Date of publication Jan. 10, 2022, date of current version Jan. 10, 2022.

Smart Contract Based Electronic Cheque Settlement Protocol

KD Zoysa[1#]

[1]University of Colombo School of Computing
[#]kasun@ucsc.cmb.ac.lk

ABSTRACT Blockchain and smart contract technologies can be used to build a significant impact on financial transactions. This research initiatives the potential of applying blockchain and smart contract technologies for the traditional cheque clearing method. The new protocol is designed based on electronic cheque concepts, blockchain, and smart contracts. As a result of this research, a new secure cheque settlement protocol is designed and implemented. It provides several rewarding features compared to the traditional cheque clearing methods. The new protocol reduces the cheque dishonoring rate and has the possibility of handling a dated cheque. Further, it can be implemented without any exceptional hardware such as heavy-duty scanners.

KEYWORDS: Cryptographic Protocol, Cheque Dishonor, Transaction Security, Electronic Cheque, Blockchain, Smart Contracts, Cheque Settlement, Electronic Payment

I INTRODUCTION

An innovative, blockchain-based secure cheque settlement protocol is designed and presented in this research paper. It holds several rewarding features such as high security, good usability, support for both macro and micropayment, and dated transactions.

The protocol design is based on an electronic cheque concept, blockchain, and smart contracts. Furthermore, the security is highly considered in this protocol as most of the cheque payment technologies offer no inbuilt security other than the standard password and communication layer protection.

A Proof of Concept (POC) of this protocol implementation is carried out with Android smartphones and Mystiko blockchain [4].

Blockchain is a peer-to-peer distributed storage that stores chronological series of transactions in a tamper-resistant manner [5]. However, when implementing a financial application with a typical blockchain, one encounters many challenges as follows [6,7].

- It does not support high transaction throughput;
- It does not scale in terms of big data storage and management;
- It does not provide keyword-based search and retrieval.

Mystiko blockchain supports high transaction throughput, high scalability, high availability, and full-text search features. Thus our Proof of Concept (POC) application is deployed and tested on Mystiko[4].

In addition, reference implementation of the settlement contract written in Solidity was published in Github [10].

II CHEQUE SYSTEMS

Although credit cards are a popular payment system, statistics show that cheques are still the fund transfer method used by the majority of Sri Lankans [9].

The reason behind this could be the following:

- History of cheque usage (people have been using cheques for decades, whereas credit cards entered the show quite recently)
- The exorbitant amounts that get debited from bank accounts due to credit card usage and especially improper credit card usage
- The fees that transfer out of the country to organisations such as Visa, Master, American Express etc. for every usage of the credit card.

A *Dated Cheques*

Through the survey conducted, it was observed that more than 75% of daily transactions are done through cheques, which confirms that cheques are still the preferred payment method in the Sri Lankan Business Community [9] and many other Asian countries. The main reason for the popularity of cheques in Sri Lanka is the possibility of issuing dated cheques [8]. The dated cheque is an agreement to pay the money on a particular date.

B *Dishonour of Cheques*

Cheques presented for payment through a bank counter are dishonored due to two reasons:

- Technical Defects
- Technical Defects
- Lack of funds

The decision to dishonor should be taken by an officer if the defect is technical. If the account does not have sufficient funds, the cheque should be referred to the Manager.

Cheque dishonoring decreases the value of a bank's cheques, which leads to less usage of the banks' cheques.

In Sri Lanka, an average daily cheque dishonoring percentage is an alarming 7.2% [9]. This leads to the denial of cheque payments. This negatively impacts the cheque payee, the cheque payer and the payer's bank.

If we can reduce the cheque dishonored rate:

- Cheque users will benefit.
- The organizations will benefit.
- The banks will benefit.
- The government will benefit (less tax to visa, master, etc)

Thus our protocol solves the cheque dishonoring issue while providing the dated cheque facility.

III PROTOCOL ARCHITECTURE

A *Participants*

To fully explain how our protocol works, we need to explain the relationships between the parties involved in the system.
Payer: The person/organization who purchases goods and services using cheque payments.
Payee: Goods and services provider who accepts cheque payments.
Issuer Bank: Bank or financial institution that issues a cheque facility to the Payer.
Smart Contract: The blockchain platform that executes the functions of Payment Settlement Smart Contract between Payer, Payee and Issuer Bank.

B *Preliminaries*

The payment settlement Smart Contract should be deployed in public or permission blockchain such as Ethereum and Mystiko, respectively [4]. This smart contract has a fixed amount of crypto tokens to be distributed among the participating banks and protocol developers.

A reference implementation of the settlement contract was published in Github [10]. This contract can be deployed in Ethereum, and it was written in Solidity. The settlement contact, which was written in Scala for Mystiko blockchain cannot be published since it is copyrighted to a commercial bank in Sri Lanka.

Initially, banks enroll in the system and receive a fixed amount of crypto tokens free of charge for their contributions. The setBank function [10] of the smart contract performs this action. The bank also receives the token when a customer deposits a cheque, as explained later on. If this system gets popular, banks may need additional crypto tokens. The additional tokens can be purchased from the developers who maintain the system.

A customer (Payer/Payee) has zero crypto token at the registration. The setCustomer function [10] of the smart contract performs this action. At any given time the token amount may be positive, negative or zero. The positive amount indicates the pending funds, and the negative amount indicates the liability level.

C *Protocol Messages*

The business logic of the entire system is deployed as a smart contract. A reference implementation was published in Github [10]. A payer and a payee of the system should use cheque payment mobile application. Standalone application was developed for banks.

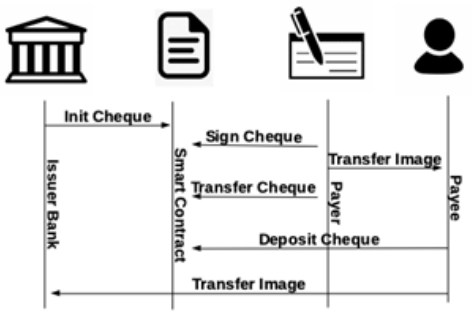

Figure 1. Message Sequence

The physical image of the cheques is transferred from the payer to the payee and finally to the issuer bank. The protocol messages are shown in the figure 1. Each participant of this protocol calls the relevant function of the smart contract as follows.

(A) On the request receives from the payer's mobile application, the electronic cheque is generated by the Issuer bank. It has the same look and feel of the physical cheque. The data relevant to the cheque such as cheque number, bank number and amount is written into the smart contract on the blockchain by calling initCheque function [10]. The Issuer Bank transfers the equivalent amount of crypto tokens associated with the cheque to the payer's address. By transferring the crypto token, the Issuer bank assures the payment.

(B) The payer authorizes payment by signing an electronic cheque using the mobile Application. The date and electronic signature are written into the smart contract on the blockchain by using the signCheque function [10]. In addition to that physical signature of the payer is embedded into the cheque image to give the same look and feel.

(C) The payer transfers the signed cheque image to the payee by using the Mobile application and call transferCheque function [10] of the smart contract. It transfers the cheque to the payee. When the electronic cheque is transferred to a payee, the payer transfers the equivalent amount of crypto tokens associated with the cheque to the payee's address. By transferring the crypto token, the payer assures the payment on the mentioned date.

(D) The payee claims the payment by presenting the signed cheque to the issuer bank on the relevant date by calling the depositCheque function [10]. When the payee executes the depositCheque function, an equivalent amount of crypto tokens associated with the cheque transfer from the payee to the issuer bank. It verifies the authenticity, and the Issuer Bank releases the funds to the payee via an inter-banking transfer.

(E) In the case of a cash cheque, the payee can also transfer the signed cheque to the third party. Then the equivalent amount of crypto tokens associated with the cheque transfer from the payee to the third party with the signed cheque image. Then the third party claims the payment by presenting the signed cheque to the Issuer Bank on the relevant date as mentioned in step 4. The cheque can be transferred to any number of third parties before it deposits to the relevant bank.

Figure 2 shows the crypto token transfer between the issuer bank, the payer, the payee and the third party. In order to complete the transaction, the payer must deposit the funds in his account on the settlement date.

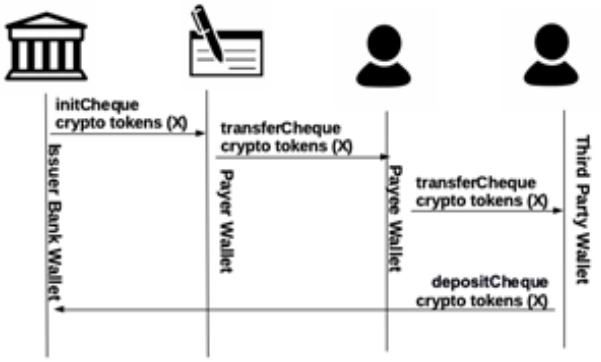

Figure 2. Crypto Token Transfer Sequence

D Transaction Settlement

In order to facilitate the settlement, the payer must deposit the funds in his account on the settlement date. If a payer does not have sufficient funds in his account on the settlement date, the Issuer Bank calls the settlementDelay smart contract function [10].

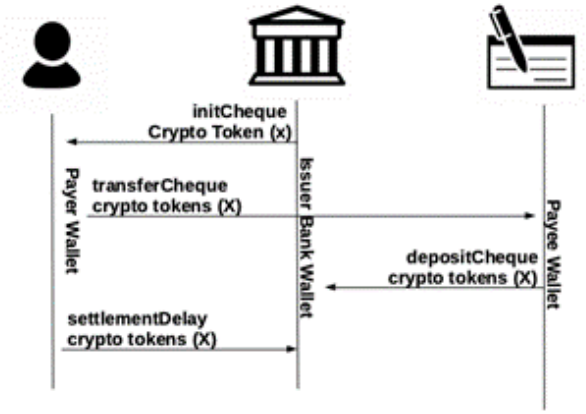

Figure 3. Settlement Delay

As shown in the figure 3 **settlementDelay** function transfers crypto tokens equal to the cheque amount from the payer account to the issuer bank account.
The following status may occur after calling the *settlementDelay* function:

(A) The crypto-token amount of the payer is zero. If he/she has some cheques to be deposited, he/she cannot do it until he/she purchases crypto token from the bank or until he/she receives some cheques. The bank can charge a fee for such settlement delays.

(B) The crypto-token amount of payer is positive. If he/she has some cheques to be deposited, he/she can deposit cheques less than or equal to the crypto token balance.

(C) The payer must settle the account balance and purchase a crypto token to deposit the other cheques. The Issuer bank can charge the fee for settlement delay.

(D) The crypto-token amount of payer is negative. The negative figure shows insufficient funds, and the payer cannot deposit any cheque if he/she has a negative balance. In addition, interest can be charged for such negative balance and settlement delays.

These actions block the payer's pending funds until the payer physically settle the funds. If he/she settles the funds, the equivalent amount of crypto tokens is transferred back to the payer's address. The bank can charge a fee for such settlement delays. These actions encourage the payer to deposit sufficient funds on the settlement date.
As previously mentioned, The payee can transfer the cash cheque to the other person or keep it until the settlement date. The present owner of the cheque can deposit the cheque, and it terminates the life cycle of the cheque.

IV EVALUATION

This protocol was evaluated by implementing a Proof Of Concept (POC) application. The POC application was evaluated under various possible use cases. Five such use cases are described in the following section.

A Case – 1

Amal issues a cheque to a Nimal equal to Rs. 5000/=. Amal deposits Rs. 5000/= to settle this cheque. Amal receives 5000 crypto tokens from the bank for his cheque, and he transfers these 5000 tokens to Nimal with the cheque. Amal has zero crypto tokens at this stage, and Nimal has 5000 crypto tokens.
Nimal deposits the cheque to the bank with these 5000 tokens and claims the money. Since Amal deposits Rs. 5000/= for his cheque, the bank does not take any action on Amal's account.

B Case – 2

Amal issues a cash cheque to a Nimal equal to Rs. 5000/=. Nimal transfers it to Saman, and he deposits it. Amal deposits Rs. 5000/= to settle this cheque.
Amal receives 5000 crypto tokens from the bank for his cheque, and he transfers these 5000 tokens to Nimal with the cheque. Nimal transfers the cheque to Saman with 5000 tokens. Thus Saman has 5000 tokens, and he can deposit the cheque to the Bank. Since Amal deposits Rs. 5000/= for his cheque, the bank does not take any action on Amal's account.

C Case – 3

Amal issues two cheques to Nimal and Kamal equal to Rs. 1000/= and Rs. 2000/=. Amal deposits Rs. 3000/= to settle these cheques.
According to the protocol, Amal receives 3000 crypto tokens from his bank at the initial stage. When he transfers the Rs. 1000/= cheque to Nimal, 1000 crypto tokens are transferred to Nimal. When he transfers the Rs. 2000/= cheque to Kamal, 2000 crypto tokens are transferred to Kamal. At this stage, Amal has zero crypto tokens, Nimal has 1000 crypto tokens, and Kamal has 2000 crypto tokens. When Nimal deposits Rs.1000/= cheque, he transfers 1000 crypto tokens to the bank. When Kamal deposits Rs.2000/= cheque, he transfers 2000 crypto tokens to the bank. Thus the bank receives 3000 crypto tokens, and both people receive the money. Since Amal deposits money on time, the bank does not claim any crypto token from Amal.

D Case – 4

Amal issues two cheques to Nimal and Kamal equal to Rs. 1000/= and Rs. 2000/= as described in case 3. However, in this case, Amal fails to deposit Rs. 3000/= to settle these cheques.
Initially, Amal receives 3000 crypto tokens for his cheques, and he transfers all 3000 crypto tokens to Nimal and Kamal. Thus he has zero tokens, as described in the previous case.
Nimal deposits Rs.1000/= cheque and transfers 1000 crypto tokens to the bank. Kamal deposits Rs.2000/= cheque and transfers 2000 crypto tokens to the bank.
Thus Nimal and Kamal received their money. Since Amal fails to deposit Rs. 3000/=, the bank claims 3000 crypto tokens from Amal. Then his crypto token balance becomes -3000. At this stage, let us assume Amal receives two cheques equal to Rs. 5000/= and Rs. 2000/=. Then he gets 7000 crypto tokens, and his crypto token balance is 4000 (7000-3000). Now he can deposit Rs. 2000/= cheque but cannot deposit Rs. 5000/= cheque. In order to deposit it, he must settle Rs. 3000/= and purchase 3000 crypto tokens. The bank can charge a commission for this delay.

E Case – 5

Amal issues a cheque to a Nimal equal to Rs. 2000/=. Amal receives a cheque from Saman equal to Rs. 5000/=. Amal fails to deposit Rs. 2000/= to settle his cheque.
Amal receives 2000 crypto tokens from the bank for his cheque, and he receives 5000 crypto tokens from Saman. Thus he has 7000 crypto tokens. When he transfers Rs.2000/= cheque to Nimal 2000 crypto tokens are transferred to Nimal. Thus Amal has 5000 crypto tokens. Since he fails to deposit Rs. 2000/= for his cheque, the bank takes 2000 crypto tokens from his account. Thus he has 3000 crypto tokens, and he cannot deposit Rs. 5000/= cheque. Either he has to purchase 2000 crypto tokens by depositing Rs 2000/=, or he should receive a cheque greater than Rs. 2000/= from someone else.

V FEATURES

Feature comparison of the proposed solution and physical cheque system is given in Table 1.

Table 1 : Features Comparison

Physical Cheques	**Proposed Solution**
Printed Cheque Book is used	Not necessary to issue a cheque book
Physical signature is applied	Physical and Electronic signatures are used
Signed on the paper	Signed on the device screen
Support inter-bank cheque clearance	Support inter-bank cheque clearance
Scanned the physical cheque and submit the cheque image to clearance	Cheque image is generated and directly submitted to clearance
Clearance may delayed	Immediate clearance
Issue cheque with future dates (dated cheques)	Issue cheques with future dates
Banks are not aware about dated cheques	Banks knows the volume of dated cheques
Cheque may dishonor	Cheque dishonoring rate can be reduced
Possible to issue cash cheque and transfer to third parties	Cash cheque is supported and electronically transfer to third parties
Banks are not aware such transfer	Banks can trace the transfer
Manually archive for dispute resolutions	Electronically save on a Blockchain for dispute resolution

VI CONCLUSION

In the existing paper-based cheque system, the Issuer Bank has no information regarding the volume of dated cheques issued by a particular customer. With our protocol, the Issuer Bank knows it, and therefore it can maintain the maximum limit of such cheques. It reduces the cheque dishonoring rate. The overhead of cheque clearing, such as scanning of the paper cheque, can be eliminated with this protocol. Thus the bank can save the cheque clearing cost. In addition, the bank can offer a credit facility to their customers based on their credibility and earn extra income. With this protocol, the customer should not need to visit a bank and manually fill a deposit slip. Thus it improves customer convenience. This protocol can coexist with the paper-based cheque system.

REFERENCES

[1] M. Tompkins, V. Galociova, Canadian Payment Methods and Trends, Payments Canada, 2018, https://www.payments.ca/sites/default/files/12-Dec-18/paymentscanada_trendsreport2018_13_0.pdf

[2] R. Balan, N. Ramasubbu, K. Prakobphol, N. Christin, J. Hong, MFERIO: the design and evaluation of a peer-to-peer mobile payment system, in Proceedings of the 7th international conference on Mobile systems, applications, and services, 2009, pp. 291–304.

[3] L. Ferdinando, InaInnovative Idea for Cheque Clearing Process through Mobile Device, DailyFT, 2016, http://www.ft.lk/article/536956/Innovative-idea-for-cheque-clearing-process-through-mobile-device

[4] E. Bandara, V. Keong Ng, K. De Zoysa, N. Fernando, MYSTIKO: Blockchain Meets Big Data, 2018, IEEE International Conference on Big Data, pp. 3024-3032

[5] P. Wolfgang, T. Axel, Blockchain and Smart Contracts Technologies, research issues and applications, University of Augsburg, 2018

[6] White Paper Of Blockchain Cheque, Blockchain-Based Cash Cheque System, BlockChain Cheque Inc., 2018, http://www.bcheque.com/file/whitepaper_en.pdf

[7] Kabra N, Bhattacharya P, Tanwar, S, Tyagi S, MudraChain: Blockchain-Based Framework for Automated Cheque Clearance in Financial Institutions, Future Generation Computer Systems, 2019

[8] K. Karunanayake, K. De Zoysa, S. Muftic, Mobile ATM for developing countries, Proceedings of the 3rd international workshop on Mobility in the evolving internet architecture, 2008, pp. 25-30

[9] Payments Bulletin, First Quarter, The Central Bank of Sri Lanka (CBSL), 2019, https://www.cbsl.gov.lk/en/publications/other-publications/statistical-publications/payments-bulletin

[10] K De Zoysa, A source code of the reference implementation of the Cheque Settlement smart contract, online available at https://github.com/kasundezoysa/solidity/blob/maste/eCheque

AUTHOR BIOGRAPHY

Kasun obtained his BSc in Computer Science from University of Colombo, Sri Lanka in 1998. He obtained his Ph.D. in the area of Information Security from Stockholm University in 2003. After a brief period of post-doctoral work at the George Washington University, USA, he joined the University of Colombo School of Computing (UCSC), Sri Lanka in 2003. At present, he works as a senior lecturer at UCSC, Co-ordinator for forensic investigation unit attached to UCSC and academic coordinator of Master of Cybersecurity Program at UCSC.