Blockchain Opens New Era in Securities Settlement

Zhu Qingyu (Student ID: 3035419080)

October 4, 2017

Abstract

In this paper, we discuss a new settlement process based on blockchain technology. The current settlement and blockchain settlement are compared and contrast. Some technical, security and regulation considerations about the new settlement solution are also investigated. Furthermore, we answer the question why do not immediately use blockchain-based settlement process in three aspects.

We finally conclude that the blockchain-based settlement journey is likely to be long and the outcome is uncertain, but it is really a new era in financial markets history.

Contents

1 Compare & Contrast Blockchain-based Settlement & Current Settlement

In this section, the current securities settlement process and the blockchain-based settlement process are introduced from two aspects: working principles and involved parties. Then similarities and differences between the two processes will be investigated and summarized.

1.1 Working principle

To clearly present the working principles of traditional and blockchain-based settlements, we will discuss their definitions, timelines and detailed processes respectively.

1.1.1 Working principle of current securities settlement

***Definition*:** Current settlement process is a electronic business process which made up by several steps like matching the buy and sell instructions, delivering related contractual obligations and subsequently moving the product's ownership from one party to another, as well as transferring the related cash. In current settlement process, since netting can be used to decrease the number of settlement transactions, the central security depository (CSD) —a central custodian—is responsible for executing the steps mentioned above via book-entry systems. CSD manages a single ledger, safekeeps the holdings and updates the securities' ownership for each transaction. Hence, CSD works as a bridge between its custodian services and central banks or correspondent banks and provides a facilitation service.

***Timeline*:** Since the current settlement process involves many manual procedures like informing custodians one by one, drafting contracts again and again, transferring material from here to there, it usually takes two or more days after trading day. In most current markets, the settlement date for securities is denoted as T+2, where T stands for the trade day.

***Detailed process*:** In this subsection, a whole settlement process in current market will be described in detailed with a flow-process diagram. Let's take delivery free-of-payment (DFP) for example. Here a full story can be hinted from Figure 1: if participant A wants to sell some Microsoft's shares via DFP, here's what goes on:

1. Participant A advises corresponding bank A to sell 100 shares of Microsoft to bank B at a price of \$100 (\$10,000 in proceeds);

2. If handy shares in bank A are big enough to execute the instruction as well as the depot and trading are all not blocked, the transfer would be valid and bank A would prepare to sell shares on behalf of participant A;

3. When the bank A executes the instruction, a central depository institution (i.e. CSD) would inform the receiver. Here, a central matching system is used to arrange delivery and receipt;

4. On the other hand, bank B receives instruction of receivables from CSD;

5. Bank B confirms the instruction via the delivery matching system of the CSD;

6. Then, the delivery instruction is executed by the CSD, shifting the ownership of shares from seller to buyer. Shares are debited from CSD 's bank A account and credited to CSD's bank B's account for $10,000 in par. Because the securities are delivered via DFP. the corresponding payment are transferred by a separate cash wire to the seller.

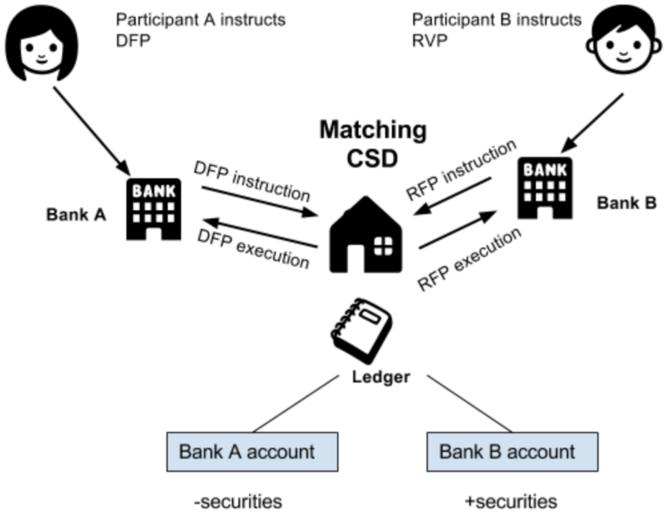

Figure 1: Detailed process of DFP in current settlement

In this story, depot and depository reconciliations would happen in regular intervals: bank A and bank B has to send a full corresponding account listing to participant A and participant B, separately; similarly, bank A and bank B also has to accomplish a reconciliation of the holdings with the CSD.

1.1.2 Working principle of blockchain-based settlement

***Definition*:** Shai(2017) defines that, "a blockchain is a secure public ledger of digital financial transactions". Blockchain-based settlement is a peer to peer (P2P), distributed, duplicated and cryptographically secure process. In that settlement system, the major purpose would be to cancel the central counterparty. In terms of technology, this system is a decentralized database system where each participant has access to the integrated database. In this database, blocks are created from a series of records and individual block is linked to the previous block using the previous block's hash value. We can see from Figure 2, that the blockchain records transactions without files and documents.

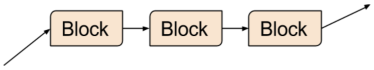

Figure 2: Blockchain

***Timeline*:** Different from the traditional settlement, blockchain technology can promote the settlement process from overnight batch processing to intra-day settlement. That's because without third-party authentication, blockchain-based settlement system can automatically process and complete transactions using computer programs.

***Detailed Process*:** In this subsection, a whole process flow of a blockchain-based settlement process will be presented. Here, we also take DFP as an example. See Figure 3[1] illustrates a real time scenario of how trades are settled on the Stock Exchange of Hong Kong (SEHK).

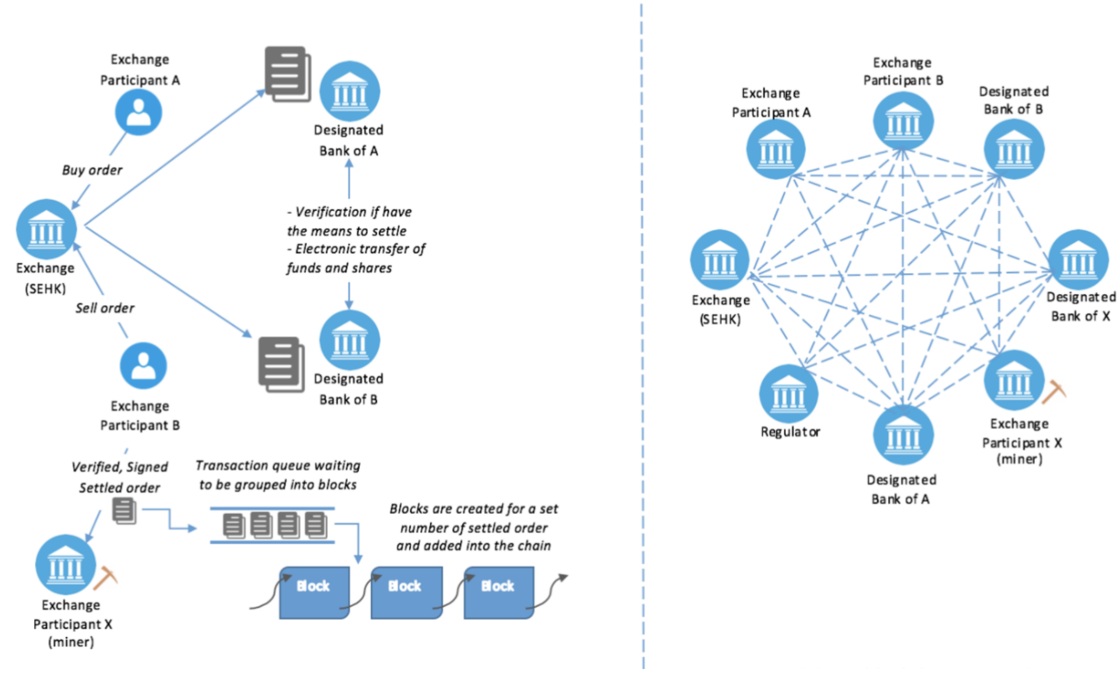
Exchange Participant A
Designated Bank of A
Buy order
- Verification if have the means to settle
- Electronic transfer of funds and shares
Exchange (SEHK)
Sell order
Exchange Participant B
Designated Bank of B
Verified, Signed Settled order
Transaction queue waiting to be grouped into blocks
Blocks are created for a set number of settled order and added into the chain
Block
Block
Block
Exchange Participant X (miner)
Exchange Participant A
Exchange Participant B
Designated Bank of B
Exchange (SEHK)
Designated Bank of X
Regulator
Designated Bank of A
Exchange Participant X (miner)

Figure 3: Detailed process of DFP in blockchain-based settlement

The completed settlement processes can be outlined step-by-step as following:

1. Participant A executes an order in the form of a smart contract to sell 100 shares of Microsoft;
2. SEHK matches this order with participant B who wants to buy 100 shares of Microsoft company;
3. Upon the trade is executed, SEHK broadcasts these two smart contracts on the blockchain system. In order to authenticate the trade, each contract is signed by SEHK, using SEHK's private key and encrypted by the bank's own public key[2];
4. Bank A (the corresponding bank of participant A) then can verify whether participant A have enough shares to implement the trade. In case bank A and bank B (the corresponding bank of participant B) confirm the two contracts are verified. Then settlement is executed with the transfer of shares ownership;

[1] Picture from: https://www.linkedin.com/pulse/blockchain-settlement-hong-kong-equity-markets-haroon-shahid-bashir

[2] "Only the designated banks in the chain would be able to decrypt the contract by using their own private key. Furthermore, from the digital signature they can also determine if the contract is valid by decrypting it from the Exchange's public key," suggested by Haroon(2016)

5. The two valid smart contracts are broadcast on the blockchain system encrypted by participant A and B public key;

6. Once A and B decipher and accept the valid transaction, they collectively sign this trade and put the trade on a queue of signed valid transactions that is managed by the data miners[3] in the blockchain system. The transaction recorded with a timestamp.

7. Once the new transaction is added on the block it is broadcast to all the nodes in the system. Then the ledger on each node is updated respectively.

In summary, a blockchain-based settlement process has a lot of advantages, for example: 1) reduce total cost of total process without third-parties; 2) settle transactions faster with smart contracts; 3) increase transparency and immutability in transaction record keeping; 4) improve system resilience through distributed data management.

1.2 Involved participants

Based on the content discussed above, it can already be implied at this section that various types of market participants perform core functions in the two different processes.

1.2.1 Involve parties in current settlement process

The current settlement system would have the following major participants:

- Central custodian (i.e. CSD)
- Exchange (i.e. SEHK)
- Central counterparties (i.e. CCP clearing)—in DVP, CCP clearing is responsible for transferring associated payment of securities.
- Banks (i.e. bank A and B)
- Clients (i.e. participant A and B)

As we can see from the Figure 4[4], their responsibilities can be described as following steps:

1. Participant A's shares recorded in the account of related broker A, who works as a custodian for safekeeping;

2. The broker A executes a sale at the SEHK;

3. The clearing house establishes everybody's respective liabilities, steps in as central counterparty and orchestrates the settlement process;

4. The buyer's and seller's custodians exchange shares for cash ("Delivery versus Payment"), using the CSD since shares need to move between custodians as a result.

[3] Haroon(2016) explains that: "The data miner responsibility is to maintain the pool of incoming verified transactions, create blocks of a set number of transaction, calculate the block's hash value and then update the block in the distributed ledger. Once the block is added it is broadcast to all the nodes in the network to update their own respective ledgers. In processing the verified transactions, miners charge a lump sum fee from the entire network based on the number of transactions they process."

[4] Picture from: Accenture Research

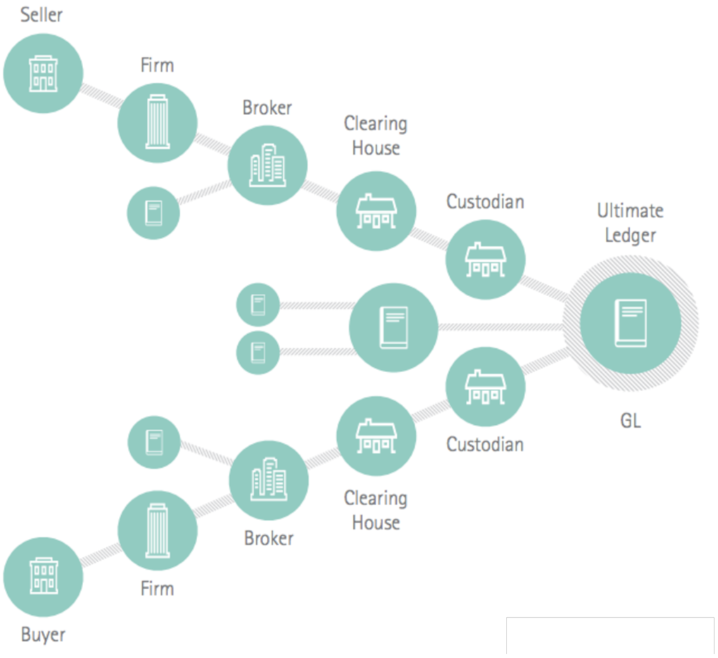

Figure 4: Structure of market participants in current settlement

In a word, current settlement process uses central authorities to settle transactions. Lots of intermediaries and lots of specialists are involved in this process, all of them there for a reason but imposing costs nonetheless. settle transactions.

1.2.2 Involve parties in blockchain-based settlement process

Some parties in the blockchain settlement process may play different roles compared to those in the current settlement process. Besides, the blockchain network may has new members:

- Central custodian (i.e. CSD)—may only acts as a gatekeeper for relevant blockchains or may be removed.
- Exchange (SEHK)
- Central counterparties (i.e. CCP))—in DVP, CCP clearing is responsible for transferring associated payment of securities.
- Banks (i.e. bank A and B)
- Brokers
- Clients (i.e. participant A and B)
- Data miner—calculates the block's hash value, creates and updates blocks in the distributed ledgers.

Accenture(2016) says that, "unlike traditional ledgers managed in CSD, distributed ledgers built on blockchains validate transactions through a protocol managed by the user community via a consensus mechanism (see Figure 5[5]).” In blockchain-based settlement process, all the participants are known and trusted. This decentralized approach changes the power distribution in the financial market, moving power from organizations to any parties. Practically speaking, this means blockchain-enabled settlement have the potential to increase trading efficiency, improve regulatory control and eliminate unnecessary intermediaries.

Beyond that, each participant in the blockchain has a list of public keys and identities of all the participants in the network. Access to this blochchain network from a new participant can only be achieved if all the current participants verify its public key.

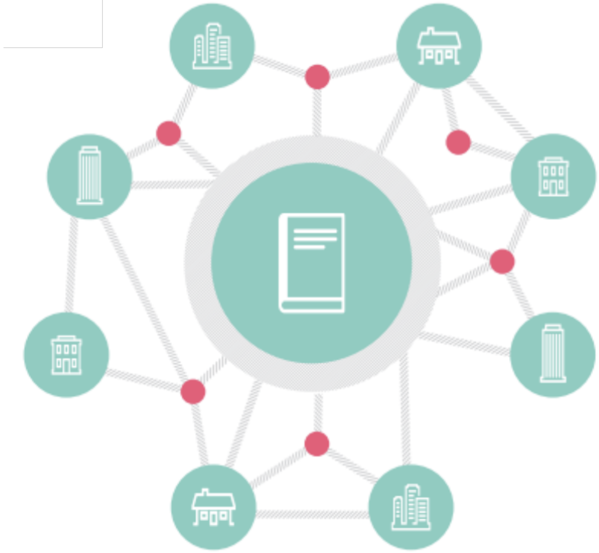

Figure 5: Structure of market participants in blockchain-based settlement

Briefly, the same parties involved in the traditional settlement and the blockchain-based settlement may take different responsibilities. And the data miner is unique to blockchain-enabled network. Furthermore, the current settlement is a centralized process while the blockchain-based settlement is decentralized. To some extent, blockchain-enabled settlement process is more reliable, transparent and efficient.

1.3 Summary of similarities & differences

In this part, similarities and differences between the current settlement process and the blockchain-based settlement process are explored and summarized.

1.3.1 Similarities

- ***Ownership of assets both can be electronically stored on ledgers.*** Assets can be represented in a variety of ways. For example, they can be recorded and traded totally within the ledgers or they can be representations of assets that exist outside the ledgers. Regardless, ownership information associated with securities can be stored on ledgers in these two different

[5] Picture from: Accenture Research

settlement processes. The ledgers maintain the ownership positions of all participants. Further more, securities in both settlement processes can be electronic form.

- ***Some risks in both settlement processes are the same.*** For example, David et.al.(2016) introduce that, "similar to traditional PCS[6] systems, one of the biggest concerns with DLT[7] solutions is endpoint security." As with any system where vulnerabilities can possibly occur within both software and hardware components, blockchain-based settlement system may confront increased exposure to cyber-attacks through its distributed endpoints, which are validating transactions. So far, endpoint risk is an increase problem for which no easy solutions may be found.

- ***These two different processes both have to face double-spend problem.*** In both blockchain-based solution and traditional settlement systems, the double-spend problem may appear, for example, identical or duplicate transaction or payment are frequently occur although only one payment or transaction can be settled. In a blockchain-based system, for example, different simultaneous orders to transfer a digital securities with the same serial number or unique identifier. Besides, a related problem can occur if a participant wants to order two valid transfers, but have no enough digital securities or funds to settle both transfers.

- ***Both have DVP and DFP methods.*** Delivery versus-payment (DVP) is a settlement method in which transfers of securities and corresponding funds occur simultaneously. In turn, delivery versus-payment (DVP) only delivers ownership of securities without a corresponding payment. The payment is transferred by a separate wire. As we can see, the principle of these two methods are the same in traditional settlement and blockchain-based settlement.

1.3.2 Differences

- ***Transfer ownership via different* methods**: In a current settlement system, the ownership transfer usually take two or more days though the transaction can be done within blink of an eye. That's because the participants have no access to others' ledgers and can't spontaneously conform those of assets are actually owned and can be transferred. In fact, there are various intermediaries work as guarantors and records of the transactions travel across organizations as well as the ledgers are independently updated. On the contrary, in a blockchain system, the transfer of securities ownership is broadcast to nodes that maintain of copies of ledgers and simultaneously accepted as the new version of the ledger. So it would be settled within microseconds without third-party intermediaries to check or shift ownership.

- ***The different role of CSDs***: Euroclear and Oliver Wyman(2016) point out that the use of blockchain in settlement will change the role of CSDs. In the existing settlement process, CSDs maintain book-entry systems where ownership of securities and other assets should be held in a centralized digitized form. Core services of CSDs typically include notary and central account maintenance services (i.e. adding transaction records) as well as oversight of the asset issuance process. However, the use of blockchain in settlement will change the role of CSDs. That means, the need for CSDs services could be more less than today. Participants, as nodes,

[6] PCS means payment, clearing, and settlement

[7] DLT means distributed ledger technology

would each hold the latest version of the ledgers, and therefore could readily provide access for its clients to account and transaction data. So CSDs , in turn, would only provide gatekeeping and oversight services of the relevant blockchain or would be removed directly.

- ***Smart contracts* vs traditional contracts:** In blockchain-based process, smart contracts also called digital contracts are computer programs used to generate and accomplish an agreed on act between two parties. But traditional contracts normally associate one or more companies, lawyers, negotiations as well as backwards and forwards drafting phases. The outcome of series processes are usually a complicated document that is signed by all related parties, assorted attachments and appendix. So the difference is that smart contracts are computer-produced and hence it is the code itself that clarifies the obligations of the parties. The smart contract aims to remove the formality and reduce cost spent by the traditional settlement chain.

2 Technical, Security & Regulatory Considerations

As illustrated in section 1, blockchain-based settlement has plenty of advantages and makes a difference to securities settlement activities. However, the financial market is at an initial stage of development regarding blockchain technology. With the financial market goes on to experiment, a variety of technical, security and regulatory challenges must be solved before blockchain solution can become a practical solution for settlement activity. This part sums up some challenges the banks and markets have to address in order to reach wide adoption of blockchain-based settlement process.

2.1 Technical considerations

2.1.1 Tracking nodes IP

Philip(2017) suggests that, “blockchain-based currencies present many legal and regulatory challenges including consumer protection mechanisms, enforcement methods and possibilities for engaging in illegal activities such as tax evasion and the sale of unlawful goods.” In the conventional settlement process, if a bank is at fault then regardless of the location, the bank can be accused by applicable jurisdictions. However, the nodes in blockchain network can be located anywhere. In that case, node IP can be a clue to identify node location. Hence, a technology used to track nodes IP address may be an important technical consideration.

2.1.2 Systems integration

The first section refers several difference between blockchain-based settlement and conventional settlement. Indeed, blockchain technology provide solutions that need significant changes to, or exhaustive replacement of current systems. In order to accomplish the switch, banks and financial companies have to put out a feasible integration strategy to integrate existing systems with blockchain system. Besides, specialized technical departments should be established to settle incompatibility issues and implement the integration project.

2.1.3 Network speed

A time cost issue of finishing a transaction settlement on the blockchain-based systems is that all the nodes in the blockchain network must come to an agreement that the transaction is authentic. It may cause that blockchain-based settlement system is far slower than current settlement system verifying transaction in an instant. On late 2016, blockchain technology can only settle around seven transactions per second. Specially, when “double-spend problem” happens, settlement may not occur instantaneously. So a technology that could be applied to blockchain-based settlement and enable instantly verified transactions is crucial in making blockchain widely applicable.

Besides, information synchronization in blockchain network would also spend plenty of time. Increasing synchronization speed for settlement process, like broadcasting transfer instructions and latest ledgers, is another network speed issue have to be addressed.

2.1.4 The expanding size of blockchain

More block, more storage. Storage usage would be an technical consideration as each node needs to store the whole history of the blockchain. It is a very tricky issue with the blockchain-based settlement system. Although the transaction size is only a few bytes, the entire blockchain size in 2016 the was 50GB and upon 2017 is up to 98GB. At the same time, U.S. current settlement systems process hundreds of millions of transactions every day. If it continues to grow at 1MB per 10 minutes, storing the complete blockchain should remain enough memory space for those that want to. It is a big issue because the health of a blockchain network is partially dependent on the amount of nodes in the network, and the spread of those nodes across the world. As the number of blockchain is continuing to boost, the storage size is a rising concern have to be solved.

2.1.5 Development handbook & APIs

A handbook introducing scientific development standards for blockchain system implementation is another critical technical consideration. Standards introduced in handbook are important as giving a base layer of interoperability across different blockchain systems, bank systems and legacy systems. If institutions ultimately connect with multiple blockchain systems, common financial market standards can also help to reduce implementation and integration funds and ensure consistent knowledge about how information in blockchain-based settlement is structured and accessed. Certainly, the industry is exploring methods of obtaining open standards. One challenge, however, is that many applications of blockchain are still being developed and tested, and the financial markets may not have plentiful information at this point to put out an appropriate standards. It is a typical emerging technical issue in the developing stage.

Besides, a strength set of APIs may help banks and other institutions to achieve operational efficiency of blokchain system without requiring striking changes to IT architecture in the short-term and reduce the hinders for IT development teams to enter the blockchain era. By the way, building public APIs by in market-standard languages and enhancing software development kits(SDKs) can promote the institutions and their IT development teams to enter the blockchain era.

2.2 Security considerations

Although solutions exist nowadays, such as private or permitted blockchains and strong encryption, there are still cyber security considerations that require to be addressed before the general public will entrust their personal data put into a blockchain-based settlement solution.

2.2.1 Cryptographic key management

How to effectively manage cryptographic keys and access credentials in blockchain network is a notably critical security concern. If keys or access credentials are lost or compromised, users would likely suffer immediate and irrevocable monetary losses without any recourse. Key compromises may generate financial losses associated with account fraud. Lost keys may hand over personal data which are indecipherable or inaccessible, leading to the irrevocable loss of the value protected by the cryptography.

Keeping private keys from being pilfered and at the same time maintaining security ownership of public key encryption is a difficult task. That's because there are many aspects should be considered, for example the robust of the cryptography and the protocols used for key generation, repository, distribution, cancellation and destruction. Addressing these challenges, many regulatory organization have settled detailed guidance for participants using cryptographic keys and designed cryptographic key administration systems. Applying the guidance to blockchain-based settlement will be an essential step for such settlement process to become feasible.

2.2.2 Data protection

Determining what data to share is another security consideration should be addressed, especially when customer individual data is open to competitors or if a buyer attempts to use the personal information for a new purpose. Corresponding privacy laws and regulations need to also be composed. By the way, participants will have to agree on the quantity of data that is shared and whether the complete set of data will still have to be assigned to a central institution, like CSD.

2.3 Regulation considerations

2.3.1 "Blockchain license"

Like drivers have driving license and enterprises possess business license, participants, banks and other parties involved in blockchain-based settlement process also have to hold the "blockchain license". The "blockchain license" can is an legal permission to using or join the blochchain-based settlement systems. This "blockchain license" can be granted by a regulatory organization. In this situation, proposing proper regulations to grant a "blockchain license" may also be a crucial considerations before adopting blochchain-based settlement solution. This consideration can ensure the total settlement process is a manageable and healthy process.

2.3.2 Justly smart contracts

As we mentioned above, blockchain-based settlement uses computer codes to automatically generate smart contracts. Without a central controlling jurisdiction, the smart contracts would be created on permissionless blockchain-based system. To solve this issue, when customers accept or use smart contracts, a central arbitrator or a dispute resolution provision should be built to address any conflicts of interest, reduce uncertainty and provide a mechanism in the case of a dispute.

3 Why Do Not Immediately Use Blockchain-Settlement

"Blockchain is not ready to replace settlement systems", said by Bank of Japan and European Central Bank. In this section, we explain why the banks and markets do not immediately use blockchain-settlement from three aspects: captical cost, solid theoretical knowledge and repeat tests.

3.1 Captical cost

3.1.1 Bitcoin is too expensive now

Bitcoin is one of cryptocurrencyies can be used in blockchain-based settlement process. Since the quantity is small, bitcoin price is very high. If banks and markets take bitcoin as a asset trading in blockchain-based settlement system, the number of customers likely to be smaller than that in current settlement process. It is right time for banks or markets to use blockchain-based settlement when bitcoin price is more stable and cheaper.

3.1.2 Data mining is not free

As mentioned in section 1, data miner in blockchain-based settlement process is a new role compared with current settlement process. For banks and markets, a special group devoted to data mining for blockchain system may be a essential approach. Before using this new settlement solution, banks and markets have to spend time considering what is the price criteria for employing the professional data miners and how much is the budget for setting up a data mining teams.

3.2 Essential knowledge training

To understand working principles, technical knowledge and regulations of blockchain-based settlement process is a great help to banks and markets to use blockchain solution well. So banks and markets have to arrange some practical and theoretical training for users. This learning process always takes some time.

3.3 Repeat tests are necessary

To total release the blockchain-based settlement system, testing should be done again and again in different cases. Banks and markets should spend enough time evaluating software and hardware. A robust blockchain system is fundamental to success.

4 Conclusions

Overall, blockchain is a relatively new concept for the financial markets. It is a source of both excitement and confusion. Even so, still look forward to the new era of blockchain-based settlement process !

References

[1] Accenture(2016). “Blockchain Technology: Preparing for Change”.

https://www.accenture.com/t20160608T052656__w__/us-en/_acnmedia/PDF-5/Accenture-2016-Top-10-Challenges-04-Blockchain-Technology.pdf

[2] David Mills, Kathy Wang and Brendan Malone et.al.(2016). “Distributed Ledger Technology in Payments, Clearing, and Settlement,” Finance and Economics Discussion Series 2016-095. Washington: Board of Governors of the Federal Reserve System.

https://doi.org/10.17016/FEDS.2016.095

[3] Euroclear and Oliver Wyman(2016). “Blockchain in Capital markets. The Prize and The Journey”.

http://www.oliverwyman.com/content/dam/oliver-wyman/global/en/2016/feb/BlockChain-In-Capital-Markets.pdf

[4] Haroon Shahid Bashir(2016). “Blockchain Settlement for Hong Kong Equity Markets”.

https://www.linkedin.com/pulse/blockchain-settlement-hong-kong-equity-markets-haroon-shahid-bashir

[5] Philip Boucher(2017). “How Blockchain Technology Could Change our Lives”.

http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/581948/EPRS_IDA(2017)581948_EN.pdf

[6] Shai Jalfin (2017). “Protecting IP in the Blockchain Sector”.

http://www.ipwatchdog.com/2017/06/30/protecting-ip-blockchain-sector/id=84581/