First tutorial:

- Start the week of 10 Feb (10 Mon/11 Tue)

A simple task

- In each tutorial group, we will form smaller groups of about 3 students.

- Each smaller group will be given a simple question, e.g. a terminology (what is a "cryptocurrency exchange"?) or a simple statement (do you think it is easy to open a bank account for anyone?)

- Each smaller group will try to investigate the question and come up with a brief presentation, TAs will observe and score your contribution as "tutorial participation".

A short review:

Q: What technologies are driving FinTech behind

(i) blockchain;
(ii) big data analytics;
(iii) AI technology;
(iv) e-payment;
(v) RegTech;
(vi) Cyber security & privacy

Remarks:

Have you heard about ICO (Initial Coin Offering)? (vs IPO, Initial Public Offering)

ICO: Roughly speaking, attract people to invest on a new cryptocurrency (token) so as to collect money for a project, app, or service
[~ blockchain-related startups to raise funds, or crowdfunding]

IPO: Investor buying the shares of a company

A simple common goal of investors: hopefully the value of the token (share) goes up, then you earn some money!

IPOs are protected by the financial authorities of a Government, but not ICOs!

China Bans Initial Coin Offerings and Cryptocurrency Trading Platforms

China Regulation Watch

September 21, 2017

By: Greg Pilarowski | Lu Yue

On September 4, 2017, the People's Bank of China (中国人民银行), Cyberspace Administration of China (国家互联网信息办公室), Ministr Industry and Information Technology (工业和信息化部) ("MIIT"), State Administration for Industry and Commerce (国家工商总局) ("SAIC"), (

According to a report from rfssfs.org, from Jan 2016 – Aug 2019, ICOs raised $13 Billion worldwide!!

Another report from Satis Research Group in 2018: ~1500 ICOs were studied, 78% of these projects were identified as scams, total value: ~$1.3 Billion.

Canadian cryptocurrency fund boss Gerald Cotten died – and US$190million of his investors' money may be encrypted forever

- Investors in QuadrigaCX, Canada's largest cryptocurrency exchange, have been unable to access funds since founder Gerald Cotten died in December, aged 30
- His widow says she does not know his passwords – leading some angry investors to question whether Cotten really died while opening an orphanage in India

Q: What it is for?

[Dec 2018]

About US$190M cannot be accessed since they claimed that only the founder (died in Dec 2018) has the access key.

However, according to a report by Ernest & Young (court appointed monitor):
The company made a mistake transferring another 103 bitcoins to a wallet that they could not access in Feb 2019 after the founder died!

Interestingly, some investigators claimed that all money in those wallets were emptied 8 months before CEO's death!

=> rumor: CEO faked his death and stole all money?

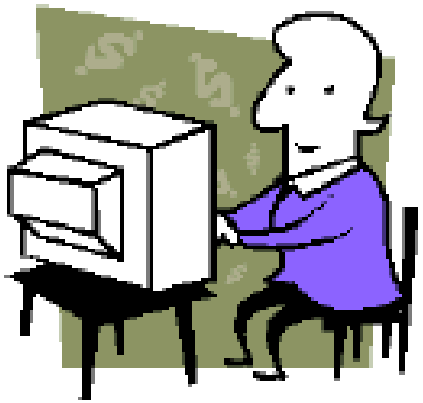
Introduction to blockchain technology

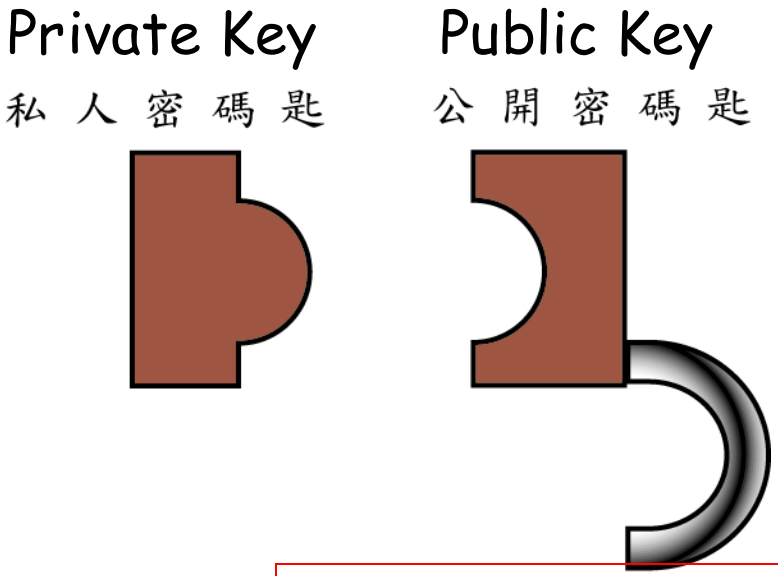
- Basic cryptographic techniques
  - Public-key, private key, digital signature
  - Cryptographic hash value
- How (a basic) blockchain works?
  - Transaction, block, blockchain
  - Concept of "proof-of-work" (PoW)

(i) Public key, private key, digital signature

- Public key & private key always go in pairs

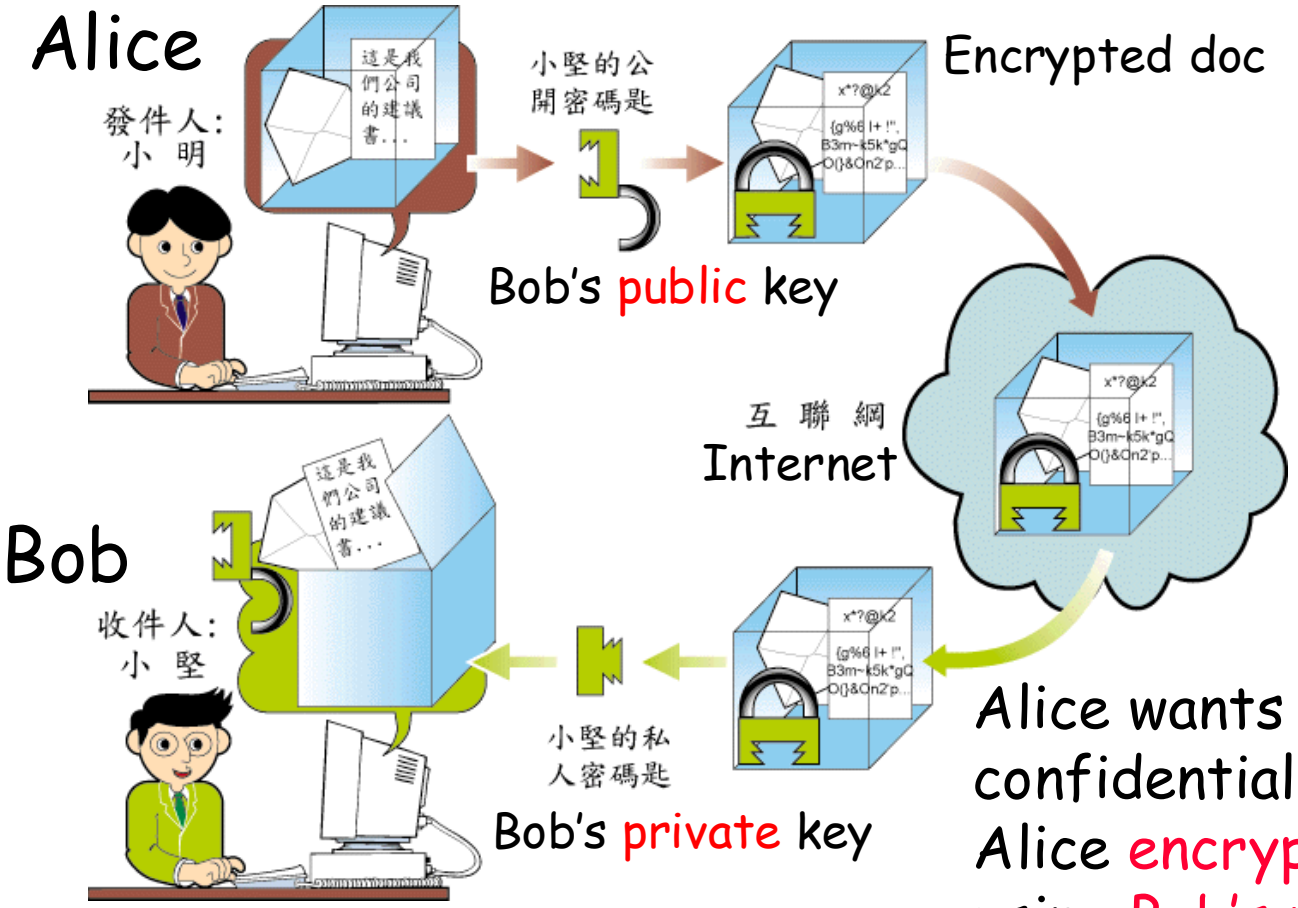
- Each user has a pair of public and private key





- Private key – keep secret;
  public key – open to public

** Knowing one's public "cannot" deduce one's private key **



To encrypt a document to be read by user A, we need to use A's public key; and only A's private key can be used to decrypt it.

Alice wants to send something confidential to Bob:
Alice encrypts the message using Bob's public key.

Bob wants to read the confidential (encrypted) message from Alice:
Bob decrypts the message using Bob's own private key.

Important property:
Without the right private key, it is very difficult to decrypt the message.

(ii) Digital signature

- Given a digital document, we can create a digital signature using your private key.

- Anyone can verify your signature using your public key.

- *** Any change (even one letter or just a bit in the document), the signature won't match! ***

An efficiency problem for digital signature:
The longer the document is, the longer the time to create the signature and the longer the signature will be.

(ii) Cryptographic hash value

Given any digital document (no matter how long it is), we can generate a fingerprint of fixed length (e.g. 160 bits), called hash value.

- Again, one change (e.g. one bit/letter) in the document, the hash won't match.

  Everybody can create the same hash on the same document using the same hash function. [The hash function is available in public]

Q: What are the differences between a hash value and a digital signature?

Usage (fast and safe):

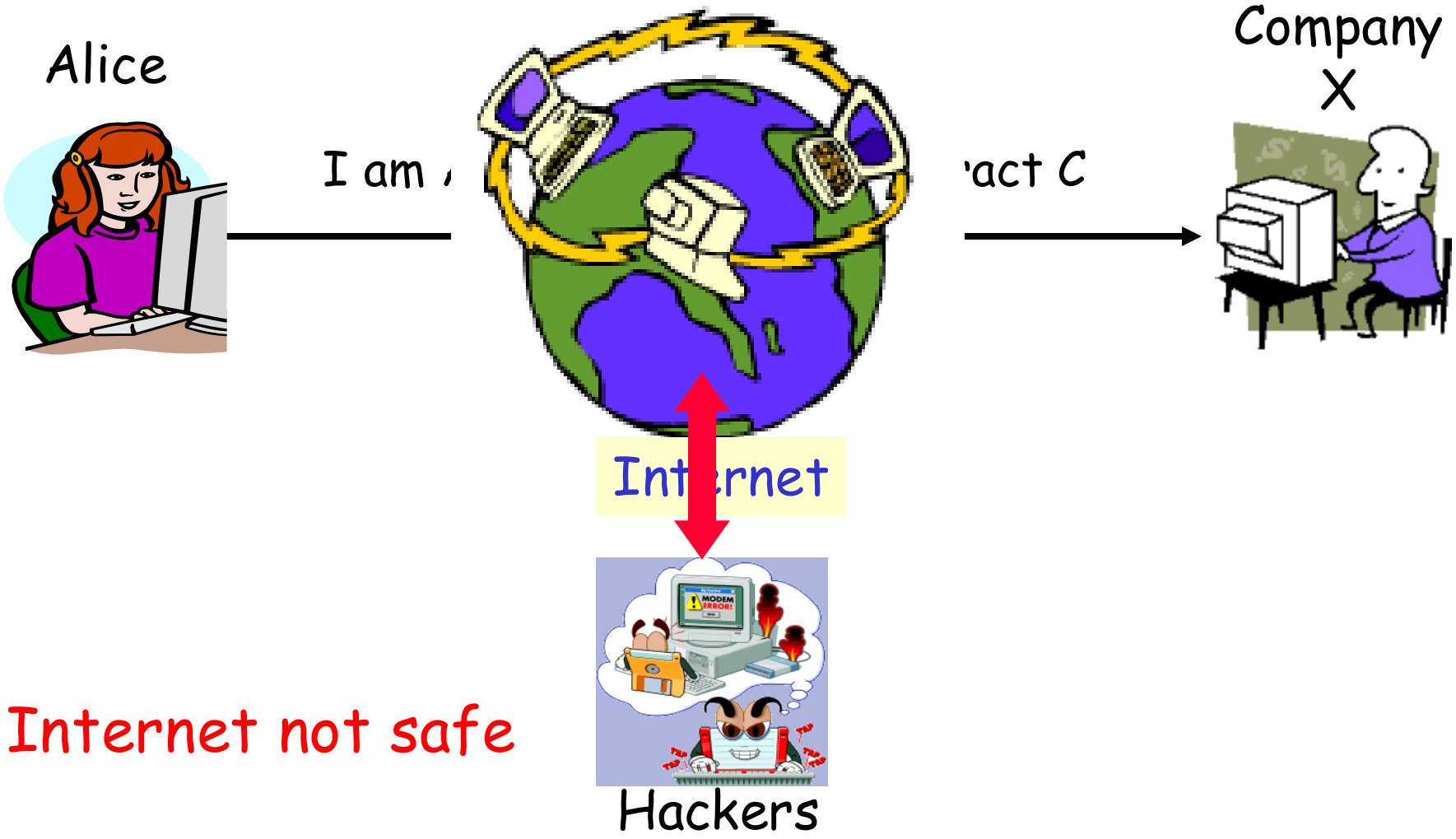
Given a document D,

(i) create a hash value of D, h(D)

(ii) sign on h(D) instead of D.

A short summary (Usage of these techniques)

Alice wants to send a contract C to Company X



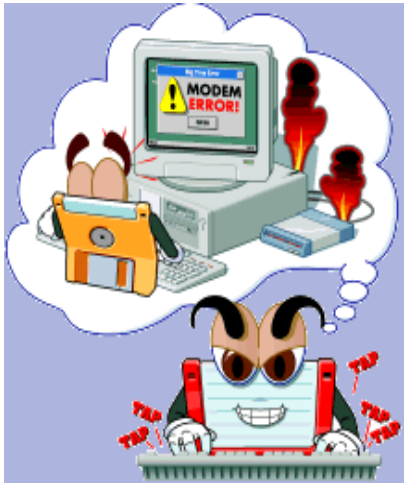
Internet not safe

Alice

I am Alice. Here is our contract C

Devil

Company X



Hackers

Devil

A short summary (Usage of these techniques)

(i) Alice does not want the contract C to be modified without being noticed.

(ii) Alice wants to confirm the ownership of C

If she sends this over, is it secure?

C + hash(C)

No, recall that hash function is public, so the attacker can change C and also hash(C):

C' + hash(C')

A better solution:

C + hash(C) + Signature(hash(C))

An attacker may be able to modify C and hash(C), but more difficult to modify Signature(hash(C)). Why?

Another poll to see if you understand this concept :-P

What is a blockchain (in the context of bitcoin for ease understanding)?

A transaction:

Create 15 coins and deposit to Alice

Or

Transfer 10 coins from Alice to Bob

Or

Transfer 6 coins from Bob to David

A transaction chain:

Create 15 coins and deposit to Alice — Authorization

↓

Transfer 10 coins from Alice to Bob — Signed by Alice

↓

Transfer 6 coins from Bob to David — Signed by Bob

Q: how to check if a transaction is valid (enough balance)?

In reality, bank is doing this and keeps track of the transactions for EACH customer

Q: How about we don't want a bank, we don't want a centralized entity to do it?

A: One solution: put the transaction chain in the Internet, everybody can get a copy & check it!

Good idea, but
a) Can anyone modify the transaction easily?

b) Who maintain the chain and who appends new transactions to the chain?

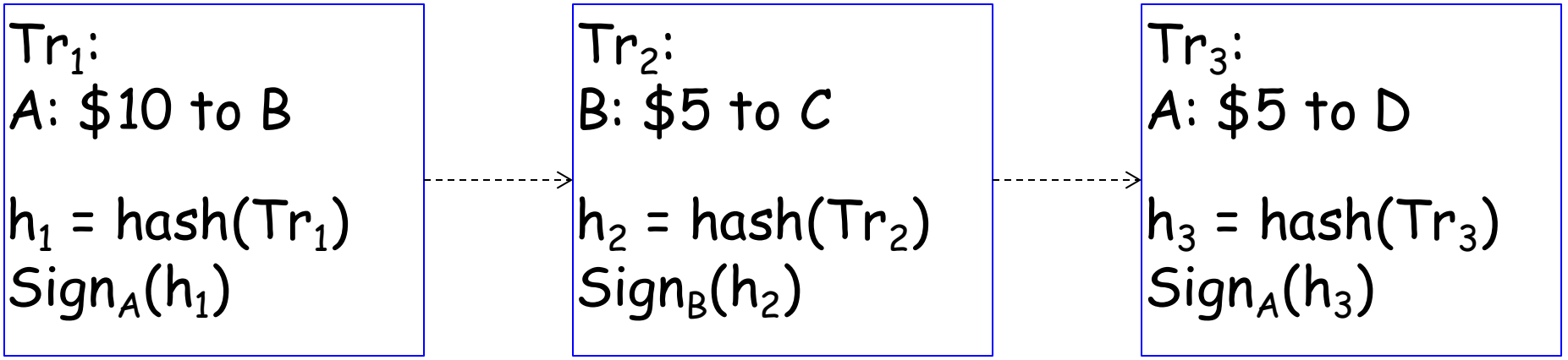
Recall:

Contract (C) + hash(C) + Signature(hash(C))

Hash of the contract

Use cryptographic operations

1st attempt

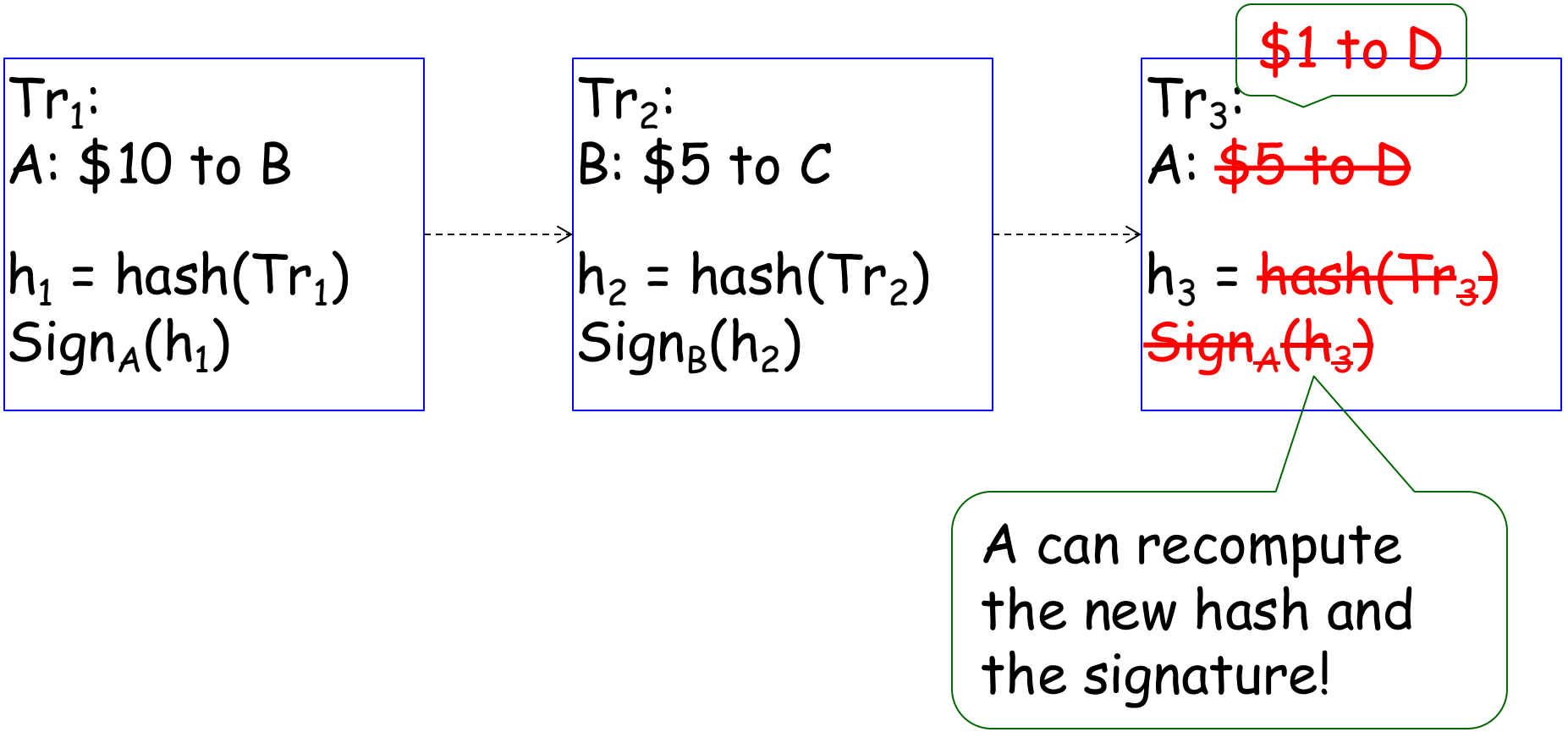


Everybody can check if each transaction is authorized and valid

Problem: A can change the transaction!

Use cryptographic operations

1st attempt



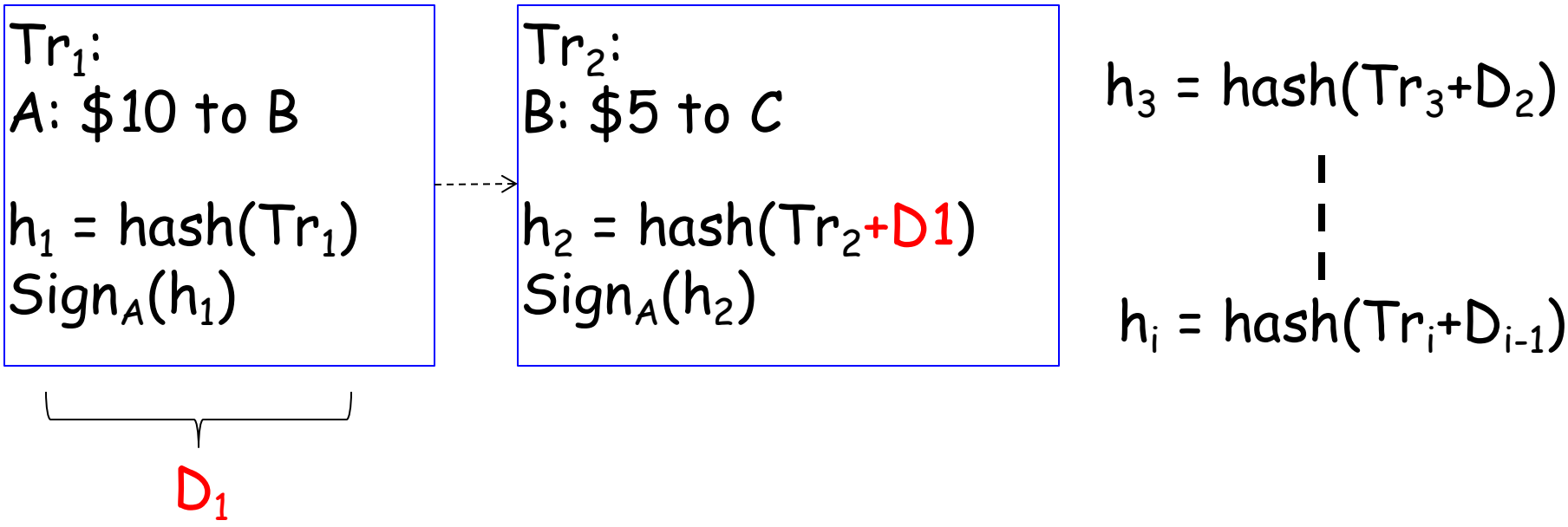
Hint:

Recall that hash can make things difficult to change!

Once you change one bit, the hash does not work.

Our problem: The text to be created a hash and the signature is from the same user *A*

Modified version



If A changes a transaction, he has to change all the following transactions!

(b) Who is going to maintain this chain and append new Tr?

A: Everybody joining the scheme in the network

- Everybody tries to keep a copy of the chain

- When A has a new transaction, he broadcasts to everyone. Everyone checks it and tries to append it to the chain

- The first one who completes it broadcast the new chain

The ones who help to check the transaction are called Miners

Chaos?

In the beginning, assume every miner got the same blockchain, but after a while, we may have:

E.g. Miner A appends a new block and broadcast, but B and C did not get it.

E.g. Miner E, who is an adversary, appends a fake block and broadcast, D is working on E's chain….

E.g. Even worse, F double-spends, send out two transactions (give the same money to two users) and broadcast….

A short review:

Q: Why it is difficult to modify a transaction without being noticed once it is stored in blockchain?

A: For Tr_i, the hash is created based on (i) information of Tr_i and (ii) information of Tr_{i-1}

=> If you change Tr_i, of course you need to change hash value for Tr_i & the signature, but then you also need to change hash value for Tr_{i+1} & its signature, hash value for Tr_{i+2} & its signature, …. which can be regarded as impossible!!

Q: Blockchain has no centralized administrator, who is responsible to maintain the chain?

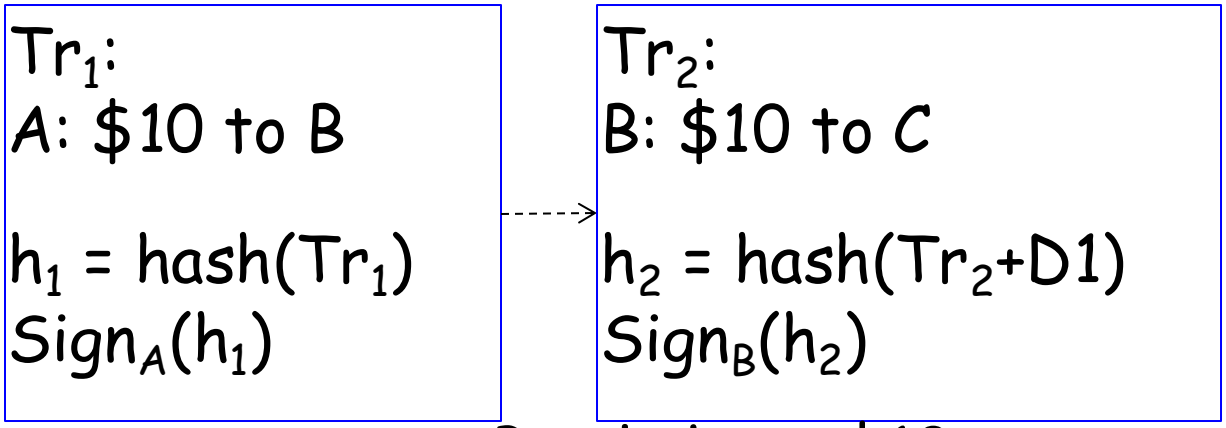
A: Miners, basically any user can be a miner

Q: Is it really ok?

(b) Who is going to maintain this chain and append new Tr?

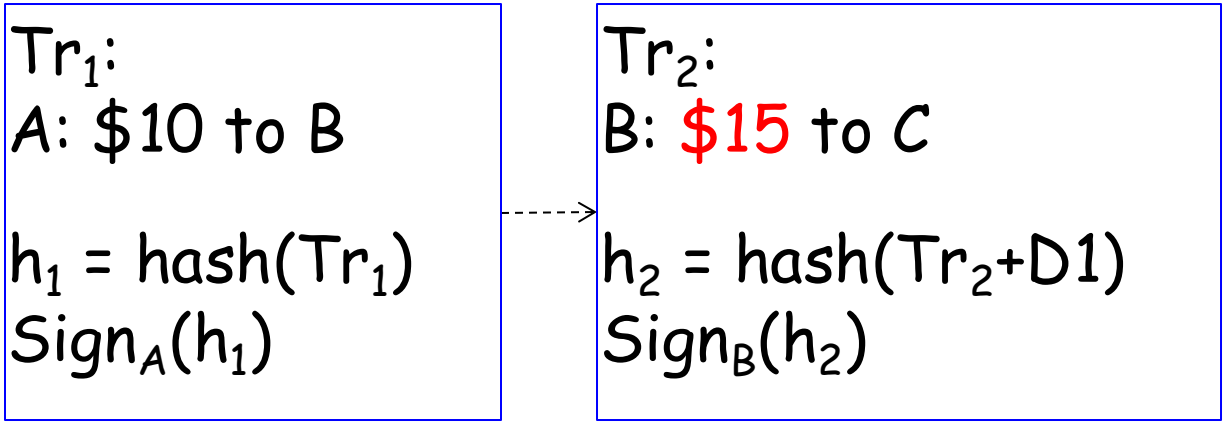
A: Everybody joining the scheme in the network can choose to be a miner

- Every miner tries to keep a copy of the chain
- When A has a new transaction, he broadcasts to the miners. A miner can select any new transaction to check and tries to append it to the chain
- The miner who completes it broadcast a new chain, when another miner sees that a particular transaction has been processed, he/she will pick another transaction to work on.

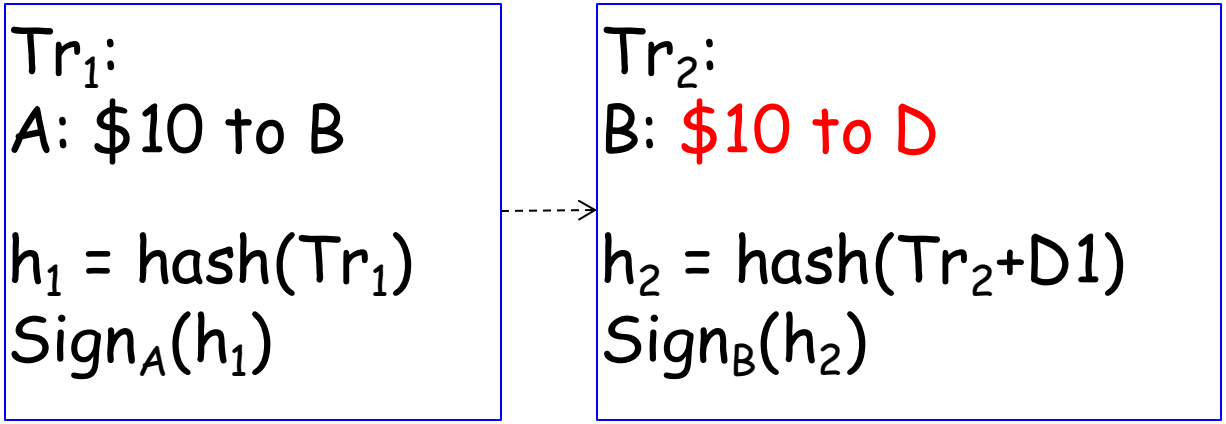


Correct

Assume B only have $10



Fake



Double Spend

A very simple rule, but it works:

Every miner follows the longest chain

Based on what principle, why only valid transactions can be added? And every miner eventually only keeps the valid chain?

A: Assuming the majority of miners are honest.

Existing chain

Tr_1:
A: \$10 to B

$h_1 = hash(Tr_1)$
$Sign_A(h_1)$

Correct

Tr_2:
B: \$5 to C

$h_2 = hash(Tr_2+D1)$
$Sign_B(h_2)$

Fake

Tr_2':
B: \$15 to C

$h_2 = hash(Tr_2'+D1)$
$Sign_B(h_2)$

Most miners will agree the correct one and produce: $Tr_1 \rightarrow Tr_2$

More miners (honest ones) accept this one and further work on it, so it becomes longer

Why people want to help?

Incentives:

In return, he can create new coins for himself + get the transaction fee (stated in the transaction).

Q: Do you think checking if a transaction is valid time-consuming?

No, should be quite easy and fast, then will it be a problem?

So, they make the addition of transaction difficult:
"Proof of work": You work on it, you get reward!

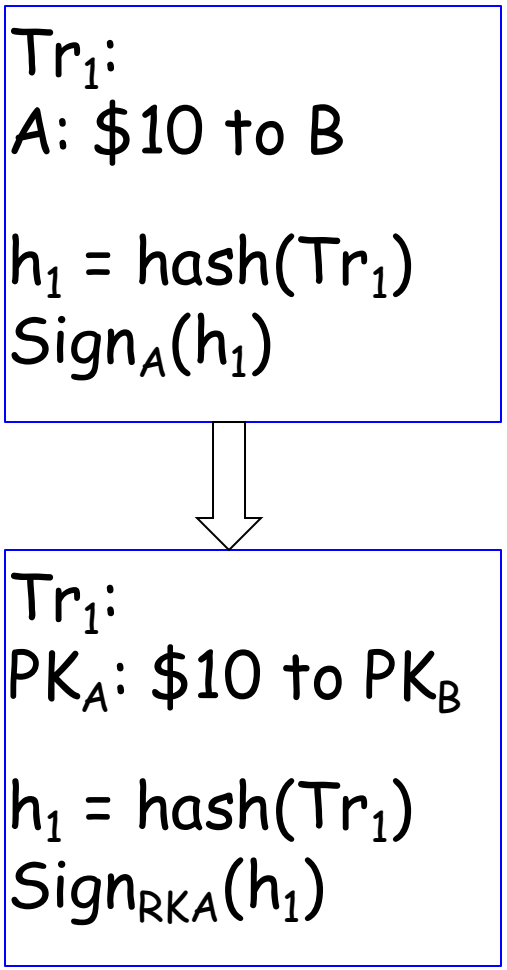
In order to append a new transaction to an existing chain, he/she needs to solve a difficult problem (computing power) besides checking the validity of the transaction.

Remark: This difficult problem has a random factor to make it fairer (i.e., the one with more computing power may not be able to get the answer faster than one with less computing power) to attract more miners to join!

I.e., In this design of the blockchain, it purposely slows down the transaction rate so that miners have time to check through the added transactions!

Last Q: How to protect privacy?

A: We do not use names in the transaction.



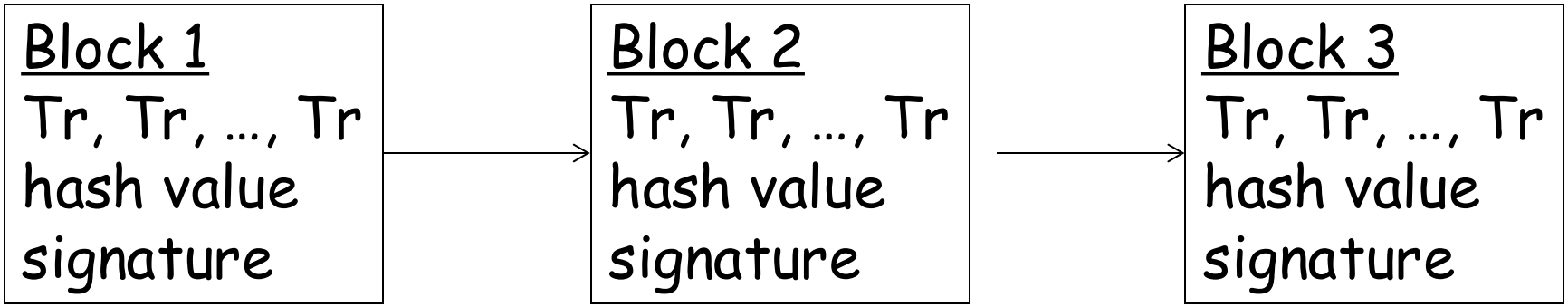
B creates a pair of public key (PK_B) and private key (RK_B) to receive A's money.

A also another pair (PK_A, RK_A) for his $10

I.e., if you don't tell anyone who you are, and only provide the private key to access the bitcoins, basically no one knows your true identity!

Hey, then what is blockchain?

To increase efficiency, we can put several transactions together into a block:



This is our blockchain!

Conclusions

✪ A lot of fine details not covered :

- when should a transaction be confirmed?
- storage issue?
- privacy issue, efficiency issue?
- really secure?

✪ A lot of new potential applications, e.g. decentralized data trading (sharing) center, collaborative data analysis….