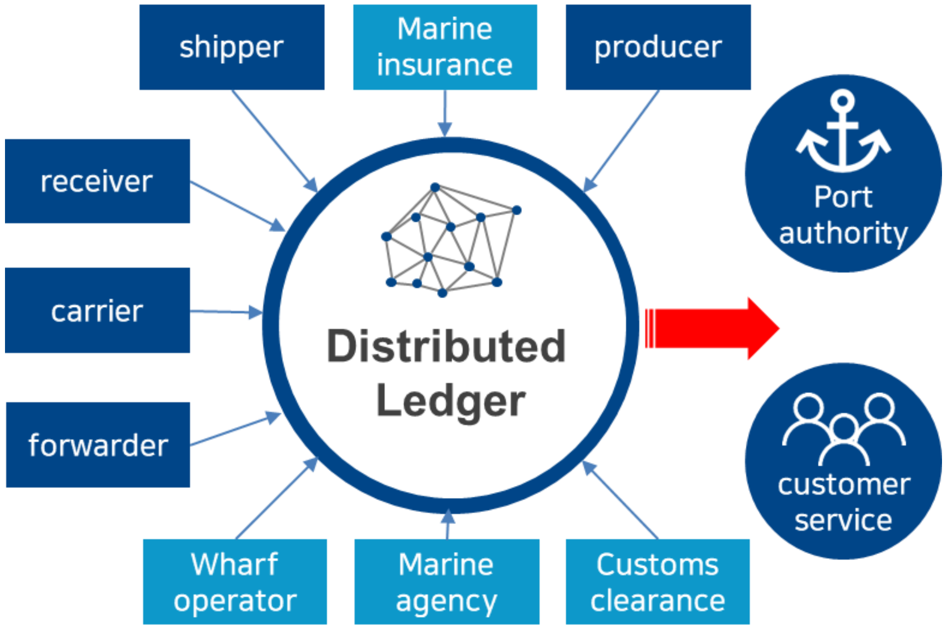
source: http://decenter.sedaily.com/NewsView/1OJVL4NSCK

Use Cases of Blockchain (4/5)

- **Marine Transport & Trade**
  - **International logistic EDI system**



Current EDI structure

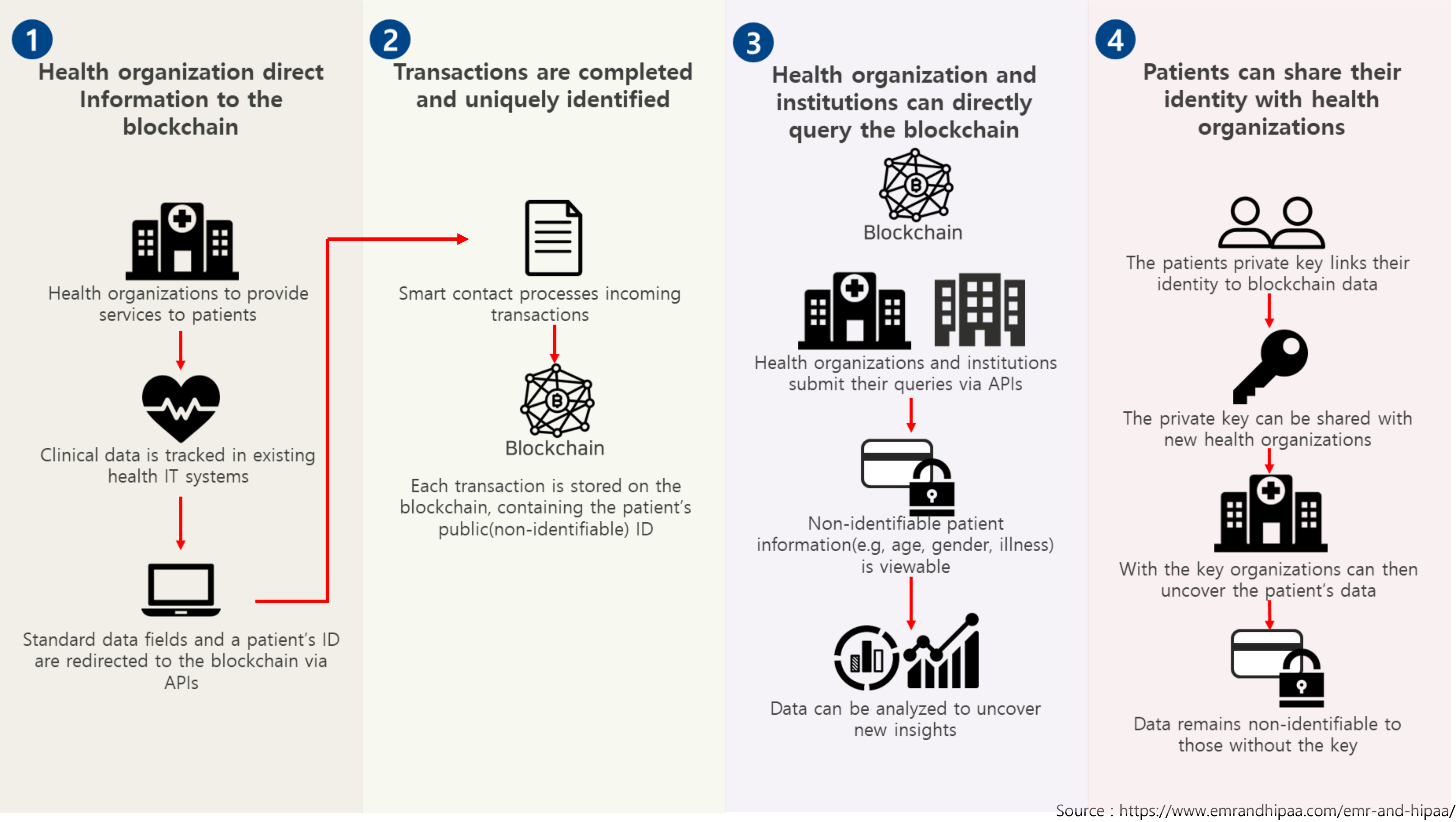


Blockchain based structure

source: http://www.mediakn.com/mobile/article.html?no=3899

Use Cases of Blockchain (5/5)

- **Medical Data Sharing**



1

Health organization direct Information to the blockchain

Health organizations to provide services to patients

Clinical data is tracked in existing health IT systems

Standard data fields and a patient's ID are redirected to the blockchain via APIs

2

Transactions are completed and uniquely identified

Smart contact processes incoming transactions

Blockchain

Each transaction is stored on the blockchain, containing the patient's public(non-identifiable) ID

3

Health organization and institutions can directly query the blockchain

Blockchain

Health organizations and institutions submit their queries via APIs

Non-identifiable patient information(e.g, age, gender, illness) is viewable

Data can be analyzed to uncover new insights

4

Patients can share their identity with health organizations

The patients private key links their identity to blockchain data

The private key can be shared with new health organizations

With the key organizations can then uncover the patient's data

Data remains non-identifiable to those without the key

Source : https://www.emrandhipaa.com/emr-and-hipaa/2017/08/03/healthcare-blockchain-use-case/

Conclusion

- **Blockchain is getting very popular as a core technology of the 4th industrial revolution in addition to AI, Big Data, IoT and Cloud computing**

- **New P2P-based shared economy is being established**

- **Many new blockchain-based services using the essential features of 1) no central authority, 2) transparency of transactions, and 3) immutability of data are being developed, trialed and commercialized**

References

- https://www.youtube.com/watch?v=Pl8OlkkwRpc&t=326s
- https://www.youtube.com/watch?v=G3psxs3gyf8
- https://www.youtube.com/watch?v=WSN5BaCzsbo
- http://slidesplayer.org/slide/11308363/
- https://tokenpost.kr/terms/2350
- https://blog.naver.com/PostView.nhn?blogId=yom28481&logNo=70159113950&proxyReferer=https%3A%2F%2Fwww.google.co.kr%2F
- https://namu.wiki/w/%EC%95%94%ED%98%B8%ED%99%94%ED%8F%90
- https://namu.wiki/w/%EB%B8%94%EB%A1%9D%EC%B2%B4%EC%9D%B8
- https://bitcoin112.com/digital-cash/%EB%B9%84%ED%8A%B8%EC%BD%94%EC%9D%B8%EC%9D%98-%EC%9E%A5%EC%A0%90/
- https://steemit.com/kr/@tintom/2fgvq8
- https://www.slideshare.net/bluegull/block-chain-82203010?from_action=save
- http://blog.naver.com/PostView.nhn?blogId=daumcood&logNo=220939981982&parentCategoryNo=&categoryNo=&viewDate=&isShowPopularPosts=false&from=postView
- https://www.slideshare.net/JaeGonLim/ss-69099728
- http://www.hani.co.kr/arti/economy/finance/816893.html#csidx85b3b55d5ac4cdb95bdb4faf3adcff3
- http://www.mediakn.com/mobile/article.html?no=3899
- http://decenter.sedaily.com/NewsView/1OJVL4NSCK
- Blockchain Revolution - https://www.amazon.com/Blockchain-Revolution-Technology-Changing-Business-ebook/dp/B0141ZP32E