2017 台灣網際網路研討會
DOI: 10.6728/TANET.201710.0110

Applying Blockchain to an Automated Clearinghouse System

Yen-Chih, Liao[1], Jen-Hung Tseng[2], Shih-wei Liao[1]

Department of Computer Science, National Taiwan University[1]
Food and Drug Administration, Taiwan[2]

jeff.yenchih.liao@gmail.com, r93626007@gmail.com, liao@csie.ntu.edu.tw

摘要

由金融科技的角度，我們分析由Gusto [1]的金融機構所提供的媒體自動轉賬業務（Automated Clearing House，以下簡稱ACH業務），經過比較雙方（ACH 業務和區塊鏈）中角色以及功能性的差異後，我們將區塊鏈技術應用於該業務，藉此來觀察區塊鏈對於Gusto媒體自動轉賬業務在安全性以及效率性的影響。

我們經由在 ACH 業務上導入區塊鏈技術進行概念驗證，發展「交易後立即清算」的運作模式，並實作ACH區塊鏈系統。我們採用模擬的 ACH 交易資料導入系統雛型做實際運行和比較，分析 Gusto 之中介角色可以如何轉型成去中心化的角色，並提出營運架構之設計建議。藉由上述的系統雛型，及其流程和使用介紹，經實際模擬後，我們能見證區塊鏈所帶來的改變，並作為後續研究發展之參考。

經過了安全性與效率性的探討比較，以及可行性分析後，我們發現導入區塊鏈系統是可以提升整體安全性，但在交易處理效率上則會有負面影響。因此，若未來要實際建置，就現有的技術要達到完全去中心化的區塊鏈架構仍有困難，建議可先朝半去中心化之模式試作發展。

關鍵詞：區塊鏈、Gcoin、去中心化、媒體交換自動轉賬業務（ACH）

Abstract

We comprehensively survey the field of Automated Clearinghouse (ACH) systems, exemplified by Gusto[1]. After comparing roles and functions in both blockchain side and Gusto side, we implement blockchain on the ACH business process. Besides, we also study its impact on the Gusto business system using our implementation. The impact study consists of two aspects, safety and efficiency.

We design and implement the blockchain-based automatic clearinghouse (ACH) business process. The ACH process is provided by Gusto. We develop a model called the SAT (Settle-right-After-Transactions) model. The SAT model is implemented in our ACH blockchain system. In addition, we adopt ACH historical trading data to test our prototype. We analyze how the original Gusto's intermediary role can be transformed into a more decentralized role. Furthermore, we propose some insights on the design of the new operational structure. Through our implementation of an ACH blockchain system, people can be more aware to the changes brought by the advent of blockchain and take this research as a reference in the future.

After performing the feasibility analysis upon ACH business process from the perspective of safety and efficiency, we find that as the safety increases, however, the efficiency drops due to the blockchain-based implementation. As the result, if people want to implement a blockchain-based ACH system elsewhere, realistically it is still difficult to build a fully decentralized blockchain system. It is recommended to start the development process in the direction of a semi-centralized system.

Keywords: Blockchain, Gcoin, Decentralization, Automated Clearing House (ACH)

I. Introduction

Many countries, such as Sweden, France, have already devoted into researching the blockchain technology, exploring the possibility of digital currencies and setting up their own research labs, after the introduction of RScoin[2]. RScoin is mentioned in the paper "Centrally Banked Cryptocurrencies" published by researchers at University College London. In Sweden, their krona in circulation has been decreasing. Physical money became an expensive and inefficient way of payment. Digital currencies controlled by a singular united system are easier to grasp the payment flow. Moreover, the combination of the real identity system and the digital currency system is even better against money laundering. It also reduces the cost of producing, transfer, and settlement in comparison with fiat currencies.

Monetary clearinghouse is a complex and costly operation. Aside from physical currencies, current settlements are mostly based on a third party such as Central bank or Gusto by depositing enough amount of money in it. The basic principle is increasing or decreasing corresponding amount of money in the third party when a transactions happens.

Taking Taiwan as an example, Taiwan Clearinghouse (TCH) operates the ACH operations and check clearinghouse. The operations all depend on the third party, the Central bank, to finally settle.

DOI: 10.6728/TANET.201710.0110

The distributed ledger is an important feature in the blockchain technology. Participants use the shared ledger to allow the transactions, the bookkeeping of the participating accounts and the settlements to accomplish simultaneously. Replaced by the distributed ledger, the concept of third party settlement disappears. The cost in economic, time and communication can be reduced dramatically as a result.

The decentralized property is fundamental to the blockchain technology. This confronts with the centralized currency management business. As a consequence, running a distributed ledger in any centralized institution presents some challenges. One of our purposes in conducting this research is to find out whether some drawbacks exist when applying the blockchain technology to a centralized business.

Assuming we already have digital currency issued, we try to apply the blockchain technology to the ACH business. ACH businesses include the direct debit and the direct credit business. There are proposals, validation, and returning steps in the service process flow. These processes help the settlement between different financial institutions, which is the target for our system. By implementing the system on this part of business, we can understand the pros and cons of the blockchain structure. It will also help us to evaluate the possibility of combining Gusto's ACH business with the blockchain technology. Our main goals in this research work are the optimization of the operation processes, highly efficient automation, and the proposals of any new operation models.

II. Related Work

A. Bitcoin and Blockchain

In 2008, a paper called "Bitcoin: A Peer-to-Peer Electronic Cash System"[3] released by Satoshi Nakamoto, whose identity is still unknown, introduced the first Blockchain — Bitcoin.

Bitcoin uses multi-signature, consensus, etc. mechanisms to reduce traditional cost on human resources. It also deals data transactions between countries more efficiently. When it comes to financial industry, Banks no longer have to wait for third parties to deal with inter-bank transactions. Furthermore, the ledger designed in Blockchain has the function of auditing trials itself. This is able to replace the transaction tracking function in traditional information system, which makes it easier to prevent money laundry and to track dubious transactions, with less effort.

Even though Bitcoin is controversial for its usage of money laundering, it's still a great innovation of cryptocurrency in history. It solves following problems:

Currency issuing. Relay on third party.

Value inconsistency. Assets could be blockade by governments or banks.

No anonymity. Transactions can't be anonymity.

B. Gcoin

The Blockchain system prototype in bottom layer we adopted is Gcoin[4], which is introduced by National Taiwan University. Gcoin is an alliance Blockchain base on Bitcoin structure. It devoted to provide a safer, more efficient and cheaper shared platform.

Different from Bitcoin, Gcoin supports various digital currencies, which makes it better to handle multiple business requirements. Hence, Gcoin can establish unchangeable links between various real-world assets. Besides, Gcoin optimized the transaction speed of financial applications and E-commerce. The speed Gcoin produce a block, which is 15 seconds per block, is much faster than Bitcoin, which is 10 minutes per block. As a result, Gcoin is more likely to realize the click-and-mortar of digital finance. Furthermore,

1. Alliance structure

Alliance structure allows data being shared only in a group. People do not have access to it unless they are members of the corresponding alliance. Alliance structure increases safety and amortizes risks by several backups in multiple nodes within the alliance. Because data will be verified by every node in alliance to reach the goal of decentralization, failure of a single node will not stop the whole blockchain system from running.

2. Role hierarchy

Gcoin is a blockchain implementation with role hierarchy. Each role has different access rights and functions. Three roles in Gcoin system are alliance member, coin issuer and common user, respectively. Among those roles, alliance member gets the highest authority.

C. ACH business

ACH[5] is batch payment system. With electronic operations, ACH mainly offers two services, Direct Debit and Direct Credit. Former one, Direct Debit, helps payees to collect various fees from payers. The other one helps payers pay wages , salaries, etc. for payees. With these services, ACH is able to enhance payment system efficiency.

1. Gusto's Direct Debit and Credit

As shown in figure 1, customer of Gusto, who is the launcher, propose their direct debit before the certain time, let's say 19:00, depends on different banks with which they have agreements. Once a proposal is approved, it will be forward to the Federal Reserve for processing around midnight, which is the time before 0:01 at the next day. After the Federal Reserve tell the corresponding bank to which receiver belongs to deal with such a proposal, the corresponding bank should finish their jobs before 5:00 at Day 2.

The above process is only for those proposals which have been accepted. When a proposal is rejected by the bank of counterpart, this process takes even longer time to complete. The rejecting message should be returned before the end of Day 3, which is the time before 0:01 at Day 4. After that, the rejecting message

DOI: 10.6728/TANET.201710.0110

is return to the launcher before 5:00 in the morning at the fourth day.

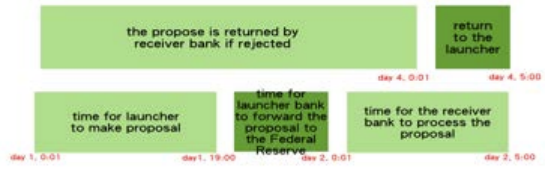


Figure 1. work flow of Gusto ACH Business

2. TCH

2.1 Direct Debit

As shown in figure 2, the bank charges fees proposes for this service at 9:00 ~ 14:00. ACH then categorizing and calculates these proposes at 14:00 ~ 15:00. The Central Bank settles these trades at the same time. After that, banks paying those fees can get their trading data detail list at 15:00 ~ 16:00 if the trading is valid. By the time of 0:00 on the next day, payers can begin to cut their payments. After clearing business is done at the following 17:00, proposer can actually get their fees. However, if there are invalid trading, ACH will categorize and calculate them at 14:00 ~ 15:00 on the next day when it was proposed. After that, Proposer can get their returned data detail list at 15:00 ~ 16:00.

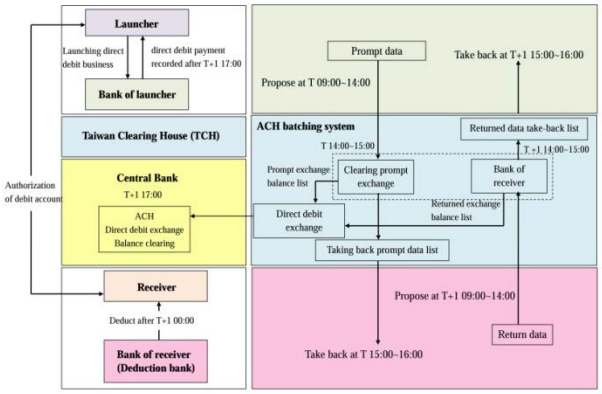


Figure 2. Workflow of direct debit

2.2 Direct Credit

As shown in figure 3, This process is very similar to the direct debit. The main difference is that payer now becomes the proposer.

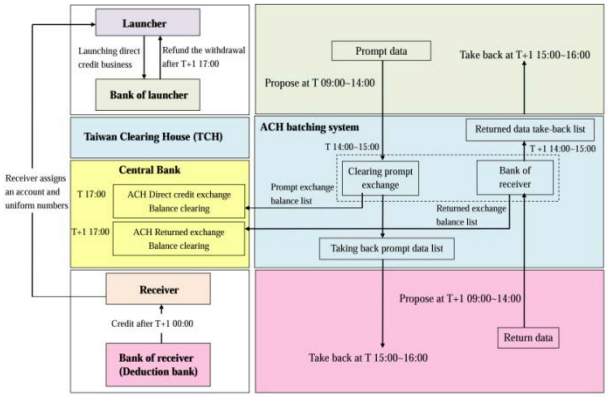


Figure 3. Workflow of direct credit

D. The European Central Bank and The Bank of Japan

Recently, the European Central Bank (ECB) and the Bank of Japan (BOJ) released a joint research, payment systems: liquidity saving mechanisms in a distributed ledger environment[6]. They have implemented blockchain technology on both BOJ and ECB along with the analysis of safety and efficiency. While experimenting on the Runtime Gross Settlement (RTGS) business with blockchain system, they have confirmed that the blockchain technology is able to handle the traffic of those banks. Besides, they have conducted experiments upon networks size and network patterns. Therefore, they confirmed the trade-off of performance and network size. Furthermore, they found that the system using blockchain technology has potential to strengthen resilience and reliability.

Even though the blockchain system we used in our experiment is Gcoin instead of Hyperledger Fabric, which is used in the joint research of BOJ and ECB, the advantage of safety and efficiency in our system is somehow similar to their research. The main difference is that our research includes something to deal with privacy issue. Also, our research is base on ACH business instead of their RTGS business.

III. System Design

A. Premise for our model

1. Privacy Issue

Privacy is one of the most important concern for all the banks. Every newly constructed system for banks should deal with privacy issue first. In the case of ACH transaction applying blockchain, such issue existed in the transparency of blockchain system. Therefore, we constructed a module in the service layer additionally to differentiate different identity so that banks can only see the transactional data related to them instead of all the transactions on the blockchain.

DOI: 10.6728/TANET.201710.0110

2. Payment flow

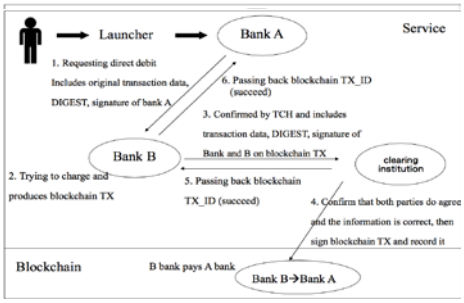


Figure 4. Life cycle of such digital currency

We assume that the settlement institution has already issued or using digital currency, which has exactly the same value with legal tender, bases on blockchain. As legal tender circulating in the physical market, the digital currency circulates in the virtual market. Hence, we can take the advantage of irreversibility and safety of blockchain. Furthermore, digital currency allows us to get settlement done digitally, which is much flexible and efficient.

As shown in figure 4, to issue such a digital currency, which has exactly the same value with legal tender, settlement institution should have a guarantee account for issuing digital currency. Whoever needs this digital currency should deposit the same amount of legal tender in the guarantee account. Reversely, people who want their legal tender back withdraw the money from the guarantee account after settlement institution eliminate that amount of digital currency.

B. Our Model

1. Members and Roles

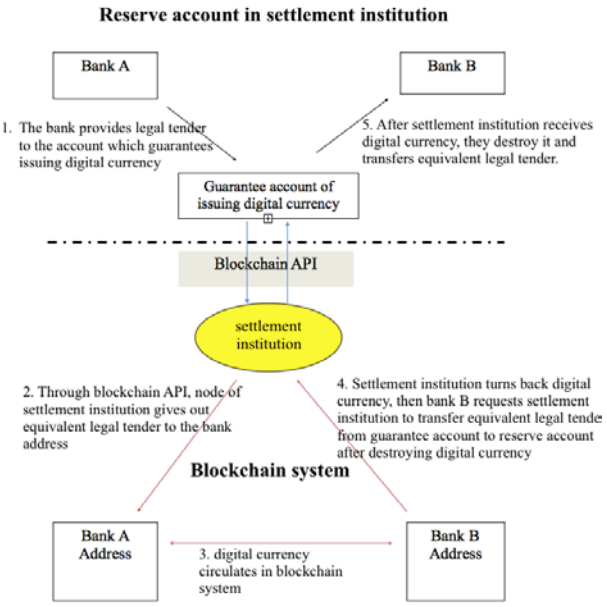
Participants of ACH business include normal banks, clearing institution and settlement institution. As for role hierarchy in Gcoin system, banks should have a corresponding role in Gcoin system.

In theory, because clearinghouse institution is the monitor of all transactions, a clearinghouse is recommended to take the role of alliance member in Gcoin system. Besides, since the settlement institution issues digital currency, it's undoubtedly true for the settlement institution to take the role of coin issuer. Miners who are in charge of verifying transactions is recommend to be bigger banks and clearing institution. The rest of banks can be full nodes who are responsible for storing a backup of historical transactions.

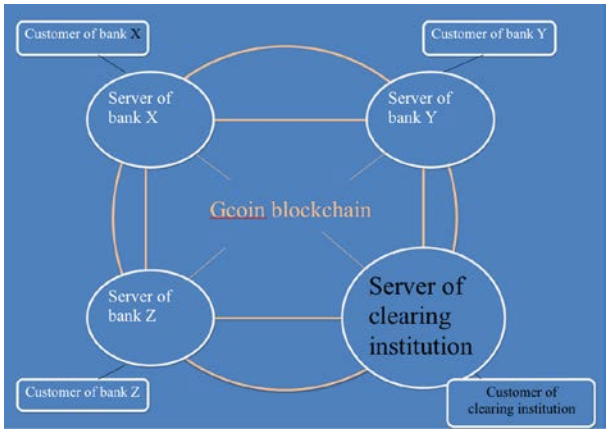
2. Workflow

Figure 5. Workflow of direct debit
Figure 6. Workflow of direct credit

As shown in figure 5 and 6, launchers who want to launch direct debit or direct credit give their transaction data to receivers directly instead of submitting to clearing institution at the specific time. After audited by clearing institution, this transaction is recorded in blockchain. There are two types of transaction data. One of them is the original transaction data, which is the format of transaction specified by clearing institution currently including all messages required. The other one is blockchain data. Having a completely different data structure with the original transaction data, blockchain data needs transformation. Verification related to business logic such as insufficient deposit, wrong account, etc. is not verified on chain. Instead, blockchain only verifies the correctness of signatures and the amount of money. As the consequence, data which will not be used to verify on chain will be hashed as a digest to be recorded on blockchain.



3. System Structure



DOI: 10.6728/TANET.201710.0110

The following figure 7 shows the structure of our model using Gcoin system. The orange circle indicates that the node on server side is connected together and knowing the existence of each other. The bigger circle of clearing institution indicates that the clearing institution has higher priority to handle this intranet system.

Figure 7. System structure of a model

IV. Experimental Results

Using the simulated data of ACH business to conduct our experiment, we tested the transaction speed, which is one of the most concerned feature when trading happens, of our model. With the fluctuating speed of transactions, the average speed of transaction of our model is 17.5~26 TPS (transactions per second). Since our experiment is conducted on a single node, the actual situation can be much faster by mining in parallel and optimizing the software. The result is shown is figure 8 and figure 9.

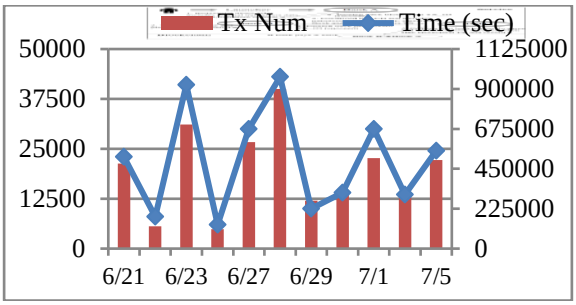


Figure 8. The result of our work 1

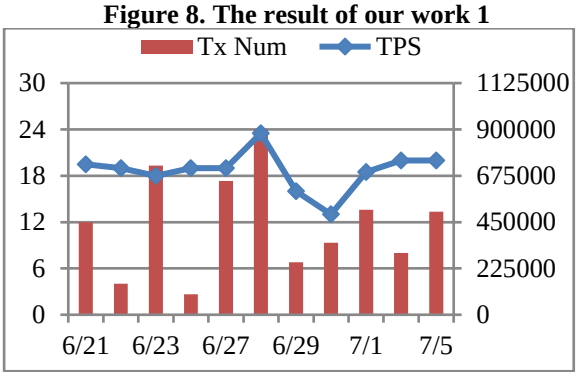


Figure 9. Result of our work 2

A. Comparison

1. Automation

ACH system is already an automated system. The only difference we made in the aspect of automation is that we shorten the process of it. Besides, we also optimized the communication process between nodes and clearing institution.

2. Safety

Aside from the safety technology applied by ACH currently, which is transaction digest and Public Key Infrastructure (PKI), we also put the transaction data on chain to further make sure the data cannot be tempered with.

Because we use blockchain verification system of Gcoin directly, we can reach the safety degree of the byzantine fault tolerance by the consensus algorithm in Gcoin system.

To ensure the privacy of transactions between banks, we constructed a module on service layer to filter out people who don't have access right to those transactions. It's not only easy to implement but also lighten the burden of server to increase the speed. However, once this module on service layer being hacked or being passed around, all the data will be endangered.

3. Efficiency

Traditional ACH systems resort to expensive yet fast hardware to enable them to deal with over 10 million transactions per day within an hour. However, since ACH system has to follow the specific timing requirement to conduct batching operations in terms of clearinghouse business, our model is still able to meet the requirement in terms of settlement. Our SAT model allows us to start the settlement process early. Our rate is 26.04 transactions per second.

B. Feasibility

It is difficult for an ACH system implemented with the blockchain technology to handle large transactions in a short period of time. The rate of producing a block is restricted to approximately four blocks per minute. Even if we increase the block size to boost the number of transactions per second, reaching consensus between financial institutions will slow down the block time. That is, the networking speed between institutions is limited by the speed of light. Centralized systems do not incur such communication overhead.

V. Conclusion

This research aims to find the impact of applying the blockchain technology to the ACH business. We introduce a model called settle-right-after-transactions, which uses Gcoin system and introduces a new workflow to the ACH business process, and experiments with it using simulated data.

Powered by the blockchain technology, we increase the safety and the degree of decentralization. We can track the history of transactions and conduct clearinghouse and settlement easily using our model. However, the use of original currency system of Gcoin still leaves room to improve on the blockchain's privacy issue and clearinghouse mechanism.

The most difficult part we encountered is the speed in dealing with the transactions. It is much slower than a centralized system for nodes to verify every transaction. Besides, there is a trade-off between ensuring privacy and enhancing the transaction speed. The more secured we want the system to be, the longer the execution of a transaction requires. Furthermore, the blockchain technology nowadays cannot enable a completely decentralized system for the ACH business. The

DOI: 10.6728/TANET.201710.0110
role of the monitoring of all the transactions is still important.

VI. Future work

A. Data Storage

Blockchain prevents others from tempering with the data by storing several copies in those nodes in a blockchain network. However, in time the data stored will become extremely large. It may not be a big deal because the cost of storage device is getting cheaper and cheaper. With over a hundred thousand transactions per day, the accumulated data can still be something to be concerned. Therefore, it would be good to have a proper way to seal all these data. This could be accomplished by sealing using UTXO data.

B. Trading of High Frequency and Privacy

Our model is able to handle two to three million transactions per day, which is fast enough for ACH system. However, it's still much slower than the centralized system used currently. To increase security or privacy, the speed is further slowed down. These issues all require breakthroughs in the blockchain technology that guarantees both speed and privacy.

Reference

1. Edward Kim, Official Gusto Engineering Blog, https://engineering.gusto.com/how-ach-works-a-developer-perspective-part-1/
2. G. Danezis, S. Meiklejohn, "Centrally Banked Cryptocurrencies," NDSS, 2016, https://eprint.iacr.org/2015/502.pdf
3. GitHub, "Gcoin White Paper," https://github.com/OpenNetworking/gcoin-community/wiki/Gcoin -white-paper-Chinese
4. N. Satoshi, "Bitcoin: A Peer-to-Peer Electronic Cash System," May 2009, https://bitcoin.org/bitcoin.pdf
5. The Taiwan clearing house https://www.twnch.org.tw/aboutDen.html
6. STELLA - a joint research project of the European Central Bank and Bank of Japan, "payment system: liquidity saving mechanisms in a distributed ledger environment ", https://www.ecb.europa.eu/pub/pdf/other/ecb.stella_project_report_september_2017.pdf