

<Short review on Blockchain Technology>

(i) Cryptographic key elements

- Public key/private key pairs
- Digital signatures
- Hash function

(ii) How these elements used in blockchain technology?

Q: How to achieve sender/receive anonymity?

Q: What are the uses of public/private key & digital signature?

Q: How about hash function?

(iii) Role of miners and what is "proof of work"?

- How to choose the correct chain?
- When to confirm a transaction?
- What is the assumption behind the bitcoin network?

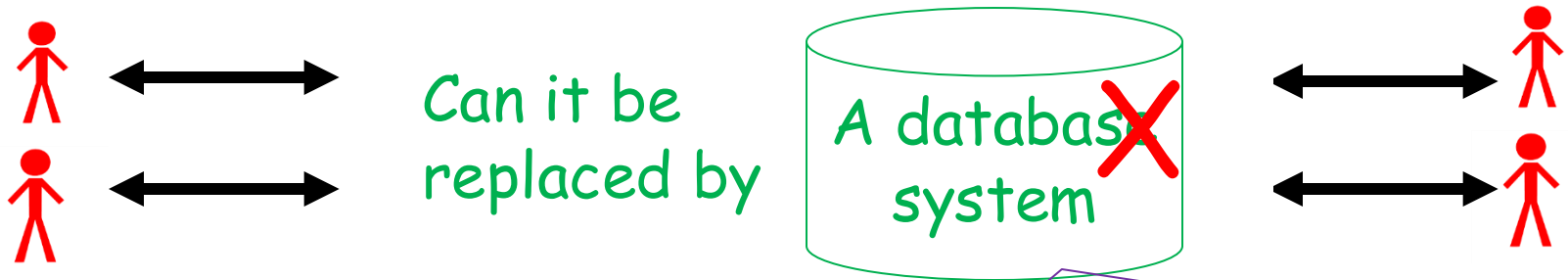
Remarks

★ 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....

<Short summary> Characteristics of blockchain



A kind of distributed ledger (transaction book)

- storing ***all*** transactions of ***all*** users.
- capable of **executing embedded programs automatically** (smart contract) [Later version of blockchain, not bitcoin].

Properties:

- Decentralized** (no centralized authority (all users/miners))
- Immutability** (no changes in records, **guaranteed by crypto**)
- Transparent** (every one can check ***all*** transactions),

Q: Why we need a decentralized system?



(i) Trust issue

No single entity to make decision

E.g. if the application involves multiple banks, who is going to manage the database? why this bank? who is the trusted party?

(ii) Transaction fee



The trusted party who manage the database of transactions (e.g. bank to hold our accounts) may not want to do it for free, they may charge the users a high transaction fee?

Some disadvantages of having a centralized party

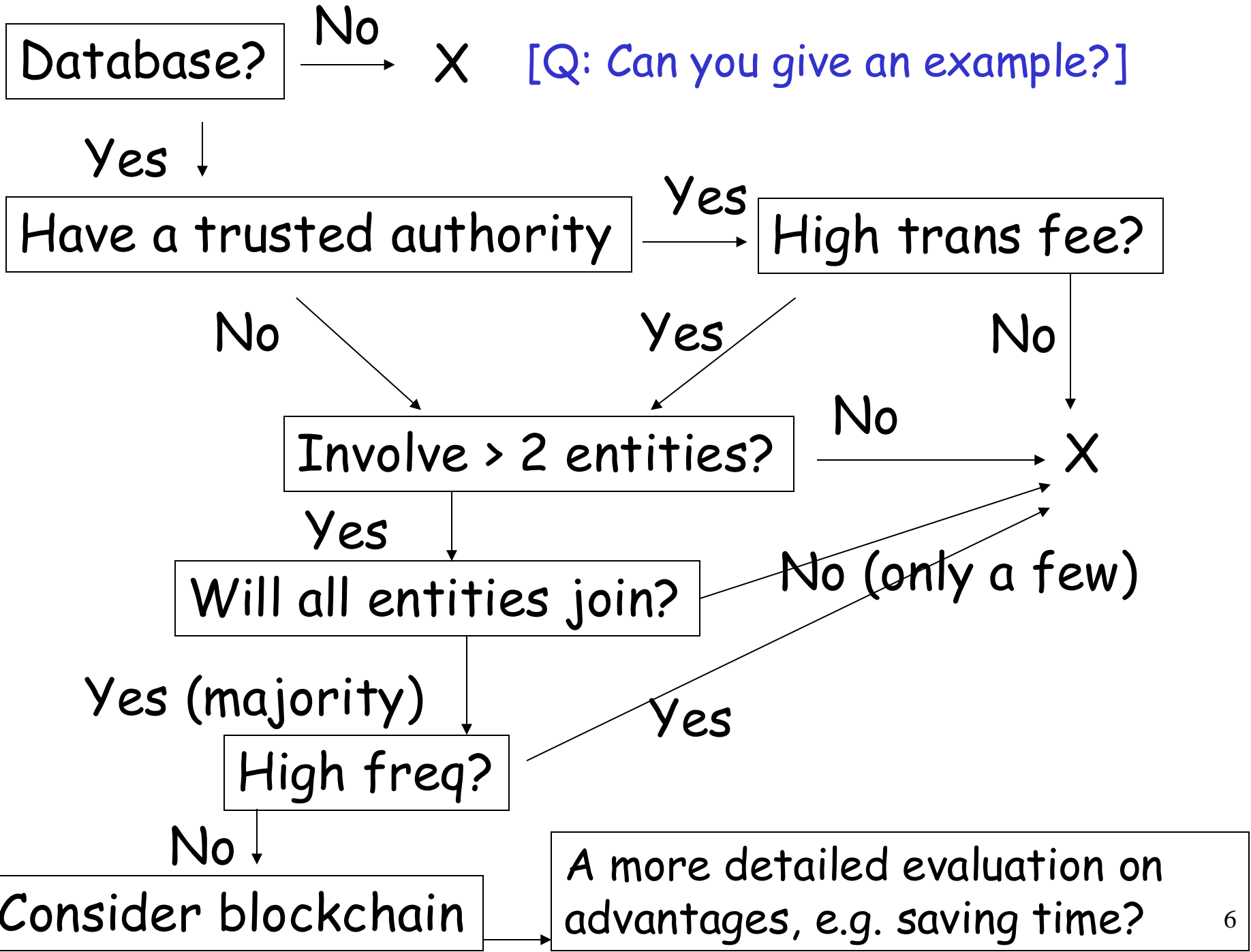
- **Trust issue** (need to trust it)
- **High transaction fees**
- **No privacy** (the centralized party has full authority to read all personal information, transaction information of the customers)
- **Processing time for the transaction** (it depends on the centralized party how fast they can complete the transaction).

Remarks:

(i) Intuitively, a blockchain system is "slower".

(ii) If there is a trusted party (e.g. the Government), transaction fee is low, don't concern about the privacy, processing time is reasonable, then why go for blockchain?

=> **Not all applications fit**



Some example applications fit well in blockchain

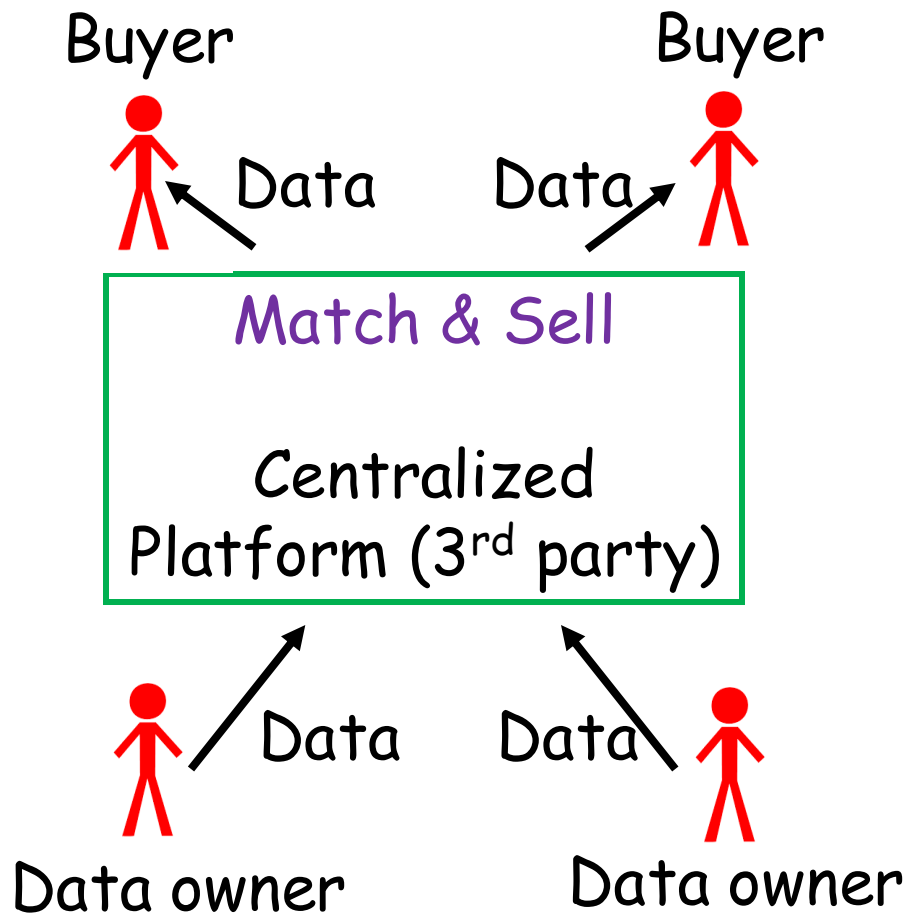
e.g.1 Applications that emphasize “**chain of custody**” (e.g. Medicine, food, wine). <Once certified, no more change>

e.g. 2 Applications involving **Tedious** (maybe even **repeated validation**) **procedures**
(e.g. Show your graduation certificates for job hunting, further study; show your identity, address proofs for opening a bank account)

e.g. 3 Applications involving **Multiple suppliers and multiple buyers** (many to many relationship) (e.g. data trading, common market place)
[Note: can be used for the problem of “financial inclusion”]

Example: The Global Big Data Exchange in Guiyang (贵阳)

It is a data trading platforms



These platform(s) making a
lot of \$\$\$\$\$

Issues:**

- (i) **Service charge is high** (up to 40% of data price);
- (ii) **Security & privacy** issues;
- (iii) **Not easy to sell various statistics** (must be provided by the data owner)

** Information obtained a few years ago, the system is evolving over the years!

Another example: How about this?



Dr Yiu is looking for a girl friend,
but he is too busy, so turn to
“love matching service”

Existing scenarios

e.g.

The screenshot shows the 'China Love' website registration page. At the top, it says 'China Love' with the Chinese characters '中国爱情' below it. Below that is a slogan in Chinese: '在亚洲大陆追寻幸福！牵起缘分的手！步入幸福的门！'. The registration form consists of four input fields: '姓名或昵称' (Name or Nickname), '真实邮箱' (Real Email), '密码' (Password), and a '试试运气' (Try Luck) button at the bottom.




For **EACH** company

- Register
- Pay membership fee
- Provide preferred characteristics of girl friend (e.g. long hair....)

=> Candidates returned by each company
may not be good!

Others: expensive, privacy,

Ex: What typical applications fit blockchain?

- (i) The application only involve 1 or 2 companies/entities. 
 - (ii) All entities/companies involved in the application trust a single authority and are willing to pay for the service charge. 
 - (iii) Applications require high frequency transactions. 
-

(a) Multiple parties, no trusted centralized authority, high service charges 

(b) With documents required repeated validation (or time-consuming) or tracing the origins is important 

E.g. Food (medicine, wine) chain, credit history, mortgage checking etc.

Key: Every stakeholder is willing to join the blockchain system!

Q: How's your **first tutorial**?

Do let me know:

- Do you think the tutorial is useful?
- Do you think the TA is helpful in motivating you for the investigation and discussion?
- Do you like the way the tutorial is conducted?

Another Short Review:

- Still remember what technologies behind FinTech?

Blockchain, Big data analytics, AI, cyber security, RegTech, and e-payment

- You all know what blockchain technology and its characteristics, right?

Public-privacy key pair, digital signature, hash
[Decentralized, immutability, transparency...]

And you know how to guarantee these properties by the technologies and protocols, right? E.g. Consensus algorithms (e.g. PoW)

- What applications best fit blockchain?

Check the flowchart (there are others in the Internet too)....

Bitcoin is not the only blockchain platform/network now. There are many, say Hyperledger, Ethereum, Ripper, Corda etc.

Roughly speaking, one approach to classify a blockchain is as follow:

Is it a "public" chain or not?

Public or not

Original design

- Public (or a fancy term: **permissionless**)
- Everybody can join without verifying your identity)
- E.g. Bitcoin.

Big enterprises:

- Only **trusted parties/parties with certain identity can join** (why?)
 - Or even can control who can see what (**access control**)
- Higher scalability/transaction speed

⇒ **Permissioned blockchain**

- Only entities who pass a verification process can join
- Not "fully decentralized".

Another extreme: **private** (owner controls everything)

Limitations: Blockchain Trilemma

- Coined by Ethereum founder Vitalik Buterin, the blockchain trilemma states that at a fundamental level, blockchains cannot achieve all three properties simultaneously
 - Decentralization, Security (or consistency?) & privacy and Scalability
- This is based on observation, not formally proven?

e.g. handle large volume of transactions with high transaction rate?

E.g. Bitcoin/Ethereum:

- fully decentralized, consistency, but NOT provide 100% privacy, is NOT scalable.

E.g. Hyperledger:

- NOT fully decentralized, consistency, privacy?, more scalable (still cannot handle very fast transaction rate).

Public resting area (permissionless)

Vs

Bedroom in your apartment (private)

Vs

Waiting room in an office building (permissioned)



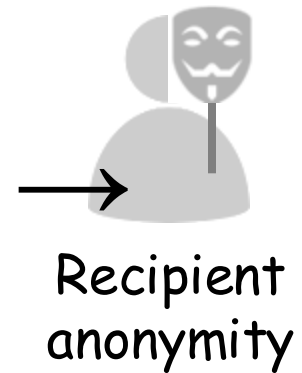
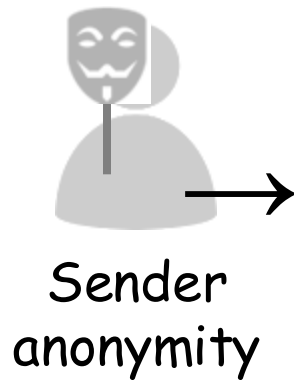
As more applications require blockchain technology, there can be many variations of blockchains

Other limitations:

E.g. 100% secure? 100% privacy?

Recall: transparency (why we need it?), is this property good or not?

3 Types of Privacy:



Use bitcoin as an example

- User generates public/private key pairs.
- Public key used as account address (also called **pseudonyms**).
- Applies to both sender and recipient => **sender and recipient anonymity guaranteed to a certain extend.**

Q: can you provide some examples that are good for having "transparency"?

Of course,

Bad for sensitive information

E.g. Account balance, transaction details between two entities.

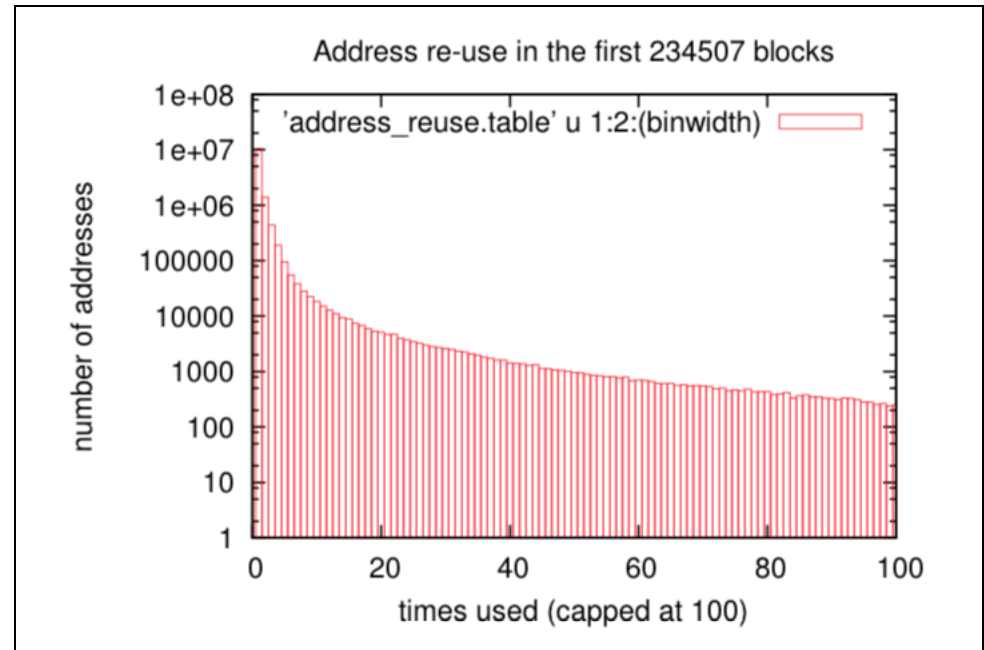
Q: Is it true that the identity of an account is 100% protected by using public key as the account address?

Depends: how information can be leaked? E.g., if the user uses bitcoin to purchase real stuff, e.g. pizza

Original design of bitcoin: Recommended NOT to reuse address!

TABLE I
ADDRESS REUSE STATISTICS

Mean	3.18
Min	1
25th perc.	1
50th perc.	1
75th perc.	1
Max	1,238,931
Number of addresses	12,963,199
Number of uses	41,244,997
Addresses used once	10,476,899
Addresses used twice	1,397,373
Used over 100 times	25,004



Jaume Barelo, "User privacy in the public bitcoin blockchain", 2007

Access control

In the original design (i.e., the bitcoin network), all users (even you are not a miner) can access to all transaction details!

Q: Is it good for all applications? Can you give an example?

More recent blockchain platforms try to solve this problem:

- (i) Provide an access control (how?)
- (ii) Encrypt the transaction details

But then how miners verify a transaction?

Big data or advanced applications with high computational requirements?

In the original design (i.e., the bitcoin network), transactions are simple, e.g. A gives 10 bitcoins to B, but nowadays, developers want to use blockchain for big data applications.

New design combining other platforms are needed!

In the original design, the blockchain system is not supposed to be used for intensive computations, such as data mining, online temperature control etc.

Researchers are working on this and other limitations such as scalability!

Assessments:

- Tutorial participation: 10%
- Assignment (1, group): 20%
- Essay/Report writing (1, individual): 30%
- Group Project: 40%

MC Quiz on lecture materials among 50%

Assignment 1 will be out today

Due date: 26 Feb 2025, Wed, 11:59pm

- can form groups (3-5 students, even NOT in the same tutorial group)
- pick any two blockchain platforms and compare their differences (50%)
- provide an example application that only fits one of the platform and explain why this application fits only that particular blockchain platform but not the other one (40%)
- references (10%)

Group Project

1. Forming a group:

- Form your own team (group) with **3-5 members**
- **To be in the same tutorial group** (otherwise, difficult to find a common time slot for presentation)

2. Topic of the project:

- Each group can pick a topic of members' own choices.
- **The topic should be related**
 - ❖ **FinTech** (i.e., make use of FinTech technologies)
 - ❖ **To solve a problem of the limitation of certain traditional finance services**
- Please submit your group members to TAs by **26 Feb (Wed) 23:59pm**

Some example topics:

- A FinTech application to help underbanked customers
- An innovative approach for risk assessment for start-up to borrow loans from banks
- A study of the limitations of traditional banking services
- Differences between a virtual bank and a traditional bank and how FinTech can play a role
- A new FinTech application for xxxx
- How computing technologies can be useful in RegTech?
- How FinTech can enable Defi?
- Issues in different e-payment systems
- A study on eCNY
- Is gender an issue in financial services and how FinTech can help?

.....

What you need to do:

1. Each group will do a **presentation in the last two/three sessions of the tutorial** (more details will be given later).
 - Basically, you need to talk about **why you want to study this problem?** What are **the limitations of traditional financial services** or why this cannot be done before? **How FinTech can help** etc.
 - Not necessary to have a prototype
2. Each group should **submit a report with at most 5 pages** excluding the list of references that describe the above points in details.
- 3 We will ask members to **self-evaluate the % of contributions of other members** (will be kept confidential)

Conclusions

★ Blockchain is good for a lot of applications, **but NOT ALL applications**

=> Always ask yourself the question: "Whether blockchain is the most appropriate platform to be used for this application/system?"

★ Blockchain technology does have limitations, **pay attention to these limitations if you want to use blockchain for a particular application** (e.g. containing trade secrets, personal information) and **pick the right platform!**

Lecture on 19 Feb

Guest speaker:



Mr. Handy BONG

- Our technical engineer
- 13+ years of experience in IT
- Extensive experience in ICO, blockchain related projects

He is the manager for our joint project with Cyberport on using blockchain to manage certificates of candidates

Title and abstract
To be confirmed