Tribhuvan University

Institute of Science and Technology

SHADOW COINS: INCLUDING CENTRAL BANKS IN CRYPTOCURRENCY ECOSYSTEM

Dissertation

Submitted to:

Central Department of Computer Science and Information Technology

Tribhuvan University, Kirtipur

Kathmandu, Nepal

In partial fulfillment of the requirements

for the Master's Degree in Computer Science and Information Technology

By

Saurav Kumar Mishra

7th February, 2019

Tribhuvan University

Institute of Science and Technology

Central Department of Computer Science and Information Technology

Student's Declaration

I hereby declare that I am the only author of this work and that no sources other than the listed here have been used in this work. No part of this thesis is reproducible without the written authority of the author.

.....

Saurav Kumar Mishra

Date: 7th February, 2019

Tribhuvan University

Institute of Science and Technology

Central Department of Computer Science and Information Technology

Supervisor's Recommendation

I hereby recommend that this dissertation prepared under my supervision by **Mr. Saurav Kumar Mishra** entitled **"Shadow Coin: Including Central Banks in Cryptocurrency Ecosystem"** in partial fulfilment of the requirements for the degree of M.Sc. in Computer Science and Information Technology be processed for the evaluation.

.....

Mr. Bikash Balami

Central Department of Computer

Science and Information Technology

Tribhuvan University, Nepal

Date: 7th February, 2019

Tribhuvan University

Institute of Science and Technology

Central Department of Computer Science and Information Technology

LETTER OF APPROVAL

We certify that we have read this dissertation and in our opinion it is satisfactory in the scope and quality as a dissertation in the partial fulfillment for the requirement of Master's Degree in Computer Science and Information Technology.

Evaluation Committee

_____

Mr. Nawaraj Poudel

Head of Department

Central Department of Computer

Science and Information Technology

_____

Mr. Bikash Balami

Supervisor

Central Department of Computer

Science and Information Technology

_____

External Examiner

_____

Internal Examiner

Date: 7th February, 2019

ACKNOWLEDGEMENTS

First and foremost, I have to thank my research supervisor, Mr. Bikash Balami. Without his assistance and dedicated involvement in every step throughout the process, this research work would have never been accomplished. I would like to thank you very much for your support and understanding.

I express my warm thanks to everyone who supported me throughout the course of this M.Sc.CSIT research work. I am thankful for their inspiring guidance, invaluably constructive criticism and friendly advice during the research work. I am sincerely grateful to them for sharing their truthful and illuminating views on a number of issues related to the research.

I like to acknowledge CoinDesk datasets and WorldBank database for providing open source dataset used for this experiment.

I express sincere thanks to all the faculty members and staffs of Central Department of Computer Science and Information Technology who helped me in any possible way to complete the work. I cannot remain silent without mentioning Mr. Bishwa Nath Lal Karn who helped me at every aspect of the thesis.

A special thanks goes to Ms. Rakhi Thakur for her words of motivation and support.

Saurav Kumar Mishra

7th February, 2019

ABSTRACT

The increasing popularity of cryptographic currencies, such as Bitcoin, has led to an interest from central banks in the possibility of issuing their own cryptographic currencies. RSCoin is the most noteworthy effort to include banks in Cryptocurrency economy till date. It is a technology developed in initiation of Bank of England in order to introduce central banks in the cryptocurrency ecosystem.

In this work, the RSCoin implementation was extended by introducing Shadow Coins to test the feasibility of the system in respect to the existing payment solutions, which was specified but not implemented in the original proposal. Shadow Coining is a way to incorporate Cryptocurrencies in the Banking system issuing shadow coin in its central ledger for another currency it stores as guarantee. Shadow coins work as the replica of existing coins such as Bitcoin without altering its value enabling the current Cryptocurrency market to thrive as it is also allowing them to be used for day to day use with very small transactions time. Experiments were conducted to study the performance of the central bank and the comparative cost analysis was carried out. The results confirmed the suitability of Shadow Coins as the basis for a centrally banked cryptographic currency model.

Keywords: Cryptocurrency, RSCoin, Central Bank Digital Currency

Table of Contents

List of Figures

List of Tables

List of Abbreviations

AML	Anti Money Laundering
CDBC	Central Bank Digital Currency
CFA	Financial Community of Africa (Communate Financiere d'Afrique)
CFT	Combating the Financing of Terrorism
DLT	Distributed Ledger Technology
DTC	Digital Trade Coin
Fintech	Technological developments that are relevant to financial markets.
KYC	Know Your Customer
ODBC	Open Database Connectivity
PoW	Proof of Work
USC	Utility Settlement Coin
XRP	Term referring to Ripple Coin

Chapter 1
INTRODUCTION

1.1 Background

Cryptocurrencies have found considerable success as an alternative trustworthy form of money. Despite a number of advantages over traditional fiat currencies as well as other centrally served digital currencies, there still is a sense of uncertainty on its use as mainstream currency. It is yet to be used as real currency than as commodity or asset. Current cryptocurrencies, starting with Bitcoin, build a decentralized blockchain-based transaction ledger. Such decentralization has benefits, such as independence from national political control, but also significant limitations in terms of computational costs and scalability. [2,3]

The cryptocurrency exchange market is already in the billions of dollars a day and is tripling yearly. At the same time, the number of cryptocurrencies is growing exponentially. There are now close to 1400 cryptocurrencies that come in various flavors. Some of these are ostensibly backed in one form or another and are intended for a variety of purposes. This level of success has caused financial institutions, regulatory bodies and governments to examine the potential impacts of cryptographic currency schemes. The European Central Bank anticipates such schemes are likely to “impact on monetary policy and price stability” whilst concerns have been raised that they are not bound by International Monetary Fund regulation. However, it is also clear that cryptographic currencies offer potential opportunities for financial institutions. Another reason why the popularity of private e-currencies grew so fast was the speculation possibilities it brought with them. Nowadays, most trades in private e-currencies are conducted for speculative reasons and success stories lead to more people engaging in this speculative behavior. The US Federal Reserve has forecasted that they may provide “faster, more secure and more efficient payment systems” whilst the Bank of England has embarked upon an innovation agenda focused on them. It is to be expected that countries and banks will release and maintain their own currencies. [5,25]

Governments are challenged on how to react on the fast growth and rapid expansion of e-currency. The rapid rise of cryptocurrencies has elicited a range of responses from central banks and governments, from trying to co-opt the changes to their advantage to resisting certain developments for fear of stoking monetary and financial instability. [22]

Attempts to bring Cryptocurrencies within the banking fold have been based on the idea of creating an alternate currency to the already existing Cryptocurrency Pool. It is now technologically feasible for a central bank to set up electronic deposit accounts for all of a country's residents, with blockchain technology making it easy for the central bank to manage a multitude of such accounts. [23, 24]

RSCoin was proposed against this backdrop by Danezis and Meiklejohn to address the scalability issues present in existing cryptographic currencies. Bitcoin, for example, has a peak throughput of 7 transactions per second and faces significant challenges in raising this rate. This is in comparison to Visa which can handle a peak of 56,000 transaction per second. RSCoin sets out a cryptographic currency scheme where monetary supply and generation of the transaction ledger is centralized. In RSCoin, the mintettes entity validates and processes transactions before combining them and presenting them to the "central bank" entity to generate the centralized transactional ledger. This negates the need for Proof-of-Work (PoW) computations which are the cause of performance bottlenecks in systems such as Bitcoin. Danezis and Meiklejohn built a test implementation of RSCoin to measure the latency and throughput of transactions from clients to mintettes. [9]

None of these systems, however, had major uptake as a result of credit card transactions becoming the de-facto payment method of internet electronic commerce. Since discarding the already existing Cryptocurrencies altogether to adopt a new one is not possible due to the market value they have acquired, new currency introduced by Central banks will only create a competition with the existing ones. [16, 17]

1.2 Aims and Objectives

This thesis aims in providing a unique solution to current dilemma of introducing centrally banked cryptocurrency by introducing a platform for all possible currencies to coexist. The principle objective of this study is to compare profitability of current currency settlement with the proposed system specifically VISA, MASTERCARD, and Remittance Agencies in terms of a metric ratio.

In particular, the following objectives are considered:

1. To implement Shadow Coin based on RSCoin architecture
2. To analyze the feasibility of this system in terms of profitability, and comparative cost for users and banks with that of VISA MasterCard and remittance

1.3 Scope

Shadow coin uses a unique idea of asset backed currency issued by the central bank for inter-currency transactions. A shadow of a currency coin is issued which can be controlled by bank by its blockchain ledger for the original currency it stores as guarantee. The shadowing information is stored as metadata as the colored coins. This method will make sure the transitioning of Central bank's into Cryptocurrency ecosystem without challenging the existing digital currency market and create a platform for both the parties to coexist. It is based on RSCoin.

In this thesis, a novel concept of using a common platform of Shadow Coin for existing cryptocurrencies is studied along with its feasibility in terms of profit it may generate for the banks so that they will be inclined to pursue such endeavor. In Shadow Coin cryptocurrency framework, central banks maintain complete control over the monetary supply but rely on a distributed set of authorities, or mintettes, to prevent double-spending. It works by keeping the existing coins as leverage/guarantee and issuing a shadow coin of same value to the user whose transactions are controlled by the bank and upon request to bank producing the shadow coin, the original coin is given back.

In this thesis, the viability of such a system is tested for profitability to banks by comparing the profits made by VISA MasterCard as well as International remitters.

1.4 Structure of the Thesis

This report is split into five chapters. Introduction of the thesis along with its objectives and scope are discussed in chapter 1. Previous works related to this thesis is discussed in chapter 2. Theoretical background of the research is introduced and past research undertaken into cryptographic currencies are discussed in this chapter. Research Methodology is discussed in chapter 3. Details of the datasets used and the proposed framework along with the tools used for implementation is discussed and understood in this chapter. Chapter 4 details the result of the experiment in different datasets. Results are also discussed for their correctness and acceptance. The concluding chapter 5 entitled Conclusion concludes the chapter explaining what have been done in the thesis and how it could be used.

Chapter 2

LITERATURE REVIEW

2.1 Background

Cryptocurrencies are a special case of virtual or digital currencies**.** While digital currencies are defined by their implementation on a computer system, cryptocurrencies additionally use cryptographic functions in the process of authorizing and verifying transactions. In doing so, they are able to dispense with central counterparties while providing non-discriminatory public access and security against fraudulent spending. Cryptocurrencies have gained increasing prominence in recent years. Not only have they become a topic in the mainstream media, but also traditional financial institutions have moved to define their reaction to this new phenomenon. While central banks around the world have set up their own research teams on this topic, traditional financial institutions try to expand their business into this space. [21]

Due to high volatility, Bitcoin and other cryptocurrencies are not generally accepted yet but this may change in the future. So far, strong fluctuations in the purchasing power of cryptocurrencies make it problematic to use them as a medium of exchange for a significant amount of people, because buyers and sellers must foresee, at least in the short term, whether a trade from today is still profitable, cost-covering or loss-making tomorrow. Considering international trade in a global economy, fluctuations as such in the purchasing power of money vary for several kinds of goods and thus are the normal case. Hence, it is a matter of subjective valuation, if and when the fluctuations of cryptocurrencies are acceptable for a substantial number of users to choose it as an exchange media. When the crypto gold rush ends, in which most people buy and sell cryptocurrencies solely to strive for profit, then fluctuations are likely to abate and the actual use case for cryptocurrencies as money may gain momentum – especially if enough people are unsatisfied with the existing monetary regime. [3, 4]

2.2 Existing Developments and Implementations

There have been attempts to simplify the crypto exchange by a number of means. Some Notable Projects are as follows:

2.2.1 FedCoin

FedCoin is a hybrid model where the central bank primarily controls money supply, while it relies on a decentralized set of authorized nodes (Nodes) to verify transactions and prevent double spending. Nodes are commercial banks. Under this regime, the expensive proof-of-work required by a cryptocurrency like Bitcoin can be avoided, while the permissioned ledger will dramatically reduce settlement latency. [19]

Fedcoin begins with a blockchain created by the Federal Reserve, the public monetary authority in control of the production of money and formulation of monetary policy. The Fed would bless this ledger with certain properties: only the Fed would have authority to create and destroy ledger entries, the Fed uses its creation and destruction ability to provide conversion between both its liabilities (the dollar and the Fedcoin) at a ratio of 1 to 1, and all Fedcoin transactions are announced to a decentralized network of nodes for verification making non-Fed nodes responsible for the integrity of the ledger. Should a paper note or reserve entry be destroyed, a Fedcoin would be instantiated, and vice versa. [19]

The goal is to create a stable (less price volatility) and dependable cryptocurrency that delivers the practical advantages of bitcoin even if this means involving the central government and abandoning the Libertarian principles that many believe underlay Bitcoin’s creation. [Koning]

Price stability is achieved by tying the value of Fedcoin to the US dollar. Fedcoin would have a fixed one-to-one exchange rate with the US dollar. The Fedcoin proposal involves two-way convertibility, but the Federal Reserve would control both the creation and destruction of Fedcoin. [16]

2.2.2 CadCoin

Project Jasper is an ongoing collaboration between R3 and six private Canadian banks, Payments Canada and the Bank of Canada that began to explore the possibility of clearing and settling large value payments using distributed ledger technology (DLT). Phase one involved a simulation of a

funds transfer that will be implemented in phase two, with the goal to conduct a set of payments between participants using DLT. The simulation begins with participants pledging cash collateral into a special pooled account held by the Bank of Canada. This is done via payments to the Bank of Canada. The Bank of Canada then issues an equal amount of a central bank issued digital asset, referred to in the presentation as CAD-coin, onto the distributed ledger and sends each bank an amount of CAD-coin equal to the amount of cash they pledged. Banks can then send payments of CAD-coin to each other in real time to meet the payment obligations that they have agreed to have settled on this platform and may also send payments back to the Bank of Canada in order to "cash out" and convert CAD-coin back into Canadian dollars. [20]

2.2.3 Digital Trade Coin

Digital trade coins (DTCs) are the asset-backed concept currently under development at MIT. It outlines an approach to building a consortium of sponsors, who contribute real assets, a narrow bank handling financial transactions involving fiat currencies, and an administrator, who issues the corresponding digital token in exchange for fiat payments and makes fiat payments in exchange for digital tokens. In short, distributed ledger technology is applied to give a new lease of life to the old notion of a sound asset-backed currency, and to use this currency as a transactional tool for a large pool of potential users, including small and medium enterprises and individuals. We intend to build a currency, which encourages legitimate commerce, but makes illegal activities difficult. At the moment there is no working prototype for the DTC. [18]

2.2.4 CDBC

Interest in CBDC has been ignited by two unrelated factors—the introduction of Bitcoin and a persistence of negative interest rates in some developed countries.

Currently, there are three approaches to creating CBDC on a large scale:

1. Economic agents, from enterprises to private individuals, can be given accounts with central banks. However, in this case, central banks would have to execute know your customer (KYC) and anti-money laundering (AML) functions, tasks which they are not equipped to perform. Besides, under duress, rational economic agents might abandon their commercial bank accounts and move their funds to central bank accounts, thus massively destabilizing the entire financial system. [21]

2. Inspired by Bitcoin, CBDC can be issued as a token on an unpermissioned distributed ledger, whose integrity is maintained by designated notaries receiving payments for their services. Given that notary efforts do not require mining and hence are significantly cheaper and faster than that of Bitcoin miners, this construct is scalable and can satisfy needs of the whole economy. Users are pseudo-anonymous, since they are represented by their public keys. Since at any moment there is an immutable record showing the balance of every public key, it is possible to de-anonymize transactions by using various inversion techniques applied to their recorded transactions, thus maintaining AML requirements. [8]

3. A central bank can issue numbered and blind signed currency units onto a distributed ledger, whose trust is maintained either by designated notaries or by the bank itself. In this case, it would have to rely on commercial banks, directly or indirectly, for satisfying the KYC/AML requirements. [8, 21]

2.2.5 USC

The CBDC is technically possible but politically complicated. Hence several alternatives have been proposed. One promising venue is USC (Utility Settlement Coin), which is developed by a consortium of banks and a fintech startup called Clearmatics.1 Initially, USC can be an internal token for a consortium of participating banks. These coins have to be fully collateralized by electronic cash balances of these banks, which are held by the Central Bank itself. Eventually, these coins can be circulated among a larger group of participants. [18]

2.2.6 RSCoin

RSCoin is a cryptocurrency framework in which central banks maintain complete control over the monetary supply, but rely on a distributed set of authorities, or mintettes, to prevent double-spending. While monetary policy is centralized, RSCoin still provides strong transparency and auditability guarantees. There are benefits of a modest degree of centralization, such as the elimination of wasteful hashing. [1]

RSCoin is an alternative approach to solving the scalability issues present within the Bitcoin protocol. The main difference is that it is predicated on a central bank issuing currency rather than currency generated through PoW computations. This allows for the centralization of “generation

of the monetary supply and the constitution of the transaction ledger". It also removes the need for computationally expensive and wasteful PoW calculations to generate monetary supply and avoid double-spending attacks. There are two logical elements to the design of RSCoin - the mintettes and the central bank. [1, 9]

Mintettes are synonymous with retail banks and it was envisioned that mintettes would be operated by them should the RSCoin framework be introduced to support a centrally banked cryptographic currency. Mintettes "collect transactions from users and collate them into blocks", similar to other cryptographic currencies. However rather than completing PoW activity each mintette is "simply authorized by the central bank to collect transactions". [9]

The operational role of the central bank in the RSCoin framework is as follows:

1. Issue currency.
2. Authorize mintettes to process transactions on a per period basis.
3. Receive lower-level blocks, validate them and combine them to generate higher level blocks which seal all committed transactions during a period in a blockchain.

2.3 Approaches Taken by Different Central Banks and Governments

The approaches of governments and central banks to permitting and/or regulating nonofficial cryptocurrencies span a wide spectrum, with individual countries often changing their positions back and forth in response to consumer demand and concerns about financial stability implications. A number of central banks are at various stages of looking into the feasibility and desirability of issuing CBDCs. The status of some key central banks is listed below. [25, 26]

- **In operation***:* Tunisia issued the first CBDC, an e-Dinar designed as a virtual account, as early as 2010. It has now been superseded by a blockchain-based centralized digital currency (using the Monetas digital platform) that also functions as a payments system. In 2015, Ecuador introduced a centralized payment system backed by a digital currency but, since the system failed to attract a significant number of users or volume of payments, is deactivating the system in April 2018.

- **Preparation for implementation/groundwork in progress:** China has successfully tested a block-chain based digital notes transaction platform and is developing a digital currency known as the Digital Currency for Electronic Payment. A consortium of Japanese banks plans to introduce a digital currency (J Coin) in time for the 2020 Tokyo Olympics. This project has the approval of the Bank of Japan, which has indicated that it is not considering issuing a digital currency by itself. The Bank of Canada has a joint initiative with the national payment system operator to develop a DLT-based settlement asset for wholesale transactions (Project Jasper). The Monetary Authority of Singapore is developing a tokenized version of the Singapore dollar on an Ethereum-based blockchain (Project Ubin). Senegal intends to issue an electronic version of the eCFA that will co-exist with physical CFA. This will be issued by a regional bank and will not rely on blockchain technology.

- **Evaluating pros and cons, with no specific plans to issue digital currency***:* None of the major advanced economy central banks have announced specific plans to issue CBDCs. Some officials of the Bank of Japan, Bank of Canada, Bank of England, European Central Bank, and the Federal Reserve have indicated they are evaluating the pros and cons of CBDCs, although none of them appear to be giving this serious consideration.

- **Active regulation:** Canada and Japan have explicit laws concerning the trading and use of cryptocurrencies. The U.S. considers Bitcoin and other cryptocurrencies as financial assets that are subject to tax laws as well as regulations concerning anti money laundering and combating of financing of terrorism (AML/CFT).

- **Soft/hard bans on cryptocurrencies*:*** India's central bank, the Reserve Bank of India (RBI), has not provided authorization for any of the institutions it regulates to trade in or conduct business using cryptocurrencies. In April 2018, the RBI prohibited banks, financial institutions, and other regulated entities from dealing in virtual currencies. Korea's regulators have taken a dim view of cryptocurrencies, although they have not banned them outright. China banned domestic Bitcoin exchanges when it was trying to restrict speculative capital outflows in 2017, and has subsequently taken steps to block access to all cryptocurrency exchanges. China has also more recently banned domestic initial coin offerings (ICOs) and prohibited individuals and institutions from participating in them.

- **Passive tolerance:** A majority of countries are in this category, not banning cryptocurrencies but discouraging their use by financial institutions and, in many cases, not clarifying the legal status of such currencies even as means of payment.

- **Governments/central banks issuing their own cryptocurrencies:** Venezuela's government issued the first official cryptocurrency, the petro, in February 2018. In April 2018, Venezuela declared the petro to be legal tender. The petro's value is in principle backed by Venezuela's oil reserves and the cryptocurrency's issuance was intended to bolster public finances and evade financial sanctions imposed against Venezuela by the U.S. and other countries. Russia has indicated that it will issue a CryptoRuble, mainly for the latter reason. Cambodia, Estonia, and the Republic of the Marshall Islands have announced plans to issue official cryptocurrencies.

Chapter 3

Methodology

3.1 Principle

The aim of this experiment is to study how the trend of cryptocurrency operating cost changed through the course of time during past two years when the crypto market was considered extremely volatile and analyze if the shadow coin model is feasible enough under such harsh economic fluctuations.

The idea behind the algorithm is to find the incentive cost of banking system to keep a threshold of digital coin capital in the central banking system. Since central bank cannot force the players in the digital currency market to adopt its blockchain, the only remaining option is to compete with them. So it can act as a trusted intermediary when required.

The methodology applied can be summed up briefly as follows:

1. Take Transaction Volume of n Digital Currencies in the system as Shadow Amount.
2. Distribute the Sum to N number of users in a random fashion.
3. Run Transactions with market-bounds and calculate charges incurred per transaction.
4. Compare the transaction charges with VISA and Master Card Charges

This scope of work was split into three areas:

- Design and build of Shadow Coin model for central bank functionality
- Creating Daily Transaction Sets of each Cryptocurrency
- Making Fee Decisions as per the actual Fee transferred as well as coin generation rewards

3.2 Data Sources

The dataset for this research is taken from open source data available at coinmetrics.io. With dataset were collected for 10 different coins for a time period of 8 Quarters of 2016 and 2017.For the Visa/Master Card, data were produced as per their quarterly profit and charges data available. Merchant fees are taken from publication of reserve bank of Australia. Values for remittance were used to compare inter country currency flow, and were also compared with the different coin's profit because the coin addresses are boundary less.

The real world data mentioned above were taken from following sources:

https://coinmetrics.io/data-downloads/

http://remittanceprices.worldbank.org

3.3 Dataset

Three different types of dataset have been used in this study. Namely,

1. Cryptocurrency Data of 10 Cryptocurrency Coins
2. Merchant Fees data of Visa and MasterCard
3. Remittance flow Data of inter country money flow

The Major Digital Currencies as per their market Capitalization Selected for transaction:

1. BitCoin
2. Dash
3. DigiByte
4. DogeCoin
5. Ethereum
6. LiteCoin
7. Monero
8. Ripple
9. VertCoin
10. Zcash

3.4 Data Preprocessing

The available data was preprocessed to fit in the requirement of the study by Data Truncation and Data Merge. The charges for every transaction was taken as main reference. The simulation was carried out so as to conciliate the data values in data set. The data was modeled in the timespan of quarters of year so as to make the accurate comparison with Master/Visa and Remittance which are also published with quarterly average. Trade Volume Based Randomization of transactions were done using Normal Distribution keeping number of transactions and total transaction amount equal to the daily transaction values of the coins selected.

Following Considerations were made while quarrying Data:

1. Daily on-chain transaction volume is calculated as the sum of all transaction outputs belonging to the blocks mined on the given day.
2. Transaction count figure doesn't include coinbase and coinstake transactions.
3. Active addresses is the number of unique sending and receiving addresses participating in transactions on the given day. For Monero, an upper bound for this metric (calculated as sum of input and output count) is reported, as the precise value is unknowable due to stealth addresses technology.
4. Payment count for coins is defined as sum of outputs' count minus one for each transaction. It is assumed that transaction with N outputs pays to N – 1 addresses and the last N-th output is change. Transactions with only one output do not contribute to payment count, as they are likely to be a self-churn.
5. Payment count for Ripple is the amount of XRP token transfers. Ripple data includes only transactions of Payment type that transfer XRP tokens.
6. Zcash figures for on-chain volume and transaction count reflect data collected for transparent transactions only. Transaction volume figures in reality are a little higher than the estimate presented here, and NVT and exchange to transaction value lower.
7. Monero transaction volume is impossible to calculate due to RingCT which hides transaction amounts.

3.5 Data Snippet

- Data Snippet for Cryptocurrency

Date	**TxVolume**	**TxCount**	**Marketcap**	**Price**	**ExchangeVolume**
01/01/2016	TsVolume 1	TxCount 1	Marketcap 1	Price 1	ExchangeVolume 1
---	---	---	---	---	---
31/12/2017	TxVolume n	TxCount n	Marketcap n	Price n	ExchangeVolume n

- Data Snippet for VISA/Master Card

Date	**Payment Module**	**TxCount**	**Charges for Credit Cards**	**Charges for Debit Cards**
01/01/2016	VISA/Master Card	TxCount 1	CreditRate 1	DebitRate 1
---	---	---	---	---
31/12/2017	VISA/Master Card	TxCount n	CreditRate n	DebitRate n

- Data Snippet for Remittance

Date	**Payment Module**	**TxCount**	**Rate: Sending Country**	**Rate: Receiving Country**
01/01/2016	Remittance	TxCount 1	SendingtRate 1	ReceivingCharges 1
---	---	---	---	---
31/12/2017	Remittance	TxCount n	SendingRate n	ReceivingCharges n

3.6 Environments

The Architecture for the simulation of data is referenced upon RSCoin model. The experimental setup of the original paper, was modified for the tests were run on localhost on Intel CORE i5 7th generation Machine with 4 GB RAM Computer because of the minimal resource requirements.

The Simulations were run in Virtual Environment using Python Language. Python 3.6 was used to build and run the model. The choice of development language was based on its ease of use and dynamic compilation. The choice of Python as a development language is well suited to rapid prototyping as a result of the rich repository of add-on modules available under open source licenses that can be used as building blocks to accelerate development. This was particularly relevant for RSCoin where the use of client / server communications and cryptographic primitives was required. Since the goal of the thesis was to extend the existing implementation, this rationale continued to apply.

Since the existing RSCoin artefact already implemented the scalability and security functionality, shadow coining did not require to validate those properties between clients and mintettes. The Network parameters were muted because the objective of the thesis was in different prototype than the RSCoin paper and significant scope of build activity was focused on to meet data processing objectives of this thesis. Hence the network latency and performance overhead were looked over. For Encryption, RSA algorithm was used.

The Data processing suffered a performance delay due to Python's dynamic nature. During the initial run of the experiments, Unexpected Program exits were the caused by fault as a result of exhausting available physical memory. Total Number of rows were in millions. This situation was remedied by using the higher specification. Database corrections were made to use Microsoft Access Database using Microsoft ODBC Driver. The Result set was copied in a spreadsheet and analytics was done using the statistical tools in Excel.

3.7 Model and Algorithm

The RSCoin Model (Appendix 7) has been modified to run in a single node machine. The Changes in the system are as follows:

1. Elimination of Network Mining
2. Normalized Coin Distribution

The message flows in the logical architecture of the Shadow Coin implementation are as follows:

1. Clients execute the PC to confirm a transaction against input and output shard mintettes.

2. The mintettes seal client transactions into lower-level blocks at the end of each epoch and place them onto the queue.

3. The central bank removes lower-level blocks from the queue, validates them and stores them until the end of the period.

4. Mintettes are notified that the current period has ended and that production of lower level blocks should pause.

5. All transactions received by the central bank in lower-level blocks during the period are sealed in the central bank blockchain.

6. Mintettes are notified that the new period has opened and that they should resume generation of lower-level blocks.

3.8 Implementation

The following stages were undertaken in the implementation of the experiments:

- System Design
    1. Active Addresses
    2. Nodes/Mintettes
    3. Network hosting on Local host
    4. Block generation

- Simulation Model
    - ➔ Wallet Generate:
      [Generate a 128 bit RSA Private-Public Key Pair]
    - ➔ Transaction Generate: Transaction Addresses and Amounts
      [Import Tuple from Database]
      [DB<CryptoCurrencyName>YEAR<2016/2017>QUARTER<Q1/Q2/Q3/Q4>]
    - ➔ Authentication
      [Check authenticity of Private-Public Key Pair]
    - ➔ Fee Calculate
      [Fee Calculate with reference to Database;]
      [DB<CryptoCurrencyName>YEAR<2016/2017>QUARTER<Q1/Q2/Q3/Q4>]
- Result Publication
    - ➔ Create Quarterly Tables in MS Access
    - ➔ Result Write: Populate Table & Export Excel
    - ➔ Data Analyze
    - ➔ Publish Graph

Chapter 4

RESULT AND ANALYSIS

4.1 Experiment 1: BitCoin

Average Fee for BitCoin were in the range of 10,000th of decimal in percent. Cost ratio with VISA/MasterCard charges ranged from 2000 in early 2016 to as much as 40,000 in late 2017. Likewise, the cost ratio with remittance charges ranged from 18,000 to 350,000.

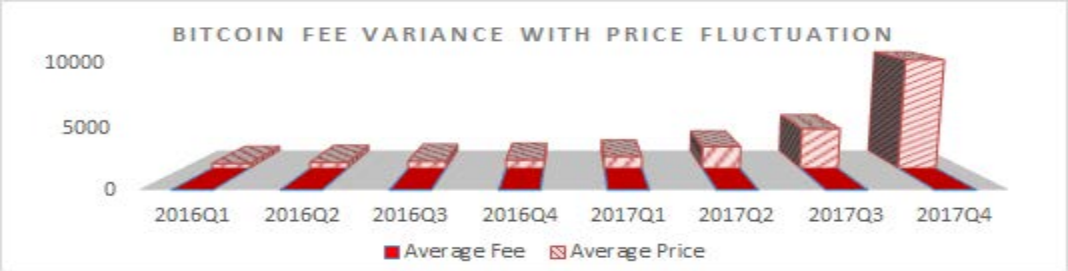


Fig. 4.1.1 Bitcoin Fee Variance with Price Fluctuation

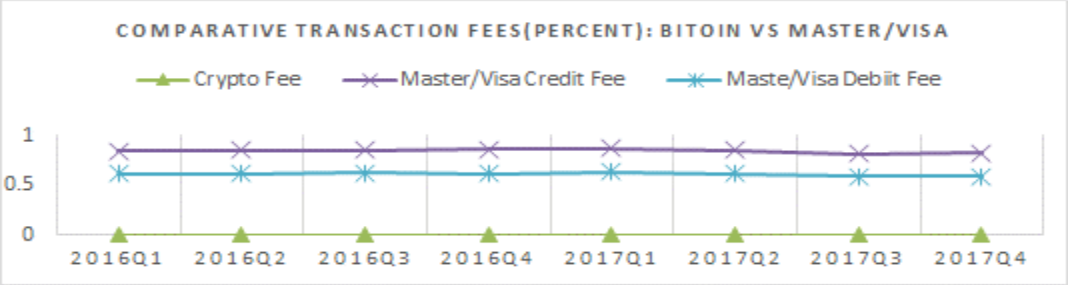


Fig. 4.1.2 Comparative Transaction Fees (Percent): BitCoin vs. Master/VISA

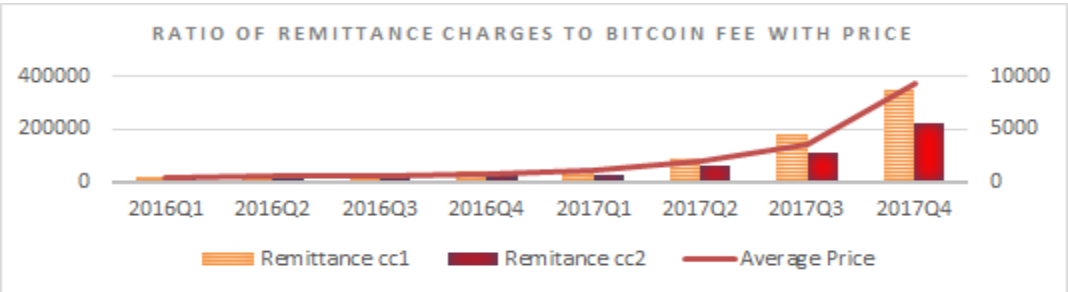


Fig. 4.1.3 Ratio of Remittance Charges to BitCoin Fee with Price

4.2 Experiment 2: Dash

Average Fee for Dash were in the range of 100^{th} of decimal in percent. Cost ratio with VISA/MasterCard charges ranged from 1 in early 2016 to as much as 300 in late 2017. Likewise, the cost ratio with remittance charges ranged from 5 to 2500.

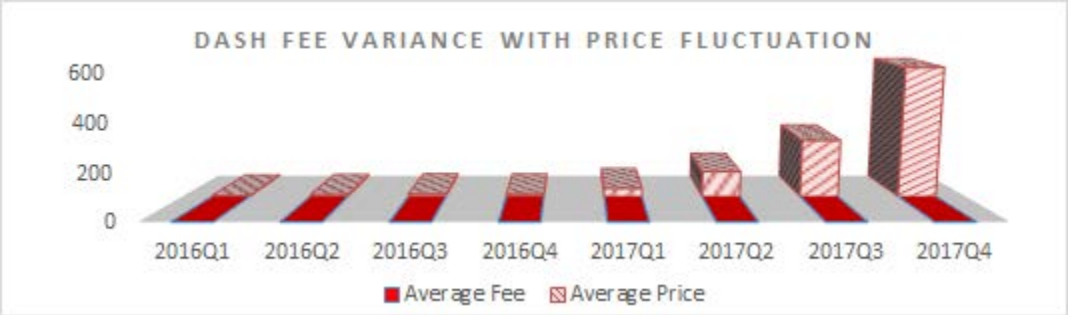


Fig. 4.2.1. Dash Fee Variance with Price Fluctuation

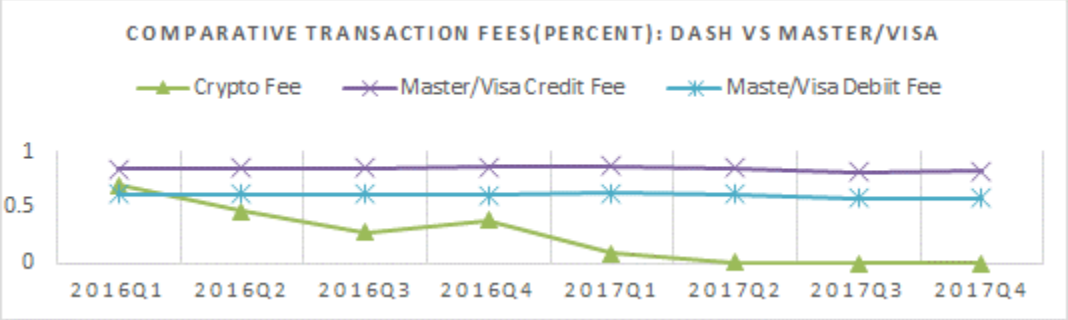


Fig. 4.2.2 Comparative Transaction Fees (Percent): Dash vs. Master/VISA

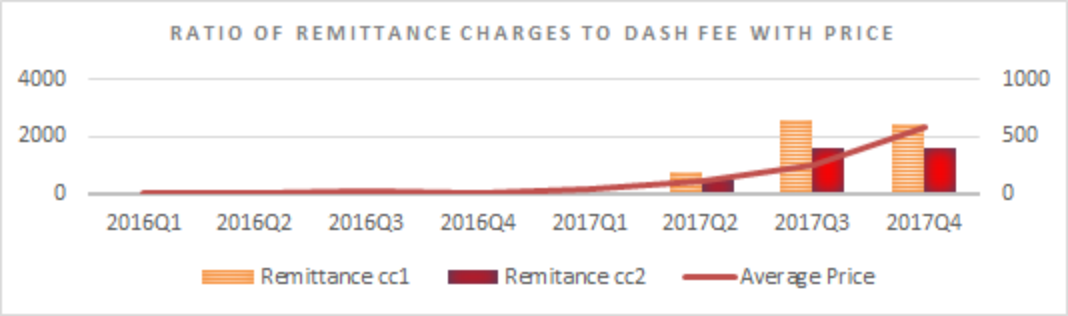


Fig. 4.2.3 Ratio of Remittance Charges to Dash Fee with Price

4.3 Experiment 3: DigiByte

Average Fee for DigiByte were in the range of 100^{th} of decimal in percent. Cost ratio with VISA/MasterCard charges ranged from 5 in early 2016 to as much as 150 in late 2017. Likewise, the cost ratio with remittance charges ranged from 50 to 1500.

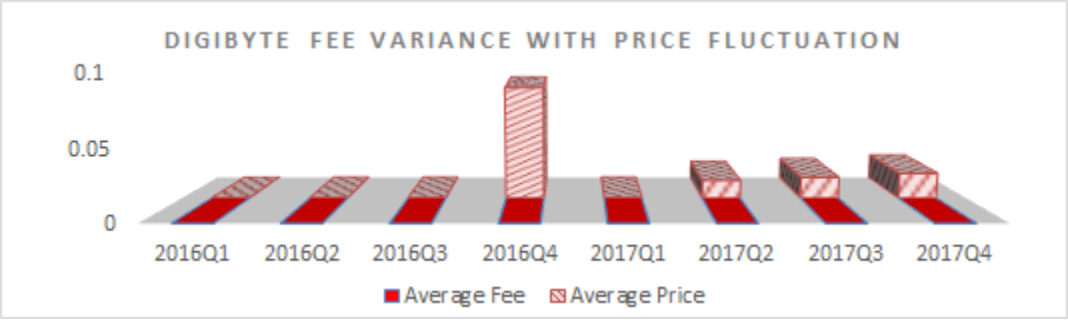


Fig. 4.3.1. DigiByte Fee Variance with Price Fluctuation

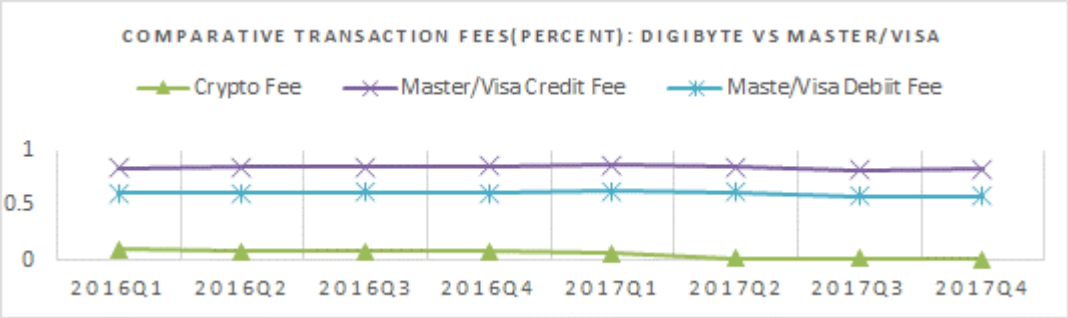


Fig. 4.3.2 Comparative Transaction Fees (Percent): DigiByte vs. Master/VISA

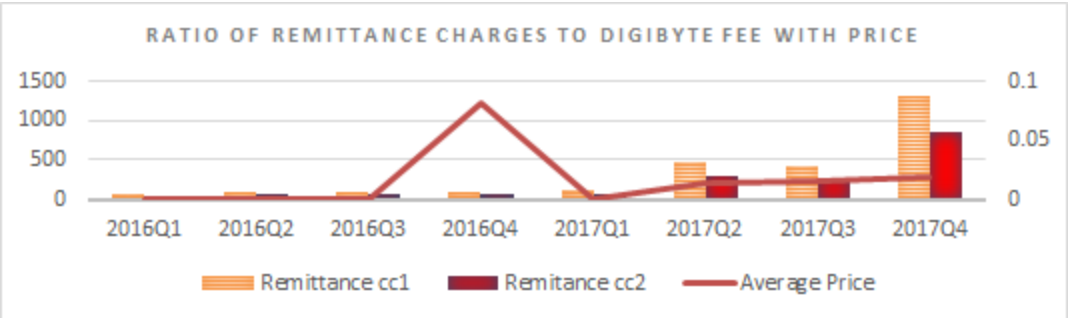


Fig. 4.3.3 Ratio of Remittance Charges to DigiByte Fee with Price

4.4 Experiment 4: DogeCoin

Average Fee for DogeCoin were in the range of 100th of decimal in percent. Cost ratio with VISA/MasterCard charges ranged from 5 in early 2016 to as much as 15 in late 2017. Likewise, the cost ratio with remittance charges ranged from 50 to 100.

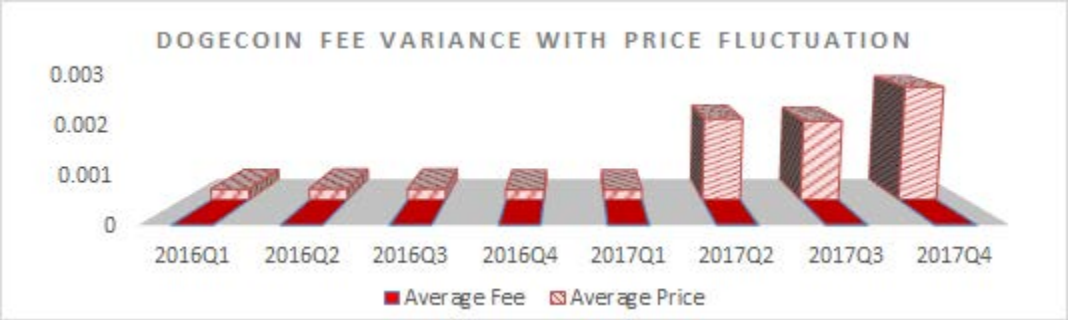


Fig. 4.4.1. DogeCoin Fee Variance with Price Fluctuation

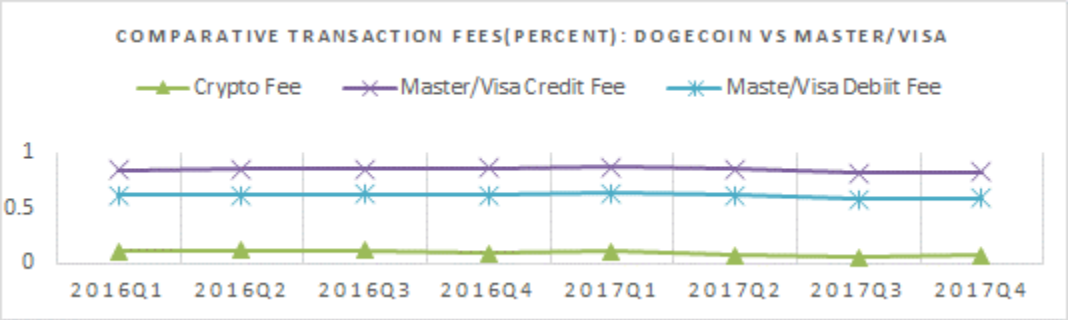


Fig. 4.4.2 Comparative Transaction Fees (Percent): DogeCoin vs. Master/VISA

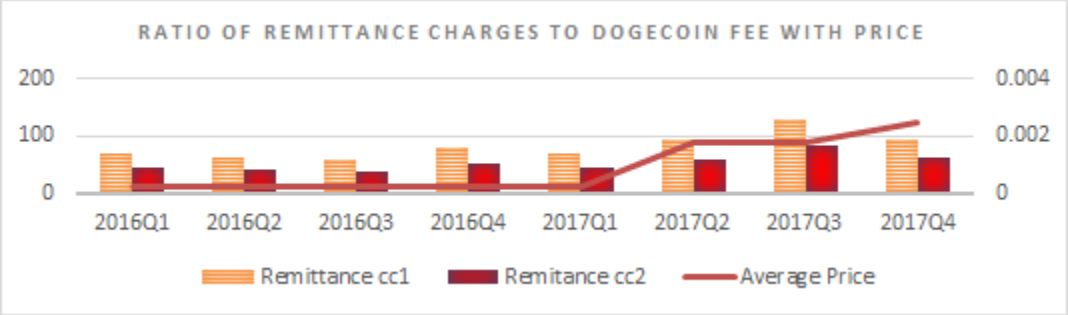


Fig. 4.4.3 Ratio of Remittance Charges to DogeCoin Fee with Price

4.5 Experiment 5: Ethereum

Average Fee for Ethereum were in the range of 10,000th of decimal in percent. Cost ratio with VISA/MasterCard charges ranged from 200 in early 2016 to as much as 85,000 in late 2017. Likewise, the cost ratio with remittance charges ranged from 1500 to 70,000.

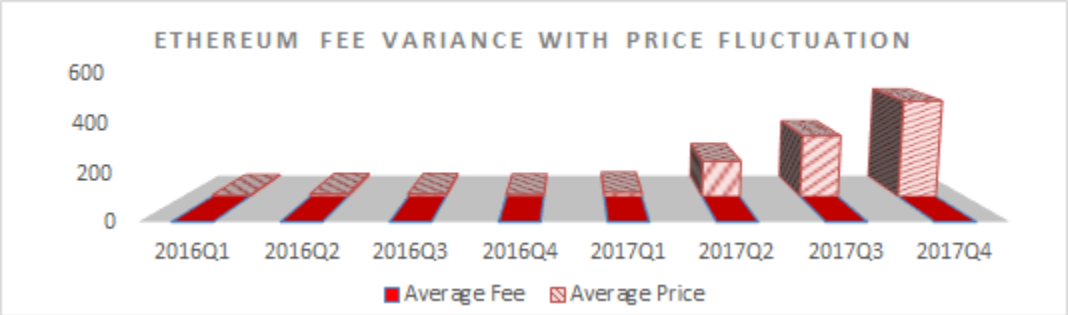


Fig. 4.5.1. Ethereum Fee Variance with Price Fluctuation

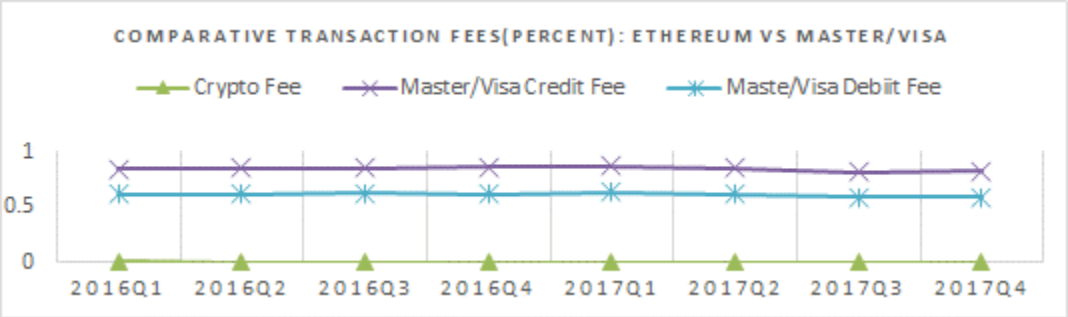


Fig. 4.5.2 Comparative Transaction Fees (Percent): Ethereum vs. Master/VISA

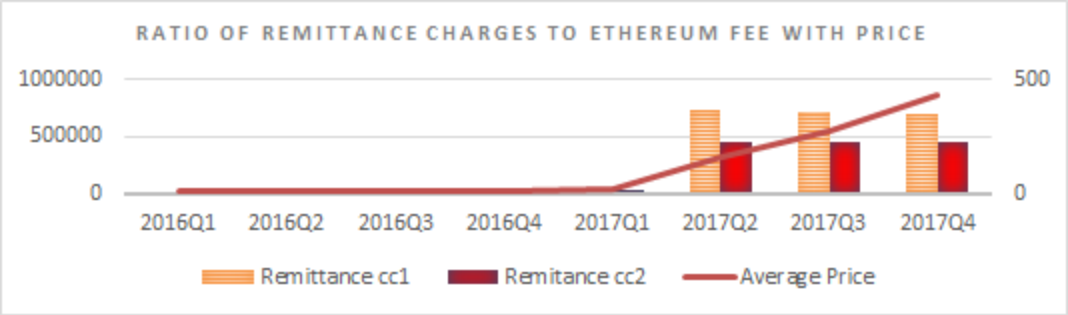


Fig. 4.5.3 Ratio of Remittance Charges to Ethereum Fee with Price

4.6 Experiment 6: LiteCoin

Average Fee for LiteCoin were in the range of 100^{th} of decimal in percent. Cost ratio with VISA/MasterCard charges ranged from 5 in early 2016 to as much as 350 in late 2017. Likewise, the cost ratio with remittance charges ranged from 30 to 3000.

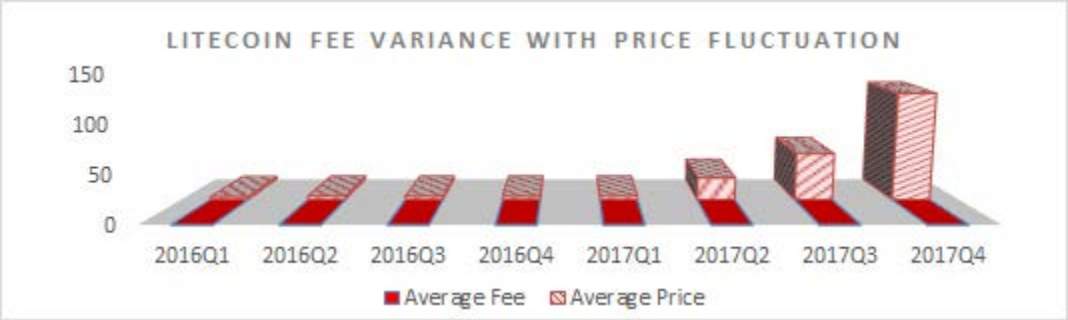


Fig. 4.6.1. LiteCoin Fee Variance with Price Fluctuation

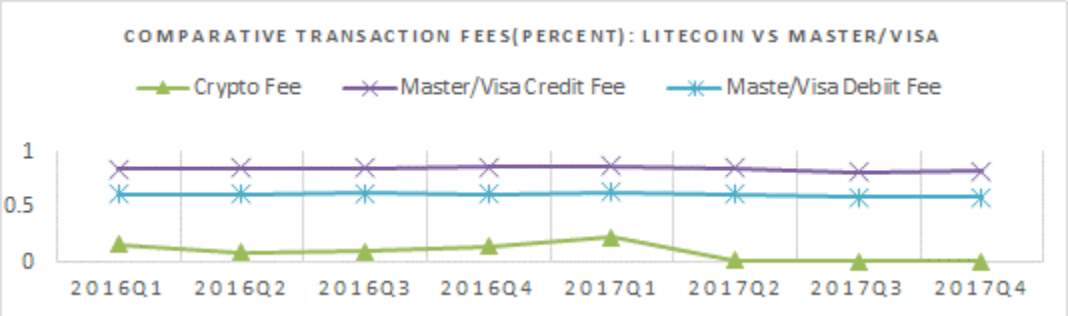


Fig. 4.6.2 Comparative Transaction Fees (Percent): LiteCoin vs. Master/VISA

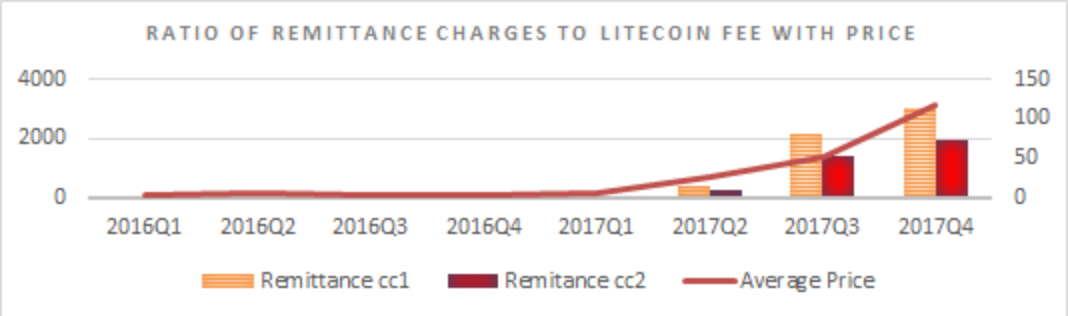


Fig. 4.6.3 Ratio of Remittance Charges to LiteCoin Fee with Price

4.7 Experiment 7: Monero

Average Fee for Monero were in the range of 1000^{th} of decimal in percent. Cost ratio with VISA/MasterCard charges ranged from 15 in early 2016 to as much as 5,000 in late 2017. Likewise, the cost ratio with remittance charges ranged from 100 to 40,000.

Fig. 4.7.1. Monero Fee Variance with Price Fluctuation

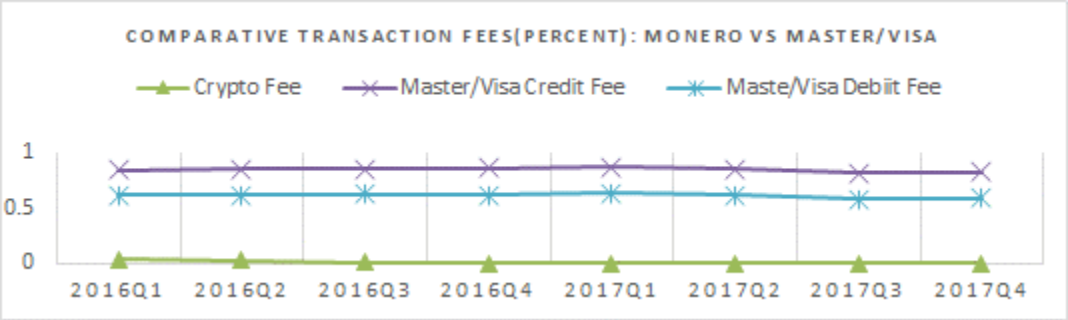


Fig. 4.7.2 Comparative Transaction Fees (Percent): Monero vs. Master/VISA

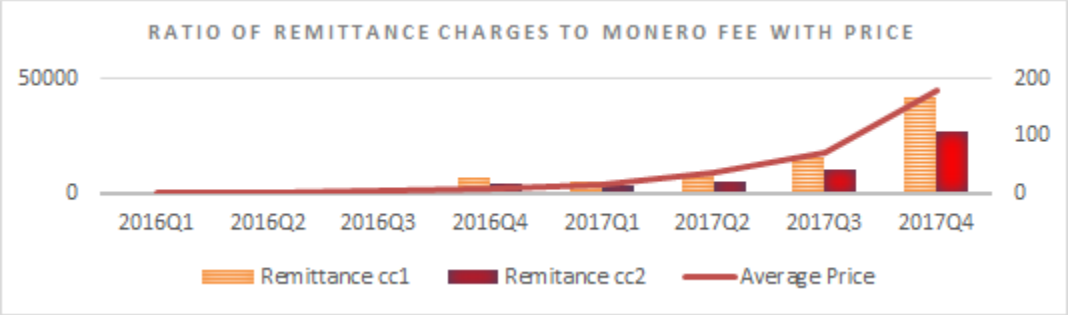


Fig. 4.7.3 Ratio of Remittance Charges to Monero Fee with Price

4.8 Experiment 8: Ripple

Average Fee for Ripple were in the range of 1000^{th} of decimal in percent. Cost ratio with VISA/MasterCard charges ranged from 20 in early 2016 to as much as 2,000 in late 2017. Likewise, the cost ratio with remittance charges ranged from 150 to 20,000.

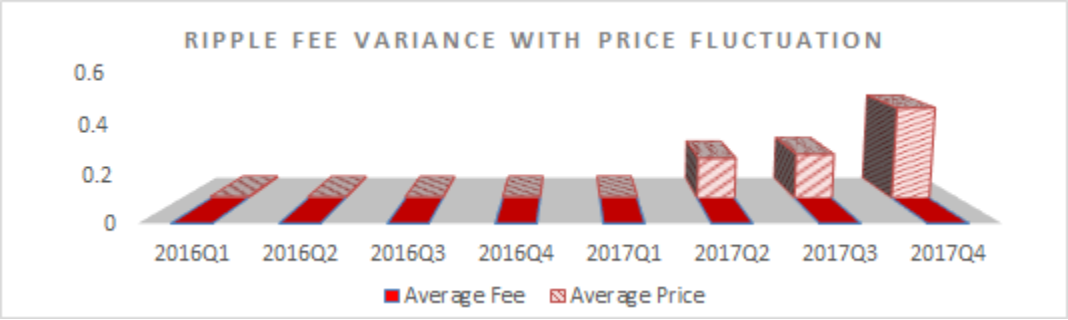


Fig. 4.8.1. Ripple Fee Variance with Price Fluctuation

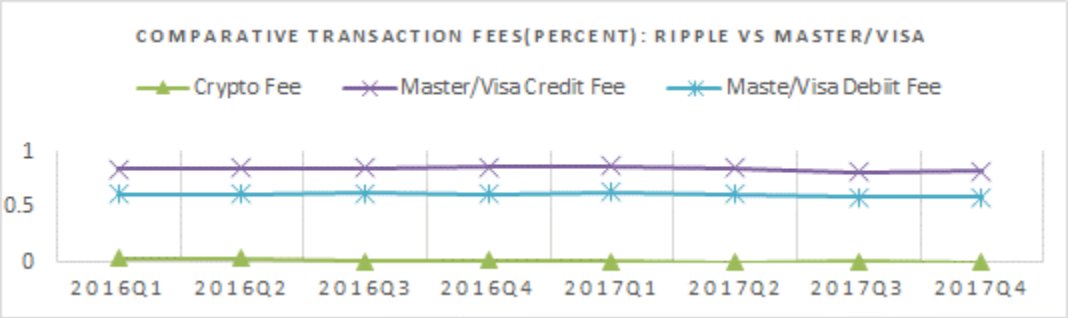


Fig. 4.8.2 Comparative Transaction Fees (Percent): Ripple vs. Master/VISA

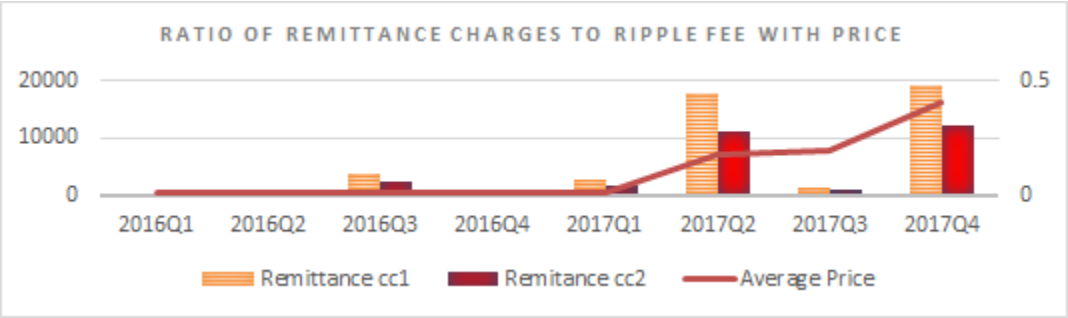


Fig. 4.8.3 Ratio of Remittance Charges to Ripple Fee with Price

4.9 Experiment 9: VertCoin

Average Fee for VertCoin were in the range of 1000th of decimal in percent. Cost ratio with VISA/MasterCard charges ranged from 200 in early 2016 to as much as 4,000 in late 2017. Likewise, the cost ratio with remittance charges ranged from 1500 to 20,000.

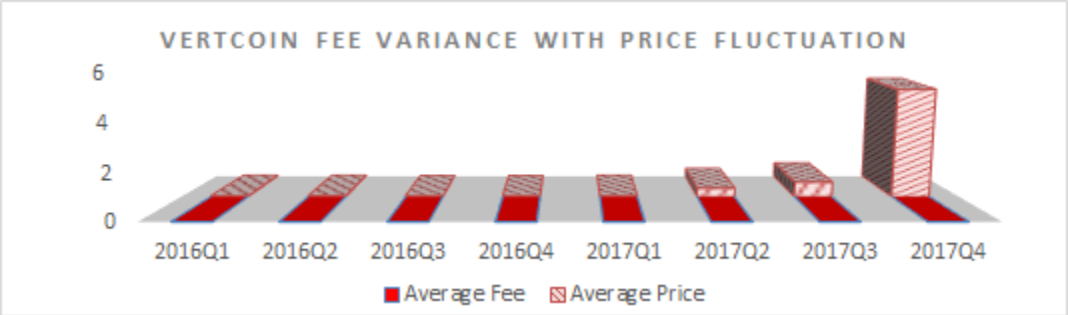


Fig. 4.9.1. VertCoin Fee Variance with Price Fluctuation

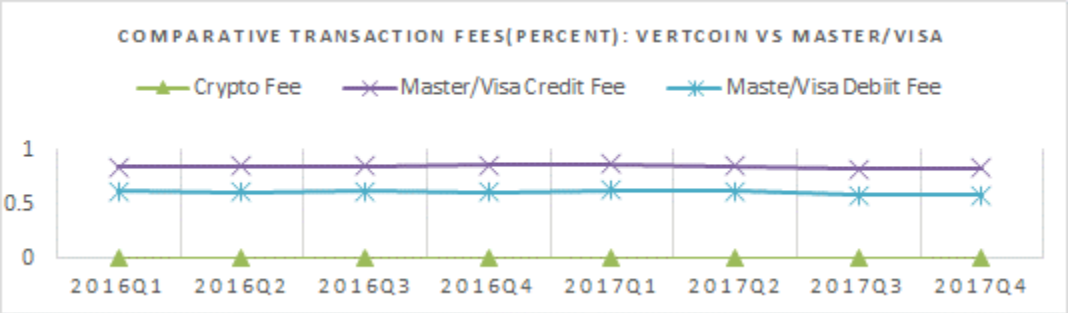


Fig. 4.9.2 Comparative Transaction Fees (Percent): VertCoin vs. Master/VISA

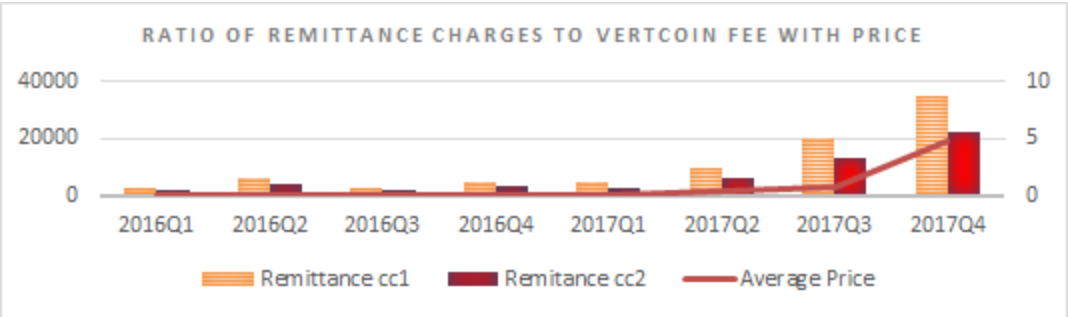


Fig. 4.9.3 Ratio of Remittance Charges to VertCoin Fee with Price

4.10 Experiment 10: Zcash

Average Fee for BitCoin were in the range of 10^{th} of decimal in percent. Cost ratio with VISA/MasterCard charges ranged from 1 in early 2017 to as much as 75 in late 2017. Likewise, the cost ratio with remittance charges ranged from 1 to 500.

Fig. 4.10.1. DigiByte Fee Variance with Price Fluctuation

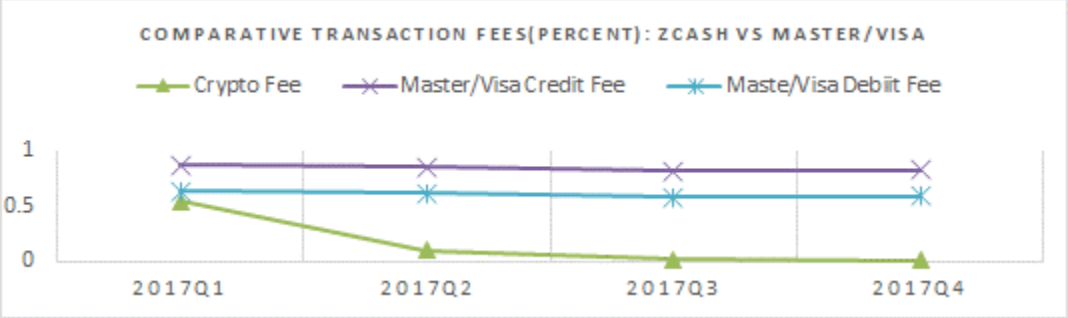


Fig. 4.10.2 Comparative Transaction Fees (Percent): Zcash vs. Master/VISA

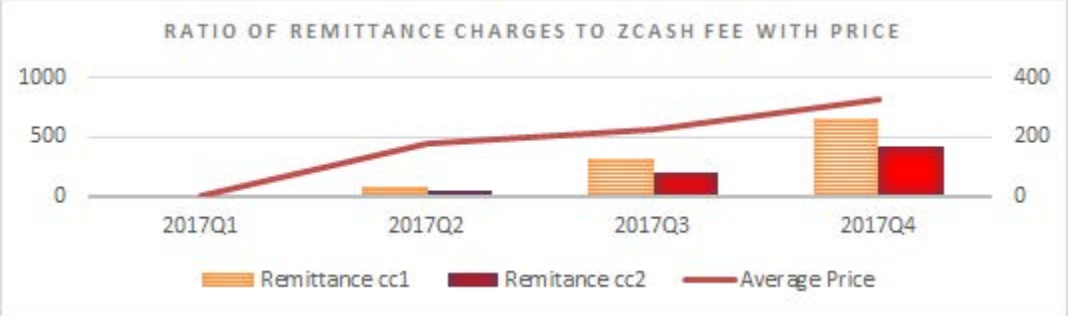


Fig. 4.10.3 Ratio of Remittance Charges to Zcash Fee with Price

4.11 Result Summary

The summary of all of above experiments are tabulated below. First Table contains the data of four quarters of year 2016, and the second table contains the data of four quarters of year 2017.

Coin	Quarter	Average Fee %	Ratio With Visa/MasterCard		Ratio with Remittance Charges	
			Credit	Debit	Outward	Inward
BitCoin	First Quarter	0.00042	1998	1466	17569	11039
	Second Quarter	0.00041	2072	1499	18135	11380
	Third Quarter	0.00025	3411	2487	29100	18231
	Fourth Quarter	0.00019	4515	3227	38335	24141
Dash	First Quarter	0.70357	1	1	10	7
	Second Quarter	0.46375	2	1	16	10
	Third Quarter	0.27543	3	2	26	17
	Fourth Quarter	0.38745	2	2	19	12
DigiByte	First Quarter	0.09821	9	6	75	47
	Second Quarter	0.08479	10	7	88	55
	Third Quarter	0.07973	11	8	91	57
	Fourth Quarter	0.08153	11	8	89	56
DogeCoin	First Quarter	0.10669	8	6	69	43
	Second Quarter	0.11733	7	5	63	40
	Third Quarter	0.12284	7	5	59	37
	Fourth Quarter	0.0903	9	7	81	51
Ethereum	First Quarter	0.00281	299	219	2626	1650
	Second Quarter	0.00029	2929	2119	25640	16089
	Third Quarter	0.00022	3876	2827	33068	20717
	Fourth Quarter	0.0004	2144	1533	18209	11467
LiteCoin	First Quarter	0.15716	5	4	47	30
	Second Quarter	0.08919	10	7	83	52
	Third Quarter	0.09427	9	7	77	48

	Fourth Quarter	0.13973	6	4	52	33
Monero	First Quarter	0.03548	24	17	208	131
	Second Quarter	0.02598	33	24	286	180
	Third Quarter	0.01094	78	57	665	417
	Fourth Quarter	0.00108	794	568	6744	4247
Ripple	First Quarter	0.03061	27	20	241	151
	Second Quarter	0.03372	25	18	221	138
	Third Quarter	0.00196	435	317	3712	2325
	Fourth Quarter	0.01176	73	52	619	390
VertCoin	First Quarter	0.00263	319	234	2806	1763
	Second Quarter	0.00129	659	476	5764	3617
	Third Quarter	0.00308	277	202	2362	1480
	Fourth Quarter	0.00153	561	401	4761	2998

Table 4.11.1 Summary of results for the Year 2016

Coin	Quarter	Average Fee	Ratio With Visa/MasterCard		Ratio with Remittance Charges	
			Credit	Debit	Outward	Inward
BitCoin	First Quarter	0.00017	5100	3710	43144	27050
	Second Quarter	0.00008	10612	7718	90342	57052
	Third Quarter	0.00004	20465	14606	178032	112676
	Fourth Quarter	0.00002	41398	29305	351783	225478
Dash	First Quarter	0.08642	10	7	85	53
	Second Quarter	0.0098	87	63	737	466
	Third Quarter	0.00278	294	210	2562	1621
	Fourth Quarter	0.0029	286	202	2426	1555
DigiByte	First Quarter	0.06475	13	10	113	71
	Second Quarter	0.01564	54	39	462	292
	Third Quarter	0.01679	49	35	424	268

	Fourth Quarter	0.00533	155	110	1320	846
DogeCoin	First Quarter	0.10746	8	6	68	43
	Second Quarter	0.07788	11	8	93	59
	Third Quarter	0.0549	15	11	130	82
	Fourth Quarter	0.07407	11	8	95	61
Ethereum	First Quarter	0.00015	5780	4205	48897	30657
	Second Quarter	0.00001	84897	61741	722738	456420
	Third Quarter	0.00001	81860	58424	712127	450702
	Fourth Quarter	0.00001	82797	58610	703565	450955
LiteCoin	First Quarter	0.22476	4	3	33	20
	Second Quarter	0.01832	46	34	395	249
	Third Quarter	0.0033	248	177	2158	1366
	Fourth Quarter	0.0023	360	255	3059	1961
Monero	First Quarter	0.00153	567	412	4794	3006
	Second Quarter	0.00091	933	678	7942	5016
	Third Quarter	0.00046	1780	1270	15481	9798
	Fourth Quarter	0.00017	4870	3448	41386	26527
Ripple	First Quarter	0.00279	311	226	2629	1648
	Second Quarter	0.00041	2071	1506	17628	11132
	Third Quarter	0.00553	148	106	1288	815
	Fourth Quarter	0.00037	2238	1584	19015	12188
VertCoin	First Quarter	0.00164	529	385	4472	2804
	Second Quarter	0.00074	1147	834	9767	6168
	Third Quarter	0.00035	2339	1669	20346	12877
	Fourth Quarter	0.0002	4140	2931	35178	22548
Zcash	First Quarter	0.54247	2	1	14	8
	Second Quarter	0.10211	8	6	71	45
	Third Quarter	0.02261	36	26	315	199
	Fourth Quarter	0.01079	77	54	652	418

Table 4.11.1 Summary of results for the Year 2017

4.12 Result Analysis and Discussion

Following assumptions were made for Fee Calculation of Coin Transactions:

1. The Number of transactions in the banking system is proportionate to that of the real world
2. The Transaction capital in the banking system is proportionate to that of the real world.

Data variations were done in some coins by including the generated coins as well in transaction amount especially at the starting period when the coin generation rates were higher than the transaction amount. The value of generated coins too were taken as charges to adjust the economic benefit value they created for cryptocurrency miners to incentivize the process similarly as the merchant and service fees in the case of debit/credit card providers. The results thus obtained can be summarized in following points:

1. Common Trend

The output of experiment results persisted to display a trend of superior performance of cryptocurrencies in comparisons to the Master/Visa Card. A further reassuring result was the corresponding performance of coins against remittance products.

The results of the experiments 1 and 5 did show a dramatic decrease in fees of as less as ten thousandth part of decimal in percentage, and in the range of tens and hundreds of thousands in card and remittance charge ratios.

Some results did show a slightly less encouraging data, namely experiment 2, 3, 4, 6, and 10, when compared with other experiment results, for example Dash in 2016 had almost the same charges as that of Master/Visa Cards. Whilst this is not a huge performance impact, investigation suggested that the results got better after the price of cryptocurrency stabilized in latter part of 2017.

2. Popular Vs. Beginner Coins

The relation between popularity viz. market capital/transaction volumes with shadow coin performance revealed that more popular coins such as Bitcoin and Ethereum performed exceedingly better than the others.

3. **Price Stabilization Effect**

   The fee percentage of Coins showed a decline in value with each quarter of both the years. This was due to the fact that the fees for coin transactions were made in cryptocurrency coins and as the price of the crypto market stabilized, the crypto to USD ratio became lower with time. Hence, the performance of the shadow coins were also exponentially improved with each quarter.

4. **Performance Variants**

   The market capital and number of transactions per day were found to be the major performance variants for the results. For instance, BitCoin and Ethereum, being the foremost runners in the crypto market performed comparatively better than all other coins. Also, Monero and Ripple showed similar outcomes compared to the remaining coins.

5. **Recommendations**

   It is apparent from the above results that, although the shadow model seems feasible for the Central Banks performance wise, Banks need to outline certain parameters esp. market capital, number of transactions, popularity of the specific cryptocurrency etc. before letting them in its shadow coin blockchain ledger.

In summary, Comparative charges for cryptocurrency were many folds less than VISA/MasterCard and Remittance Charges. Even with price fluctuations, the fees remained a constant low.

Chapter5

Conclusion

5.1 Conclusion

On the basis of the Experimental Results, it is concluded that the proposed shadow coin system indeed provided better incentive for banks to incorporate cryptographic currencies in their economic ecosystem based on performance against Credit/Debit Card Service Providers and Remittance Service Providers. Crucially, there could be one-for-one convertibility with incorporated cryptocurrencies, and hence a retail central bank cryptocurrency would not suffer from the high price volatility that undermines the usefulness of existing cryptocurrencies.

Through the experiments conducted with this extended RSCoin artefact, it was concluded that central bank could benefit from user inducement of reduced charges by a considerable factor. Thus Shadow Coin can be recommended for further consideration by central banks pursuing cryptographic currencies as part of their innovation agendas if other parameters such as network overheads and security performance are made consistent with set benchmarks.

5.2 Future Work

There are a number of areas of interest for future study following on from this work. This can also be used in International trades and cross country transactions. Also, it is assumed that eradicating the proof of work will considerably speedup the transactions and reduce the energy consumption, it is yet to study the exact improvements of the system. Furthermore, Shadow Coining has a prospect of extending its use to international trades and facilitation of money transfers between countries/international corporations across borders.

Appendix 1: Cryptocurrency Data Format Original

date	txVolume(USD)	txCount	marketcap(USD)	price(USD)	exchangeVolume(USD)	generatedCoins	fees	activeAddresses	averageDifficulty	paymentCount	medianTxValue(USD)	medianFee
1/1/2016	377378302.3	123957	6473530000	430.72	36278900	3375	19.82080598	316727	1.04E+11	236696	49.96946824	0.0001
1/2/2016	316594070.8	148893	6533630000	434.62	30096600	3625	31.37600479	419640	1.04E+11	304961	35.91438908	0.0001
1/3/2016	338119275.4	142463	6519500000	433.58	39633800	3625	24.08304879	394144	1.04E+11	335121	45.76945489	0.0001
1/4/2016	401155747.8	181173	6468180000	430.06	38477500	4525	30.74684308	418266	1.04E+11	310239	43.006	0.0001
1/5/2016	540247572.8	182214	6515380000	433.07	34522600	3925	32.27846687	435329	1.04E+11	321804	50.90691512	0.0001
1/6/2016	516845826.8	171949	6498830000	431.86	34042500	3525	30.40324362	379421	1.04E+11	267082	50.21511315	0.0001
1/7/2016	623150086.7	190087	6472580000	430.01	87562200	3675	37.02453793	430305	1.04E+11	342857	49.31243737	0.0001
1/8/2016	479399674.7	181234	6888600000	457.54	56993000	4325	32.53002298	413787	1.04E+11	307044	47.47358631	0.0001
1/9/2016	320799059.8	179817	6828000000	453.38	32278000	3775	30.22393822	450627	1.04E+11	369357	25.17826335	0.0001
1/10/2016	451010194.8	161142	6752210000	448.24	35995900	4375	27.95780106	432753	1.04E+11	350177	32.06734958	0.0001
1/11/2016	583638254	191026	6761090000	448.7	40450000	4250	35.90416653	448116	1.04E+11	336698	49.31275369	0.0001
1/12/2016	492862438.1	194704	6755220000	448.18	115607000	4250	34.70749772	456763	1.04E+11	360623	44.36982	0.0001
1/13/2016	535522814.5	187983	6553350000	434.67	173888000	3700	34.27954249	425792	1.10E+11	297528	43.467	0.0001
1/14/2016	463348416.2	183049	6519110000	432.29	43945500	3325	31.82088874	427601	1.13E+11	309807	49.99573047	0.0001
1/15/2016	661250823.1	183520	6489870000	430.25	153351000	3050	35.76071656	415708	1.13E+11	293530	51.78511373	0.0001
1/16/2016	494970210.8	191158	5507790000	365.07	120352000	3550	34.77336876	501450	1.13E+11	354177	32.55556629	0.0001
1/17/2016	3971865434	203977	5842270000	387.15	45319600	3775	36.326795	536461	1.13E+11	447028	36.15408405	0.0001
1/18/2016	3560807940	213732	5761940000	381.73	54403900	4325	39.48023545	472936	1.13E+11	344242	39.08925125	0.0001
1/19/2016	3353775385	186725	5843510000	387.03	46819800	3325	39.67840683	419190	1.13E+11	301559	49.19568131	0.0001
1/20/2016	1460825926	208919	5734760000	379.74	121720000	3800	46.47964248	625563	1.13E+11	388247	44.56183964	0.0001
1/21/2016	2126986590	222606	6338800000	419.63	68338000	3425	50.3603795	516771	1.13E+11	370087	55.87067959	0.0001
1/22/2016	3094994091	213507	6190940000	409.75	91546600	4400	45.16359551	501601	1.13E+11	355696	51.93150603	0.0001
1/23/2016	11326116600	190221	5779890000	382.43	56247400	4475	38.59889347	473146	1.13E+11	376171	49.41275156	0.0001
1/24/2016	26097822216	201254	5867300000	388.1	54824800	4275	40.1824236	487622	1.13E+11	384082	73.86495009	0.0001
1/25/2016	6925342919	221988	6083900000	402.32	59062400	4050	45.9839664	517175	1.13E+11	375474	44.67545945	0.0001
1/26/2016	4009141319	230363	5929520000	392	58147000	4000	47.01650631	533783	1.16E+11	387126	66.5616	0.0001
1/27/2016	5393340988	229522	5937780000	392.44	47424400	3875	49.12850373	529075	1.20E+11	365156	69.37621427	0.0001
1/28/2016	2347344945	224879	5980180000	395.15	59247900	3650	47.43453192	522089	1.20E+11	363400	51.55789171	0.0001
1/29/2016	2673975338	224225	5753970000	380.11	86125300	4225	46.98023086	531737	1.20E+11	338071	67.14823702	0.0001
1/30/2016	1249346525	194607	5736760000	378.87	30284400	4675	38.97923245	497567	1.20E+11	385893	72.12995257	0.0001
1/31/2016	600405945.2	175864	5729870000	378.29	37894300	4525	34.55384553	480130	1.20E+11	382270	63.28412653	0.0001

Appendix 2: Randomized Transactions Format

Day1 Tx List	Day2 Tx List	Day3 Tx List	Day4 Tx List	Day5 Tx List	Day6 Tx List	Day7 Tx List	Day8 Tx List	Day9 Tx List	Day10 Tx List	Day11 Tx List	Day12 Tx List	Day13 Tx List	Day14 Tx List	Day15 Tx List
210.31052	190.07196	200.93733	216.85764	125.1636	111.51927	170.02663	130.41183	88.72492	129.98168	101.64539	126.75547	109.73207	74.76392	173.28318
166.69717	117.80942	168.35395	149.72709	174.34337	142.81738	107.34918	159.13918	129.36681	122.90095	154.65359	96.88587	132.05496	104.75305	118.24902
152.30137	199.57906	139.6995	137.36044	164.23395	147.70789	117.97237	151.21859	140.1995	92.8536	136.62489	116.7548	143.09011	130.17048	117.53028
143.04152	136.56149	80.74533	118.33299	101.09301	180.52832	114.85787	97.82164	116.94278	90.56061	130.80827	146.68431	125.77068	91.54399	77.38705
179.46549	119.18185	112.64069	147.52835	155.26961	110.247	153.24914	152.18789	118.48591	75.89422	133.55157	127.75201	187.70314	94.40375	130.10116
90.76616	142.09604	178.94945	112.77234	124.87399	155.52517	134.7278	136.91546	98.01295	118.22654	113.18575	108.37212	168.78588	77.2745	127.29028
110.95737	193.14082	214.52099	137.09722	167.73763	106.04347	142.76678	163.93486	102.76834	90.61943	125.84599	133.33913	142.8344	118.99849	152.87485
103.98945	126.79082	94.2652	126.90944	181.05987	140.35238	126.25967	113.75451	124.36466	101.26384	139.09328	89.60149	100.92883	110.28901	153.21801
142.05588	202.49473	126.55264	149.94606	95.92314	92.23972	133.79316	137.11921	100.02881	123.1342	104.18085	169.29744	160.00787	123.73682	105.41855
153.99041	222.13031	166.26238	127.74403	161.42712	135.63565	126.41421	133.91574	122.40167	74.43432	175.1172	129.75711	109.9928	104.5541	105.18809
148.87338	178.98712	140.878	164.02142	154.17228	105.23397	126.74093	102.33333	131.74321	69.57639	152.13387	107.20459	179.16974	119.71619	99.20848
161.8553	159.49699	116.70359	137.24362	165.77656	126.78543	99.76226	93.70537	86.11495	80.14879	177.93179	105.80244	115.95587	99.2678	78.90505
149.68259	186.47286	142.99444	98.63311	169.48283	95.54072	140.24733	157.3091	131.60014	94.4082	186.35345	144.38332	132.84842	102.7217	134.08728
121.91604	102.25303	123.39557	87.74614	111.65104	134.05946	149.15501	149.06501	143.18829	99.22966	117.09956	140.92194	110.04921	107.99952	90.26434
125.7833	173.22909	153.00152	99.59862	157.03317	109.57102	114.924	111.22294	137.81792	70.37261	168.16237	128.81296	103.00453	87.15619	133.47248
154.98393	161.63538	149.1642	156.34784	114.24456	166.84736	143.22006	129.21128	115.35751	95.28941	155.66292	166.20917	147.91175	104.18003	137.86456
142.72221	184.43234	90.80801	176.47765	187.42468	156.19759	132.99035	90.16606	188.21842	114.63472	118.72853	115.52322	132.26765	95.8302	127.89659
165.1127	141.40977	176.10219	164.28763	202.54258	153.05549	157.54934	113.36284	111.7078	125.02006	110.79558	155.9621	75.27827	104.6354	133.19054
108.6609	146.57667	94.67785	119.02018	133.95733	131.4632	153.0096	120.85519	139.40811	80.25469	83.86999	126.28525	185.26188	92.15497	157.44947
172.0328	146.83311	171.07088	108.47141	145.60583	132.08588	173.03966	122.86468	106.34416	76.97813	130.79574	145.69036	155.64684	110.96937	121.27634
133.22956	130.24072	188.10603	150.19229	106.65117	115.94698	152.67861	139.31646	110.17327	119.17508	131.44177	94.67272	103.46971	81.22218	97.80331
185.02031	170.46421	131.87631	98.66222	147.07985	151.15963	113.59789	122.5852	132.81022	99.32099	132.01362	107.63465	92.49791	102.21268	136.3637
110.55183	105.85543	116.88571	179.15248	126.47769	122.26111	144.3345	69.72631	141.83777	71.12946	143.3388	147.56369	88.61266	112.93216	125.25655
121.47633	127.56657	101.46155	107.10249	128.19495	153.83269	73.72479	96.72386	128.04261	122.52169	141.08657	117.15275	100.47325	105.10673	147.2744
154.04355	127.8483	125.31457	180.41805	140.04617	122.66951	139.66644	101.08448	112.01629	125.37091	145.97959	100.91733	130.59082	76.87186	106.28682
114.37825	167.74664	158.71397	167.94912	199.42467	136.24368	121.10094	120.75914	121.2937	120.40633	106.78347	152.3121	131.20323	104.36824	135.78866
149.17448	173.93262	135.80833	136.95907	140.17869	125.8093	100.91542	59.1641	89.0004	116.78436	99.64779	82.31852	122.77783	98.0009	146.3616
142.9987	143.03527	122.41588	103.30254	111.31381	105.6088	123.35891	112.99738	101.07154	113.055	149.33327	95.98528	139.38428	95.57893	90.1233
153.24357	184.3702	184.04009	89.54239	131.12909	100.89727	187.13608	133.77344	109.01105	95.72526	65.19685	119.85282	168.30391	88.20908	113.72082

Appendix 3: Result Set Format after Fee Calculation

date	txVolume(USD)	txCount	marketcap(USD)	price(USD)	exchangeVolume(USD)	generatedCoins	fees	activeAddresses	averageDifficulty	paymentCount	medianTxValue(USD)	medianFee	feePercent
1/1/2016	377378302.3	123957	6473530000	430.72	36278900	3375	19.82080598	316727	1.04E+11	236696	49.96946824	0.0001	0.00089958
1/2/2016	316594070.8	148893	6533630000	434.62	30096600	3625	31.37600479	419640	1.04E+11	304961	35.91438908	0.0001	0.00115491
1/3/2016	338119275.4	142463	6519500000	433.58	39633800	3625	24.08304879	394144	1.04E+11	335121	45.76945489	0.0001	0.00107923
1/4/2016	401155747.8	181173	6468180000	430.06	38477500	4525	30.74684308	418266	1.04E+11	310239	43.006	0.0001	0.001135655
1/5/2016	540247572.8	182214	6515380000	433.07	34522600	3925	32.27846687	435329	1.04E+11	321804	50.90691512	0.0001	0.000732494
1/6/2016	516845826.8	171949	6498830000	431.86	34042500	3525	30.40324362	379421	1.04E+11	267082	50.21511315	0.0001	0.000687904
1/7/2016	623150086.7	190087	6472580000	430.01	87562200	3675	37.02453793	430305	1.04E+11	342857	49.31243737	0.0001	0.000595687
1/8/2016	479399674.7	181234	6888600000	457.54	56993000	4325	32.53002298	413787	1.04E+11	307044	47.47358631	0.0001	0.000908956
1/9/2016	320799059.8	179817	6828000000	453.38	32278000	3775	30.22393822	450627	1.04E+11	369357	25.17826335	0.0001	0.001186171
1/10/2016	451010194.8	161142	6752210000	448.24	35995900	4375	27.95780106	432753	1.04E+11	350177	32.06734958	0.0001	0.000976244
1/11/2016	583638254	191026	6761090000	448.7	40450000	4250	35.90416653	448116	1.04E+11	336698	49.31275369	0.0001	0.000734343
1/12/2016	492862438.1	194704	6755220000	448.18	115607000	4250	34.70749772	456763	1.04E+11	360623	44.36982	0.0001	0.000869352
1/13/2016	535522814.5	187983	6553350000	434.67	173888000	3700	34.27954249	425792	1.10E+11	297528	43.467	0.0001	0.000697315
1/14/2016	463348416.2	183049	6519110000	432.29	43945500	3325	31.82088874	427601	1.13E+11	309807	49.99573047	0.0001	0.00072447
1/15/2016	661250823.1	183520	6489870000	430.25	153351000	3050	35.76071656	415708	1.13E+11	293530	51.78511373	0.0001	0.000466655
1/16/2016	494970210.8	191158	5507790000	365.07	120352000	3550	34.77336876	501450	1.13E+11	354177	32.55556629	0.0001	0.00072424
1/17/2016	3971865434	203977	5842270000	387.15	45319600	3775	36.326795	536461	1.13E+11	447028	36.15408405	0.0001	9.59581E-05
1/18/2016	3560807940	213732	5761940000	381.73	54403900	4325	39.48023545	472936	1.13E+11	344242	39.08925125	0.0001	0.00012257
1/19/2016	3353775385	186725	5843510000	387.03	46819800	3325	39.67840683	419190	1.13E+11	301559	49.19568131	0.0001	0.000100325
1/20/2016	1460825926	208919	5734760000	379.74	121720000	3800	46.47964248	625563	1.13E+11	388247	44.56183964	0.0001	0.000263309
1/21/2016	2126986590	222606	6338800000	419.63	68338000	3425	50.3603795	516771	1.13E+11	370087	55.87067959	0.0001	0.000163394
1/22/2016	3094994091	213507	6190940000	409.75	91546600	4400	45.16359551	501601	1.13E+11	355696	51.93150603	0.0001	0.000143624
1/23/2016	11326116600	190221	5779890000	382.43	56247400	4475	38.59889347	473146	1.13E+11	376171	49.41275156	0.0001	3.98512E-05
1/24/2016	26097822216	201254	5867300000	388.1	54824800	4275	40.1824236	487622	1.13E+11	384082	73.86495009	0.0001	1.65346E-05
1/25/2016	6925342919	221988	6083900000	402.32	59062400	4050	45.9839664	517175	1.13E+11	375474	44.67545945	0.0001	5.91449E-05
1/26/2016	4009141319	230363	5929520000	392	58147000	4000	47.01650631	533783	1.16E+11	387126	66.5616	0.0001	0.000100945
1/27/2016	5393340988	229522	5937780000	392.44	47424400	3875	49.12850373	529075	1.20E+11	365156	69.37621427	0.0001	7.27588E-05
1/28/2016	2347344945	224879	5980180000	395.15	59247900	3650	47.43453192	522089	1.20E+11	363400	51.55789171	0.0001	0.000157516
1/29/2016	2673975338	224225	5753970000	380.11	86125300	4225	46.98023086	531737	1.20E+11	338071	67.14823702	0.0001	0.000159761
1/30/2016	1249346525	194607	5736760000	378.87	30284400	4675	38.97923245	497567	1.20E+11	385893	72.12995257	0.0001	0.000377316
1/31/2016	600405945.2	175864	5729870000	378.29	37894300	4525	34.55384553	480130	1.20E+11	382270	63.28412653	0.0001	0.000759412

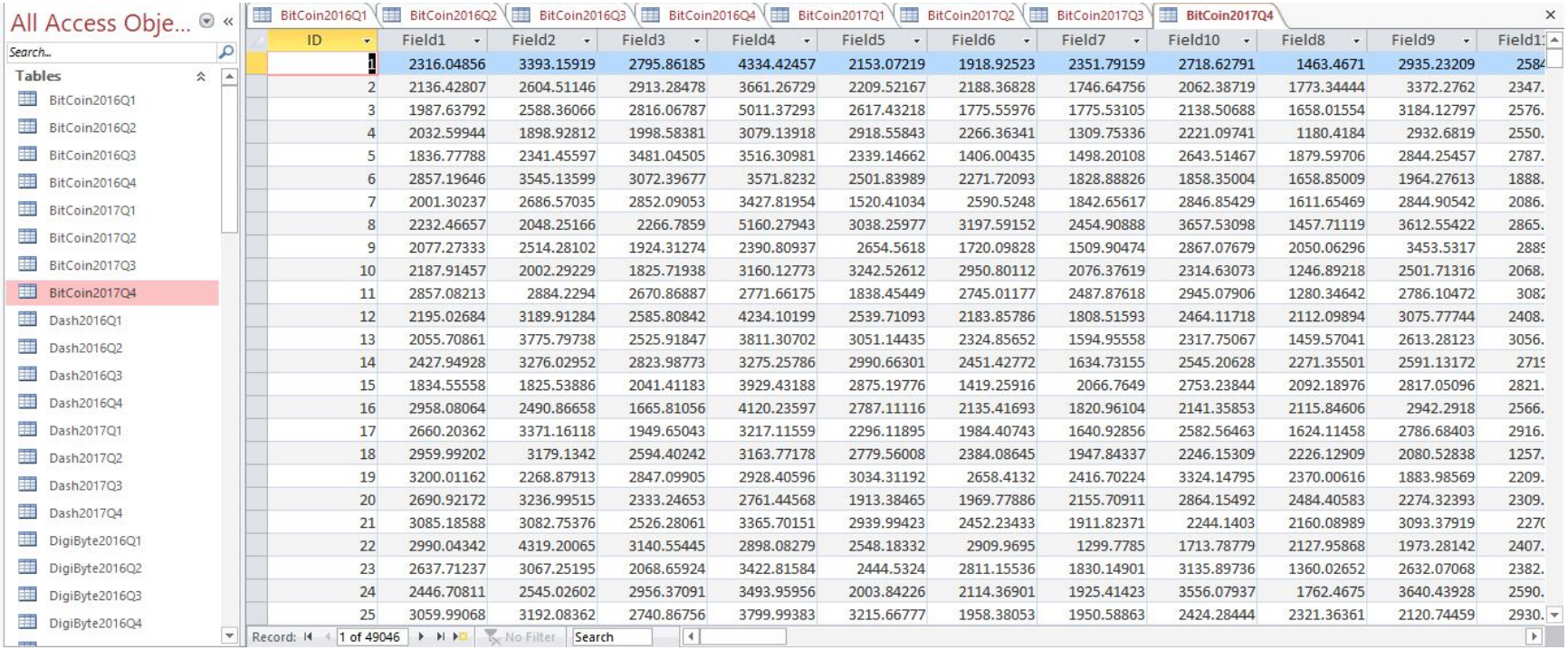
Appendix 4: MasterCard and Visa Service Charge Data Format

Date	MasterCard and Visa merchant service fees . Units: Per cent ; Series ID: CMFCBMVMS	MasterCard and Visa other merchant fees . Units: Per cent ; Series ID: CMFCBMVO	MasterCard and Visa total merchant fees . Units: Per cent ; Series ID: CMFCBMVT	MasterCard and Visa credit merchant service fees . Units: Per cent ; Series ID: CMFCMVMS	MasterCard and Visa credit other merchant fees . Units: Per cent ; Series ID: CMFCMVO	MasterCard and Visa credit total merchant fees . Units: Per cent ; Series ID: CMFCMVT	MasterCard and Visa debit merchant service fees . Units: Per cent ; Series ID: CMFBMVMS	MasterCard and Visa debit other merchant fees . Units: Per cent ; Series ID: CMFBMVO	MasterCard and Visa debit total merchant fees . Units: Per cent ; Series ID: CMFBMVT
12/31/2017	0.676068418	0.06060377	0.736672188	0.764843765	0.063125869	0.827969633	0.529658541	0.056444281	0.586102823
9/30/2017	0.668754347	0.062149075	0.730903422	0.754275387	0.064320366	0.818595752	0.525726534	0.058517747	0.584244281
6/30/2017	0.705061949	0.061593399	0.766655348	0.785972939	0.062998829	0.848971769	0.558361793	0.059045205	0.617406998
3/31/2017	0.723536341	0.060626586	0.784162927	0.804969349	0.061975127	0.866944476	0.572568893	0.058126546	0.630695439
12/31/2016	0.72121268	0.051983126	0.773195806	0.805558909	0.052235788	0.857794697	0.561542092	0.051504827	0.613046918
9/30/2016	0.718745995	0.054655368	0.773401363	0.798025999	0.054760763	0.852786762	0.567396057	0.054454164	0.621850221
6/30/2016	0.719875563	0.053130624	0.773006187	0.796456389	0.053027231	0.84948362	0.561063355	0.053345038	0.614408393
3/31/2016	0.714405526	0.052685039	0.767090565	0.786530553	0.052452065	0.838982618	0.562484483	0.053175765	0.615660248

Appendix 5: Remittance Data Format

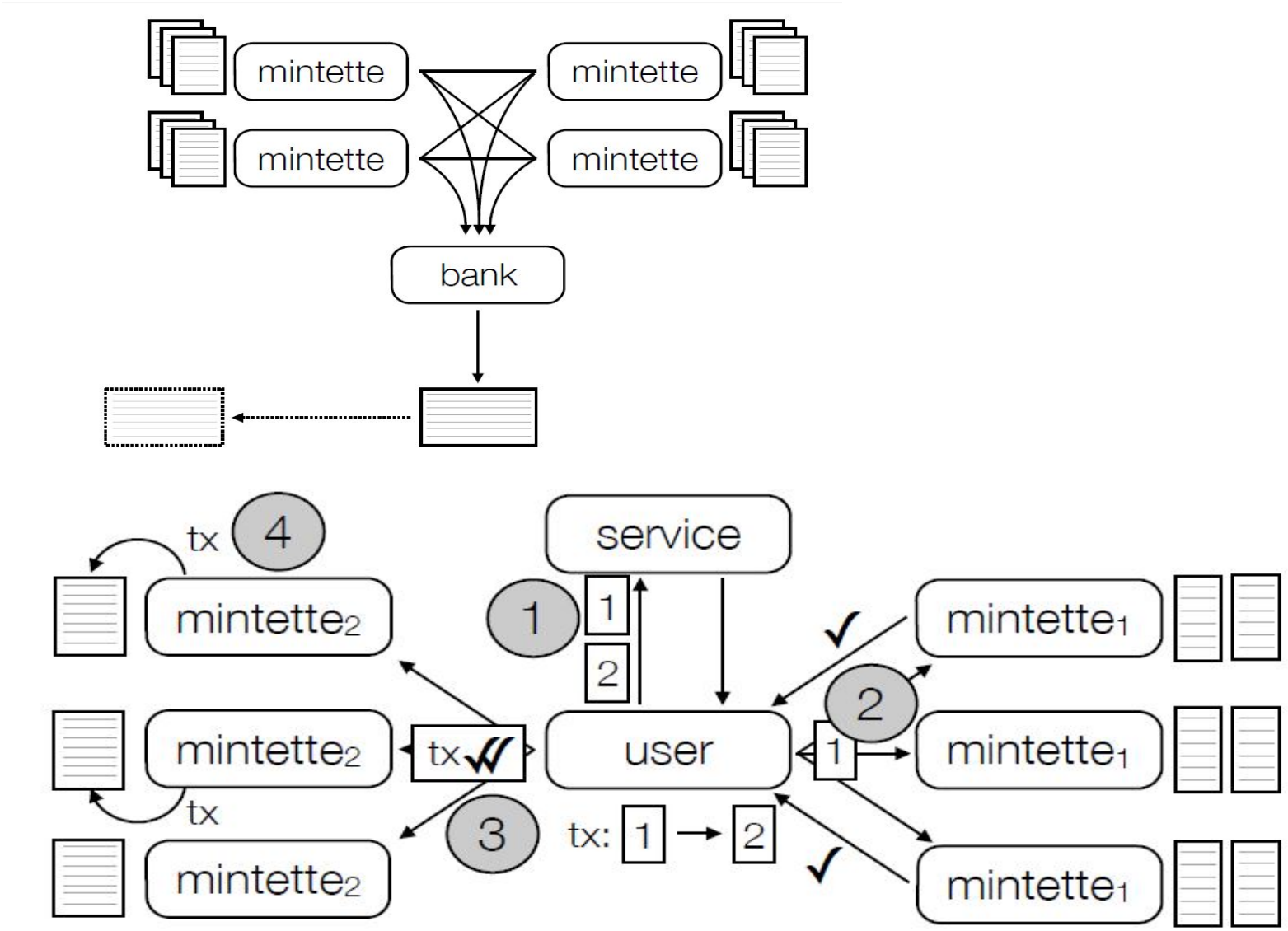
period	source_code	source_name	source_income	destination_code	destination_income	firm	cc1 total cost %	cc2 total cost %
2016_1Q	ARE	United Arab Emirates	High income: nonOECD	NPL	Low income	Al Halia	2.38	1.43
2016_1Q	ARE	United Arab Emirates	High income: nonOECD	NPL	Low income	Al Ansari	2.38	1.43
2016_1Q	ARE	United Arab Emirates	High income: nonOECD	NPL	Low income	Al Fardan Exchange	3.75	1.43
2016_1Q	ARE	United Arab Emirates	High income: nonOECD	NPL	Low income	Al Ansari	2.38	1.43
2016_1Q	ARE	United Arab Emirates	High income: nonOECD	NPL	Low income	Lari	2.45	1.23
2016_1Q	GBR	United Kingdom	High income: OECD	NPL	Low income	Orbit Remit	0.73	0.73
2016_1Q	GBR	United Kingdom	High income: OECD	NPL	Low income	Xpress Money	5.81	3.31
2016_1Q	GBR	United Kingdom	High income: OECD	NPL	Low income	Small World FS-LCC	4.81	3.31
2016_1Q	GBR	United Kingdom	High income: OECD	NPL	Low income	Kantipur Services	4.94	3.44
2016_1Q	GBR	United Kingdom	High income: OECD	NPL	Low income	Western Union	7.62	4.67
2016_1Q	MYS	Malaysia	Upper middle income	NPL	Low income	Al Rajhi Bank i-Tahweel	3.13	1.56
2016_1Q	MYS	Malaysia	Upper middle income	NPL	Low income	Merchantrade Money Transfer	2.49	1.44
2016_1Q	MYS	Malaysia	Upper middle income	NPL	Low income	Western Union	3.47	1.91
2016_1Q	MYS	Malaysia	Upper middle income	NPL	Low income	E-remit	2.68	1.64
2016_1Q	MYS	Malaysia	Upper middle income	NPL	Low income	IME (International Money Express)	3.2	2.19
2016_1Q	QAT	Qatar	High income: nonOECD	NPL	Low income	Al Dar Exchange	3.03	1.39
2016_1Q	QAT	Qatar	High income: nonOECD	NPL	Low income	Xpress Money	2.82	1.34
2016_1Q	QAT	Qatar	High income: nonOECD	NPL	Low income	Xpress Money	2.82	1.34
2016_1Q	QAT	Qatar	High income: nonOECD	NPL	Low income	City Exchange Company	2.72	1.32
2016_1Q	QAT	Qatar	High income: nonOECD	NPL	Low income	Eastern Exchange Co	3.16	1.52
2016_1Q	SAU	Saudi Arabia	High income: nonOECD	NPL	Low income	Enjaz Bank	1.12	-1.27
2016_1Q	SAU	Saudi Arabia	High income: nonOECD	NPL	Low income	Al Zamil Exchange	5.03	2.19
2016_1Q	SAU	Saudi Arabia	High income: nonOECD	NPL	Low income	TeleMoney	4.73	2.13
2016_1Q	SAU	Saudi Arabia	High income: nonOECD	NPL	Low income	Al-Rajhi Bank	4.93	2.26
2016_1Q	SAU	Saudi Arabia	High income: nonOECD	NPL	Low income	MoneyGram	4.76	2.25

Appendix 6: MS Access Database Store Snippet



ID	Field1	Field2	Field3	Field4	Field5	Field6	Field7	Field10	Field8	Field9	Field11
1	2316.04856	3393.15919	2795.86185	4334.42457	2153.07219	1918.92523	2351.79159	2718.62791	1463.4671	2935.23209	2584
2	2136.42807	2604.51146	2913.28478	3661.26729	2209.52167	2188.36828	1746.64756	2062.38719	1773.34444	3372.2762	2347.
3	1987.63792	2588.36066	2816.06787	5011.37293	2617.43218	1775.55976	1775.53105	2138.50688	1658.01554	3184.12797	2576.
4	2032.59944	1898.92812	1998.58381	3079.13918	2918.55843	2266.36341	1309.75336	2221.09741	1180.4184	2932.6819	2550.
5	1836.77788	2341.45597	3481.04505	3516.30981	2339.14662	1406.00435	1498.20108	2643.51467	1879.59706	2844.25457	2787.
6	2857.19646	3545.13599	3072.39677	3571.8232	2501.83989	2271.72093	1828.88826	1858.35004	1658.85009	1964.27613	1888.
7	2001.30237	2686.57035	2852.09053	3427.81954	1520.41034	2590.5248	1842.65617	2846.85429	1611.65469	2844.90542	2086.
8	2232.46657	2048.25166	2266.7859	5160.27943	3038.25977	3197.59152	2454.90888	3657.53098	1457.71119	3612.55422	2865.
9	2077.27333	2514.28102	1924.31274	2390.80937	2654.5618	1720.09828	1509.90474	2867.07679	2050.06296	3453.5317	2885
10	2187.91457	2002.29229	1825.71938	3160.12773	3242.52612	2950.80112	2076.37619	2314.63073	1246.89218	2501.71316	2068.
11	2857.08213	2884.2294	2670.86887	2771.66175	1838.45449	2745.01177	2487.87618	2945.07906	1280.34642	2786.10472	3082
12	2195.02684	3189.91284	2585.80842	4234.10199	2539.71093	2183.85786	1808.51593	2464.11718	2112.09894	3075.77744	2408.
13	2055.70861	3775.79738	2525.91847	3811.30702	3051.14435	2324.85652	1594.95558	2317.75067	1459.57041	2613.28123	3056.
14	2427.94928	3276.02952	2823.98773	3275.25786	2990.66301	2451.42772	1634.73155	2545.20628	2271.35501	2591.13172	2715
15	1834.55558	1825.53886	2041.41183	3929.43188	2875.19776	1419.25916	2066.7649	2753.23844	2092.18976	2817.05096	2821.
16	2958.08064	2490.86658	1665.81056	4120.23597	2787.11116	2135.41693	1820.96104	2141.35853	2115.84606	2942.2918	2566.
17	2660.20362	3371.16118	1949.65043	3217.11559	2296.11895	1984.40743	1640.92856	2582.56463	1624.11458	2786.68403	2916.
18	2959.99202	3179.1342	2594.40242	3163.77178	2779.56008	2384.08645	1947.84337	2246.15309	2226.12909	2080.52838	1257.
19	3200.01162	2268.87913	2847.09905	2928.40596	3034.31192	2658.4132	2416.70224	3324.14795	2370.00616	1883.98569	2209.
20	2690.92172	3236.99515	2333.24653	2761.44568	1913.38465	1969.77886	2155.70911	2864.15492	2484.40583	2274.32393	2309.
21	3085.18588	3082.75376	2526.28061	3365.70151	2939.99423	2452.23433	1911.82371	2244.1403	2160.08989	3093.37919	2270
22	2990.04342	4319.20065	3140.55445	2898.08279	2548.18332	2909.9695	1299.7785	1713.78779	2127.95868	1973.28142	2407.
23	2637.71237	3067.25195	2068.65924	3422.81584	2444.5324	2811.15536	1830.14901	3135.89736	1360.02652	2632.07068	2382.
24	2446.70811	2545.02602	2956.37091	3493.95956	2003.84226	2114.36901	1925.41423	3556.07937	1762.4675	3640.43928	2590.
25	3059.99068	3192.08362	2740.86756	3799.99383	3215.66777	1958.38053	1950.58863	2424.28444	2321.36361	2120.74459	2930.

Appendix 7: RSCoin Model Schema



REFERENCES

[1] George Danezis, Sarah Meiklejohn, Centrally Banked Cryptocurrencies, 2016

[2] Erik Hillbom, Tobias Tillstrom, Applications of smart-contracts and smart-property utilizing blockchains, 2016

[3] Eric Wall, Gustaf Malm, Using Blockchain Technology and Smart Contracts to Create a Distributed Securities Depository, 2016

[4] Mabvuto Mwale, Modelling the Dynamics of the Bitcoin Blockchain, 2016

[5] U.S. Department of Homeland Security, Risks And Threats Of Cryptocurrencies, 2014

[6] Banji Inoue, Performane of Bitcoin Protocol Variants, 2016

[7] Meni Rosenfeld, Overview of Colored Coins, 2012

[8] Michal Zima, Coincer: The Decentralized Cryptocurrency Exchange, 2015

[9] Matthew D. Sheppard, Implementing the Central Bank Functionality of RSCoin, a Centrally Banked Cryptocurrency. 2016

[10] Bc. Michal Zima, Coincer: The Decentralized Cryptocurrency Exchange, 2015

[11] The Komodo Organization, BarterDEX: A Decentralized, Open-Source Cryptocurrency Exchange, Powered by Atomic-Swap Technology, 2017

[12] Loi Luu , Yaron Velner, KyberNetwork A trustless decentralized exchange and payment service, 2017

[13] Dmitry Zaretskii, Sergei Dobrovolskii, Victor Laskin, Michael Berman, Open Trading Network Uniting the Crypto World, 2017

[14] Iddo Bentov, Yan Ji, Fan Zhang, Yunqi Li, Xueyuan Zhao**,** Tesseract: Real-Time Cryptocurrency Exchange using Trusted Hardware, 2017

[15] Vitalik Buterin, Chain Interoperability, 2016

[16] JP Koning, Fedcoin: A Central Bank-issued Cryptocurrency, 2016

[17] Rodney J. Garratt, The Future of Money: Digital Currency, 2018

[18] Alex Lipton, Thomas Hardjono, Alex Pentland, Digital trade coin: towards a more stable digital currency, 2018

[19] Sahil Gupta, Patrick Lauppe, Shreyas Ravishankar, Fedcoin A Blockchain-Backed Central Bank Cryptocurrency, 2017

[20] Rod Garrat, CAD-coin versus Fedcoin, 2016

[21] European Union, Virtual Currencies, Monetary Dialogue 2018

[22] Marco Koevoets, Monetary Policy Implications for the trade-off between a Private Digital Currency and a Central Bank Issued Digital Currency, 2017

[23] European Central Bank, Impact of digital innovation on the processing of electronic payments and contracting: an overview of legal risks, 2017

[24] Eswar Prasad, Central Banking in a Digital Age: Stock-Taking and Preliminary Thoughts, 2018

[25] Paolo Tasca, Digital Currencies:Principles, Trends, Opportunities, and Risks, 2015

[26] Garrick Hileman, Michel Rauchs, Global Cryptocurrencybenchmarking Study, 2017