Blockchain and Smart Contract Exam **107356003 廖信堯**

Q1. If the Taiwan government would like to build its own "blockchain-based digital currency (crypto-currency)", what hardware and software it should be deployed? How many full nodes should be deployed by the government and how do you estimate this number?

As professor mentioned formerly, a currency is a unit of storage and a means of exchange. A cryptocurrency is mostly defined as a digital currency relying on encryption to generate new units and confirm the transactions. It has all the functions of the currency except for a single centralized platform. However, compared with coins or banknotes, blockchain-based digital currency has some advantages, like better security mechanism, lower fraud risks and lower operating cost.

If Taiwan government wants to build its own crypto-currency, it has to choose a blockchain platform to set up the whole infrastructure. According to the latest list of popular blockchain platform, I guess Ethereum has the biggest probability to be chosen as the basic platform. After choosing the platform, government has to design the nodes. For example, the level of permissions: private, public, or hybrid? Picking a base operating system (like Windows, Mac or Ubuntu) And, selecting necessary hardware details, such as processors, memory, disk size, etc. According to an article on internet[1], the run a full validated Ethereum node, it requires:

- A SSD able to perform: 68 MB/s of random writes and 30.9 MB/s of randoms reads on average. +112GB of capacity.

[1] http://bit.ly/2wn0Jlj

- 15 GB RAM
- A CPU able to handle a lot of interrupts

With the above hardware, the block synced per minute average of 340.2 and the synced rate is 4.29. However, related to the node design, how many full nodes should be deployed by the government? My naïve concept is to compare the circulating volume of New Taiwan Dollar and Bitcoin and then approximate the possible nodes necessary by dividing the circulation volume by number of full nodes which are calculated by the BitNodes. So, here is my calculating process:

	Circulating Volume	exchange rate(USD/TWD)	# of full nodes	adjustment	NTD/Nodes
Bitcoin	1.39654E+11	31	9420	9891	437698312
NTD	2.28571E+12		5222		

Resource:
https://www.coinbase.com/price/bitcoin
https://www.cbc.gov.tw/ct.asp?xItem=85035&ctNode=410&mp=1
https://bitnodes.earn.com/nodes/

About the adjustment column, due to the “protection” of China’s internet Great wall, the number of nodes there might be underestimated. So, I multiplied the number of full nodes to a number to estimate the real situation.

For the software part, taking care of APIs. According to the service the crypto-currency contains, government has to check whether these functions are supported by the pre-built APIs by the chosen blockchain platform. Otherwise, government has to rely on blockchain API providers. Besides of APIs, Communication is the key and a well-thought-out interface ensures a smooth communication between your blockchain and its participants. There are things to think about: Web, mail and FTP servers, external databases and the front end and programming languages (e.g. HTML5, PHP, C#, Java, Javascript, Python, etc.).

Q2. State your opinion of building crypto-currency by the government.

In my opinion, I am not optimistic about building crypto-currency by the government, especially in Taiwan. Taiwan is a country which has over 50% transactions are paid by cash. Even at 2012, when credit cards are easily applied, most people were used to pay by cash. Although, now, many mobile payments, like Line Pay, Apple Pay, are taking some market shares of payments, most people still use cash as their primary tool and many merchants are not accepted credit cards or digital payments. I think the context behind their behaviors is complicated, but I will discuss why I think it's not applicable in Taiwan.

First of all, government's crypto-currency creates the shifts of power. When customers and merchants are willing to pay and accept crypto-currency, withdrawals will be transferred to government's blockchain, which causes the decrease of lending power in commercial banks. And, this will lead to the resistance of banks. Some of them might buy advertisements, issue news or any other means to smear the vulnerability of crypto-currency, which has great impact on the confidence of customers and merchants who are wondering to use it or not, especially blockchain is still a techy term for the whole society.

Secondly, tax is another big issue. We knew that some merchants or companies used some tricks to avoid heavy tax. Under the mechanism of blockchain, each transaction will be recorded and thus no merchants can deny to pay tax. For those who follow the rule of regulation, the implementation of crypto-currency can improve the efficiency of payments and of tax filing. Not to mentioned that the reduction of transaction fee will largely increase profits of firms. On the other hand, for those who are not included in the tax mechanism, this implementation will cost them a lot with the little improvement of their business process. And, the latter forms the backbone of people' living. Therefore, unless the mechanism can provide enough subsidies, I don't think most of them will be willing to join

the mechanism. Without them, customers have less motivation to join either.

Q3. Overstock (https://www.overstock.com/) is one of the e-commerce websites that accepts bitcoin. What are the pros and cons of using bitcoin in e-commerce?

From the perspective of running e-commerce store, more payment options for your customers mean increased conversions and sales, but you would worry about the increase risk of fraudulent payments. Large firms have the budget to take risks, but others must take more factors into consideration. In the case of Overstock, here are some pros and cons about using bitcoin in e-commerce.

For pros, avoiding fraud is one of the advantages of using bitcoin. Chargebacks are a serious factor of providing payment method. It not only causes more fees and administrative problems for merchants, but also affects the reliability of merchant at bank. Thanks to the irreversibility of bitcoin, payments are a one-way only transaction, which makes chargebacks impossible. This shifts the risk taker from the merchants to the customers. Secondly, transaction fee is another important factor. Without blockchain, for example, customers may pay by credit cards or PayPal. Both of them charges merchant 2 to 3 % transaction fee per transaction. These can add up, reducing the profits earned through transaction. Thirdly, supply chain management is correlated to the life or death of e-commerce. Through the monetary flow of traditional banks, merchants have to wait for a week or more to get the money, not to mention the chargebacks. But, accepting bitcoin increase the ability of merchants to get account receivable faster, which makes merchants have more monetary resource to run the business.

For cons, price volatility is the major concern of people buying cryptocurrencies. The bitcoin market is very volatile and its value could fluctuate drastically by hours. This makes

holding funds in bitcoin comparably risky. Besides, the volatile condition has adverse impact on consumers. Deflation may occur when consumers know that this currency is pretty unstable. Additionally, getting set up of accepting bitcoin may cost a lot, depending on merchants' decision. When they choose to build their own wallet directly, it takes lots of efforts to set it up but it provides the best margin for merchants. On the other hand, they can choose third-party providers to fulfill their requirements. And, thirdly, poor security is another issue. If merchants' wallets are hacked, their profits, which is bitcoins, will be lost. Although merchants can overcome this issue by using well-known payment processor, no one can guarantee that hackers will invade one day.

Q4. Please take a look at Wiki's "Bitcoin scalability problem" and provide some possible solutions to increase the number of transactions that bitcoin can handle per second.

As we know, Bitcoin uses blocks to process transactions. In its infrastructure, the maximal block size is limited to only one megabyte. This mechanism makes Bitcoin more secure, but it also set constraint on the capability of processing multiple transaction at once within a 1MB block. On average, Bitcoin process about 7 transactions per second, which is slow compared to Visa (24,000 transactions per second).

Most people in the crypto world agree to this scalability problem so there' re lots of solutions came up. At first, increasing the block size to 2MB, 4MB or even 32MB was discussed by developers, miners and other related stakeholders. For instance, Bitcoin Cash (BCH), in May 2018, quadrupled its block size to 32MB. However, it led to increasing cost to operating full nodes, which could cause less decentralized in network. On the other hand, supporters of BCH said its enhanced block size is one of the reasons why

BCH is superior to Bitcoins, which led to the hard fork in Bitcoin network in August 2017.

However, except for leasing block size limit, Bitcoin's developer community has come up with two possible solutions: SegWit and Lightning Network. Let's talk about SegWit first. Segregated Witness (SegWit), which is proposed in December 2015, works by separating signature and transactional data, which reduce the spaces needed by each transaction and create more room in any given block. SegWit doesn't increase the block size, but it does increase the amount of possible transaction.

After SegWit, Lightning Network is another solution to the scalability problem. Lightning Network is a secondary layer which operates on top of a blockchain. It is a protocol that enables transactions to be processed off chain and the end outcome added to the blockchain later. For example, Peter and John want to send money to each other frequently, so they set up a channel on the Lightning Network. In the case, they have to create a multisignature wallet, which both of them can access with their own private keys then they deposit a certain amount of Bitcoin into it. By doing that, they can do unlimited transactions between two of them, which is the redistributions of funds in shared wallet by signing updated balance sheet with both of private keys. And, the actual distribution of funds happens when the channel gets closed. Only after the channel is closed, the information about the shared wallet's initial and final balance is broadcasted to Bitcoin network. Therefore, Lightning Network enables processing numerous transactions outside of main chain and then added them as a single record.

Q5. What is "Security Token Offering"? What is the difference between "STO" and "ICO"? (You have to explain why STO is NOT a regulated ICO.) How do we enforce the STO issuer to fulfill some regulation or law? What is the problem of STO?

Before talking about security token offering (STO), what is security token? **Security tokens** are cryptographic tokens that represent financial asset, which is security, such as stocks, options, bonds and etc. Holding security tokens means having a way to own a part of a company without actually taking possession of it. Then, what is STO? STO means that governments and companies can utilize security tokens to raise money for investors through STO based crowd sales. With security tokens, STO investors can gain dividends paid on a predefined date in the form of tokens via smart contract.

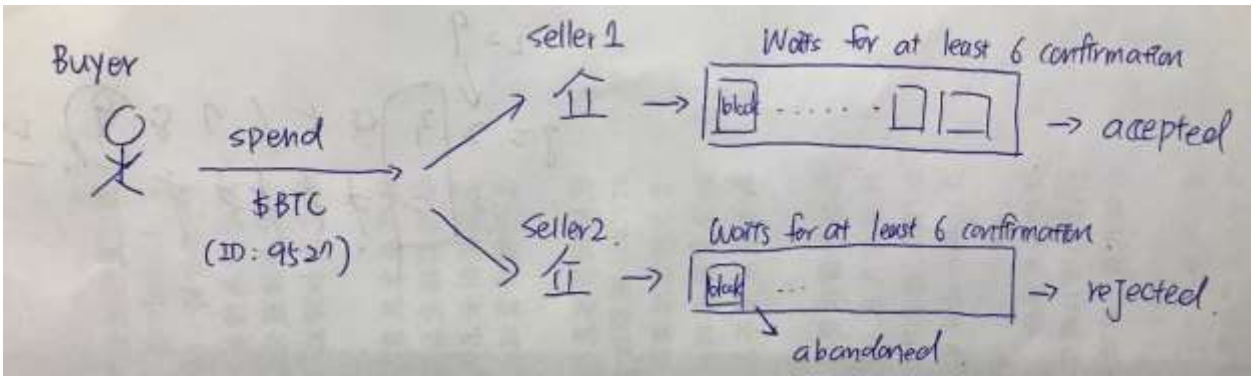
It sounds like ICO, then **what's the difference between them**? First and the most important, **most ICO raised funds in an unregulated environment**. Most ICO actually take their offering as utility tokens to circumvent regulations, which is different to STO's security tokens. Utility tokens represent future access to a company's product or service, which is different to the definition of security by the SEC laws. Such line of reasoning lets ICO projects to avoid regulations with SEC or other regulators. On the other hand, STO must either be registered with the SEC and other laws or qualify for an exemption. They are registered with required government bodies, meet all the legal requirements and are 100% lawful, just like any other security investing tools. And, STO is bundled with actual assets while ICO is relied on utility tokens, with no collateral and is not protected by securities law. Besides, **the entry barrier for buys and sellers are un-identical**. In ICO, theoretically, anyone can launch and participant in an ICO, but only regulatory companies or known investors can sell and buy security token. Due to these differences mentioned above, ICO and STO are fundamentally different although both of them follow similar process. Even ICO is regulated by laws, their tokens mean different rights: ICO's tokens mean right to access future service or product but STO's tokens mean ownerships to company with fractionalized dividends.

However, how STO enforces the surveillance mechanism? Of course, since blockchian is new, there's no specific law exist for STO, but the applicable legal requirements can be categorized in four different areas: Securities Laws, KYC/AML, corporate law and Contracting. To guarantee the compliance of STO, many restrictions in transferability of tokens have to be in place and such **restrictions can be programmed into smart contract of the tokens themselves**, which largely increases efficiencies across capital markets.

STO seems prefect but it still has some obstacles along the way. **The level of liquidity in STO** is an acute problem. Restriction of the entry of STO, there is only a small number of licensed platforms that allow to STO trading. Compared with other traditional securities, the level of liquidity in STO is still in low. Although there may be some debates about liquidity, it is a problem that has to be clarified in the future. Besides, **the attitude of regulators is important**. Their approval of new schema of fund-raising has great impact on the future widespread adoption of STO. It may be too early to say whether STO will revolutionize the fund-raising area. But, STO is an attractive tool for businesses that cannot afford the costs of traditional private placement of securities. Therefore, STO has the potential to change the future landscape of fund-raising area, but it still has a long way to go.

Q6. Why bitcoin can prevent "double spending attack"? (You may draw a picture to explain your answer.)

Before answering how bitcoin prevent double spent attack, I want to explain what is double spent. Double spending means spending the same digital currency twice. Since bitcoin is digital currency, its transactions have a possibility of being rebroadcasted and being spent twice by its owner. However, bitcoin solves the double spending problem by implementing confirmation mechanism and building a universal ledger which is also called blockchain.



From the figure above, suppose that a buyer spends the same BTC (ID:9527) to 2 sellers sequentially. Both transactions would enter the unconfirmed transaction pool, but only the first one would get enough confirmations and be verified by miners. The other would not get enough confirmations because miners took is as invalid transaction. On the other hand, how about sending the two transactions simultaneously? Well, it depends on which transaction gets more confirmations. Although this is kind of unfair, that's why developers recommend merchants to wait for at least 6 confirmations to avoid transaction failure. Frankly speaking, confirmations are nothing but more blocks being added to the ledger. Each transaction and blocks are mathematically related to the previous one due to the hash mechanism. The irreversibility of blockchain make sure that waiting for 6 confirmations, merchants can be positive that the bitcoin is not double spent by buyer.

In double spending attack, there are, theoretically, two possibilities. The first possibility is attack 51%. It means that an attacker gains 51% or more of the computational power of the network. If an attack has this level of power, he or she can reverse any transaction and make other miners consider that these faked blocks are valid. As far, there is no such attack because it's only theoretically feasible. Controlling 51% computational power is related to many aspects, including mining difficulty, cost of hardware and electricity cost. To acquire one of them is nearly impossible, not to mention acquiring all of them to evoke initiate attack 51%.

The other possibility is race attack. Remember that I have mentioned that merchants should wait at least 6 confirmations. So, if an attacker sends the same coin to the address of merchant and his or her address, there's 50% chance that merchant got the double spent coin which equals to nothing. And the attacker can use the mechanism vulnerability to spend the same coin repeatedly. However, the confirmation mechanism suggests that merchants should wait at least six confirmations. If the transaction, which transferred the same coin to the address of attacker, gets six confirmations first, the real transaction will be discarded but merchants won't have any loss since he or she follow the suggestion of 6 confirmations.

Q7. There will be a "blockchain phone". Please make a comment on the blockchain phone (e.g., pros, cons, difference between it and Apple Pay.)

As far, there are few blockchain on the market: Finney, HTC Exodus 1 and Samsung Galaxy S10. These blockchain phones are similar in both hardware and software, but, depending on the strategy of different companies, these phones are embedded with different blockchain service. From the article on Bloomberg, we knew that Finney is

designed to help owners securely store and use digital coins without knowing the mechanism of blockchain. Among the competition against digital wallets and USB sticks, Finney tries to bring the cryptocurrency to the ordinary world.

In my opinion, blockchain phone, for public, is a gate way to mysterious blockchian world. It mitigates the technical entry gap for beginners to start using services provided by blockchain. Starting with cryptographic key management, instead of complicated address and keys, security will be protected via fingerprint scans or traditional passwords, which provides better user experience. Besides, Finney has its own dapps store which includes decentralized applications that look and feel like the mobiles apps we people used today. It integrates all kinds of tokens, allows converting cash into specialized tokens, and serves as a payments tool.

However, the security design seems to pose an unexpected risk on users. Since the security controlling is switched from virtual address and key to biometric or password, it is unable to prevent rubbery or thieves. Additionally, these phones just keep your keys safe, which is able to be done by some third party digital wallet as well. And the decentralized web, or the dapps future, is still mostly a dream. Its foundational infrastructure is still under construction and there is no killer dapps on the market so far.

Compared with Apple Pay, blockchain phones utilize the mechanism of blockchain to reduce transaction fee and increase transaction efficiency. Well, on the other hand, Apple Pay relied on the traditional mechanism of commercial banks, but it utilizes tokenization to erase the sensitive transaction information, which lower the possibility of fraudulent. From my perspective, both using mobile phones as the channel to touch with potential users, but they build their framework or mechanism on different technology. As an end user, I cannot see any big difference between blockchain phone and Apple Pay.

Q8. Do you care about who actually execute your smart contract? Why or why not?

In my opinion, I think who actually execute my smart contract matters. I know, considering the properties of blockchain, it's kind of contradictory to the anonymity. I will explain my view about the issue as follow. To begin with, smart contract is a protocol built on blockchain, which digitally facilitate, verify or enforce the contract. Smart contract has the properties of autonomy, decentralization and auto sufficiency, which sounds prefect because people can not only enjoy the services provided by decentralized application but also protect the privacy of sensitive and personal information. However, it leads to other potential questions.

First, some illegal activities are compatible with the context of smart contract. So far, there are some concerns that Bitcoins are widespread on "Darknet". Someone utilized the intractability of Bitcoin to make transactions with some secret companies to make some illegal deals. Now, rethinking about the properties of smart contract, it seems like the issue is bigger. For instance, I could design a contract which is not different from other contracts, but the contract is actually fulfilled the needs of money laundering, ransom payments or other illegal task payments. Based on the mechanism of consensus, miners don't care about what actually the contract do, and both initiator and beneficiaries are anonymous. Except for the appearance of appropriate regulation on blockchain, I am pessimistic about the prevention of illegal usage of smart contract. That's why I think who actually execute my smart contract is important.

Secondly, from the viewpoint of service provider, users' opinions and users' experience are significant for the improvement of service. For example, I am the owner of a smart contract which provides online gambling service. Of course, the service is

designed for all country's citizens, but casinos could collect information and know the majority citizenship of its gamblers. However, on blockchain, without the information of who requests service, it's difficult to know who are your primary users, how to profile them, how to improve your services and the most important how to formulate your company's developing strategies. Although decentralized application can have the same rating mechanism on Google Play or Apple Store, I think the customer relationship management is important in decentralized application as well. Therefore, the illegal usages and the lacking of customer relationship management of smart contract make me feel that knowing the executors of your smart contracts is necessary.