A Survey of Blockchain Security Issues and Challenges

Iuon-Chang Lin[1,2] and Tzu-Chun Liao[2]
(Corresponding author: Iuon-Chang Lin)
Department of Photonics and Communication Engineering, Asia University[1]
500, Lioufeng Rd., Wufeng, Taichung 41354, Taiwan
Department of Management Information Systems, National Chung Hsing University[2]
145 Xingda Rd., South Dist., Taichung City 402, Taiwan
(Email: corresponding_iclin@nchu.edu.tw)
(Invited Jan. 12, 2017)

Abstract

Blockchain technologies is one of the most popular issue in recent years, it has already changed people's lifestyle in some area due to its great influence on many business or industry, and what it can do will still continue cause impact in many places. Although the feature of blockchain technologies may bring us more reliable and convenient services, the security issues and challenges behind this innovative technique is also an important topic that we need to concern.

Keywords: Blockchain; Smart Contracts; Security

1 Introduction

Bitcoin is the first application of blockchain, it's a kind of digital currency based on blockchain technologies, using for trade things on the internet like money as we do in the real world. Because the success of Bitcoin, people now can utilize blockchain technologies in many field and service, such as financial market, IOT, supply chain, voting, medical treatment and storage.

But as we use these tools or services in our daily life, cybercriminals also get opportunity to engage in cybercrime [16, 18]. For example, 51% attacks is a classic security issue in Bitcoin that hacker try to take control the system's mechanism, using the same technology base.

In this paper, we will have a quick study about what is blockchain in Section 2, then we'll discuss different application in blockchain and what service do they offer in Section 3, at the end, we shall talk about the security issues and those challenges we need to overcome in Section 4. The paper is concluded in Section 5.

2 The Concept of Blockchain

Blockchain technologies is not just only single one technique, but contains Cryptography, mathematics, Algorithm and economic model, combining peer-to-peer networks and using distributed consensus algorithm to solve traditional distributed database synchronize problem, it's an integrated multi- field infrastructure construction [5, 6, 15].

The blockchain technologies composed of six key elements.

Decentralized. The basic feature of blockchain, means that blockchain doesn't have to rely on centralized node anymore, the data can be record, store and update distributedly.

Transparent. The data's record by blockchain system is transparent to each node, it also transparent on update the data, that is why blockchain can be trusted.

Open Source. Most blockchain system is open to everyone, record can be check publicly and people can also use blockchain technologies to create any application they want.

Autonomy. Because of the base of consensus, every node on the blockchain system can transfer or update data safely, the idea is to trust form single person to the whole system, and no one can intervene it.

Immutable. Any records will be reserved forever, and can't be changed unless someone can take control more than 51% node in the same time.

Anonymity. Blockchain technologies solved the trust problem between node to node, so data transfer or even transaction can be anonymous, only need to know the person's blockchain address.

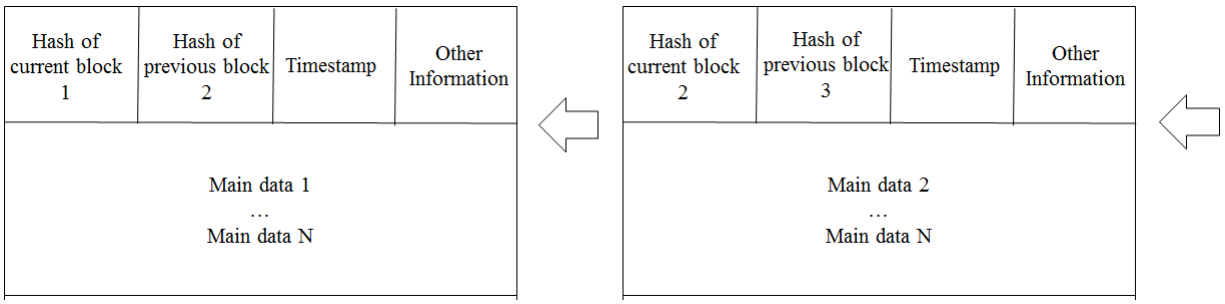

Figure 1: The structure of block chain

2.1 How Blockchain Works?

The main working processes of blockchain are as follows:

1) The sending node records new data and broad casting to network.

2) The receiving node checked the message from those data which it received, if the message was correct then it will be stored to a block.

3) All receiving node in the network execute proof of work (PoW) or proof of stake (PoS) algorithm to the block.

4) The block will be stored into the chain after executing consensus algorithm, every node in the network admit this block and will continuously extend the chain base on this block.

2.2 The Structure of Blockchain

Generally in the block, it contains main data, hash of previous block, hash of current block, timestamp and other information. Figure 1 shows the structure of block.

Main data. Depending on what service is this blockchain applicate, for example: transaction records, bank clearing records, contract records or IOT data record.

Hash. When a transaction executed, it had been hash to a code and then broadcast to each node. Because it could be contained thousands of transaction records in each node's block, blockchain used Merkle tree function to generate a final hash value, which is also Merkle tree root. This final hash value will be record in block header (hash of current block), by using Merkle tree function, data transmission and computing resources can be drastically reduced.

Timestamp. Time of block generated.

Other Information. Like signature of the block, Nonce value, or other data that user define.

2.3 How to Get Consensus?

Consensus function is a mechanism that make all blockchain nodes have agreement in same message, can make sure the latest block have been added to the chain correctly, guarantee the message that stored by node was the same one and won't happened "fork attack", even can protect from malicious attacks.

2.4 Proof of Work (PoW)

A proof of work is a piece of data which is difficult (costly or time-consuming) to produce but easy for others to verify and which satisfies certain requirements. Producing a proof of work can be a random process with low probability so that a lot of trial and error is required on average before a valid proof of work is generated. Bitcoin uses the Hashcash proof of work system.

When calculating PoW, it's called "mining". Each block has a random value called "Nonce" in block header, by changing this nonce value, PoW have to generate a value that makes this block header hash value less than a "Difficulty Target" which has already been set up. Difficulty means how much time it will take when the node calculating hash value less than target value.

In order for a block to be accepted by network participants, miners must complete a proof of work which covers all of the data in the block. The difficulty of this work is adjusted so as to limit the rate at which new blocks can be generated by the network to one every 10 minutes. Due to the very low probability of successful generation, this makes it unpredictable which worker computer in the network will be able to generate the next block [1, 7].

2.5 Proof of Stake (PoS)

Because Proof of Work method will cause a lot of electricity power and computing power be wasted, Proof of Stake doesn't need expensive computing power. With Proof of Stake, the resource that's compared is the amount of Bitcoin a miner holds - someone holding 1% of the Bitcoin can mine 1% of the "Proof of Stake blocks" [12].

A Proof of Stake method might provide increased protection from a malicious attack on the network. Additional protection comes from two sources:

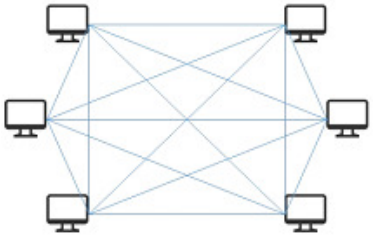

Figure 2: Public blockchain

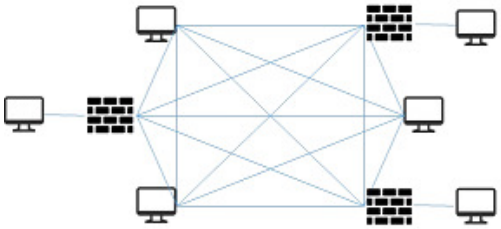

Figure 3: Consortium blockchain

1) Executing an attack would be much more expensive.

2) Reduced incentives for attack. The attacker would need to own a near majority of all bitcoin. Therefore, the attacker suffer severely from his own attack.

2.6 Type of Blockchain

Blockchain technologies can be roughly divided into three types.

1) **Public blockchain:** Everyone can check the transaction and verify it, and can also participate the process of getting consensus. Like Bitcoin and Ethereum are both Public Blockchain. Figure 2 shows public blockchain.

2) **Consortium blockchains:** It means the node that had authority can be choose in advance, usually has partnerships like business tobusiness, the data in blockchain can be open or private, can be seen as Partly Decentralized. Like Hyperledger and R3CEV are both consortium blockchains. Figure 3 shows consortium blockchains.

3) **Private blockchain:** Node will be restricted, not every node can participate this blockchain, has strict authority management on data access. Figure 4 shows private blockchain.

   No matter what types of blockchain is, it both has advantage. Sometimes we need public blockchain because its convenience, but sometimes we maybe need private control like consortium blockchains or private blockchain, depending on what service we offer or what place we use it.

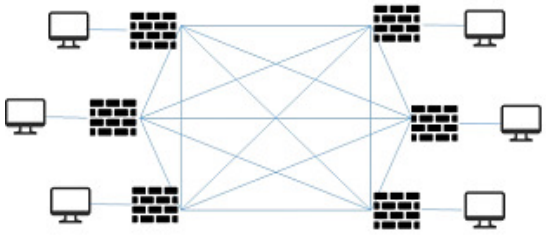

Figure 4: Private blockchain

3 Application of Blockchain Technologies

Blockchain technologies can be using in many area, not only in financial application, but also in others industries.

3.1 Digital Currency: Bitcoin

Bitcoin's data structure and transaction system was built by blockchain technologies, makes Bitcoin became a digital currency and online payment system. By using encrypted technique, funds transfer can be achieved and doesn't need to rely on central bank. Bitcoin used public keys address sending and receiving bitcoin, recorded the transaction and the personal ID was anonymous. The process of transaction confirm needs other user's computing power to get consensus, and then records the transaction to network.

3.2 Smart Contract: Ethereum

Smart Contract is a digital contract that controls user's digital assets, formulating the participant's right and obligation, will automatically execute by computer system. It's not only just a computer procedure, it can be seen as one of a contract participants, will response to message what it receive and store the data, it can also send message or value to outside. Smart Contract is just like a person can be trusted, can hold the assets temporarily and will follow the order which has already been program [13].

Ethereum is an open source blockchain platform combining Smart Contract, offering decentralized virtual machine to handle the contract, by using its digital currency called ETH, people can create many different services, applications or contracts on this platform [21].

3.3 Hyperledger

Hyperledger is an open source blockchain platform, started in December 2015 by the Linux Foundation, to support blockchain-based distributed ledgers. It is focused on ledgers designed to support global business transactions, including major technological, financial, and supply chain companies, with the goal of improving many aspects of performance and reliability. The project aims

to bring together a number of independent efforts to develop open protocols and standards, by providing a modular framework that supports different components for different uses. This would include a variety of blockchains with their own consensus and storage models, and services for identity, access control, and contracts.

3.4 Other Applications

There still have many use case of blockchain technologies, like protection of Intellectual property, traceability in supply chain, identity certification, insurance, international payments, IOT, patient's privacy in medical treatment or prediction market [14, 20].

4 Security Issues and Challenges

So far, blockchain has been gotten many attention in different area, however, it also exists some problems and challenges needs to face it [2, 9].

4.1 The Majority Attack (51% Attacks)

With Proof of Work, the probability of mining a block depends on the work done by the miner (e.g. CPU/GPU cycles spent checking hashes). Because of this mechanism, people will want to join together in order to mining more blocks, and become "mining pools", a place where holding most computing power. Once it hold 51% computing power, it can take control this blockchain. Apparently, it cause security issues [3, 4].

If someone has more than 51% computing power, then he/she can find Nonce value quicker than others, means he/she has authority to decide which block is permissible. What it can do is:

1) Modify the transaction data, it may cause double-spending attack [11, 17].
2) To stop the block verifying transaction.
3) To stop miner mining any available block.

A majority attack was more feasible in the past when most transactions were worth significantly more than the block reward and when the network hash rate was much lower and prone to reorganization with the advent of new mining technologies [8].

4.2 4.2 Fork Problems

Another issue is fork problem. Fork problem is related to decentralized node version, agreement when the software upgrade. It is a very important issue because it involving a wide range in blockchain.

- Types of Forks

  When the new version of blockchain software published, new agreement in consensus rule also changed to the nodes. Therefore, the nodes in blockchain network can be divided into two types, the New Nodes and the Old Nodes. So here come four situations:

  1) The new nodes agree with the transaction of block which is sending by the old nodes.
  2) The new nodes don't agree with the transaction of block which is sending by the old nodes.
  3) The old nodes agree with the transaction of block which is sending by the new nodes.
  4) The old nodes don't agree with the transaction of block which is sending by the new nodes.

  Because of these four different cases in getting consensus, fork problem happens, and according to these four cases, fork problems can be divided into two types, the Hard Fork and the Soft Fork. In addition to distinguish the new nodes and the old nodes, we have to compare the computing power of new nodes with old nodes, and assume that the computing power of new nodes are more than 50

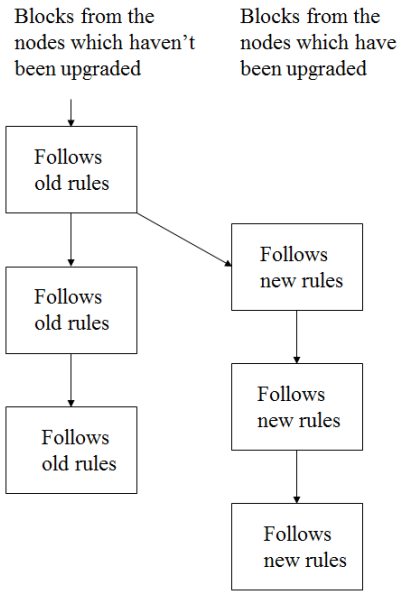

Figure 5: Hard Fork

- Hard Fork

  Hard Fork means when system comes to a new version or new agreement, and it didn't compatible with previous version, the old nodes couldn't agree with the mining of new nodes, so one chain became two chains. Although new nodes computing power were stronger than old nodes, old nodes will still continue to maintain the chain which it though was right. Figure 5 shows the hard fork problem.

  When Hard Fork happens, we have to request all nodes in the network to upgrade the agreement, the

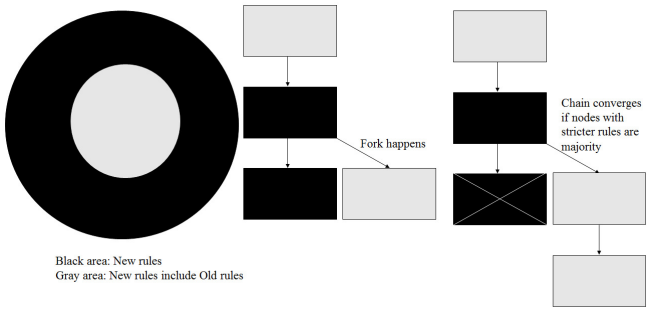

Figure 6: Hard Fork happens because the old node verification requirement is much stricter than the new node

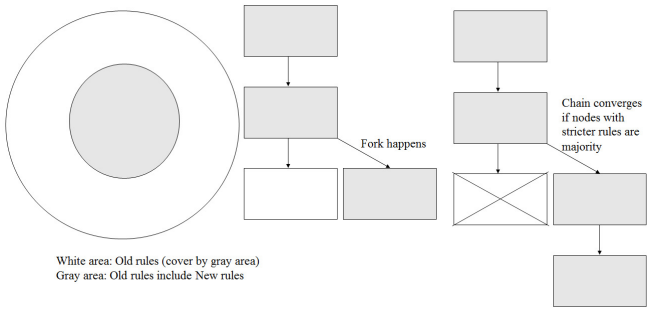

Figure 8: Soft Fork happens because the new node verification requirement is much stricter than the old node

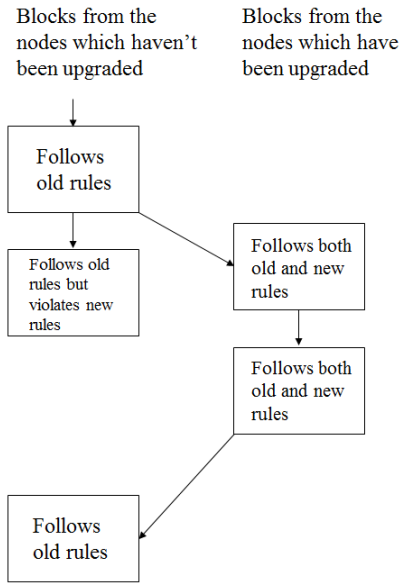

Figure 7: Compatible hard fork

nodes which haven't been upgrade will not continue to work as usual. If there were more old nodes didn't upgrade, then they will continue to work on the other completely different chain, which means the ordinary chain will fork into two chains. Figure 6 shows the reason of why hard fork will happens.

- Soft Fork

  Soft Fork means when system comes to a new version or new agreement, and it didn't compatible with previous version, the new nodes couldn't agree with the mining of old nodes. Because the computing power of new nodes are stronger than old nodes, the block which is mining by the old nodes will never be approve by the new nodes, but new nodes and old nodes will still continue to work on the same chain. Figure 7 shows the soft fork problem.

  When Soft Fork happens, nodes in the network don't have to upgrade the new agreement at the same time, it allows to upgrade gradually. Not like Hard Fork, Soft Fork will only have one chain, it won't affect the stability and effectiveness of system when nodes upgrade. However, Soft Fork makes the old nodes unaware that the consensus rule is changed, contrary to the principle of every nodes can verify correctly to some extent. Figure 8 shows the reason of why soft fork will happens.

4.3 Scale of Blockchain

As blockchain growing, data becomes bigger and bigger, the loading of store and computing will also getting harder and harder, it takes plenty of time to synchronize data, in the same time, data still continuely increase, brings a big problem to client when running the system [10].

Simplified Payment Verification (SPV) is a payment verification technology, without maintain full blockchain information, only have to use block header message. This technology can greatly reduce user's storage in blockchain payment verification, lower the user's pressure when transaction drastically increased in the future.

4.4 Time Confirmation of Blockchain Data

Compared to traditional online credit card transaction, usually takes 2 or 3 days to confirm the transaction, bitcoin transaction only have to use about 1 hour to verify, it's much better than the usual, but it's still not good enough to what we want it to. **Lightning Network** is a solution to solve this problem [19].

Lightning Network is a proposed implementation of Hashed Timelock Contracts (HTLCs) with bi-directional payment channels which allows payments to be securely routed across multiple peer-to-peer payment channels. This allows the formation of a network where any peer

on the network can pay any other peer even if they don't directly have a channel open between each other.

4.5 Current Regulations Problems

Use Biction for example, the characteristics of decentralized system, will weak the central bank's ability to control the economic policy and the amount of money, that makes government be cautious of blockchain technologies, authorities have to research this new issue, accelerate formulating new policy, otherwise it will have risk on the market.

4.6 Integrated Cost Problem

Of course it will have lot of cost including time and money to change existing system, especially when it's an infrastructure. We have to make sure this innovative technology not only create economic benefits, meet the requirements of supervision, but also bridge with traditional organization, and it always encounter difficulties from internal organization which is existing now.

5 Conclusions

There's no doubt that blockchain is a hot issue in recent years, although it has some topics we need to notice, some problems has already been improved along with new technique's developing on application side, getting more and more mature and stable.

The government have to make corresponding laws for this technology, and enterprise should ready for embrace blockchain technologies, preventing it brings too much impact to current system.

When we enjoy in the advantage of blockchain technologies bring to us, in the same time, we still have to stay cautious on its influence and security issues that it could be have.

Acknowledgments

This study was supported by the National Science Council of Taiwan under grant NSC 105-2410-H-005 -023 -MY2. The authors gratefully acknowledge the anonymous reviewers for their valuable comments.

References

[1] I. Bentov, A. Gabizon, and A. Mizrahi, "Cryptocurrencies without proof of work," *CoRR*, vol. abs/1406.5694, 2014.

[2] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, and E. W. Felten, "Sok: Research perspectives and challenges for bitcoin and cryptocurrencies," in *IEEE Symposium on Security and Privacy*, pp. 104–121, May 2015.

[3] N. T. Courtois and L. Bahack, "On subversive miner strategies and block withholding attack in bitcoin digital currency," *CoRR*, vol. abs/1402.1718, 2014.

[4] I. Eyal and E. G. Sirer, "Majority is not enough: Bitcoin mining is vulnerable," *CoRR*, vol. abs/1311.0243, 2013.

[5] J. Garay, A. Kiayias, and N. Leonardos, *The Bitcoin Backbone Protocol: Analysis and Applications*, pp. 281–310, Springer Berlin Heidelberg, Berlin, Heidelberg, 2015.

[6] A. Gervais, G. O. Karame, V. Capkun, and S. Capkun, "Is bitcoin a decentralized currency?," *IEEE Security Privacy*, vol. 12, pp. 54–60, May 2014.

[7] A. Gervais, G. O. Karame, K. Wüst, V. Glykantzis, H. Ritzdorf, and S. Capkun, "On the security and performance of proof of work blockchains," in *Proceedings of ACM SIGSAC Conference on Computer and Communications Security (CCS'16)*, pp. 3–16, New York, NY, USA, 2016.

[8] A. Gervais, H. Ritzdorf, G. O. Karame, and S. Capkun, "Tampering with the delivery of blocks and transactions in bitcoin," in *Proceedings of the 22Nd ACM SIGSAC Conference on Computer and Communications Security (CCS'15)*, pp. 692–705, New York, NY, USA, 2015.

[9] E. Heilman, A. Kendler, A. Zohar, and S. Goldberg, "Eclipse attacks on bitcoin's peer-to-peer network," in *24th USENIX Security Symposium*, pp. 129–144, Washington, D.C., 2015.

[10] G. Karame, "On the security and scalability of bitcoin's blockchain," in *Proceedings of ACM SIGSAC Conference on Computer and Communications Security (CCS'16)*, pp. 1861–1862, New York, NY, USA, 2016.

[11] G. O. Karame, "Two bitcoins at the price of one? double-spending attacks on fast payments in bitcoin," in *Proceedings of Conference on Computer and Communication Security*, pp. 1–17, 2012.

[12] S. King and S. Nadal, *Ppcoin: Peer-to-peer Crypto-Currency with Proof-of-Stake*, 2012. (`https://archive.org/stream/PPCoinPaper/ppcoin-paper_djvu.txt`)

[13] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts," in *2016 IEEE Symposium on Security and Privacy (SP'16)*, pp. 839–858, May 2016.

[14] L. Luu, V. Narayanan, C. Zheng, K. Baweja, S. Gilbert, and P. Saxena, "A secure sharding protocol for open blockchains," in *Proceedings of ACM SIGSAC Conference on Computer and Communications Security (CCS'16)*, pp. 17–30, New York, NY, USA, 2016.

[15] S. Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, Feb. 24, 2013. (`http://bitcoin.org/bitcoin.pdf`)

[16] E. U. Opara, O. A. Soluade, "Straddling the next cyber frontier: The empirical analysis on network

security, exploits, and vulnerabilities," *International Journal of Electronics and Information Engineering*, vol. 3, no. 1, pp. 10–18, 2015.

[17] M. Rosenfeld, "Analysis of hashrate-based double spending," *CoRR*, vol. abs/1402.2009, 2014.

[18] J. Singh, "Cyber-attacks in cloud computing: A case study," *International Journal of Electronics and Information Engineering*, vol. 1, no. 2, pp. 78–87, 2014.

[19] Y. Sompolinsky and A. Zohar, *Secure High-Rate Transaction Processing in Bitcoin*, pp. 507–527, Springer Berlin Heidelberg, Berlin, Heidelberg, 2015.

[20] W. T. Tsai, R. Blower, Y. Zhu, and L. Yu, "A system view of financial blockchains," in *IEEE Symposium on Service-Oriented System Engineering (SOSE'16)*, pp. 450–457, Mar. 2016.

[21] H. Watanabe, S. Fujimura, A. Nakadaira, Y. Miyazaki, A. Akutsu, and J. Kishigami, "Blockchain contract: Securing a blockchain applied to smart contracts," in *IEEE International Conference on Consumer Electronics (ICCE'16)*, pp. 467–468, Jan. 2016.

Biography

Iuon-Chang Lin received the B.S. in Computer and Information Sciences from Tung Hai University, Taichung, Taiwan, Republic of China, in 1998; the M.S. in Information Management from Chaoyang University of Technology, Taiwan, in 2000. He received his Ph.D. in Computer Science and Information Engineering in March 2004 from National Chung Cheng University, Chiayi, Taiwan. He is currently a professor of the Department of Management Information Systems, National Chung Hsing University,and Department of Photonics and Communication Engineering, Asia University, Taichung, Taiwan, ROC. His current research interests include electronic commerce, information security, cryptography, and mobile communications.

Tzu-Chun Liao graduated from National Chung Hsing University, Taichung, Taiwan, Republic of China, in 2015; He is currently an M.S. student of the Department of Management Information Systems, National Chung Hsing University.