Digital cash and anonymous fair-exchange payment protocols
Danushka Jayasinghe

Technical Report
RHUL–ISG–2016–6
5 April 2016
Title: Digital Cash and Anonymous Fair-Exchange Payment Protocols.

Supervisor: Dr Kostantinos Markantonakis

Submitted as part of the requirements for the award of the MSc in Information Security at Royal Holloway, University of London.

I declare that this assignment is all my own work and that I have acknowledged all quotations from published or unpublished work of other people. I also declare that I have read the statements on plagiarism in Section 1 of the Regulations Governing Examination and Assessment Offences, and in accordance with these regulations I submit this project report as my own work.

Signature:

Date:
Acknowledgments

This project would not have been possible without the support and guidance from a number of people. First and foremost, I am grateful to my supervisor, Dr Konstantinos Markantonakis for his supervision during the full lifecycle of the project and for many enlightening discussions related to the project. I am thankful for his approachability, invaluable feedback and encouragement.

I special thank goes to my parents, sisters, Madu and all my friends for their love, support and encouragement throughout the project.

Last but not least, I would like to thank everyone who participated in my online survey.
Executive Summery

The e-commerce market is growing and is expected to double from a value of €755 billion in 2010 to an expected €1460 billion in 2015 [57]. Recently, consumers have shown interest in Alternative Payment methods other than credit/debit card based transactions. This fact is further established by the online survey carried out by the author of this project. The online survey attracted 73 anonymous participants. The full results analysis is attached in Appendix C.

Anonymity and Fair-exchange are two important attributes that consumers anticipate in e-commerce payment transactions. The main contribution of this project is the proposed protocol discussed in Chapter 6. The protocol guarantees anonymous fair-exchange in e-commerce transactions by using BitCoin with improved unlink-ability. The proposed protocol is a practical and widely deployable solution in the current e-commerce system.

This project carried out an extensive research to thoroughly identify Digital Cash and Anonymous Fair-exchange Payment Protocols. The report thoroughly examined the BitCoin payment system and identified a vulnerability of BitCoin transactions that significantly draw anonymity and privacy concerns. The vulnerability makes it possible to link BitCoin transactions from the payer to payee which in some cases could reveal their identity.

The proposed protocol uses BitCoin as the anonymous payment method and finds a solution to resolve BitCoin transaction linking. The protocol involves a Trusted Third Party (TTP) to achieve strong-fairness. The previously mentioned BitCoin transaction unlink-ability is achieved by the proposed TTP key generation, key management and transaction tracking solution as illustrated in Table 6.2.

Lastly the report suggests recommended future work based upon the project achievements and online survey results analysis. The recommended work addresses further improvements to the proposed protocol and research in the field of Digital Cash & Anonymous Fair-exchange.
List of Figures

Figure 2.1: E-Commerce Payment Systems, Fieldwork. ..................................................6
Figure 2.2: E-Commerce Compound Annual Growth Rate (%), [57]. ..............................7
Figure 2.3: Two Distinct Types of Electronic Money, Fieldwork. ..................................9
Figure 2.4: Fundamental properties of Digital Cash, Fieldwork. .................................13
Figure 2.5: The Basic Structure of a Digital Cash Transaction, Fieldwork ..................15

Figure 3.1: Generation of a Standard BitCoin Public Key, Fieldwork .........................30
Figure 3.2: The chain of transactions [24]. .......................................................................31
Figure 3.3: Transaction Hashes in a Merkle Tree [24]. ................................................33
Figure 3.4: Traditional privacy vs BitCoin privacy of transactions [24]. ...........................34

Figure 4.1: Two Distinct Types of Fair-exchange protocols, Fieldwork .......................36
Figure 4.2: Coffey & Saidha non-repudiation protocol, Fieldwork ..............................40
Figure 4.3: Participants and inter-relationships of the protocol [54]. ..............................48

Figure 5.1: Alternative electronic payment methods, Online survey results. ...............57
Figure 5.2: Payment attributes importance, Online survey results. ..............................58
Figure 5.3: Privacy concerns, Online survey results. ....................................................59
Figure 5.4: Checkout app, e-wallet, payment page crashed, Online survey results. .........60
Figure 5.5: Acceptance of a TTP in a payment system, Online survey results. ..........60
Figure 5.6: A TTP increases confidence in a payment system, Online survey results. ......61
Figure 5.7: WordCloud of what consumers said, Online survey results .......................61

Figure 6.1: Proposed protocol message flow, Fieldwork. .............................................65

Figure A-D1: BitCoin Payment, Screenshot .....................................................................106
Figure A-D2: BitCoin Mining, Screenshot ........................................................................108
List of Tables

Table 2.1: E-Commerce Alternative Payment Growth Share (%), [57]. ........................................... 8

Table 5.1: Comparison of four On-line TTP Protocols, Fieldwork. ............................................. 56

Table 6.1: Notation used in the proposed protocol. ........................................................................ 63
Table 6.2: TTP BitCoin Keys Generation, Key Management & Tracking Solution, Fieldwork. ... 75
Table 6.3: Proposed Protocol & Other On-line TTP Protocols Comparison, Fieldwork. .......... 80
Abbreviations

C Consumer / Customer

M Merchant

TTP Trusted Third Party

BP2P BitCoin Peer to Peer Network

Peer Node in the BitCoin network

Pseudo-ID-C Unique Pseudonym-Identity of C registered with the TTP.

Pseudo-ID-M Unique Pseudonym-Identity of M registered with the TTP.

AP Alternative Payment

EM Electronic Money

BS Blind Signature

TPM Trusted Platform Module

CFN Chaum, Fiat & Naor Scheme

POS Point of Sale

EMV Europay, MasterCard and Visa standard

CPU Central Processing Unit

GPU Graphics Processing Unit

ASIC Application Specific Integrated Circuit

ECDSA Elliptic Curve Digital Signature Algorithm

NRS Non-Repudiation Server

PPOO Partial Proof Of Origin

POO Proof Of Origin
<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DoS</td>
<td>Denial Of Service</td>
</tr>
<tr>
<td>EPO</td>
<td>Electronic Payment Order</td>
</tr>
<tr>
<td>SS</td>
<td>Secure Server</td>
</tr>
<tr>
<td>EOO</td>
<td>Evidence Of Origin</td>
</tr>
<tr>
<td>MO</td>
<td>Mobile Operator</td>
</tr>
<tr>
<td>SIM</td>
<td>Subscriber Identity Module</td>
</tr>
<tr>
<td>DC</td>
<td>Delivery Cabinet</td>
</tr>
<tr>
<td>PA</td>
<td>Payment Applet</td>
</tr>
<tr>
<td>MA</td>
<td>Merchants Applet</td>
</tr>
<tr>
<td>MP</td>
<td>Mobile Phone</td>
</tr>
<tr>
<td>APDU</td>
<td>Application Protocol Data Unit</td>
</tr>
<tr>
<td>NFC</td>
<td>Near Field Communication</td>
</tr>
</tbody>
</table>
# Table of Contents

Acknowledgments ......................................................................................................................................... ii  
Executive Summary ................................................................................................................................. iii  
List of Figures ........................................................................................................................................ iv  
List of Tables ........................................................................................................................................ v  
Abbreviations .......................................................................................................................................... vi  
Table of Contents ................................................................................................................................... viii  

1 Introduction............................................................................................................................................ 1  
1.1 Motivation of the thesis .................................................................................................................. 1  
1.2 Objectives of the thesis ................................................................................................................ 4  
1.3 Structure of the thesis .................................................................................................................... 5  

2 E-Commerce Payment Systems ........................................................................................................... 6  
2.1 Current Electronic Payment Systems .......................................................................................... 6  
2.2 Electronic Money .......................................................................................................................... 9  
2.3 What is Digital Cash? .................................................................................................................. 10  
2.4 Properties of Digital Cash.......................................................................................................... 11  
2.5 Anonymity .................................................................................................................................... 13  
2.6 The Basic Structure of a Digital Cash System .......................................................................... 14  
2.7 The Fundamental Problems ....................................................................................................... 15  
2.8 A Solution that Revolutionized Digital Cash ........................................................................... 16  

3 Anonymous Payment Protocol Schemes & Implementations .......................................................... 17  
3.1 Payment Protocol Categories ....................................................................................................... 18  
3.1.1 On-line payment schemes ........................................................................................................ 18  
3.1.2 Off-line payment schemes ....................................................................................................... 19  
3.2 Protocol Schemes ......................................................................................................................... 21  
3.2.1 Chaum, Fiat & Naor Scheme (Basic anonymous Cash) .............................................................. 22  
3.2.2 Ferguson scheme (Revocable Anonymous Cash) .................................................................. 24  
3.3 Real World Implementations ........................................................................................................ 26  
3.3.1 DigiCash ................................................................................................................................... 26  
3.3.2 CyberCash ............................................................................................................................... 26  
3.3.3 Mondex wallet ......................................................................................................................... 27  
3.3.4 BitCoin ..................................................................................................................................... 28  

4 Fair-exchange Protocol Schemes & Implementations ....................................................................... 35
4.1 Two party based protocols (Gradual-exchange).................................................................37
4.2 Protocols based on a Trusted Third Party........................................................................39
  4.2.1 In-line TTP based protocols .........................................................................................39
  4.2.2 On-line TTP based Protocols ....................................................................................43
  4.2.2 Off-line TTP based protocols .......................................................................................51
5 Security Attacks & Online Survey Results........................................................................52
  5.1 Potential threats and attacks..............................................................................................52
  5.3 What is stopping Digital Cash?.........................................................................................57
    5.3.1 Consumer Perspective of Digital Cash.................................................................59
6 Proposed Protocol..............................................................................................................62
   Anonymous Fair-Exchange Payment Protocol using BitCoin with Improved Unlink-ability ....62
7 Conclusion...........................................................................................................................81
  7.1 Summary & Conclusion ................................................................................................71
  7.2 Recommended Future Work..........................................................................................84
Bibliography..........................................................................................................................85
Appendix A............................................................................................................................95
  Cryptographic Primitives..................................................................................................95
Appendix B............................................................................................................................98
  Definitions.........................................................................................................................98
Appendix C............................................................................................................................99
  Online Survey Results .....................................................................................................99
Appendix D............................................................................................................................105
  BitCoin Walkthrough.......................................................................................................105
CHAPTER 1

Introduction

1.1 Motivation of the thesis

Modern technological advancements have given a dramatic boost towards the evolution of the Internet. Since the time CERN first opened their external TCP/IP connections to the outside World and their immense contribution to the development of the World Wide Web; the Internet has rapidly expanded to interconnect most of the parts of our World together and even beyond [55]. A strong outcome of this global expansion of internetworked technology is the emergence of electronic commerce. E-commerce touches every aspect of our day to day lives; from shopping with your local supermarket chain to get your necessities delivered to your door step to making an online payment for your music downloads to a merchant who operates in the other side of the world. In the last few decades there have been a significant increase in the number of consumers opting in for online shopping and the number of E-commerce transactions carried out every day, globally is simply incomprehensible [15, 56, 57, 58]. E-commerce is a fruitful platform for merchants and businesses by giving them the ability to reach out towards a diversified consumer base from different parts of the world. Likewise, E-commerce has given consumers the freedom of choice to select from a large number of merchants that best suit the consumer’s need and requirement. E-commerce transactions between consumers and merchants occupy a significant proportion of the overall transactions carried out and these transactions are paid for by using Electronic Payment Schemes.

According to a recent report published by Worldpay, the e-commerce market is growing and is expected to double from a value of €755 billion in 2010 to an expected €1460 billion in 2015 [57]. While Credit/Debit card payment schemes dominate a majority of the e-commerce payment transactions, there are other Alternative Electronic Payment schemes such as Real Time Bank Transfers, Offline Credit, Direct Debit, eWallets, Mobile Payments and Digital Cash which also provide a way to complete payment transactions at present [13, 57]. In a traditional Point-of-Sale (POS) transaction, the parties involved does not have to be much concerned regarding the
guaranteed delivery of the purchased product or the guaranteed payment for the sold product visa-versa. This is due to the fact that the transaction is carried out in a face to face environment in a physical shop. Furthermore, the consumer can make a simple payment by using cash for the goods and services he/she purchased without handing in their personal or financial details to the merchant and other third parties. However, a buying and selling transaction in e-commerce is much different from the previously explained [12]. E-commerce transactions between the involved consumers and sellers occur over the internet in a virtualized environment. In such an environment where transacting parties do not see each other physically makes it possible for a dishonest party to misbehave. As such, a merchant could simply not deliver the goods to a consumer once the payment is received or a consumer could simply disappear without paying a merchant once goods have been received. This fact places immense pressure upon e-commerce services, genuine merchants and payment solution providers to implement mechanisms that would guarantee payment settlement for purchases. Due to this reason, unlike in conventional cash payments during a POS transaction, in an e-commerce setting a consumer might lose privacy by having needed to provide personal and financial information to merchants and third parties.

Most of the current electronic payment methods do not provide anonymity of consumer to protect consumer privacy and provide security of financial information to guarantee the security of the transferred value at the same time [13, 59]. This makes it a trade-off between security of financial information and anonymity of consumer. An example of this is a bank card user is secured from money loss but the payment is not anonymous. In contrast to this, a consumer using a gift card or a top up card is anonymous but there is no security for the money stored in the card, as it cannot be linked to the customer’s identity. Nonetheless, current payment schemes have failed to replace real cash (notes & coins) by providing users with properties such as anonymity, divisibility (ability to break into smaller denominations) and transferability (ability to pass from one owner to the other). The concerns discussed above have attracted attention of e-commerce service providers, financial institutions as well as researches to find a solution to give involved parties the freedom of making anonymous payments without unnecessarily having to reveal personal details and to guarantee fair-exchange of goods and services without any misbehaving [7, 11, 13, 24, 33].
The underlying mechanism which provides payment services for involved parties in an e-commerce transaction is called an e-commerce payment protocol. A protocol is “a set of rules governing the exchange or transmission of data between devices” [60]. Protocols that are built to achieve fairness in e-commerce transactions are called Fair-exchange Protocols. Protocols that help realise anonymity and user privacy during payment are called Anonymous Payment Protocols. Digital Cash which would be introduced in Chapter 2, is a variant of Anonymous Payment Protocols that provides true anonymity similar to conventional cash. A combined solution that would realise fairness as well as anonymity is called an Anonymous Fair-exchange Payment Protocol.

A number of Digital Cash / Anonymous Fair-exchange Payment Protocols for exchanging electronic content have been proposed in academic literature along with few real world implementations [1, 7, 8, 24, 35, 40, 54]. The thesis involves identifying these initiatives (e.g. digital cash with anonymity, BitCoins, Fair-exchange protocols etc), considering attack strategies and more importantly propose improvements to realise fairness and anonymity. The project is intended to add value to current academic literature and support real-world implementations by strengthening the protocols with improved fairness, anonymity and against attack strategies discussed. The thesis will propose a new protocol in Chapter 6 to achieve fair-exchange in an e-commerce transaction which can be used in conjunction with a real-world anonymous payment implementation. The need for a payment scheme that facilitates properties of real money, guarantee fairness and that could equally compete with current payment schemes is foreseeable in the near future. In the context of fair exchange should there be a dispute or misuse the protocols should provide a feature of tracing back transactions by the intervention of a trusted authority only when needed. Eventually the consumer as well as the merchant shall benefit from a more secure and an anonymous payment scheme providing privacy and fair exchange.
1.2 Objectives of the thesis

The following have been identified as the main objectives to achieve the aim of the project.

- Identify digital cash protocols/fair-exchange anonymous protocols.
- Examine existing security measures, fairness, anonymity and vulnerabilities.
- Propose countermeasures and improvements for underlying protocols.
- Propose an anonymous fair-exchange payment protocol which is a practical and widely deployable solution in the current e-commerce system.

A methodical structure for the thesis is introduced to achieve the objectives listed above. Firstly, a brief overview of the current e-commerce protocols and payment schemes is carried out to differentiate anonymous and fair-exchange payment protocols from other conventional e-commerce payment schemes. The report should identify and elaborate the differentiated protocols in detail. The thesis will identify properties of digital cash and the fundamental problems of anonymity and double spending will be elaborated.

The thesis will carry out a research to identify the building blocks of these protocols, where cryptographic primitives such as blind signatures and zero knowledge proofs are examined. After identifying the primitives, different protocol schemes and real world implementations are reviewed to discover existing security measures, potential vulnerabilities and importantly for what extent the protocol achieve fair-exchange and anonymity is analysed.

What learned from the protocol analysis and shortcomings in identified protocol schemes will be considered while proposing further improvements for the underlying protocols. Furthermore, an online survey will be conducted to gain insight of consumer perspective of the use of Digital Cash and Fair-exchange in e-commerce. The results will be analysed to find out answers to questions such as; Are consumers more concerned about anonymity while making payments? and What consumers see as needed requirements in a viable anonymous and fair exchange payment system for the future? Finally, an Anonymous Fair-exchange Protocol for a currently implemented Anonymous Payment Solution will be proposed. The proposed protocol will be analysed to identify for what extent the protocol achieve fairness and anonymity.
1.3 Structure of the thesis

The entire thesis is categorized into seven main chapters. Discussed above in Chapter 1, the report explained the motivation of the thesis, main objectives, structure of the thesis. Chapter 2 will explore current e-commerce payment systems and gradually attempt to distinguish Digital Cash from other payment models while referring past literature to identify properties of Digital Cash. The chapter will further introduce basic structure of anonymous payment protocols and key milestones in past research in the field.

Chapter 3, the report will carry out an extensive research into Anonymous Payment Protocol Schemes and Implementations. These include a study of used cryptographic primitives and identifying various proposed anonymous payment schemes. Furthermore, the research will identify real-world implementations of anonymous payment systems including the handful of protocols which have succeeded. Chapter 4, the report will carry out an extensive research into Fair-exchange Payment Protocol Schemes and Implementations. The chapter will define fairness in e-commerce and emphasise the importance of fair-exchange for both consumers and merchants. The report will extensively research proposed protocols and examine the protocol runs in detail to evaluate how fair-exchange and anonymity is achieved.

Chapter 5, will look into the security aspects of these protocols and attempt to find vulnerabilities and potential attacks. The report will analyse protocols to identify to what extent fairness and anonymity is realised. The results of the online survey will be analysed to give a consumer perspective of the use of Digital Cash and Fair-exchange in e-commerce. Based on the results the report will critically analyse current technological advancements and attempt to identify reasons as to why anonymous and fair exchange payment protocols have not succeeded compared to other payment schemes.

Chapter 6, the thesis will propose a Fair-exchange Protocol with the Anonymity Payment support with a real-world implementation. The proposed protocol will be analysed to evaluate fairness and anonymity. Potential vulnerabilities and attacks will be identified. Chapter 7, will summarize the entire thesis with a brief discussion to future work related in the field and laying out a conclusion of thesis findings.
CHAPTER 2

E-Commerce Payment Systems

2.1 Current Electronic Payment Systems

Electronic Commerce is a model of buying, selling, exchanging products and services over the internet by using electronic devices such as computers and mobile phones [15]. In e-commerce the buyers are given the opportunity to make purchase decisions, and follow a series of steps electronically rather than in a physical store. “The series of steps include enabling a consumer to access information, select items to purchase, make secure payments and having the payment settled financially”[61]. As described in Chapter 1, modern e-commerce ecosystem has developed dramatically over the last few decades and holds a multi billion market. A recent report published by Worldpay predicts that the e-commerce market is growing and is expected to double from a value of €755 billion in 2010 to an expected €1460 billion in 2015 [57]. The payments for these e-commerce transactions are carried out using electronic payment systems also known as payment models [16]. There are a number of electronic payment systems (payment models) available to facilitate e-commerce transactions and these payment models are implemented by using a variety of different payment schemes [56, 57]. Some of the widely used payment models are shown in Figure 2.1.

![E-Commerce Payment Systems](image-url)

*Figure 2.1: E-Commerce Payment Systems, Fieldwork.*
Credit/Debit Card based online payments dominate more than 60% of overall e-commerce payment processing [56]. However, Alternative Payment (AP) methods (other electronic payment methods except for card based payments) that compete with card based market leaders are growing fast in a rapid phase. Worldpay estimates that there are over 230 individual AP methods globally and processed €165 billion e-commerce transactions out of €755 billion in 2010, which is about 22% market share. The graph shown below illustrates recent e-commerce payments market shares between card based online payments and AP. The graph also illustrates a projected growth rate by 2015. It is evident by observing the graph that the growth rate of Alternative Payments is believed to surpass the growth rate of card based payments by 2015.

Figure 2.2: E-Commerce Compound Annual Growth Rate (%), [57].
Furthermore, the table shown below compares a few widely used AP methods from an estimated spectrum of over 230 schemes. The comparison also shows that significant percentage wise growth or decline of each individual payment type by 2015. According to the table, eWallets, Real-time Bank Transfers and Mobile Payments achieve significant growth while Paper Based (cheques to postal orders and even cash on delivery), Offline Credit and Direct Debit payments lose market share.

<table>
<thead>
<tr>
<th>Type</th>
<th>Share of AP Today</th>
<th>Share of AP by 2015</th>
</tr>
</thead>
<tbody>
<tr>
<td>Real time bank transfer</td>
<td>12%</td>
<td>20%</td>
</tr>
<tr>
<td>Offline credit</td>
<td>20%</td>
<td>15%</td>
</tr>
<tr>
<td>Direct debits</td>
<td>10%</td>
<td>8%</td>
</tr>
<tr>
<td>eWallets</td>
<td>36%</td>
<td>43%</td>
</tr>
<tr>
<td>Paper based</td>
<td>22%</td>
<td>14%</td>
</tr>
<tr>
<td>Mobile</td>
<td>0.8%</td>
<td>1.2%</td>
</tr>
</tbody>
</table>

*Table 2.1: E-Commerce Alternative Payment Growth Share (%), [57].*

By statistically comparing the data in Figure 2.2 and Table 2.1, it is evident that due to the open nature in e-commerce, consumers are migrating from traditional methods that dominate current e-commerce payment market to Alternative Payment methods. Shown in the table above are just a few candidates from a large variety of AP methods. Another type of Alternative Payment method which has attracted consumer attention and interest is Digital Cash [17, 24]. Digital Cash will be introduced in section 2.3 of the report. It is a variant under the alternative payment category called Electronic Money. Electronic Money (EM) will be defined under the next section 2.2. The underlying protocol mechanism of Digital Cash falls under Anonymous Payment Protocols category. One of the motivations of this project as described in Chapter 1, is to find improvements that could enhance anonymity and fairness between merchants and consumers engaged in an e-commerce transaction. The thesis will discuss these underlying protocols in detail in Chapter 3 and 4. However, it is wise for the reader to have a flavour of Digital Cash and its properties within this chapter.
2.2 Electronic Money

Electronic Money in the context of e-commerce can be broadly defined as an electronic storage of monetary value on hardware or software system that is used to make payments and can be exchanged electronically [17]. Electronic Money can be categorized into two distinct types as shown below.

![Identified e-money](image1)

![Anonymous e-money](image2)

**Figure 2.3: Two Distinct Types of Electronic Money, Fieldwork.**

Identified e-money reveals the payer’s identity, who initially withdrew electronic cash from the issuing bank. As the money gets transferred through the economy an audit-trail of payers and payees are also left by these identified e-money schemes [18]. In contrast, anonymous e-money does not reveal the identity of the payer or payee and does not leave any transaction trail. Digital Cash comes under this category of Electronic Money and provide anonymity for the user. As mentioned in the previously the underlying mechanism or set of instruction that manages the operation id called anonymous payment protocols.

The report distinguished two categories of Electronic Money. These Identified and Anonymous e-money can be implemented in a payment mechanism in two ways. The implementation sometimes may require the participants of the transaction to contact a Bank or a Trusted Third Party (TTP – An honest authority that would not collude with the participating parties) during the transaction to get verifications. Depending whether the protocol requires the participants to connect to Bank or a TTP categorises implementations into two types called On-line systems and Off-line systems. The two categories are described below.
- **On-line system** – the participants who engage in an e-commerce transaction have to connect to the bank or a trusted third party (TTP) during the transaction (protocol run) to authenticate the transaction.

- **Off-line system** – the participants do not have to directly interact with a bank or a TTP during the transaction to validate the electronic money. Offline anonymous e-money protocols are also known as *True Digital Cash* which are complex designs due to possible double spending which is discussed in section 2.7 [18].

### 2.3 What is Digital Cash?

The report gave a brief introduction to Digital Cash in *Chapter 1* and *section 2.1.*, as a payment scheme that could replace current payment protocols by adapting properties of real cash while providing anonymity to preserve user privacy. The concept of providing anonymity in payment schemes was first proposed by David Chaum in 1982 [9]. He introduced *Blind Signatures* as an cryptographic primitive that would allow to construct untraceable payment solutions. Since his proposal was published, a whole new research era began in the field of anonymous payment protocols [10]. Chaum’s protocol will be thoroughly investigated later in *Chapter 3*.

Digital Cash is a form of digital currency informally known as electronic cash, crypto currency, digital coins, e-cash, D-cash, ect. Digital Cash provides anonymity for the user by safeguarding identity of the digital cash holder, financial sensitive information and consumer spending habits from Merchants, Banks and Other Third Parties [10, 12]. It is important to distinguish Digital Cash from other e-commerce payment protocols due to its properties that enhance the security and privacy of an e-commerce user. Unlike other payment schemes that dominate e-commerce payment transactions, anonymous payment protocols provide true properties of real money and are easily distinguishable. These properties are discussed in the next heading.
2.4 Properties of Digital Cash

Digital Cash was invented to provide its users the ability to enjoy the freedom of real money (conventional notes and coins) while carrying out e-commerce payment transactions. Due to this reason these protocols mimic some properties of real cash. In 1991, T. Okamoto and K. Ohta first identified six key properties that Digital Cash should have to equally match real money [14]. Further to this, in 1995, J. Matonis proposed a further four properties for a successful Digital Cash system [11]. From time to time as consumer requirements grow in-line with technological advancements, these properties may change and have new properties added on. Some of the properties identified by the authors mentioned above are mentioned below respectively;

1. **Security** – the payment scheme should provide a higher level of security by preventing forgery and misuse. This means that, either participating parties or a third party cannot manipulate values or reproduce Digital Cash.

2. **Anonymity** – this is by far the most influential property of real cash, that it is anonymous and by examining money it cannot be traced back to a transaction or even to a single individual. This gives money holders freedom of making payments without disclosing any personal information. True Digital Cash is proposed to have the same property by making a user’s digital coin unlikeable to an individual and by making it untraceable to a transaction. This way a user’s privacy is protected.

3. **Transferability (Two-way)** – this property emphasise the ability of transferring digital coins with other parties. This eliminates the need of having to contact the bank and to be valid registered users of merchants before any transaction is carried out. This is similar to the way real money is transferred from one person to the other.

4. **Portability** – this property indicates that digital cash should not be restricted to one substantial location but should be easily moved to other storage devices. This also highlights the fact that digitally stored values are easily accessible and not restricted to a single computer network.
5. **Off-line capability** – this means that the payment protocol should provide the capability to carry out a digital cash transaction without having to be connected to an online third-party to obtain authorization. These also mean that neither party is required to be connected to the host during the transaction [14].

6. **Divisibility** – this means that an original digital coin value can be subdivided into smaller denominations. This gives smaller digital coin values to make small value transactions. This also allows making off-line transactions without having a collection of all the smallest denominations.

7. **Infinite Duration** – this proposed property characterises that digital cash does not expire and it holds value for a very long period of time, provided that the issuer is still in business [11].

8. **Wide Acceptability** – this property states that the digital cash should be well recognised and accepted in a large commercial zone. With a number of digital cash providers advertising wide acceptability a user can use a preferred unit in a wider zone other than restricting to a local environment [11].

9. **User Friendly** – for the end user the protocol should be easy to use in both paying and receiving aspects. A protocol that is very simple attracts consumers than a very complex payment scheme that users find difficult to handle. If the system is difficult then users may change issuers. Due to this reason simplicity leads to mass use and mass use lead to wide acceptability [11].

10. **Unit of value freedom** – J. Matonis in his paper proposed that the digital cash scheme should have the freedom of paying by digital cash regardless to the country’s or governments fixed currency. The user should be able to digital cash in any defined unit to merchants and other users by not being restricted to a single digital cash unit [11].
The properties mentioned above are proposed and ideal properties but it will be evident from later chapters that it is extremely difficult to achieve all these properties in a single payment scheme. Illustrated in Figure 2.4 below are the above mentioned fundamental properties of Digital Cash.

![Properties of Digital Cash Diagram](Image)

Figure 2.4: Fundamental properties of Digital Cash, Fieldwork.

2.5 Anonymity

As discussed in section 2.4 under properties of digital cash, anonymity is a key property that could map real cash with electronic cash. The property of anonymity gives the bearer the freedom of making a purchase in the world of e-commerce without having to reveal personal information such as names and card details to merchants or banks.
Unlike Digital Cash systems, most of the e-commerce payment schemes are ‘privacy invading systems’ as they make the user disclose privacy. Most of current protocols emphasize in making the payment transactions secured from fraudulent activities and unauthorised interceptions. Due to the increased security to prevent fraud users have to provide personal and financial information during transactions. This factor makes it difficult to protect consumer privacy while making purchases with current payment systems [4]. The legitimate consumer has a right to remain anonymous to safeguard their payment history, shopping history, shopping patterns, account details and consumer behavioural patterns as they are personal information. While this is true for a genuine user in the wrong hands, anonymity could result in money laundering, blackmailing, illegal purchasing and forgery. More anonymity means less security vice versa [4]. Due to this reason since Chum’s initial proposal to provide unconditional anonymity, further research began to find ways to revoke anonymity should a user acted fraudulently or miss behaves by double spending [8].

2.6 The Basic Structure of a Digital Cash System

There are three main participants in a basic Digital Cash system. They are; The financial bank, The consumer (payer) and The merchant (payee). During a basic Digital Cash transaction, the above mentioned parties engage in three basic protocols. They are;

- **Withdrawal** – this is when the payer withdraws Digital Cash from the bank.
- **Payment** – the payer transfers the coins to the payee.
- **Deposit** – the payee deposit the received Digital Cash in the bank.
2.7 The Fundamental Problems

When it comes to Anonymous payment schemes and protocol design such as Digital Cash, there are two major problems that should be taken in to consideration. They are;

1. Is it guaranteed that the protocol provide anonymity?
   What if the issuing bank, knows what digital coins it gives Alice and on a later date Bob deposits the same digital coins that the bank recognised, and then the bank can infer that Alice has paid Bob. This breaches anonymity by revealing users identity.

2. How does the protocol prevent double spending?
   As discussed in section 2.4: ‘properties of digital cash’, portability is a fundamental property of a digital cash system. This makes it easy to copy or move digital cash from one media to another such as a portable storage and as electronic content can be easily duplicated, it is a big challenge to stop users from spending the same digital coins more than once. This multiple spending is called double spending and a good implementation should address this issue.
2.8 A Solution that Revolutionized Digital Cash

The theoretical background to provide anonymity in e-commerce protocols was first proposed by D. Chaum in 1982 after his introduction to blind signatures. In his paper he proposed a way to achieve untraceable electronic payment using blind signatures (BS) \[9\]. BS falls under digital signatures category. Unlike in digital signatures where a person is familiar with the content which is signed, a person placing a blind signature will have no or only partial information of what is being signed. Similar to digital signatures, blind signatures also provide data origin authentication but while providing anonymity to the user identity. This way Digital Cash protocols can be designed using this cryptographic primitive which will be discussed in aChapter 3.

As discussed in section 2.2, Electronic Money is categorised in to Online and Offline e-money payment systems during implementation. Online systems prevent double spending by verifying the digital coins during transactions to see whether the coin has been used in the past or to see whether it has been duplicated. If a coin was found compromised during this verification the protocol stops. In contrast to Online systems, double spending is a major concern in Offline digital cash systems. Since the coins are not verified during transfer there must be extra mechanisms to prevent double spending. There are two distinct ways this issue is addressed. They are;

- By using cryptographic protocols that reveals the identity of payer if double spent.

- By using an “Observer Device” that keeps database of all the transactions of a coin. This prevents a coin from being double spent as the database will indicate whether the coin was used before. A strong candidate for the “Observer Device” is a Smart Card which is tamper resistant from outside parties and provides a secure execution environment \[23\].
CHAPTER 3

Anonymous Payment Protocol Schemes & Implementations

Anonymity in e-commerce is useful in three main scenarios. The first is when only one of the involved parties wants to be anonymous. This could be a Business-2-Customer model where only the consumer wants to remain anonymous to protect personal information and spending habits but on the other hand the merchant does not want to be anonymous. Second scenario is when both parties involved in an e-commerce transaction wants to remain anonymous. This might be the case in a Customer-2-Customer setting where both buying and selling individual wants to remain anonymous to each other. Thirdly, it would be a scenario that two parties might already know each other but want to remain anonymous so that they would not learn about each other’s transactions. For an example it could be a merchant who has a very long commercial relationship with a customer and both parties does not want any other party knowing this fact.

Depending on the above mentioned three scenarios existing anonymous e-commerce schemes uses anonymity channels [30]. These channels carry a number of messages between nodes and then change using a cryptographic process in an unrecognisable way to make eavesdropping difficult and to communicate anonymously with the involved parties. Even though, anonymity channels help hiding the true identity of the sender from the receiver and eavesdropper, it still does not provide stable anonymity as the message itself could leak the sender’s identity [8].

Furthermore, Jakobsson M. et al. identified e-commerce schemes based on three types of anonymity levels. They are; perfect privacy, revocable privacy and limited privacy [33]. Perfect privacy provides unconditional anonymity to the protocol entities while making their identity unknown. However, criminals and malicious users can take advantage of this feature to engage in fraudulent activities and even to double-spend used coins. Due to this reason the second type of privacy was needed. Revocable privacy is achieved in a protocol by the introduction of a Trusted Third Party (TTP) who can revoke the identity of an anonymous owner of a coin if the
coin gets double-spend. The last category of limited privacy makes a user only anonymous to a merchant but not the coin issuing bank.

In section 2.4 the report introduced ten fundamental properties for a successful Digital Cash payment system. Practically it is extremely difficult to build a payment system with simultaneously provides all of the properties. Due to this reason and the reasons discussed above there are a number of different e-money payment schemes proposed in literature and implemented. The report elaborates upon some of the important schemes and real world implementations.

3.1 Payment Protocol Categories

Anonymous payment protocol systems can be categorised as on-line payment systems and off-line payment systems. These two systems are described below.

3.1.1 On-line payment schemes

David Chaum in 1985 proposed the first on-line anonymous payment system [34]. In an on-line scheme the payer, payee and the bank needs to be connected on-line at least once during the protocol for verification of coins. In the withdrawal phase the customer obtains a valid signature of a coin from the issuing bank without revealing his/her identity. Secondly when the customer wants to pay a merchant anonymously, he/she sends the signed coin to the merchant as payment. The merchant straight away direct it to the bank for validation. The bank then checks whether the coin has been double-spent and if not credits the merchants account. The protocol was the first implementation of blind signatures to achieve user anonymity which was introduced in section 3.4.

In the year of 1989, Burk and Pfitzmann introduced a new payment scheme that uses a special type of user account called ‘standard values’ to achieve anonymity [35]. The system operates by the digital coin issuing bank keeps an anonymous account for each customer with a pre-defined value already deposited in the account. The customers are linked to each account by pseudonyms which make their identity unknown to the bank. After a financial transaction the bank change the
pseudonym of a standard value from the payer to the payee’s pseudonym. This way anonymity is achieved but there is a drawback when the payee of the first transaction is the payer of the second, the bank can link the two transactions to the same user.

Supporting the above mentioned accounts which are kept in a large database in banks, Camenisch at al. in 1994 proposed a new scheme that considerably reduces the size of these databases [28]. The protocol was proposed to benefit the banks by having this new type of anonymous account as an add-on feature to the bank’s current financial infrastructure. The system introduces two main accounts to each customer. One is the personal account and the other is the anonymous account giving the user the ability to transfer money between accounts anonymously. The banks had to query this anonymous database during transactions to detect double-spending. This protocol and the once discussed before that required the participants to connect on-line for the bank to validate the digital coins before the payment was finalised as a deposit to the merchant. This was a major drawback for users and a system that would let them engage in a more flexible without the intervention of the bank during the transaction was much needed. This requirement made researchers propose new anonymous payment schemes that worked in an off-line setting.

### 3.1.2 Off-line payment schemes

Most of the proposed and existing off-line anonymous payment protocols transactions follow an overall similar structure as illustrated in figure 4 in chapter 2. The three transactions are; withdrawal, payment and deposit. The significant aspect in off-line schemes is the fact that the Trusted Third Party (TTP) in this case the bank does not have to be on-line during the protocol run between the payer and the payee. Instead the bank verifies whether coins have been double-spent when the payee presents the coins to the bank to be deposited in to his/her account. The convenience of this protocol is that the payer can make a payment to the payee anonymously without revealing any identity and the payee can accept the payment without having to verify the coins by the bank before accepting the payment. Furthermore this gives flexibility to the involved parties to operate in off-line setting for fast transactions.
However, since the bank does not involve in the protocol run on-line and only gets to check the coins after deposit, this protocol have the drawback of being only able to detect double-spending but not to prevent it. As mentioned above the protocol has three stages, withdraw, payment and deposit. The stage where anonymity is realised depends on the cryptographic primitive used. Both blind signatures and zero-knowledge proofs are equally used in off-line anonymous payment schemes. While using blind signatures the user in the withdrawal stage obtains a signed digital coin. This is when anonymity is given to the user. In contrast while using zero-knowledge proofs the user obtains a certificate from the bank in the withdrawal stage that serves as a digital coin. It is only when the user presents the certificate (here the coin) and the related secret to the payee, anonymity is achieved by the user.

Double-spending is relatively easy in this off-line setting and a way to revoke anonymity to stop black-mailing, money-laundering, illegal purchase and double-spending was needed. In 1988, Chaum et al. proposed an off-line anonymous payment scheme using blind signatures which could revoke anonymity upon detection of double-spending [1]. This protocol will be thoroughly discussed in section 4.2.1. Chum further realised that this scheme only detects double-spending but not prevent it.

In 1988 Chaum introduced an interesting solution by proposing an anonymous payment scheme called wallets with observers [37]. This scheme was proposed to guarantee prevention of double spending as well as detection of compromise, should the wallets had failed. These wallets was devices such as smart cards which is a tamper resistant secure storage micro chip devices, which could be used to store sensitive secret keys and information in a secured manner from attackers [23]. These devices provided a secure environment similar to trusted platform modules (TPM). The observers kept an up-to-date database to prevent coins from being double-spent.

In 1992, Pfitzmann et al. proposed a two-party computational protocol which generated the signature of the coins with the intervention of both the customer and the bank. This operation was carried out in the withdrawal phase in a way that only the customer gets the signed coin and when challenged by the bank the customer can prove that the banks signature is on the coin by issuing a zero-knowledge proof. Due to the number of messages this system increases both
message complexity and encryption complexity making it inefficient even though it provides good privacy.

Comparing both on-line and off-line payment protocols it can be concluded that off-line schemes only provide detection of double-spending and fraudulent activities after the coins get deposited to the bank. In contrast on-line schemes provide on-the-fly prevention and detection of double-spending and fraudulent activity during a protocol run between a customer and a merchant. But on-line schemes require the involvement of a TTP such as a bank to carry out this task of validation of coins before a transaction is completed. Based on this it could be concluded that off-line protocols are more ideal for low-value transactions that does not require prior-verification but require fast transactions. On-line protocols on the other hand are more suitable for high-value transactions that require prior-verification to prevent fraudulent activity such as double-spending.

### 3.2 Protocol Schemes

At present there are a number of real world implementations of digital cash payment systems. While years of research in to conventional centralised Anonymous Payment Schemes and Implementations have not achieved large scale deployment, de-centralised BitCoin by far is the most popular and widely used. Before BitCoin there have been a number of digital cash protocol schemes and real world implementations. It is wise to explore these predecessors to BitCoin to understand the evolution of modern digital cash systems.
3.2.1 Chaum, Fiat & Naor Scheme (Basic anonymous Cash)

Chaum D., Fiat A. and Naor M (CFN) proposed one of the very first off-line anonymous digital cash schemes in late 1980’s. This protocol was build upon Chaum’s blind signature scheme based on RSA and Cut-and-Choose method (as defined in section 3.2.10) [1]. The protocol provides anonymity to the user’s transactions by signing the presented coins in a way that the bank does not learn what it is signing. This prevents the bank from recognizing the same coins when it comes back to the bank for payments. In other words the bank cannot link a specific withdrawal to a specific deposit [4].

However, the protocol detects a user from misbehaving or double-spending by having a method to detect when a coin has been double spend and reveals the coin owner’s identity. Suppose a bank’s public RSA key is \((e, n)\) and two functions \(f\) and \(g\) without any collisions. Here \(f\) acts as a random oracle (something that respond to a unique query with a true randomness) and \(g\) as a one-to-one function. Alice’s bank has a bank account \(u\) and the bank linked the account to Alice using a counter \(v\). \((\oplus\) represents exclusive or and \(||\) represents concatenation).

The withdrawal protocol

1. Alice generates \(k\) number of units, \(U_i\). Each unit is given a random serial numbers, \(a_i, c_i, d_i\), \(1 \geq i \geq k\), from a large pool of numbers to name each one unique [1],[4].

\[
U_i = f(x_i, y_i), \text{ for } 1 \geq i \geq k, \text{ where } x_i = g(a_i, c_i), \quad y_i = g(a_i \oplus (u || (v + i)), d_i)
\]

2. Alice uses random blinding factors \((r_1, ..., r_k)\) to blind all \(k\) units and send them to the bank. This prevents the bank from seeing the content that is given to sign.

\[
B_i = r_i^{k!} U_i \mod n
\]

3. \(k/2\) units are selected randomly by the bank to check what it is signing.

4. Alice provides the bank \(r_i, a_i, c_i, d_i, 1 \geq i \geq k/2\) (assumed that the bank chooses \(i\))

5. Then the bank unblinds \(k/2\) units with the intention of checking whether Alice has not tried to cheat by making the bank sign suspicious content that could be fraudulent. Upon discovering no fraudulent activity the bank finally signs the remaining units with the Bank’s private key and forwards the signed coins to Alice.
The payment protocol

1. Alice sends C to Bob
2. Bob sends Alice a random binary string $z_1, z_2, ..., z_{k/2}$
3. Alice responds by sending the following for all $1 \leq i \leq k/2$ , if $z_i = 1$, then Alice sends Bob $a_i, c_i$ and $y_i$
   $z_i = 0$, then Alice sends Bob $x_i, a_i \oplus (u \parallel (v + i))$ and $d_i$
4. Bob checks whether C is valid before taking Alice’s payment.

The deposit protocol

1. Bob provides the transaction history of the digital coins that he wants to deposit.
2. Bank checks whether its digital signature is valid.
3. Bank checks whether the coins have been already used.
4. The bank records the coins in the used-coins database and records the binary string and the equivalent reply from Alice to facilitate the detection of double spending if the coins are used again [4].

The security of the protocol makes Bob to check the coins he receives are valid. When Bob deposit the money the bank can detect double spending if Alice has used them twice. The bank can identify Alice’s true identity if she double spends. This way Alice’s identity is only revealed to the bank if she double spends as only a half of her identity is provided each time. However, this scheme does not let users to transfer coin ownership from one to another. It also does not provide the property of divisibility.
3.2.2 Ferguson scheme (Revocable Anonymous Cash)

Ferguson scheme is a digital cash system that falls under the category of transferable cash. Transferability as described in section 2.4 is the ability of transferring ownership of a digital coin to a new owner without having been to issue a whole new coin to the new owner. The scheme uses a randomized blind RSA-based signature to blind the coins. Similar to the chum’s scheme the bank does not know completely what it is signing but the bank knows that it is not signing something malicious. The scheme uses three numbers; C, A and B to generate the following [4, 69].

\[ C = c g^{\hat{h}_c}, \quad A = a g^{f(a)}, \quad B = b g^{\hat{f}_b} \]

Where \( g_c, g_a \) and \( g_b \) are publicly known. The numbers \( h_c \) and \( h_b \) are elements of one-way function \( f \). \( U \) is Alice’s identity and \( V \) is the bank’s identity. The Randomised RSA based blind signature scheme works in the following way. The signing bank publishes the public key \((v, n)\), a one-way function \( f \) and a random number \( g \).

Alice selects a random \( a_1 \), and two blinding factors \( \tau \& \sigma \). Alice generates \( \tau a_1 g^\sigma \) and send it to the bank. The bank chooses its own condition \( a_2 \) and sends it back to Alice. Alice generates \( f(a_1 a_2) - \sigma \) and send it again to the bank. The bank multiplies \( \tau a_1 g^\sigma \times a_2 \times \tau a_1 a_2 g^{f(a_1 a_2)} \) together and computes the \( v^{th} \) root of this outcome, which the bank send to Alice. Alice divides the number she receives with the blinding factor \( \tau \) to get the pair of numbers \( a \) and \( (ag^{f(a)})/v \). Here \( a = a_1 a_2 \) and it is also known as the signature’s base number.

The withdrawal protocol

The withdrawal includes three similar protocol runs of the randomised blind signature scheme as shown below.

1. Alice chooses \( a_1, b_1, c_1, b, \sigma, \tau, \varnothing, \alpha, \beta \) and the blinding factor \( \gamma \) and generates

\[ \gamma c_1 g^\alpha, \quad \alpha' a_1 g^\tau, \quad \beta' b_1 g^\varnothing \]

and send them to the bank.

2. The bank sends \( h_c a_2^2, h_b b_2^2 \) and \( a_2 \) to Alice.
3. Alice computes \( e_a, e_b, e_c \) and sends to the bank.

\[
\begin{align*}
  e_c &= f(h_c, e, e_c) - \sigma \\
  e_b &= f(h_b, e, e_b) - \emptyset \\
  a &= (a_a f_2(e_c, e_b))^{k_1} \\
  e_a &= (1/k_2) f(a) - \tau \\
\end{align*}
\]

4. The bank computes the blinded A, B, and C.

\[
\begin{align*}
  C' &= Y c g_c^{f(h, c)} \quad \text{for } c = c_1 c_2 \\
  B' &= \beta^b g_b^{f(h, b)} \quad \text{for } b = b_1 b_2 \\
  A' &= \alpha^a g_a^{(1/k_2) f(a)} \quad \text{the bank chooses random number } k_2 \text{ and send } c_2, b_2, k_2, \\
  &\quad (C'^{k_2} A'^{1/v}) \text{ and } (C'^{-U} B'^{-1/v}) \text{ to Alice.} \\
\end{align*}
\]

5. Alice constructs the numbers

\[
\begin{align*}
  A &= a g_a^{f(a)} \\
  B &= b g_b^{f(h, b)} \\
  C &= c g_c^{f(h, c)} \\
\end{align*}
\]

Alice now can calculate signatures \( S_a \) and \( S_b \).

**The payment protocol**

1. Alice send Bob the numbers \( a, b, \) and \( c \).
2. Bob sends a random number \( x \).
3. Alice sends \( r = kx + U \) and the signed \( (C'^x A'^x B)^{I/v} \) to Bob.
4. Bob accepts the payment by verifying the two responses from the previous message.

**The deposit protocol**

1. Bob sends a, b, c, x and the responses to the bank.
2. The bank verifies the coins and finally credits Bob’s account.

The payment scheme detects double spending and reveals Alice’s identity as part of the payment protocol phase. The scheme provides anonymity as the bank cannot link the identity of Alice to a transaction as the bank does not know what it has signed until Alice double spends. The protocol provides a very weak transferability as the transferred cash grows in size. Double spending might be possible as the same coin floats many times which needs a robust online setting to detect this.
3.3 Real World Implementations

In the previous section the report examined two very important protocols. In this section the report will examine real world implementations of digital cash systems. The report will carry out an extensive research in to BitCoin and its operation. The reach evaluation of BitCoin in this section will provide knowledge needed in Chapter 6, to propose a protocol that uses BitCoin in an improved manner to provide anonymity and fair-exchange for e-commerce transactions.

3.3.1 DigiCash

DigiCash Inc was founded by David Chum in 1990 following his proposals and research in the area of anonymous electronic money [71]. Ecash was a main product of the company and the system was based on Chum’s protocol the report discussed in the beginning of this chapter but worked in an On-line setting. However, the company did not succeed and in the year of 1998 DigiCash Inc signed bankruptcy.

3.3.2 CyberCash

CyberCash Inc was founded in 1994 by Daniel Lynch, William Melton, Steve Crocker and Bruce Wilson. The company provided a wallet application for its e-commerce customers. The company also offered a micropayment system called CyberCoin, designed with the use of Netbill protocol which the report will discuss in chapter 4 [49]. The company published a RFC 1898 as a proposal called CyberCash Credit Card Protocol [72]. The proposed protocol used both a credit card and electronic money system. The company however claimed bankruptcy in 2001, which got acquired by VeriSign and in the year 2005 VeriSign’s CyberCash payment service was bought over by PayPal.
3.3.3 Mondex wallet

Mondex is a digital cash system that is based on Smart Card technology. The project was initiated in 1991 by Tim Jones and Graham Higgns at National Westminster Bank, UK. Unlike ordinary e-commerce based payment system, Mondex was aiming to transform traditional notes and coins payment in to a secured smart card based digital cash system. Security wise Mondex was evaluated under Information Technology Security Evaluation Criteria (ITSEC) and achieved an evaluation score of 6, which is ITSEC’s highest, granted security level classification. The proposal was first implemented as “The Byte” card with NatWest employees in 1992 and a further pilot trial in the city of Swindon in the year 1995[72]. The Swindon implementation included; cards, wallets, 20 Mondex cash machines, 12 Mondex car park ticket machines, card readers in 80 metropolitan busses, Mondex ready BT pay phone booths and a Mondex shop in Swindon high street[73]. Within a year 10,000 Mondex cards were in circulation in Swindon which was a 24% penetration of 43,000 NetWest customer base. Over 700 retailers (70% of overall retailers) in the city implemented the Mondex payment system with overall 1800 Point of Sale (POS) devices.

During the same period of time Visa, MasterCard and Europay were establishing the EMV project to standardise chip card applications. However, in November 1996 MasterCard International announced that it is willing to purchase a 51% shares of Mondex International. At present Mondex is part of the MasterCard worldwide suite of smartcard product [75]. Even though Mondex at first achieved a good start it could not expand as expected in to wider deployment.
3.3.4 BitCoin

BitCoin is a decentralised digital cash system which works on a peer to peer network. The system was first proposed and developed by Satoshi Nakamoto who self published his proposal in a crypto forum in October 2008. Soon after the publication of Nakamoto’s paper an open-source project was started to work on the development of BitCoin. In 3rd January 2009, the first hash block called the Genesis Block was created and a publically available global ledger called the Block Chain was broadcasted on the BitCoin peer to peer network. While BitCoin was gaining its momentum, Nakamoto moved away while leaving the project with the BitCoin community. Since April 2011, he has not been heard from and many believe that his name “Satoshi Nakamoto” is a pseudonym.

BitCoin is a completely distributed currency system that is not controlled, governed or managed by authorities or financial institutions. The entire network runs with the support of all the peers connected in the peer to peer network. BitCoin has its own monetary value which is based on BitCoin supply and demand in the BitCoin eco-system. BitCoin falls under the Crypto-Currency (Digital Cash) category which is built upon publicly scrutinised cryptographic algorithms. The BitCoin system is widely used to make anonymous payments over the Internet. Every payment that occurs in the BitCoin network is broadcasted to all network nodes. There are two types of broadcasts; Transactions and Blocks. Transactions are BitCoin transfers from one entity to the other. These transactions are represented in hash values during broadcasting. The other type of broadcast in the network is Blocks. Blocks are also hash values of different transactions using SHA-256 hashing algorithm. If a block is verified to be accurate by random BitCoin peers, it is added to the Block Chain record. The Block Chain has every BitCoin transaction that has ever occurred and it is available publically.

The system is built to have a static number of BitCoins in circulation; this amount is roughly 21 Million BitCoins. Currently as of August 2013 there are about 11.5 Million BitCoins in circulation [66]. BitCoin.org estimates that the last block ever to be generated in the BitCoin network will be in near the year 2140 [64]. The currency supports 8 decimal places in transactions. Users connected to the network contribute towards new BitCoin creation and transaction authorisation. Users get rewarded with BitCoins for their contribution. The process of
BitCoin peers authorising transactions and creating new BitCoins is called BitCoin mining. Miners use GPU (Graphics Processing Units) to solve mathematical problems (hashes). Some uses mining rigs with 100’s of motherboards attached with GPU’s. ASIC (Application Specific Integrated Circuit) miners are another type of dedicated hardware used for hashing and are very popular at present for their computational power. Transaction authorisation is the process of verifying whether a BitCoin transaction from one user to the other is genuine, correct and not an attempt to double spend. Verification of transactions is assigned randomly to network peers and the verifying peers get a small portion of BitCoins. However, the creation of a valid new block pays the creator 25 BitCoins at the current level which is also known as Coinbase within the BitCoin community [64, 65]. This amount halves every four years to balance out the increase of computational power over time.

A user can start using BitCoins in the BitCoin peer to peer network by running a BitCoin wallet software. A user can generate a unique BitCoin address also known as a BitCoin Public Key by using Elliptic Curve Digital Signature Algorithm (ECDSA). Every user needs to have a BitCoin address to receive BitCoins from other parties and a corresponding Secret Key is needed to transfer BitCoins to other parties. The process of generating a Standard BitCoin Public Key (BitCoin Address) is illustrated below.

**Step 1:** Generate Private ECDSA key

88754C0A0EFAD1EC0B58C82068A0CD526D4DE306641652816CE9C8147B56EE72

**Step 2:** Generate Public ECDSA key

0412DB059944669D4D330A21FC4241A87641D7C0B6D36738248321307EC20B63A2C6631EC563DD06407A412D2EAAA4740A150475DD24915E81AD83B99EA3C3

**Step 3:** SHA -256 hash of step 2

2B67D8CFDF3203B579D410AB885723548DB193ECE6C7655EBC45E5AA3C7CCA667
Step 4: RIPEMD-160 hash of step 3

20EFC0680C5D356082796627BCCA1368350E260E

Step 5: Add Network bytes 00 to the front of step 4

0020EFC0680C5D356082796627BCCA1368350E260E

Step 6: SHA -256 hash of step 5

2DCA27BFFC25A1920D5267534AE26D0B5A40D1F298FF1C988B1851DADB68943D

Step 7: SHA -256 hash of step 6

ACC0B8C2B36A5D01B6565BDE20A62F21EEA7B0B5D90B0BBDB99759023D96B5CD

Step 8: Take first 4bytes of step 7

ACC0B8C2

Step 9: Add these 4bytes at the end of step 5

0020EFC0680C5D356082796627BCCA1368350E260EACC0B8C2

Step 10: Base58 encoding of step 8

1419qNWnJeiT3vqg21yYTBDcGzTCWMDr9F

*Figure 3.1: Generation of a Standard BitCoin Public Key, Fieldwork.*
Most of other digital currencies require an owner of a coin to get a string of data that represent a coin signed by an issuing bank and once spend the coin needs to be deposited back by the new owner of the same coin to be named as the new owner [1, 7, 14]. BitCoin works in a slight different way by having a globally broadcasted transaction record that link ownership to a BitCoin instead of a unique string that represent a coin. A BitCoin transaction is the process of transferring a BitCoin by digitally signing a hash of a previous transaction together with the next owner’s public BitCoin address and adding this record to the end of the coin. The chain of signature ownership that link past transactions to the present is shown below.

![Diagram of BitCoin transactions]

**Figure 3.2: The chain of transactions** [24].

A illustrated in Figure 3.2 a payee can verify the ownership of the signature chain but the payee at the same time cannot detect whether a payer has double spent the same coin. Due to the fact that in the BitCoin network there is no TTP to verify double spending, there should be a process that could detect double spending before a transaction completes. One such way is for the payee as well as the entire BitCoin network to be aware of all the transactions that has occurred in the past. The Block Chain provides the solution to the problem identified by having a transaction history record of all BitCoin transactions.
The Block Chain records blocks of hashes. These hashes are time stamped to prove that the data existed before it was hashed. The concept of a time stamping server is distributed on a peer to peer basis in the BitCoin network. The creation of blocks and verification of BitCoins by peers in the network is made a fair and non-trivial task by introducing a “Proof of Work” method. The concept of proof of work was first introduced by Adam Back in 2002 as a counter-measure against unsolicited junk mail and denial of service attacks [67].

This method requires a user to exhaust some computational power and time before a task is completed. This concept was adhered by BitCoin making the peers generate hashes until a hash value is generated with a certain number of Zero bits at the beginning of the hash. The work needed increases exponentially as the required number of bits in the beginning increases. As a result a constructed block cannot be easily changed without redoing the whole work [24].

Furthermore, proof of work solves the problem of a party gaining advantage over the BitCoin network by having a large computational power to create a new block chain record. The correct and genuine record in the BitCoin network is the longest chain. With proof of work an attacker trying to infer this chain has to create all the transactions in the past and catch up with the longest chain that every peer has claimed is genuine. This indeed is not a trivial task. To compensate the creation of blocks against increase of hardware computational speed, the proof of work is increased if blocks are generated too fast by exponentially incrementing the Zero bits discussed above.

The need for having continues relationship with past transaction hashes to the present once incur the need for storage space to store all the hashes. The system over comes this drawback and not to break the block’s hash chain, transactions are hashed in a Merkle Tree [68]. This makes the hash only needing to record the Root Hash as shown in the figure below [24, 68].
The security of BitCoin transactions rely on the correctness of the Block Chain. The protocol ensures that only the longest chain of blocks is accepted by the peers. The creation of a block discussed previously require finding of matching hash collisions in a given period of time. Currently the proof of work is set to approximately 10 minutes to create a new block. This makes a transaction to be verified the parties have to wait approximately 10 minutes but this prevents double spending of BitCoins as the fraudster has to recreate all the blocks to change the transaction record [24, 64, 65, 69]. This makes a malicious peer unable to change the longest block chain as long as the majority of users are honest.

The BitCoin network provides anonymity by keeping each BitCoin user’s public key anonymous. By looking at one’s BitCoin address (Public Key) the true identity of the user cannot be revealed. However, due to the necessity of having to broadcast all transactions publicly prevents the anonymity of BitCoin payment transactions. As shown in Figure 3.4 unlike the level of privacy provided in traditional TTP involved payment systems, BitCoin publishes all the transactions that take place to be visible to public. This has become a major drawback within the BitCoin community and with the advancements in computational and access to Big Data analysis
capabilities it has been challenged that it may be plausible to link BitCoin transactions to real user identities [62, 63, 70].

A BitCoin transaction can be identified in the Block Chain given an examining party knows a Public key of one of the participants. Furthermore if a BitCoin user is using the same Public Key then all the transactions for that BitCoin address can be linked. One way to overcome this problem is to use a unique onetime BitCoin Public Key on every transaction. This is common practise with BitCoin users but when a user with multiple addresses pays change back to him/her self then all the transactions can be linked to the same user.

Another concern with BitCoin transactions is that due to its anonymous nature and one-way transaction without any reversals, an online consumer who makes a BitCoin payment may never receive his/her purchase. The consumer would not be able to request a refund or prove to any party that the product was not delivered. BitCoin is a real world implementation with a considerably large number of users. A solution for the above mentioned problems is proposed in this project in chapter 6. The proposed protocol will guarantee fair-exchange with the use of BitCoin as an anonymous payment method while preventing the linking of transactions.

Please read the detailed walkthrough of BitCoin in Appendix D.
Chapter 1 of the report gave an introduction to the evolution of the internet and emergence of e-commerce. Over the last few decades the world has seen a large consumer turnover migration from traditional high-street shops to online services on the internet. Transactions between consumers and merchants over the internet are carried out electronically. E-commerce transactions most of the time involve buying and selling of electronic content, goods and services between parties that have no prior trust-relationships with each other. This required e-commerce payment, contract signing, digital content exchange, certified delivery etc protocol schemes and implementations to improve fairness between involved parties. Asokan defines a fair-system as “that does not discriminate against a correctly behaving player, as long as a player behaves correctly, a fair system must ensure that other players will not gain any advantage over the correctly behaving players” [40].

Furthermore, Ray Indrajt & Ray Indrakshi also explains that fairness is a stronger requirement in secure e-commerce protocols and defines a fair exchange protocol as “a protocol that ensures that no player in an electronic commerce transaction can gain an advantage over the other player by misbehaving, misrepresenting or by prematurely aborting the protocol” [39]. In other words this means, suppose there is a merchant who sells digital audio files online and a customer who is willing to pay for one of the merchant’s audio files. A fair-exchange between the two parties should prevent the merchant from not delivering the file to the customer after receiving the payment or the customer not paying the merchant for the audio files he received. Fairness can be categorised in to two types. They are;
1. **Weak fairness**: this is when two parties engage in an electronic transaction, after the transaction protocol run, the honest party can prove to a third party that he/she followed the protocol even though the dishonest party did not send or pay to the honest party or aborted the protocol. Protocols that gather evidence through a protocol run and can later present the gathered evidence for dispute resolution in a court of law are called “weak fair-exchange” protocols [39]. Here the dispute resolution is not part of the same protocol but instead a external judge gives a verdict “after-the-fact” (after the event or protocol run has finished).

2. **Strong fairness**: in contrast strong fairness or true fairness ensures that during a protocol run, the protocol itself tries to avoid disputes and misbehaving of parties and resolve any disputes within the protocol without going to an external judge in a court of law. Protocols that meet these properties are called true fair-exchange protocols or strong fair-exchange protocols. These protocols make sure that an honest party engaged in a transaction does not get penalised when a dishonest party misbehaves. This is achieved by either parties are guaranteed to receive their items or none of them receives anything.

In the context of fair-exchange, protocols can be mainly separated in to two main categories considering the involvement of a trusted third party or not. They are: “Two Party based (Gradual Exchange) protocols” and “Trusted Third Party Based Protocols”.

*Figure 4.1: Two Distinct Types of Fair-exchange protocols, Fieldwork.*
4.1 Two party based protocols (Gradual-exchange).

Two party based or mostly known as *Gradual-exchange* protocols can be identified as the first type of fair-exchange protocols proposed by researchers to achieve fairness between two parties engaging in an electronic transaction. As the name suggest, these protocols does not rely on a TTP to achieve fairness but employ a process of gradual exchange of several messages between the transacting parties to augment the probability of fairness over the rounds of exchanged messages.

Blum in 1983 proposed a two party based protocol without the involvement of a TTP and this was based on gradual-exchange of bit by bit information from both parties almost simultaneously so that no party could gain more advantage of the other party. The mechanism of the protocol assumes that both involved parties have the same computational power. Supposing Alice and Bob wants to exchange similar documents. First Alice sends a bit of her document and verifies as correct once received, soon after that Bob sends Alice a bit from his document and verifies as correct almost simultaneously. In this gradual way they share equal chunks which eventually let both exchange each other’s documents. Blum in his proposal showed how the process could be used with digital signatures to sign contracts and send certified e-mails [39], [41].

Even at al. in 1985 proposed a system called the “1-out-of-2 oblivious transfer protocol” which allows a party to transfer one secret out of two recognisable secrets to another party. To explain the protocol, suppose Alice is the sender and Bob is the receiver and they do not have a trust relationship but Bob wants to receive the message and Alice is reluctant to send it. By using the 1-out-of-2 oblivious protocol, Alice sends 1 out of her two recognisable secrets so that the receiver gets the message with the probability of 0.5. Upon receipt Bob cannot guess the full message but can authenticate it as to have come from Alice. Alice has the conditional probability of 0.5 to say that Bob received the message. Similar to Blum’s protocol this is also a gradual exchange protocol [42].

Both of the above mentioned protocols needed equal computational power to assure fair-exchange between the exchanging parties. Due to this reason a party with more computational power than the other could gain advantage by conducting brute-force attacks on received
message to compute the remainder [44]. Furthermore having to have the same computational power was a major drawback when it comes to practical implementation.

Ben-Or et al. in 1990 proposed a solution what would overcome the computational issue mentioned above. This approach was called a probabilistic protocol, where two parties gradually exchange messages to increase the probability of fairness. Each participating party sends a message to the other party with a probability $\lambda$ the contract signed by both parties is valid at the point in time $T$ which is previously agreed. $\lambda$ increases by each message passed and the protocol finishes when $\lambda = 1$ or when the deadline reaches $T$. A judge can declare whether two parties bond in a contract by looking at a last message received by a participant and if $\lambda$ on that message is greater than or equal to a chosen random value between 0-1 by the judge. This protocol does not require both participating parties to have equal computational power [8, 43, 44].

However, Ray Indrajit & Ray Indrakshi mentions on their report that all the three protocols discussed above are not suitable for value exchange over the internet such as digital currency due to lack of simultaneity of exchange where parties could misbehave for their own advantage during transactions [39]. Furthermore, due to the number of messages that needs to be transmitted either way, in a busy network the protocol could significantly take up a lot of bandwidth and cause congestion.

Sandholm T. and Lesser V. in 1996 proposed a protocol that uses game theory as an approach to make the participants motivated to remain in the transaction. In this protocol if a participant wants to stop participating in a transaction due to an incident or misbehaving, can leave the protocol by paying a penalty fare. The drawback of this protocol is that it assumes both parties behave rationally throughout the protocol run but in reality this might not be the case.
4.2 Protocols based on a Trusted Third Party.

Due to the shortcomings of two-party based protocols which were addressed above, researchers had to introduce third parties in to fair-exchange protocols to achieve fairness between participants. The TTP based fair-exchange protocols can be classified in to three main types depending on the TTP’s involvement in the fair-exchange protocol. They are;

1. In-line TTP based protocols
2. On-line TTP based protocols
3. Off-line TTP based protocols

4.2.1 In-line TTP based protocols

The TTP involved in an In-line based protocol, interferes between the participating parties, collects exchanged items, check their accuracy and correctness and finally forwards them to the intended parties [8].

*The Believers Protocol*

Bahreman A. and Tygar D. proposed the first In-Line TTP protocol in 1994. The researchers introduced two protocols called “The Believers Protocol” and “The Skeptics Protocol”. The protocols were introduced to guarantee confirmation of sending and receiving of certified electronic mail between two parties who do not have a trust relationship. The Skeptics protocol was similar to a two-party based protocol but the Believers Protocol involved a TTP. In the Believers protocol, every message transferred and received by both parties goes through the TTP. The TTP keeps a record of all the transferred messages securely, with the intention of having the ability to resolving a future dispute within a short time. This method, according to the authors will guarantee non-repudiation and prevent participants from cheating [46]. This gives the protocol to achieve strong fairness. If S is sender, R is receiver and Postmaster P is the TTP, the protocol run in brief is shown below;
1. \( S \rightarrow P : \text{The Certified e-mail to } R \)

2. \( P \rightarrow S : \text{Proof of mailing} \)

3. \( P \rightarrow R : \text{Encrypted e-mail} \)

4. \( R \rightarrow P : \text{Receipt from } R \)

5. \( P \rightarrow R : \text{Decryption key} \)

6. \( P \rightarrow S : \text{Receipt from } R \)

**Coffey & Saidha Non-repudiation Protocol**

Coffey T. and Saidha P. proposed an In-Line fair-exchange protocol which adopts a TTP as a “non-repudiation server” (NRS). In this protocol the sender and the receiver of information never communicates directly with each other but uses the NSR as an intermediary. Furthermore to the use of the NRS the protocol relies on a “time stamping authority” to generate reliable timestamps [47]. The protocol run can be broken down to eleven steps. If A is the message originator, B is the recipient, NRS is the non-repudiation server and TSA is the ticket stamping authority, a simple illustration of the protocol is shown in the Figure 4.2 below.

![Figure 4.2: Coffey & Saidha non-repudiation protocol, Fieldwork.](image-url)
1. A → TSA : \{Partial Proof of origin\}_K_{TSA}

   The originator creates a “partial proof of origin” (PPOO) and sends it to TSA to get a time stamp, before communicating with NRS. \(dsgA\) = digital signature of A.

\[\text{PPOO} = \{\text{type1,A,B,message}\}_dsgA\]

2. TSA → A : \{Proof of origin\}_K_{A}

   TSA add a timestamp \(ts1\) to the PPOO and make it a complete Proof of origin (POO). The POO is send to A who can verify whether it is valid.

3. A → NRS : \{Non-repudiation request\}

   The originator request a non-repudiation data transfer service from the NRS and starts communication.

4. NRS → A : \{n1\_NRS\}_K_{A}

   NRS sends a challenge nonce \(n1\_NRS\) to A encrypted with \(K_{A}\). Only the authentic A can decrypt this message.

5. A → NRS : \{[n1\_NRS,POO,PPOO]\}_dsgA}_K_{NRS}

   The Originator sends POO,PPOO, n1-NRS (to indicate that it is not a replay) with the digital signature of A and encrypted by Key \(K_{NRS}\).
6. **NRS → B : {[n2_NRS,PPOR]dsgNRS}KB** 
   
   The NRS starts the “proof of receipt” generation by sending n2_NRS challenge nonce and Partial proof of receipt to the recipient.

7. **B → TSA : [SPPOR]K_{TSA}** 
   
   The recipient signs the PPOR to obtain the Signed partial proof of receipt (SPPOR) = [type2, B, A, h(POO)]dsgB and send it to TSA to obtain a time stamp.

8. **TSA → B : [POR]KB** 
   
   The TSA time stamp the message received previously to generate a complete POR. POR = [SPPOR, TSA, ts2]dsgTSA.

9. **B → NRS : {[n2_NRS,POR]dsgB}KNRS** 
   
   NRS can verify whether the complete POR is valid.

10. **NRS → B : {POO}KB** 
    
    NRS sends the POO to the recipient and keeps a copy for future user.

11. **NRS → A : {POR}KA** 
    
    NRS finally sends a confirmation copy of the POR to the originator.
As evident from the above two protocols, the involvement of an In-Line TTP provides strong fairness in the exchange protocol. However, due to the heavy involvement of the TTP during most of the steps in the protocol run causes some significant drawbacks. The TTP is required to manage and maintain a large database of all the messages communicated between involved parties. The manageability of such a database is a mission critical task when dealing with a large number of different transactions. This requires sufficient storage and computational resources to guarantee the availability of the TTP service to the communicating parties. The any-time availability is vital for the smooth running of the protocol and due to this reason the TTP could be targeted by Denial-of-service (DoS) attackers. Furthermore since the TTP handles very sensitive client data and information, the TTP need to conduct reliable and adhere to strict information security measures to prevent any compromise of sensitive information by attackers. The above mentioned drawbacks had a significant effect when it came to practical implementation. A solution to reduce the heavy involvement of the TTP in each communicated message was needed. This led to the introduction of On-Line TTP protocols.

### 4.2.2 On-line TTP based Protocols

Research in to On-line TTP protocols have found a solution to address the drawbacks in In-line TTP protocols discussed in the previous section. On-line TTP protocols are proven to be more efficient than In-line TTP protocols. This is due to the fact that the TTP involves in the protocol run, but not in every message transmitted. However, the On-line TTP still engage in the protocol run to guarantee fairness by validating, storing and generating transmitted messages by the parties involved in the transaction. The TTP use these stored messages as evidence to resolve disputed should a party misbehaves in the transaction exchange. To clearly understand how On-line TTP protocols have evolved, the report will elaborate on some proposed protocols in literature.
**Netbill Protocol**

Cox B. et al. in 1995 proposed one of the first On-line TTP protocols which achieved strong fairness between two engaged in an e-commerce transaction. The TTP used in this protocol is called the “Netbill Server”. This TTP keeps separate accounts for both customer and merchant which are linked to financial institutions of the two parties respectively. If customer is C, merchant is M and Netbill server is N, the Netbill protocol is shown below [49].

1. $C \rightarrow M : \text{Price request}$

   \[ = T_{CM}(\text{Identity}), E_{CM}(\text{Credentials, PRD, Bid, RequestFlags, TID}) \]

2. $M \rightarrow C : \text{Price quote}$

   \[ = E_{CM}(\text{ProductID, Price, Request-Flags, TID}) \]

3. $C \rightarrow M : \text{Goods request}$

   \[ = T_{CM}(\text{Identity}), E_{CM}(TID) \]

4. $M \rightarrow C : \text{Goods encrypted with key } K$

   \[ = E_k(\text{Goods}), E_{CM}(CC(E_k(\text{Goods})), EPOID) \]

5. $C \rightarrow M : \text{Signed electronic payment order (EPO)}$

   \[ = T_{CM}(\text{Identity}), E_{CM}(\text{[EPO]C}) \]
The protocol begins by the customer requesting the merchant for the product in step 3. The merchant sends the product encrypted but without the key in step 4. After receiving the goods, the customer sends the merchant a purchase order with the payment details only readable by the Netbill server in step 5. The merchant attaches the decryption key to the received purchase order and send it to the Netbill server in step 6. The Netbill server transfers funds from the customer to the merchant debiting and crediting the relevant accounts. The Netbill server sends a signed confirmation of the transaction to the merchant with an encrypted receipt and the decryption key which can only be read by the customer in step 7. The merchant forwards the message to the customer in step 8 [49].
**Zhang N. and Shi Q. Protocol**

In 1996, Zhang N. and Shi Q. proposed an On-line TTP protocol aiming at Electronic Data Interchange (EDI) systems to achieve non-repudiation [48]. The authors used two simple ideas to put together their protocol. One was the use of a randomised protocol such as Even at al. 1-out-of-2 oblivious protocol, discussed in section 4.1. The second idea was the use of a public notice board. The protocol uses a TTP called the “Secure Server” (SS). Suppose the originator is A, recipient is B and the TTP is SS, the protocol run is shown and explained below.

1. \[ A \rightarrow B : \{ PC_A || \{ M \} K_{AB} || PK_B \} || Sig_A(H(\{ M \} K_{AB}) || N_A) \]

   The originator initiates the protocol by sending an encrypted message to the recipient encrypted with the recipient’s public key. The message includes the originator’s public key certificate and the message M digitally signed by A and a nonce [48].

2. \[ B \rightarrow A : Sig_B(H(\{ M \} K_{AB}) || N_A || N_B || t_B) \]

   B signs the encrypted M and appends a new nonce N_B and a new timestamp t_B. Before sending the message to A. A can verify whether B’s signature and timestamp is valid if not terminate the protocol.

3. \[ A \rightarrow SS : \{ PC_A || Label || t_B || PK_{SS} \} || Sig_A(H(\{ M \} K_{AB}) || K_{AB} || t_B) \]

   The Label gives instruction for the SS on what to publish. The server records the time on the stamp. SS decrypts the message and obtain A’s public certificate to verify A’s signature on the appended part. SS checks the validity of t_B and publishes information needed for B. SS at the same time keeps a record of the message for future dispute resolution purposes.
**Zhou J. and Gollmann D. protocol**

Furthermore Zhou J. and Gollmann D. in the same year of 1996, proposed another On-line protocol which tried to reduce the workload of the TTP. The protocol was designed to provide evidence for sender and receiver, during the protocol run as well as after completion. The protocol splits the message $M$ in to a commitment part $C$ and a key $K$. The originator sends $C$ to the recipient and $K$ is kept safe with the TTP. Should there be a dispute both parties needs to acquire this key from the TTP to resolve the dispute [50, 51, 52]. Suppose the originator is A, recipient is B and the trusted third party is TTP, the protocol run is shown and explained below.

1. $A \rightarrow B : L , t_A , E_{d(M)}, EOO$

   The originator initiates the protocol by sending an encrypted message to the recipient encrypted with session key $K$, a label $L$ that identifies the session, a timestamp $t_A$ that includes a timeout value for the session key to reach the TTP by and the message includes a signed evidence of origin (EOO). $EOO = \text{Sig}_A(L, t_A, E_{d(M)})$.

2. $B \rightarrow A : L , EOR$

   B signs the evidence of receipt (EOR) and send it back to A. $EOR = \text{Sig}_B(L, t_A, E_{d(M)})$.

3. $A \rightarrow TTP : L , t_A , k , \text{Sub}_k$

   A sends TTP a message with a label to identify the session, timestamp, key $k$ and a signed evidence of origin and submission of key $k$. The $\text{Sub}_k = \text{Sig}_A(L, t_A, k)$. During the protocol run the TTP only receives one submission for a party. From this submission TTP can verify A’s digital signature and check the timestamp for replay attacks. If the timestamp is within the valid time slot the TTP can issue the corresponding key to B for decryption of message M.

4. $B\leftrightarrow TTP : L , k , \text{Con}_k$

   B obtains the session key $k$ after the timeout of $t_A$ and a non-repudiation origin evidence by the TTP. Conformation of key $k$ ($\text{Con}_k = \text{Sig}_{TTP}(L, t_A, k)$)
5. $A \leftrightarrow TTP : L, Con_k$

A also contact the TTP to obtain a confirmation of non-repudiation receipt evidence to prove that B accessed the key $k$. Both A and B can obtain the session key $k$ from the TTP and relevant evidence to prove non-repudiation from either sides. In this protocol it should be noted that the key $k$ is not encrypted on transmission and there is a possibility of interception. It is important that both parties have access to the non-repudiation evidence from the TTP in a timely manner.

Zhang Q., Markantonakis K. and Mayes K. Protocol

Zhang Q., Markantonakis K. and Mayes K. in 2005 proposed “A User Centric M-Payment Solution” which would provide fair-exchange, user anonymity and privacy payments over the internet [54]. Even though this solution is a mobile payment system, it still can be classed as an electronic payment model under the mobile payments category, as explained in section 2.1 of the report.

Figure 4.3: Participants and inter-relationships of the protocol [54].
As shown in the above figure, there are seven participants in the protocol including a TTP. Before the transaction protocol begins the authors make the following assumptions. First a consumer purchases a pre-paid SIM from a mobile operator (MO) without revealing personal identity. Subscriber Identity Module (SIM) is a tamper resistant module which provides a secure storage and process execution [23], [8]. The MO maintains billing account associated with the SIM which has a “Commit Buffer” that keeps transactions in a suspension state before completion. Merchants have current accounts registered with the MO. The MO has issued public key pairs for every SIM and it is inside each pair. The On-Line TTP generates a public and private key pair. The TTP generated public key is stored in the SIM. There is also a bio-metric authentication device linked with the mobile phone and a finger print template is stored in the SIM. The mobile phone stores the address for the delivery cabinet. Mobile phone and the payment applet share a symmetric encryption session key $K_{pay}$. The mobile phone and the Bio-app share the symmetric session key $K_{bio}$. If payment applet is (PA), mobile phone (MP), Biometric Applet in SIM (BA), Merchant’s Applet (MA), trusted third party (TTP), delivery cabinet (DC), $zVx(Z)$ is the result of encryption of data string $Z$ using public key $Vx$, $sSx(Z)$ is the resulting signature by using the private key $S$ and $eKx(Z)$ is the encryption of string $Z$ using a symmetric key $Kx$ [54]. The steps and description of the proposed protocol is shown below [23].

1. $MA \rightarrow MP : Invoice || P_{MA}$

   $Invoice = \{Amount || M || agreed_price || product_ID || Quantity\}$

   When the customer visits the merchant’s website and “checkout” to purchase the goods by entering his mobile phone number the merchant sends the above message. It includes the invoice and the public key of the merchant.

2. $MP \rightarrow BA : T_{MP} || eK_{bio}(BIO\_DATA)$

3. $BA \rightarrow MP : T_{BA} || eK_{bio}(BIO\_RESULT)$

   Once the MP receives the message it activates an authentication alert asking for the user to give biometric details. If the biometric entered by the user matches the one kept in the
SIM template the BA sends a confirmation message to the MP. If the result does not match the protocol is aborted.

4. $MP \rightarrow PA : e K_{pay} (\text{Payment request} \ || \ Invoice \ || \ P_{MA} \ || \ P_{TP})$

Once the user is verified then the MP sends the above message to the PA following the customer’s agreement with the terms and conditions. This message command is an Application Protocol Data Unit (APDU) command used to communicate to SIM.

5. $PA \rightarrow MP \rightarrow MA : z P_{MA} \{ z E_k (\rho) \ || \ s S_{PA} (\text{purchase order}) \ || \ P_{PA} \}$

Payment token $(\rho) = s S_{PA} (\text{amount} \ || \ M \ || \ tel\_number)$

$\text{purchase order} = \{\text{Invoice} || \text{tel\_numberC} || \text{Address} || \text{Nc}\}, \text{Ek} = K1 \times K2$

The PA constructs the purchase order, payment token and generates K1, K2 key pairs.

6. $PA \rightarrow MP \rightarrow TTP : z K_1 (\rho) \ || \ z P_{TTP} (K_1^{-1} \ || \ K_2^{-1}) \ || \ P_{PA}$

This is the message sent to the TTP. The payment token is encrypted using K1. The merchant verify the validity using this encryption as well. Upon receipt the TTP decrypt the message to obtain the payment token. The TTP send the payment token to the MO. The MO using the token transfer’s credit from the customer’s account to the credit buffer [54].

7. $TTP : z P_{MA} \{ s S_{TTP} (\text{amount}) \ || \ z K_1 (\rho) \} \ || \ P_{TTP}$

This message is generated by the TTP and available for the merchant to download from a server. It includes the amount of the customer payment signed by the TTP, token encrypted by K1 and TTP’s public certificate to use for verification of the signature. By downloading this and decrypting, the merchant can check whether the amount sent by the TTP matches the price in the purchase order. The merchant sends a signed message of the customer’s signature on the purchase order to the customer as a proof of evidence.
Lastly, the merchant posts the products to the Delivery Cabinet and SMS the cabinet password through SMS to the customer. Once the customer is happy with the product he/she sends the decryption key $K_2$ to the merchant to obtain the payment token $\rho$. The merchant finally sends this token to the MO to be credited into the merchants account.

4.2.2 Off-line TTP based protocols

Off-line fair-exchange protocols provide the transacting parties the freedom of exchanging products without the intervention of a TTP unless one of the parties tries to misbehave. The TTP only involves in the protocol if there is misbehaving between parties. These protocols are also called “Optimistic Protocols”

Burk H. and Pfitzmann A. proposed the first optimistic protocol in 1989 [35]. Their protocol included a TTP but only involved in the protocol run following detection of misbehaving by the participants. The protocol heavily relied on verification of signatures and the whole protocol was intended for signature exchange rather than product transactions. Bao et al. Have proposed three variations of the same optimistic protocol in 1998. The protocol introduces a theory to verify that a signature to be received is exactly the one intended before receiving the signature. The protocol involves the TTP if there is any misbehaving.

Asokan et al. in 1997, introduce an improved protocol that allows exchange of two digital contents. Two parties who is willing to exchange items first agrees to continue, if for any reason a party fails to agree then the protocol is aborted. In such situation the TTP intervene and run the recovery protocol or gather enough evidence of the dishonest party to present in front of a judge [77]. Asokan et al. is also believed to have proposed the first optimistic protocol that involves real goods or exchange of generic items with only five protocol messages [40].

However, Franklin M. And Reiter M. have proposed a similar fair-exchange protocol using a Semi-Trusted Third Party (STTP) [78]. As defined in the definitions in the Appendix B, a STTP is an external party that would misbehave on its own but would not collude with the participants.
CHAPTER 5

Security Attacks & Online Survey Results

In this Chapter the report will briefly discuss potential attacks in anonymous and fair-exchange protocols. The Chaum, Fiat and Noar protocol will be taken as an example to show how each potential attack could compromise the protocol. The report will also elaborate the online survey findings and draw conclusions to the consumer’s perspectives to e-commerce payment systems.

5.1 Potential threats and attacks

The Chaum, Fait and Naor protocol is taken as an example to explain each of the below mentioned attacks.

Chaum, Fiat & Naor Scheme

• Collusion Attack

This is a possible attack that could compromise this protocol. Suppose there is collusion between Alice and Charlie. Alice who just made a payment transaction to merchant Bob, sends the spent coins and Bob’s chosen binary string to Charlie who is another merchant. This way Charlie will have the same payment history as Bob and when both Bob and Charlie present the coins to be deposited in to their accounts, the bank would not be able to determine which merchant is lying [1].
**Impersonation by malicious insiders**

In the CFN protocol the customer’s secret key, which in this case is also the customer ID is stored in a bank database. If this database environment is not securely managed, one possible attack is the ability for an malicious employee could steal a genuine customer’s private key (customer ID in this scenario) and impersonate as the genuine customer to withdraw digital coins [22]. This is called the malicious insider attack and the malicious employee can even double spend without getting caught instead compromising the identity of a genuine user.

**Chosen Message Attack**

A chosen message attack is when an attacker fools a signer to sign a message of his choice. In this context the protocol uses blind signatures and as explained in Appendix A- Blind Signatures, since r is random, the bank does not learn anything about the signed message. This makes Alice present any arbitrary message to the bank with the intention of compromising the protocol [25],[27].

For an example if \((N, e)\) be Bob’s public key and \((N, d)\) his private key. Mervin wants Bob to sign \(M\) but Bob refuse to sign \(M\). Suppose Bob only sign \(X’\) messages. Mervin uses a random \(r\) and makes \(M’ = r^eM \mod N\). Now Bob provides his signature \(S’\) on \(M’\). Since,

\[
S’ = (M’)^d \mod N
\]

Mervin can simply remove the blinding factor and get Bob’s signature on original message \(M\).

\[
S = S’/r \mod N
\]

\[
S^e = (S’)^e /r = (M’)^e /r^e \equiv M’/r^e = M \mod N
\]
• **RSA based attacks**

The protocol relays on blind signature scheme base on RSA. Due to this reason certain attacks on RSA could be valid on this protocol as well. The security of RSA depends on two separate functions being one-way. One is that the encryption is a trapdoor one way function which is believed to be difficult to reverse without knowledge of the private key. Secondly factoring the outcome of two large primes is believed to be very difficult. In other words using the RSA public key to determine RSA private key by factoring modulus n is believed to be extremely difficult [26].

As mentioned above there are two ways in RSA or generally in any public cryptosystem where an attacker can compromise the security. They are,

1. Decrypting a ciphertext without knowing the private key.
2. Determine the private key directly from the public key.

The CFN protocol can be compromised by an attacker if managed to factor RSA modulus n as in a brute-force attack where the attacker tries every possible combination. This way if the attacker manages to obtain the values of \( p \) and \( q \), then the attacker can generate the private key.

Another possible way is by guessing the values of \((p-1)(q-1)\) which is difficult than factoring n. the attacker could also try all possible secret key \( d \) until a matching key is found. This is similar to a brute-force attack but is a very non-efficient way for the time and effort it takes.

Furthermore, there are other ‘guessed plaintext attacks’ where an attacker examine a ciphertext and deduces what the plaintext might be and encrypt it to see whether the outcome is correct.
The report will now take Zhang Q., Markantonakis K. and Mayes K. Protocol as an example and carry out an informal analysis of the proposed protocol to evaluate fairness (Section 4.2.2).

With the use of the TTP the protocol achieves fair-exchange by preventing the involved parties from gaining advantage over the other. The On-line TTP also supports the protocol to resolve disputes within the period of the protocol run instead of “after-the-fact” solutions. It also provides proof of evidence for false claims due to the use of digital signatures. For instance, message 8 provides some guarantee that the merchant has agreed with the purchase order of the customer.

However even though the protocol provides strong fairness there are some weaknesses that can be identified. Strong fairness as defined in definition 5 is the ability to prevent one party gaining advantage over the other in an e-commerce transaction. In a scenario where a fraudulent consumer collects his/her goods in the delivery cabinet (DC) and falsely claim that the product was not delivered; the customer gains significant advantage during the dispute resolution time period. This is due to the fact that the TTP has to request the merchant to provide DC reports, proof of postage and other messages before submitting the decryption key $K_1$ to the merchant or to settle the payment. This process could be time consuming and during this time-period the customer has gained significant unfair advantage.

Another weakness can be shown by looking at a scenario where a merchant gains more advantage over a genuine customer. Suppose a fraudulent merchant makes a claim that a customer provided or did not provide a decryption key after receiving the product. The TTP will try to contact the customer but if the customer is missing for a genuine unavoidable reason then the TTP sends the merchant the key needed to decipher the payment token out from the encrypted message. In this scenario the merchant gains significant unfair advantage over a genuine customer.
The Table 5.1 below compares four fair-exchange protocols including the protocol discussed above against fairness, TTP’s involvement in storing transferred data, transfer type and the number of protocol messages.

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Fairness</th>
<th>TTP stores product</th>
<th>Product type</th>
<th>Number of messages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Netbill Protocol</td>
<td>Strong fairness</td>
<td>No</td>
<td>Digital content</td>
<td>8</td>
</tr>
<tr>
<td>Zhang N. &amp; Shi Q. Protocol</td>
<td>Strong fairness</td>
<td>Yes</td>
<td>Digital content</td>
<td>3 + Pre-protocol messages</td>
</tr>
<tr>
<td>Zhou J. &amp; Gollmann D. protocol</td>
<td>Strong fairness</td>
<td>No</td>
<td>Digital content</td>
<td>5 + Pre-protocol messages</td>
</tr>
</tbody>
</table>

*Table 5.1: Comparison of four On-line TTP Protocols, Fieldwork.*

It is evident that none of these protocols achieve strong anonymity or provide anonymous payment services. Only Zhang Q. Et al. Protocol provides weak anonymity only between the consumer and merchant as described in section 4.2.2. Anonymous payment is a property that the proposed protocol intends to achieve along with strong fairness in Chapter 6.
5.3 What is stopping Digital Cash?

The purchase of goods with notes and coins has been around for centuries. It is not an easy task to switch from traditional payment methods to digital cash in a short period of time. Even though the physical currency is much harder to be replaced, electronic cash in e-commerce is rather different. There have been a number of real world digital cash systems implemented in e-commerce at present. Humans have been exposed to a lot of technological advancements in the last decade than they ever have. This has made behavioural changes in to the way how humans adapt new tools to make their day to day tasks convenient. A good example is the wide deployment and use of Near Field Communication (NFC) at present. The NFC technology is embedded in to most of consumer mobile phones and consumers can use their phones to make NFC payments. This is also the same with contactless bank cards. If the same technology was suddenly implemented two decades ago there might not be the same take up of the systems as it has today. This is due to exposure of consumers to technology over a period of time. Similarly the consumer awareness of digital cash systems is increasing. To support this statement, the author’s online survey results revealed that over 18% of 73 anonymous candidates even know about BitCoin as shown in Figure 5.1 below.

Which of the below mentioned payment methods have you heard before but not necessarily used?

![Pie chart showing payment methods](image)

*Figure 5.1: Alternative electronic payment methods, Online survey results.*
There are some important attributes to be considered to make a payment system get recognition by consumers. The online survey results show some of these attributes rated by consumers.

![Survey Results]

Consumer awareness could make a major difference in terms of widespread use of digital cash. The consumers must be made aware of both good and bad side of using digital cash. There are a lot of advantages of using digital cash but there are little social damage caused by digital cash as well. Silk Road is an anonymous market place which is hosted online and only accessible using a Tor Browser (Tor browser is software that works under a distributed network which hides the user’s real IP address to something else to provide anonymous browsing of the Internet) [81].

Unfortunately Silk Road is the most popular anonymous market place for illicit purchases and transactions. These include unlawful purchase of drugs, weapons and other fraudulent activities. The transactions are paid for using electronic cash using e-wallets or BitCoins due to its anonymous properties. The consumers must be made aware of issues such as this from the early stages. It is only through prior awareness this can be rectified permanently.

Implementing digital cash system in to mobile phones with NFC could be a positive way forward to improve wider acceptability and usage of digital cash. Solutions to provide fair-exchange in digital cash payment would increase consumer trust in the payment system and dispute resolutions.
5.3.1 Consumer Perspective of Digital Cash

As part of the project the author carrying out an online survey to analyse consumer perspectives of e-commerce payment systems. The survey was hosted over the internet and 73 anonymous participants completed the survey. A full info-graphic analysis of the survey findings is attached in Appendix C.

The survey results showed that 44% of the participated consumers purchased products online very often and 16% shopped online extremely often. From the 73 participants 68% had used alternative payment methods other than credit/debit card based payments. As shown in Figure 5.1 above consumers had a sound knowledge of existing electronic cash systems. While a majority of 49% had used PayPal as an alternative payment method, there were 6% who had used BitCoin, 8% used Amazon payments, 6 % used Google checkout and 7% used other services.

Interestingly 43% consumers said privacy concerns prevented them buying online and 12% said this was always the case as shown in Figure 5.3.

![Figure 5.3: Privacy concerns, Online survey results.](image-url)
When asked about bad consumer experience during/after purchasing online; 12% said the product never got delivered more than one occasion and 27% said this happened in one occasion. 34% of the participants said that there was one occasion the received product was not as described by the seller and 18% said this happened more than once. The response to the question regarding wallet, payment page crash is shown in Figure 5.4.

One of the perspectives of consumers that needed to be established is the acceptance of a TTP between their payment transactions. This question was relevant as the proposed protocol involve an On-line TTP between the consumer and merchant to achieve strong fairness. When asked if a TTP was involved to improve security and fairness of consumer transactions 38 % said that they are very likely to accept the TTP and 15% said extremely likely as shown in Figure 5.5.

---

**Figure 5.4: Checkout app, e-wallet, payment page crashed, Online survey results.**

**Figure 5.5: Acceptance of a TTP in a payment system, Online survey results.**
Furthermore, 40% said it is very likely that a TTP would increase consumer confidence in the payment system and 18% said it is extremely likely as shown in Figure 5.6.

![Pie Chart]

**Figure 5.6: A TTP increases confidence in a payment system, Online survey results.**

Optionally the survey asked participants to suggest improvements to e-commerce payment schemes. Illustrated below in a *WordCloud* is what consumers said.

![WordCloud]

**Figure 5.7: WordCloud of what consumers said, Online survey results.**

The findings from the online survey discussed above will be considered while designing the proposed protocol in the next chapter.
CHAPTER 6

Proposed Protocol

Anonymous Fair-Exchange Payment Protocol using BitCoin with Improved Unlink-ability.

The main goal of the project was to propose an anonymous fair-exchange payment protocol which is practical and widely deployable solution in the current e-commerce system. In the previous chapters the report carried out an extensive research into the field of anonymous payment protocols and fair-exchange protocols. The report identified design and functionality of proposed protocols as well as some real world implementations. Having reviewed how these protocols work, potential weaknesses and needed improvements, in this chapter an e-commerce payment protocol is proposed which guarantees fair-exchange and anonymity by using the real world implementation of BitCoin. The proposed protocol realises strong fair-exchange and improved anonymity within BitCoin users with the intervention of a Trusted Third Party (TTP).

Mentioned below in Table 6.1 are the notation used in the proposed protocol.

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Discretion</th>
</tr>
</thead>
<tbody>
<tr>
<td>C</td>
<td>Consumer / Customer</td>
</tr>
<tr>
<td>M</td>
<td>Merchant</td>
</tr>
<tr>
<td>TTP</td>
<td>Trusted Third Party</td>
</tr>
<tr>
<td>BP2P</td>
<td>BitCoin Peer to Peer Network</td>
</tr>
<tr>
<td>Peer</td>
<td>Node in the BitCoin network</td>
</tr>
<tr>
<td>Pseudo-ID-C</td>
<td>Unique Pseudonym-Identity of C registered with the TTP.</td>
</tr>
<tr>
<td>Pseudo-ID-M</td>
<td>Unique Pseudonym-Identity of M registered with the TTP.</td>
</tr>
<tr>
<td>Px</td>
<td>Public Encryption Key of entity X.</td>
</tr>
<tr>
<td>ePx{Z}</td>
<td>Encryption of data string Z using a public algorithm with the Public Key Px of entity X.</td>
</tr>
<tr>
<td>Symbol</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>$S_X$</td>
<td>Private signature key of entity X.</td>
</tr>
<tr>
<td>$sS_X[Z]$</td>
<td>Digital Signature outcome from applying the private signature transformation on data string Z using the private signature key $S_X$ of entity X.</td>
</tr>
<tr>
<td>$BP_X$</td>
<td>BitCoin Public Key of entity X. (This is also X’s BitCoin address)</td>
</tr>
<tr>
<td>$BS_X$</td>
<td>BitCoin Private Key of entity X. (This is also X’s Signature key)</td>
</tr>
<tr>
<td>$sBS_X[Z]$</td>
<td>Digital Signature outcome from applying the private signature transformation on data string Z using the private BitCoin signature key $BS_X$ of entity X.</td>
</tr>
<tr>
<td>$K$</td>
<td>Symmetric encryption key $K$ used by M to encrypt data and later issued to an intended party to decrypt the encrypted data.</td>
</tr>
<tr>
<td>$CTTP$</td>
<td>Symmetric Encryption Key $CTTP$, shared between C and TTP.</td>
</tr>
<tr>
<td>$MTTP$</td>
<td>Symmetric Encryption Key $MTTP$, shared between M and TTP.</td>
</tr>
<tr>
<td>$E_K(Z)$</td>
<td>Symmetric Encryption of data string Z by using key K.</td>
</tr>
<tr>
<td>$E_{CTTP}(Z)$</td>
<td>Symmetric Encryption of data string Z by using shared key $CTTP$ between C and TTP.</td>
</tr>
<tr>
<td>$E_{MTTP}(Z)$</td>
<td>Symmetric Encryption of data string Z by using shared key $MTTP$ between M and TTP.</td>
</tr>
<tr>
<td>$A</td>
<td></td>
</tr>
<tr>
<td>$h (Z)$</td>
<td>Hash of data string Z.</td>
</tr>
<tr>
<td>$N_{1X}$</td>
<td>First nonce issued by entity X.</td>
</tr>
<tr>
<td>$N_{2X}$</td>
<td>Second nonce issued by entity X.</td>
</tr>
<tr>
<td>$N_{3X}$</td>
<td>Third nonce issued by entity X.</td>
</tr>
<tr>
<td>$X\rightarrow Y : Z$</td>
<td>Entity X sends message Z to entity Y</td>
</tr>
<tr>
<td>$T$-info</td>
<td>Other information relevant to a particular BitCoin transaction.</td>
</tr>
<tr>
<td>$T_X$</td>
<td>BitCoin transaction from C to TTP, in this scenario in the formation of a hash.</td>
</tr>
<tr>
<td>$T_{(X-1)}$</td>
<td>Previous BitCoin transaction that has occurred in the past but directly link to $T_X$ in the formation of a hash.</td>
</tr>
<tr>
<td>$T_Y$</td>
<td>BitCoin transaction from TTP to M, in this scenario in the formation of a hash.</td>
</tr>
</tbody>
</table>

**Table 6.1: Notation used in the proposed protocol.**
The notation used in the proposed protocol was introduced in Table 6.1 above. Before the protocol is introduced in more detail, it is assumed that the below mentioned assumptions have taken place prior to the protocol run.

Assumption 1:

*Both the Customer “C” and the Merchant “M” registers with TTP by giving a Pseudonym-Identity “Pseudo-ID”. The TTP makes sure that each Pseudo-ID is unique and has not been registered before. It should not be possible for the TTP and External Parties to deduce the real identity of the registered parties by examining the Pseudo-ID. This fact is the same for C and M to find each other’s real identity.*

Assumption 2:

*The TTP issues shared symmetric keys $K_{CTTP}$ and $K_{MTTP}$ to both C and M respectively. These keys provide confidentiality to communication between the TTP and the two participants.*

Assumption 3:

*The participants are BitCoin users with access to a BitCoin wallet. The users can present their public BitCoin address when needed.*

Assumption 4:

*The customer’s and merchant’s public/private key pairs are certified by the TTP to the corresponding Pseudo-ID provided. The public certificates needed to verify each other’s digital signatures can be easily obtained by the TTP’s online server.*

Assumption 5:

*The consumer obtains TTP’s BitCoin Public Key also known as the BitCoin Address upon registration.*
Illustrated in *Figure 6.1* is a diagram of the proposed protocol’s message flow in the numbered order between the protocol entities that was introduced in *Table 6.1*. The overall protocol includes ten messages to complete an anonymous fair-exchange transaction using a real world anonymous payment implementation. The protocol can be broken down to three main phases. The first two messages run of the protocol falls under the “*Product/Price Negotiation Phase*” and can be exchanged by the consumer and merchant any number of times until they agree to continue. Messages three to seven, falls under the “*Digital Content Delivery Phase*” and message eight to ten, falls under the “*Payment Phase*”. 

---

**Figure 6.1: Proposed protocol message flow, Fieldwork.**
The overview of the proposed protocol can be described as the following. In the first two messages the consumer and the merchant agrees on the digital content (product) and negotiate the price for that particular product. Once the product/price negotiation is completed, the merchant sends the consumer an encrypted copy of the digital content but without the decryption key. Once the consumer receives the encrypted product he/she forwards BitCoin payment details to the TTP. The TTP request the merchant’s BitCoin address and the decryption key for the consumer. The TTP after receiving these details forwards a message to the BitCoin peer-to-peer network to transfer the consumer’s BitCoins to the TTP. Upon securing the BitCoin transaction the TTP forwards the key to the consumer to decipher the digital content and make another payment arrangement for the merchant in a BitCoin transaction. Unlike in an ordinary BitCoin transaction, the protocol proposes a TTP key generation, key management and key tracing solution that improve BitCoin transaction anonymity.

The report gave an overview to the proposed protocol above. Discussed and elaborated below is the proposed protocol in more detail.

1. $C \rightarrow M : e_{PM} \{ \text{product-ID}||\text{product-price}||\text{payment-method}||\text{Pseudo-ID-C}||P_{C}||N_{1C} \}$

The e-commerce consumer initiates the protocol by sending the merchant an encrypted message using the merchant’s public key. The consumer obtains the product-ID, price of the product that he/she wants to purchase and the merchant’s public key from the online website where the merchant has advertised his products. This website is not necessarily the merchant’s own website. It should be noted that in the given scenario, the merchant would also like to remain anonymous without revealing the real identity. The consumer sends the product-ID, product-price the consumer is willing to pay and payment method of the consumer indicating BitCoin. The consumer also includes his/her public encryption key to receive encrypted messages from the merchant and a fresh nonce $N_{1C}$ which would help the consumer to detect replay messages. The consumer appends the Unique Pseudonym Identity of the consumer “Pseudo-ID-C” making the merchant uniquely identify the consumer in forward communication. The messages are encrypted to provide confidentiality to the content of the transferred message.
2. \( M \rightarrow C : e_{PC} \{ Invoice || Transaction-ID || N_{1C} || N_{1M} \} \)

\[ Invoice = \{ product-ID || Pseudo-ID-M || Pseudo-ID-C || product-price || payment-method \} \]

Once the merchant decrypts the received message number 1, the merchant queries the product-ID in the products database to find out whether the customer is willing to pay the correct price and identify the customer’s payment method. The merchant creates a new Transaction-ID for the ease of tracing the customer and the particular transaction in the merchant’s records. Furthermore, the merchant generates a fresh nonce \( N_{1M} \) to detect replay messages and a new Invoice which includes details of the product, price, merchant’s pseudonym, customer’s pseudonym and payment method.

The nonce \( N_{1M} \) is generated by the merchant where as the nonce \( N_{1C} \) in the previous message was generated by the consumer. The consumer uses nonce \( N_{1C} \) to relate the previous message to the merchant and to confirm that the message 2 is not a replay from a different session than the one C and M are actively engaged in. The merchant sends both the Invoice and the Transaction-ID encrypted by the consumer’s public key (\( P_C \) received on previous message) to the consumer.

3. \( C \rightarrow M : e_{PM} \{ X \} || s_{Sc} \{ h(X) \} \)

Where, \( X = Invoice || Transaction-ID || N_{2C} || N_{1M} \)

After receiving message 2, the consumer can check whether the merchant agrees with the product negotiation by looking into the content in the Invoice. Up to this stage the consumer can abort the protocol if the product, price or payment method does not meet the customer’s requirement. The consumer and merchant can exchange message 1 and 2 any number of times before message 3.

The consumer appends a second nonce \( N_{2C} \) to detect replay messages from previous sessions. The consumer appends the merchant’s first nonce to the message for the merchant to identify the
consumer and to confirm that it is not a replay. The consumer encrypt the message which includes; the Invoice, Transaction-ID, \( N_{2c} \) and \( N_{1m} \) using the merchants public key.

In message 3, the consumer agrees to make a purchase by creating a digital signature by applying the private signature transformation on the hash of the merchant’s previous message \( X \) using the consumers private signature key \( S_C \).

The consumer appends the digital signature to the encrypted message and sends it to the merchant. Upon receiving this message, the merchant obtains the consumer’s public key certificate linked to the Pseudo-ID of the consumer from the TTP’s server hosted online. By having the signature verification key from the consumer’s public key certificate the merchant can verify the unique identity of the consumer. This proves the merchant that the originator of the message is the consumer with the pseudonym.

The merchant uses the Transaction-ID to trace the consumer in the merchant’s records and uses the nonce to detect replay messages. The digital signature on the signed message provides Data Origin Authentication. The nonce adds timeliness to the message. By combining data origin authentication and message freshness, entity authentication is achieved. Entity Authentication provides a stronger sense of data origin authentication which indicates to the merchant that the consumer is actively engaged in the transaction.

4. \( M \rightarrow C : e_{P_C}(X) || s_{S_M}[h(X)] \)

Where, \( X = \text{Invoice} || \text{Transaction-ID} || N_{2c} || N_{2m} || E_K(\text{Data}) \)

Upon receiving message 3, the merchant encrypts the digital content that the consumer intends to purchase using a newly created symmetric key \( K \) which is only used for this particular transaction. The merchant has not shared this key \( K \) with any other party, making the consumer unable to decrypt the product until the merchant supply him/her with the same key \( K \) to decrypt the product.
The message includes the Invoice, Transaction-ID, consumer’s nonce $N_{2C}$, a newly generated nonce $N_{2M}$ by the merchant and the encrypted data. The entire message is encrypted with the consumer’s public key. Since the entire message is encrypted using the consumer’s public key, the message achieves confidentiality.

The merchant creates a digital signature by applying the private signature transformation on the hash of $X_1$ using the merchant’s private signature key. The merchant appends the digital signature to the encrypted message and sends it to the consumer.

Upon receiving the message, the consumer obtains the merchant’s public key certificate from the TTP’s online server. The consumer, using the signature verification key also generally called the public key, verifies the merchant’s digital signature of the message.

5. $C \rightarrow TTP : E_{CTTP} \{ X_2 \| BP_C \| sBS_C \{ T_X \| BP_{TTP} \} \| sS_C \{ h(X_2) \} \}$

Where, $X_2 = Invoice \| Transaction-ID \| N_{3C} \| N_{2M} \| h(E_K(Data))$

$T_X = h (T_{(X,1)} \| BP_C \| T-info)$

$T_X$ is a hash of the BitCoin transaction from C to the TTP. The hash includes the previous transaction hash linking to this transaction, BitCoin public key of C and other transaction information relevant to this transaction.

$X_2$ includes the Invoice, Transaction-ID, a new nonce generated by C, the merchant’s nonce and the consumer generates a hash of the received encrypted digital content. Including only hash of the encrypted data prevents the TTP from having to keep storage capacity to store full encrypted data received from consumers relating to their purchases. The simple solution of sending a hash of the encrypted data which would be signed cross checked by the merchant in the next protocol message prevents the above mentioned potential drawbacks.
This is the message sent to the TTP by the consumer. The message also includes some information relevant to BitCoin payments.

The consumer creates a message which includes $X_2$, consumer’s BitCoin Public Key, digital signature created by applying the private signature transformation on the transaction hash $T_X$ and the BitCoin public key of the TTP (obtains upon registration) using the consumer’s BitCoin private key.

The consumer encrypts the entire message using the symmetric key CTTP shared between the consumer and the TTP. The consumer appends a digital signature to the message by applying the private signature transformation on the hash of $X_2$ using consumer’s private signature key. The consumer sends both parts of the message to the TTP.

Upon receiving this message the TTP verify the identity of the signature $s_S\{h(X_2)\}$ and decrypt the content in the encrypted messages.

$$6. \text{TTP} \rightarrow \text{M} : E_{\text{MTTP}}\{X_2\} || N_{\text{TTP}} || s_{\text{TTP}}\{s_S\{h(X_2)\}\}$$

The TTP sends $X_2$ of the previous message sent by the consumer to the merchant and a newly generated nonce $N_{\text{TTP}}$ encrypted by the symmetric key MTTP shared between the merchant and the TTP.

The nonce will help the TTP to determine future communication from M as to be in-time and not replayed messages. The TTP also creates a digital signature by applying the private signature transformation over the consumer’s signature of the previous message using the TTP’s private signature key.

The TTP appends the digital signature to the encrypted message and sends it to the merchant. The digital signatures provide proof of evidence to the merchant, confirming that the consumer
received the encrypted product as he/she has signed a message that includes a hash of the encrypted product.

Similarly the TTP’s signature over the consumer’s signature confirmers that the consumer received the encrypted digital content and the TTP was aware of this fact. The digital signature achieves non-repudiation which prevents the consumer from denying that he/she sent a confirmation of receipt of delivery on a late date. Upon receiving the message the merchant examines the nonce $N_{2M}$ that the merchant sent to C in message 4 and confirm that the message sent from the TTP is not a replay.

7. $M \rightarrow TTP : E_{MTTP}\{ X_3 \} || s_{SM}[h(X_3)]$

Where, $X_3 = Invoice || Transaction-ID || N_{3C} || N_{1TTP} || K || BP_M$

This is the message sent to the TTP by the merchant. The merchant construct $X_3$ which include the Invoice, Transaction-ID, consumer’s third nonce, TTP’s nonce, key K for decryption of the encrypted content and merchant’s BitCoin public key (BitCoin address).

The merchant encrypt $X_3$ using the symmetric key MTTP shared between the merchant and the TTP. The merchant appends a digital signature created by applying the private signature transformation on the hash of $X_3$ using the merchant’s private signature key. The merchant sends both parts to the TTP.

Upon receiving the TTP can verify the signature of the merchant which provides data origin authentication and the nonce $N_{1TTP}$ confirms that the message is not a replay of a previous session.
8. TTP → BP2P : \{ amount || BP_C || BP_TTP || sBS_C \{ T_X || BP_TTP \} || T_X || T-info \}

\[ T_X = h (T_{(X,i)} || BP_C || T-info) \]

The hash \( T_X \) includes hash of the previous BitCoin transaction, BitCoin Public key of consumer and other information related to the transaction (please refer to section 3.3.4 for a detailed explanation on how transactions are created).

This is the message the TTP constructs and send to the BitCoin Peer to Peer Network. The message includes the transferring amount, consumer’s BitCoin public key, TTP’s BitCoin public key, digital signature created by the consumer by applying the private signature transformation on the transaction hash \( T_X \) and the BitCoin public key of the TTP (obtains upon registration) using the consumer’s BitCoin private key, a hash of this transaction \( T_X \) (BitCoin transfer from C to TTP) and other information related to the transaction \( T-info \).

Upon receiving this message a random peer in the BitCoin network start creating a new block with the transaction information as mentioned below.

Peer – BP2P : a BitCoin network peer computes a new block which includes the hash \( T_{(x+1)} \) from this transaction. In the BitCoin network every peer engage in computing blocks simultaneously. Due to this reason only the first valid block created is verified by other peers to be genuine and a new record is added to the Block Chain. The BitCoin network at the same time check whether the BitCoins have been spent previously to detect double spending. The Block Chain is a publicly distributed ledger that records every transaction of BitCoin that ever takes place in the entire BitCoin peer to peer network.
9. TTP $\rightarrow$ C : $E_{CTTP} \{ X_4 \} || sS_{TTP}[h(X_4)]$

Where, $X_4 = Invoice || Transaction-ID || N_{3C} || K$

The merchant as well as all the participants in the protocol can view the public BitCoin ledger (Block Chain) which includes all past and present BitCoin transactions. Once TTP receives the consumer’s BitCoins which is verified to be true and genuine by the BitCoin network, the TTP sends the consumer the decryption key K on behalf of the merchant.

This is the message the TTP sends the consumer. It includes the Invoice, Transaction-ID, nonce $N_{3C}$ which was generated by the consumer in message 5 and the decryption key K. The message is encrypted by the symmetric key CTTP which provides confidentiality.

The TTP creates a digital signature by applying the private signature transformation on the hash of $X_4$ using the TTP’s private signature key. The TTP sends both parts to the consumer.

Upon receiving the consumer can verify the signature of the TTP which provides data origin authentication and the nonce $N_{3C}$ confirms that the message is not a replay of a previous session. In a practical implementation the TTP could request a key confirmation message from the consumer to confirm that the decryption was successful.

10. TTP $\rightarrow$ BP2P : $\{ amount || BP_M || BP_{TTP} || sBS_{TTP} \{ T_Y \} || BP_M \} || T_Y || T$-info $\}$

$T_Y = h \left( T_{(Y-1)} \right) || BP_{TTP} || T$-info $\}$

The hash $T_Y$ includes hash of the previous BitCoin transaction $T_{(Y-1)}$ linking to this transaction, BitCoin Public key of the TTP and other information related to the transaction.
Up to this point the consumer is secured from not receiving the purchased content following payment to the merchant. As mentioned before in a practical implementation the TTP could request a key K confirmation message from the consumer to verify the decryption of the digital content was successful. Subsequent to sending the decryption key to the consumer, the TTP forwards instructions to the BitCoin network to make a payment to the merchant.

The message sent to the BitCoin peer to peer network by the TTP includes; the transferring amount, merchant’s BitCoin public key, TTP’s BitCoin public key, a digital signature created by the TTP applying the private signature transformation on the transaction hash $T_Y$ and the BitCoin public key of the merchant using the TTP’s BitCoin private key, a hash of this transaction $T_Y$ and other details associated with the particular transaction.

Upon receiving this message a random peer in the BitCoin network start creating a new block with the transaction information as mentioned below.

Peer – BP2P: a BitCoin network peer computes a new block which includes the hash $T_{(y+1)}$ from this transaction in the similar way as described in message 8. The first valid block created by a BitCoin network peer is verified by other peers to confirm the transactions are accurate. Once this verification is completed the new record is added to the Block Chain. The BitCoin transaction from the TTP to the merchant is automatically updated in each other’s BitCoin electronic wallets. Furthermore both the TTP and the merchant can examine the Block Chain records to confirm whether the payment transaction was successful.
<table>
<thead>
<tr>
<th>Transaction ID</th>
<th>Consumer BitCoin Address (Payer)</th>
<th>TTP Pseudo-Random Public Keys</th>
<th>Merchant BitCoin Address (Payee)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2981</td>
<td>1Es8sjMKMYn81XGID46Se me6gN53JsUY2E</td>
<td>1ET8jJSUr3cJsVWTysxLC7QT07t5nerCwy</td>
<td>1245h4Xy4V3GrXRnojyPbthQN1s9E5KRAF</td>
</tr>
<tr>
<td>2982</td>
<td>1Mkcpyq2l6X0SwqZTlPHu TG6gK5UJyam</td>
<td>1FjGzmGkFtszDSwrmEco1j6 Bmn2o7Yd</td>
<td>125xhdZqj2S8B82bnSodcN2kd3cSULMsaX</td>
</tr>
<tr>
<td>2983</td>
<td>138PYUgsFLbxsQSXoDu rS09jG6vSPaBX</td>
<td>1KQjgFkXisYlqkJTLpifFcXd B1ur22KB</td>
<td>1L8x5c2kfnxwuoAF6ztR51KfDe8mcUUsq6Q</td>
</tr>
<tr>
<td>2984</td>
<td>12jQZL8ycNh7hu6xzf8d8u3 EsPQD7PucDS</td>
<td>1KzqgZvhsidNJT6Y6TwF2dLB xPLujVF8t</td>
<td>13HyjGHsSpba9zchBM1ZpUTscXFgMBJUA</td>
</tr>
<tr>
<td>2985</td>
<td>1DjA6RDS86QNKnfxZfnK6 dl2vSDuGhv2zi</td>
<td>16xV1EEnh1zLaYRToGfrsuw 5ehnt4Q5c</td>
<td>1NbTkcDoyoMyNpNYB4SvJE6Yc3NqFDxY</td>
</tr>
<tr>
<td>2986</td>
<td>157hBfXqqXFJzhRCSKdqFm N1zm256QaKYY</td>
<td>1n2cWd9FLgEj6okVkJtw9rUA X5AdF22ZB</td>
<td>1DwCWF68v83hgeSPvZHcvJ4e5UE5KRN</td>
</tr>
<tr>
<td>2987</td>
<td>1BmV6da53JgEAB5v7WP WCyGdazo6YqgTta</td>
<td>12Be8Dm2p5dqLVRZxhmJjTb qVGB9F9RI</td>
<td>17nDii6QrRk3KWHV42KWansgQ177U9mFE</td>
</tr>
<tr>
<td>2988</td>
<td>1Akc35Xa99ECzjUYbfB5 q44TMCJXMNk</td>
<td>13Tq5aJK1oW8VmPBukrUSEtvBnv6MiyE</td>
<td>1N9mZYwmm2Ms37JJK7bHRWv aD4k66UjkH</td>
</tr>
</tbody>
</table>

Table 6.2: TTP BitCoin Keys Generation, Key Management & Tracking Solution, Fieldwork.
However, the consumer who purchased from the merchant would not be able to trace or identify the BitCoin transaction from the TTP to the Merchant by examining the publicly available Block Chain ledger. Similarly any outside party would not be able to link the BitCoin payment transaction between the Consumer and the TTP to the BitCoin payment transaction between the TTP and the Merchant.

The above mentioned BitCoin transaction unlink-ability is achieved due the proposed TTP key generation, key management and transaction tracking solution as illustrated in Table 6.2. In a standard BitCoin transaction there is a link to the previous BitCoin transaction and there is an audit trail recorded in the Block Chain. It can be argued that by examining the publically available BitCoin transaction records the real identity of a user cannot be deduced as the BitCoin addresses are anonymous. However, the use of BitCoin addresses sometimes could make the user behind a BitCoin address linkable to different transactions. Especially if a user is continuing to use the same BitCoin address for multiple transactions, it is a trivial task to link all the transactions to the same user’s BitCoin address by examining the Block Chain. To overcome this it is a common practice to generate new BitCoin address for each individual transaction. However, even with adhering to the onetime BitCoin addresses if a user transfers change of multiple transactions at the same time it could be deduced that all the onetime addresses belongs to the same user.

Furthermore if a merchant advertise his/her BitCoin address on a website or in public for consumers to make payments, any third party knowing this fact could examine the Block Chain and filter out all the consumers’ BitCoin addresses who have transferred BitCoins to the particular merchant regardless of using onetime addresses. This kind of linking could be used by different parties to carry out attacks on privacy, anonymity analysis or even fraud investigations [62]. If any single address on a transaction chain could be linked to an actual identity then it might be possible to work back from that point to link all the other identities to actual users [79].
Suppose the same Consumer and Merchant used in the proposed protocol engaged in a direct BitCoin transaction outside the proposed protocol, both the Consumer and Merchant can identify their transaction in the Block Chain as well as in their wallets. The identification would not reveal each other’s real identity but it leaves an audit trial to each other. If either of the parties does not want to be linked in a transaction the participants do not have any other alternative option.

Furthermore, it would be a trivial task for an outside party to identify the transaction given the outside party has knowledge of one of the BitCoin addresses. The outside party could carry out thorough analysis of the entire Block Chain to identify similar payment amounts, similar addresses, and similar return change addresses to link the consumer to the merchant. For an example, suppose a very popular merchant selling one particular product at a fixed price to a large number of anonymous consumers taking BitCoin payments each day, the significant transactions can be identified by filtering out transactions with similar amounts to the value of the product. This would link BitCoin addresses that are plausible buyers of that particular merchant.

The proposed protocol solves the direct likability drawback of BitCoin transactions which was discussed above. The proposal introduces a TTP key generation, management and key tracking solution. The solution significantly improves the unlink-ability of participants to their purchases. The TTP make use of onetime BitCoin addresses (BitCoin Public Keys) for each individual transaction to provide improved anonymity. This makes the TTP to use a very large number of BitCoin Public Keys (BitCoin addresses) and similar number of BitCoin Private Keys. The private keys need to be securely stored out of reach from other parties as a private key can be used to authorise a transfer to any another BitCoin address. This dynamic increase of private keys to the corresponding public keys needs to be managed adequately. The proposed solution to support manageability of dynamic keys gives the TTP the ability to generate Public/Private key pairs pseudo-randomly by using a static secret. By using a static secret and the pseudo-random function the TTP can generate its own key pairs with increased manageability of tracking and storing keys.
In section 3.3.4 the report discussed the operations of BitCoin and relevant standards. BitCoin Public Keys (BitCoin addresses) needs to be generated according to a standard that should be compatible with the rest of the BitCoin network. The keys are generated by using Elliptic Curve Digital Signature Algorithm (ECDSA) which is a variant of DSA. The process of converting the Public ECDSA key to a standard BitCoin key was discussed in section 3.3.4. In the proposed protocol the TTP issues a pseudo-randomly generated TTP’s BitCoin Public Key to the Consumer to make a BitCoin payment. The TTP tracks the transaction, the issued key, consumer and the merchant using the Transaction-ID. The TTP keeps in record all the issued Public Keys mapped to each individual consumer and stores the corresponding Private Keys securely. In the protocol run message 8, the keys involved and the transaction instruction is passed to the BitCoin Peer to Peer Network.

Once the BitCoins from the Consumer gets transferred to the TTP’s unique BitCoin adders, the TTP does not use the same transaction to pay the Merchant in protocol message 10. Instead the TTP unlinked the transaction trail between the Consumer and the Merchant by selecting a random transaction other than this particular consumer’s transaction to the TTP. This makes the transaction link between the Consumer and the Merchant during a normal BitCoin transaction separated into an unlinked transaction. For an example suppose the Transaction-ID 2981 in Table 6.2 represent the Consumer and Merchant used in the proposed protocol. The Merchant does not receive the same BitCoin transfer from the Consumer but receives BitCoins from Transaction-ID 2987. Due to this randomisation and shuffling the Consumers, Merchants or External Parties cannot link a real transaction from a particular Consumer to a Merchant. This improves anonymity of participants as the solution further makes transactions unlinked.

Further improvements to unlinked-ability of transactions can be achieved by making some simple changes to the TTP’s key management solution. For instance the TTP can pay a Merchant by using a multiple number of Transaction-ID’s or the TTP can gather consumer transfers to the TTP and trade it to another monetary currency. This unlinks the BitCoin transaction completely. The TTP could use a new onetime BitCoin Public Key (BitCoin address) and pay the Merchant with another source of BitCoin transaction other than from consumers. Furthermore, the TTP
could buy new BitCoins from the traded currency and pay the Merchant which would further improve the unlink-ability of BitCoin transactions.

The report elaborated on how the proposed protocol achieves fair-exchange during the protocol run. The protocol includes ten messages in total to complete an anonymous fair-exchange transaction using a real world anonymous payment implementation. The first two message runs of the protocol falls under the “Product/Price Negotiation Phase”. Messages 3 – 7, falls under the “Digital Content Delivery Phase”. Message 8-10, falls under the “Payment Phase”. The first two messages can be exchanged by the consumer and merchant any number of times until they agree to continue. The proposed protocol guarantees fair-exchange for both the consumer and the merchant. The consumer does not receive the decryption key K until valid BitCoins have been transferred to the TTP and the merchant does not get paid the BitCoins until the consumer confirms that he/she has received the encrypted digital content.

The protocol achieves “Real-time” dispute resolution within the protocol run other than “After the fact” dispute resolution. If any misbehaving is identified by the TTP that makes the protocol unfair, then the protocol is forced to abort. If the TTP identifies a resolvable dispute such as an incorrect message has been sent, the TTP may request a re-send of that particular message from a party. Furthermore, due to the use of registered pseudonym-ID and digital signatures the protocol provides non-repudiation of messages. For instance message 6, gives proof of evidence to the merchant that the consumer has received the encrypted digital content and the TTP agrees to this fact. Non-repudiation is achieved by the double digital signature $s_{TTP} [s_{C} [h(X)]]$ where the TTP has digitally signed over the consumer’s signature.

Mentioned below in Table 6.3 is a comparison of the proposed protocol with four other On-line fair-exchange protocols discussed in Chapter 4. The protocols were compared against whether the protocol provides anonymity, fair-exchange, whether the TTP stores the exchange digital content, provided services and the number of total protocol messages. The proposed protocol achieves full anonymity, strong-fairness, payment, TTP does not store purchased products and the protocol achieves all these aspects within a total of ten protocol messages.
It can be concluded that the proposed protocol guarantees anonymous fair-exchange by using BitCoin with improved unlink-ability. The protocol can be easily adopted by any party to be implemented in to a real world system. The major drawback with most of anonymous fair-exchange protocols is the need for an accepted and widely used payment or digital cash system. However this protocol addresses this issue by adopting BitCoin payment solution which is a real world implementation and by far the most successful and widely used digital cash system.

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Anonymity</th>
<th>Fairness</th>
<th>TTP stores product</th>
<th>Number of messages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nathill Protocol</td>
<td>No</td>
<td>Strong fairness</td>
<td>No</td>
<td>8</td>
</tr>
<tr>
<td>Zhang N. &amp; Shi Q. Protocol</td>
<td>No</td>
<td>Strong fairness</td>
<td>Yes</td>
<td>3 + Pre-protocol messages</td>
</tr>
<tr>
<td>Zhou J. &amp; Gollmann D. protocol</td>
<td>No</td>
<td>Strong fairness</td>
<td>No</td>
<td>5 + Pre-protocol messages</td>
</tr>
<tr>
<td>Zhang Q., Markantonakis K. and Mayes K. Protocol</td>
<td>Weak anonymity (Only between C &amp; M)</td>
<td>Strong fairness</td>
<td>Yes</td>
<td>12 (Including delivery messages )</td>
</tr>
<tr>
<td>The Proposed Protocol in this project</td>
<td>Fully anonymous</td>
<td>Strong fairness</td>
<td>No</td>
<td>10 (Exactly)</td>
</tr>
</tbody>
</table>

**Table 6.3: Proposed Protocol & Other On-line TTP Protocols Comparison, Fieldwork.**
CHAPTER 7

Conclusion

7.1 Summary & Conclusion

The internet has gone under dramatic development in the last few decades. One major outcome of this dramatic development is the emergence of electronic commerce. E-commerce has change the way consumers used to purchase products and services. There has been a large turnover migration from traditional high-street shop based purchases to online purchases. The e-commerce market is growing and is expected to double from a value of €755 billion in 2010 to an expected €1460 billion in 2015 [57]. Online purchases in e-commerce are carried out by Electronic Payment transactions. While Credit/Debit card payment schemes are the most popular e-commerce payment method, recently consumers have shown interest in other Alternative Electronic Payment schemes such as Real Time Bank Transfers, Offline Credit, Direct Debit, eWallets, Mobile Payments and Digital Cash [13, 57]. Anonymity and Fair-exchange are two important properties in e-commerce. There have been a number of research proposals in academic literature as well as few real world implementations to realise these two properties [1, 7, 8, 24, 35, 40, 54].

This project is an extensive research to thoroughly identify Digital Cash and Anonymous Fair-exchange Payment Protocols. The main contribution of the project to ongoing research is the proposed protocol discussed in Chapter 6. The protocol guarantees anonymous fair-exchange in e-commerce transactions by using BitCoin with improved unlink-ability. The main goal of the project was to propose an anonymous fair-exchange payment protocol which is a practical and widely deployable solution in the current e-commerce system.

To facilitate the main goal of the project further objectives were introduced. These objectives include; clearly identifying anonymous and fair-exchange payment protocols, examine existing security measures, fairness & anonymity of payment systems, identifying vulnerabilities and proposing improvements to achieve higher levels of fairness and anonymity.
In Chapter 1, the project report first introduced the motivation of the project. The report justified the relevance of the project topic at present by carrying out a background research. In the same chapter the project objectives and the structure of the project was outlined. In Chapter 2, the report discussed current e-commerce payment systems and justified the recent consumer interest in alternative payment methods. The justification was carried out by examining statistics from an annual report from Worldpay and analysing the results from the author’s online survey carried out in support with this project [57]. A full detailed list of survey findings are attached in Appendix C. The report gave an introduction to Digital Cash while distinguishing it from ordinary e-commerce payment systems. In Chapter 3, the report carried out an extensive research under the heading Anonymous Payment Protocol Schemes and Implementations. In this section the report identified important anonymous protocol schemes as well as some real world implementations. The report thoroughly examined the BitCoin payment system and identified a vulnerability of BitCoin transactions that significantly draw anonymity and privacy concerns. The identified vulnerability is the possibility of linking BitCoin transactions from the sender to the receiver.

In Chapter 4, the report carried out an extensive research in to Fair-exchange Protocol Schemes and Implementations. The report defined between weak and strong fairness with in payment transactions. The main two types of fair-exchange protocols; gradual exchange and TTP based protocols were clearly distinguished. The TTP based fair-exchange protocols were broken down to three categories; In-line, On-line and Off-line TTP based protocols. Each type of these protocol categories were clearly elaborated with detailed proposed protocols. More emphasis was given to On-line TTP based protocols as this is the category used in the proposed protocol in Chapter 6.

In Chapter 5, generic attacks against anonymous and fair-exchange payment protocols were discussed. Taking an anonymous fair-exchange protocol for an example these attacks were described showing how the attack would compromise the anonymity and fairness of the system. A comparison of previous protocols with the proposed protocol was carried out detailing the aspects of level of anonymity, fairness, and protocol messages. In the same section of the report the results from the author’s anonymous online survey to identify consumer perspectives of e-commerce payment systems were discussed. This survey results were used to reassure the
consumer acceptability of a TTP between payment transactions from consumer to merchant as a positive solution in the proposed protocol. Furthermore the results gave insight in to how much consumer’s value aspects such as anonymity, privacy, security, fairness and speed of payment transactions.

The Chapter 6 of the report brings the most significant contribution to ongoing research in the field of anonymous fair-exchange from the proposed protocol. The proposed protocol was constructed and put-together by having identified past proposed protocols and with the lessons learned from their strengths and weaknesses. By proposing the protocol the project achieves its main goal of proposing an anonymous fair-exchange payment protocol which is a practical and widely deployable solution in the current e-commerce system.

The proposed protocol involves an On-line TTP to realise anonymity and fairness. The report first makes the reader familiarised with the notation and assumptions used in the protocol. Following a brief overview of the protocol with a diagram of the protocol message flow, each run of the protocol is discussed in detail. The protocol includes ten messages between the three involved parties in total to complete an anonymous and fair-exchange payment transaction. The protocol is broken down to three main phases; product/price negotiation, content delivery phase and payment phase. The proposed protocol guarantees fairness between the consumer and the merchant. The protocol with the intervention of the TTP achieves “Real-time” dispute resolution within the protocol run other than “After the fact” dispute resolution.

The protocol while guaranteeing anonymity and fairness of transactions further improves the consumer-merchant anonymity by solving the BitCoin transaction linking problem. This vulnerability that could compromise BitCoin anonymity was introduced in sections 3.3.4 and Chapter 5. The proposed protocol uses the BitCoin as the anonymous payment method and finds a solution to resolve the problem and improve the transaction unlink-ability. The above mentioned BitCoin transaction unlink-ability is achieved by the proposed TTP key generation, key management and transaction tracking solution as illustrated in Table 6.2.

In Chapter 7, the project is summarised and the project achievements are compared with the objectives of the project. The report based on the project findings recommended future work is suggested in the field of e-commerce payment systems and anonymous fair-exchange.
7.2 Recommended Future Work

Form background research of publicly available literature and to the author’s knowledge this work is an inventive attempt to design a practical e-commerce payment protocol which guarantees anonymity and fair-exchange, with the intervention of an On-line TTP to improve unlink-ability of BitCoin transactions while guaranteeing strong fairness. Based upon the research carried out, the proposed protocol and the online survey results analysis, the following recommended future work has been identified.

First of all we would like the proposed protocol to be formally verified by modelling the protocol under a formal verification technique such as Communicating Sequential Processes (CSP) and Failure Divergence Refinement (FDR). The formal analysis can be used to evaluate the security of the protocol and make further security improvements if found.

Secondly the idea of implementing the proposed protocol in real world setting for testing purposes is possible. This is due to the fact that the protocol uses BitCoin (a real world implementation) to make payments. A real test bed would make the protocol to be formally evaluated on its security and efficiency.

Thirdly in a real world setting, the accuracy of the TTP used in the protocol could be identified in terms of how the TTP handles simultaneous transactions without failing. Furthermore, countermeasures for the TTP to prevent denial of service attacks (DoS) could be examined.

Fourthly it is possible to make few changes in order to make the protocol exchange physical products. A delivery cabinet that preserves the consumers’ postal address and identity is a simple option to guarantee fairness and anonymity at the same time.

Last but not least, while years of research in to conventional centralised Anonymous Payment Schemes and Implementations have not achieved large scale deployment, de-centralised BitCoin by far is the most successful. What has been learned from BitCoin should be carefully harvested to apply on future research in fair-exchange and development of next generation digital cash systems which could one day replace notes and coins as we know it.
Bibliography


[18] Miller J. *E-Money Mini-FAQ*, Available at:  

[19] Crescenzo G and Rubin A. *Financial Cryptography and Data Security, 10th*  
International Conference, FC 2006 Anguilla, British West Indies, February 27 - March 2, 2006, Revised Selected Papers, pp 252, Available at:  
http://books.google.co.uk/books?id=VKP843PtYkEC&pg=PA251&dq=blind+signatures &hl=en&sa=X&ei=jBEwUb7fEdKa1AXYu4G4CQ&ved=0CEwQ6AEwAw [Accessed: 27-02-2013]

[20] Financial Crimes Enforcement Network (FinCEN), *A Survey of Electronic Cash,  


[42] Even S., Goldreich O. and Lempel A. “A Randomized Protocol for Signing”. Available at: 
http://www.lix.polytechnique.fr/~catuscia/teaching/papers_and_books/SigningContracts.pdf
[Accessed: 21-07-2013]


[54] Zhang Q., Markantonakis K. and Mayes K. “A User Centric M-Payment Solution”. 
Smart Card Centre, Information Security Group, Royal Holloway, University of London, 
2005.

[55] Segal B. “A Short History of Internet Protocol at CERN”. Available at: 

[55] Segal B. “A Short History of Internet Protocol at CERN”. Available at: 

Available at: http://www.worldpay.com [Accessed: 12-08-2013].


[59] Khu-smith V. “Enhancing the security of electronic commerce transactions”. PHD 


[Accessed: 14-08-2013].


[71] MNTnews. “Boom then Bust: How Electronic Cash Faltered”. Available at:  


[74] Ives B and Earl M. “Mondex International: Reengineering money”. London Business School, Available at:  
http://wings.buffalo.edu/academic/department/som/isinterface/is_Syllabus/mondex/mondex.html [Accessed: 02-08-2013].


[79] DailyAttack, 2013. “Maintaining anonymity while using BitCoins”. Available at:
http://thedailyattack.com/2013/06/maintaining-anonymity-while-using-bitcoins/
[Accessed: 26-08-2013].


Appendix A
Cryptographic Primitives

Trapdoor One-Way Functions

Professor Keith Martin in his book “Everyday Cryptography” explains that a one-way-function should have the property of being ‘easy’ to compute but ‘hard’ to reverse. However, he mentions that public key encryption should not always be a one-way-function but ‘almost’ always be a one-way-function except when it comes to the intended recipient of the ciphertext who can overcome the one-way property. One-way functions, where there exists a trapdoor to obtain plaintext from ciphertext is called ‘Trapdoor One-Way Functions’ [26].

RSA

Rivest, Shamir and Adelman proposed RSA function as the first implementation of a trapdoor function in 1977 [25]. RSA can be used as a public key cryptosystem for encryption as well as digital signatures. RSA works in modulo arithmetic and both encryption and decryption is achieved by raising numbers to a power modulo. A modulus which is a product of two large primes, typically 512bits or longer [26]. Generating the key pair;

Given \( p, q \) are two large primes modulus \( n = pq \)

\( e \) = a number greater than 1 and less than \( (p-1)(q-1) \). \( e \) should have no factors in common with \( (p-1),(q-1) \) except for 1. That makes \( e \) and \( (p-1)(q-1) \) coprime. The pair of numbers \( (n,e) \) forms the RSA public key.

\( d \) = private key, given a \( (n,e) \) there can only be one possible \( d \).

This is the inverse of \( e \text{ mod } (p-1)(q-1) \) this is expressed by \( ed = 1 \mod (p-1)(q-1) \)

RSA encryption: given a message is \( M \) then the corresponding ciphertext \( C \) is,

\[ C = M^e \mod n \]

RSA decryption: given a ciphertext is \( C \) then the corresponding plaintext \( M \) is,

\[ M = C^d \mod n \]
Digital signatures

Digital signatures were initially defined by Diffie and Hellman in 1976 and the first implementation was by using RSA trapdoor one-way function [36]. A signature scheme allows a user with a private key to sign a document and send to anyone who is then able to verify the signature of the document using the public key of the signer [29]. Digital signature schemes provide data origin authentication which it validates the underlying data in a sense of assurance of integrity and the identity of the signer. Furthermore, it is used as a strong assurance of non-repudiation which is a participant in a protocol cannot later deny sending a message or receiving a message during a protocol run. A digital signature could be later presented to a dispute resolution third party as evidence of content or origin of underlying data [23].

Blind signatures

As described in section 2.3, the theoretical concept of anonymity in e-commerce payment protocols using blind signatures was first proposed by David Chaum in 1982 [9].

An analogy to blind signatures; A user paste a carbon paper on a check that he wants to get signed by a bank and seals it in an envelope. The user gives it to the bank, who then signs the envelope with a pen without seeing the actual check inside and give the envelope back to the user. The user now takes the check inside which is now signed and pay somebody else with it. The bank on has no knowledge of what it signed and when the check comes back to the bank to be deposited it cannot be linked to the user which makes the whole transaction anonymous while preserving the user identity [21], [29].

A blind signature scheme based on RSA can be explained in the following method. Given \((n, e)\) is the bank’s publicly known values and \((n, d)\) is the bank’s private key.
Alice chooses a random blinding factor $R$ in a way that $gcd(R, n) = 1$. If $M$ is the message to be signed and she calculates $M'$ and gives it to the bank to sign.

$$M' = M R^e \mod n$$

The bank signs $M'$, say $S' = (M')^d \mod n$, which is also

$$S' = (M')^d = M^d (R^e)^d = M^d R$$

Once Alice gets the signed message since she knows $R$, she divides $S'$ by $R$ to obtain,

$$S = M^d$$

It is evident that the bank has not learned any information about what it signed.

**Zero knowledge proof**

Zero knowledge proof is another important cryptographic primitive that is equally used as blind signatures to achieve anonymity. It was first defined by Quisquater et al. In 1990 and was first implemented by Goldreich et al. In 1991 in his paper as a implementation for a secure multiparty computation proposal [31], [32]. It is the method used by one party to prove to another party that it knows a secret without telling the any information or revealing the secret. The method should hold the below properties true [8].

1. If the statement is true, an honest prover could convince an honest verifier who follows the protocol properly.
2. If the statement is false, a cheating prover cannot convince an honest verifier.
3. If the statement is true, a cheating verifier cannot learn anything other than the fact.

**Cut-and –Choose method**

Michael Rabin proposed a method in 1978 to divide something in a fair way between the involved parties. This method was called the cut-and-choose method. Given Alice and Bob are the involved parties [4].

1. Alice cuts the thing to be shared in to two equal halves.
2. Bob chooses one half for himself.
3. Alice then keeps the other half.
Appendix B
Definitions

**Definition 1:** *Fair-exchange* in the context of e-commerce the exchange of items between two parties in a fair manner for both parties where no party can gain unfair advantage over the other party by misbehaving, misrepresenting or prematurely aborting the protocol. A protocol that meets this property is called a fair-exchange protocol.

**Definition 2:** *Trusted third party (TTP)* in a fair-exchange protocol is a party that is not a customer or a merchant but who participate in a protocol to make sure that the other parties do not misbehave. It is assumed that a trusted third party will not misbehave or collude with the other parties.

**Definition 3:** *Semi-trusted third party* in a fair-exchange protocol is a trusted third party who may misbehave on its own but will not collude with the other participating parties.

**Definition 4:** *Weak fair-exchange protocol* is a fair-exchange protocol that gathers evidence through a protocol run and can later present the gathered evidence for dispute resolution in a court of law [39]. Here the dispute resolution is not part of the same protocol but instead an external judge gives a verdict "after-the-fact" (after the event or protocol run has finished).

**Definition 5:** *Strong fair-exchange protocol (True fair-exchange protocol)* is a fair-exchange protocol that tries to avoid disputes and misbehaving of parties and resolve any disputes within the protocol without going to an external judge in a court of law. These protocols make sure that an honest party engaged in a transaction does not get penalised when a dishonest party misbehaves. This is achieved by either parties are guaranteed to receive their items or none of them receives anything.

**Definition 6:** *Gradual exchange protocol* is a fair-exchange protocol that gradually increases the probability of fairness between involved parties in a transaction by exchanging a series of messages on several rounds [39].

**Definition 7:** *Optimistic protocol* is a fair-exchange protocol that relies on a trusted third party (TTP) but does not involve the TTP actively in the protocol assuming that the parties involved in the transaction does not usually misbehave. The TTP only involve when a party misbehave or a disruption causes the protocol to not work properly, then the TTP resolve the dispute [40].
Appendix C
Online Survey Results

As part of the project under the title- "Digital Cash / Anonymous Fair-exchange Payment Protocols", The Author carrying out an online survey to analyse consumer perspectives of e-commerce payment systems. The survey was hosted over the internet and 73 anonymous participants completed the survey. The info-graphic analysis of the survey finding;

How often do you purchase products online?

- 44% Very often
- 37% Slightly often
- 16% Extremely often
- 1% Never

Have you used an Alternative Payment method to make an online payment other than Credit/Debit card based payments? (Such as: PayPal, Real-time bank transfers, BitCoin, ...)

- 61% Yes
- 38% No

Which of the below mentioned payment methods have you heard before but not necessarily used?

- PayPal: 28.70%
- Amazon Payments: 18.09%
- Liberty Reserve: 2.13%
- Google Checkout: 14.98%
- BitCoin: 18.62%
- AllPay: 2.13%
- Litecoin: 3.19%
- Monedex: 7.08%
- Other: 1.06%
- Dwolla: 2.13%
-
Other than Credit/Debit Card based payments, which of these methods have you used to make online payments?

![Pie chart showing payment methods]

How often do privacy concerns prevent you from buying products online?

- 43% Once in a while
- 22% Most of the time
- 12% Always
- 12% About half of the time

In the context of online payments. Please rate the following attributes in order of importance to you.

<table>
<thead>
<tr>
<th>Question</th>
<th>Count</th>
<th>Score</th>
<th>Least Important</th>
<th>Somewhat Important</th>
<th>Neutral</th>
<th>Very Important</th>
<th>Extremely Important</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Security of payment system</td>
<td>72</td>
<td>4.85</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Privacy of personal information &amp; spending habits</td>
<td>72</td>
<td>4.38</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Anonymity of user identity</td>
<td>76</td>
<td>3.81</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. Convenience of making payments</td>
<td>72</td>
<td>4.00</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5. The speed of payment processing time</td>
<td>76</td>
<td>3.80</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Have you come across any of the following bad experiences during/after purchasing online?

Paid items/goods/digital content never got delivered

- 60% Never
- 27% One Occasion
- 12% More than One Occasion

Did not receive payments for delivered goods

- 54% Never
- 33% N/A
- 7% One Occasion
- 4% More than One Occasion

Received a wrong product or the product was not as described by merchant

- 45% Never
- 34% One Occasion
- 18% More than One Occasion
- 1% N/A

The Checkout app/ Electronic wallet/ Payment page crashed

- 44% More than One Occasion
- 30% Never
- 20% One Occasion
- 4% N/A
In brief, receiving goods that you paid for or receiving payments for the goods you delivered, vice versa is called Fair-exchange. If an e-commerce payment system guarantees fair-exchange for your transactions, how would you rate your perspectives to the following?

You would be more comfortable making online payments

43% Very likely

28% Extremely likely
16% Neutral
8% Somewhat likely

You would choose this payment system from others

47% Very likely

21% Neutral
15% Extremely likely
11% Somewhat likely

You would recommend it to someone else

43% Very likely

25% Neutral
18% Extremely likely
6% Least likely

You would choose to pay more online for your purchases

31% Very likely

27% Neutral
16% Extremely likely
13% Somewhat likely
Other than desktops/laptops, how do you use the following devices to make online purchases?

**Mobile phone**

- **67%** Never
- **22%** Once a week
- **5%** 5+ weekly
- **4%** 3-5 times weekly

**Tablet**

- **71%** Never
- **26%** Once a week
- **2%** 2-5 times weekly

One way to improve Security and Fairness of an online transaction is to introduce a Trusted Third Party in-between the consumer and the merchant. (TTP – Trusted Authority that would not collude with participants) If a TTP is introduced to make online payments more secured and fair, how would you rate the following?

**Your acceptance of a TTP in the system.**

- **38%** Very likely
- **15%** Extremely likely
- **12%** Somewhat likely
- **25%** Neutral

**Increase your confidence in the payment system.**

- **40%** Very likely
- **18%** Extremely likely
- **8%** Somewhat likely
- **27%** Neutral
Which of these aspects would help you to trust the TTP?

- Digital certificates: 29%
- Brand name: 28%
- Number of users: 23%
- Word of mouth: 14%

You suggested - Formal verification by regulators, Reputation, Statutory banking...

In order to achieve higher levels of security and fairness of an e-commerce payment system, would you be willing to sacrifice some speed of the transaction processing time?

- Yes: 76%
- No: 9%
- Not sure: 8%
- Other: 5%

Optional - Do you have any suggestions for improvement that needs to be done in e-commerce payment schemes? How about improving the user privacy and fair-exchange?

Consumers said...

- Consumer awareness
- Separate payments from identity
- Improve trust between parties
- High privacy and speed of transactions
- Security of payment information
- Immediate fixing of security
- Payer should never give card details to merchant but only instruct the bank to do so
- Balancing security & usability
Appendix D
BitCoin Walkthrough

To start using BitCoin is fairly easy. Before starting there are things you must remember the following;

1. Secure your wallet (Use strong passwords and back up your wallet).
2. BitCoin payments are irreversible.
3. The BitCoin currency value fluctuates.
4. Transactions are publicly broadcasted but do not reveal users real identity. It only reveals the BitCoin address, so you need to use one address per transaction.

The next step would be to choose a wallet for you to store your BitCoins. At present there are wallets for both computers and mobiles. There are a few wallet providers. For this walkthrough we will use the “Bitcoin-Qt” wallet which is also the original BitCoin which was developed. The wallet can be downloaded from the below mentioned URL.

http://bitcoin.org/en/choose-your-wallet

The very first time when a user opens the new wallet it would take some time to synchronise with the BitCoin peer-to-peer network. The reason for this in brief is, the wallet downloads the latest Block Chain which is the public ledger that contains all the past transactions.

Once you have a BitCoin wallet the next step is to get BitCoins. There are two ways you could get BitCoins to your wallet. You either could request BitCoins as a payment method for your wallet address or you could use a BitCoin exchange to buy BitCoins using a conventional currency such as USD or GBP.

Once you have BitCoins in your wallet you could start making payments. To make a payment to someone, all you have to do is to put their BitCoin address in the SEND section of your wallet and mention how much as illustrated in the screenshot Figure A-D1.
In contrast to receive payment you go to the RECEIVE section and generate a new key and give it to the party whose sending you the payment. When the sending party make a payment to the address you gave him/her the amount will be transferred to your wallet.

![Figure A-D1: BitCoin Payment, Screenshot](image)

BitCoin is a decentralised currency. The transactions are authorised by peers in the BitCoin peer-to-peer network. Similarly new BitCoins are created by peers in the BitCoin network. These mentioned BitCoin transaction approving and creating new BitCoins; within the BitCoin community is called “BitCoin Mining”.
Other than making and receiving BitCoin payments. A b-BitCoin user could choose to support the process of transaction authorisation and creation of new BitCoins. The incentive behind doing so is that the users get rewarded BitCoins for their work. For authorising random transactions the network pays the authorising node (peer) a small authorisation charge. A node gets rewarded 25 BitCoins to the current level for creating new BitCoins (which is called a Coinbase payout). The current exchange value of a BitCoin is roughly £86.

A simple way to start mining is by joining a mining pool. Joining a pool gives you more success rate than mining on your own. A user could use a simple mining tool to carry out mining. In this walkthrough we will join the pool called the “Slush’s Pool” and use a simple mining tool called the “GUI Miner”.

You could join the pool with this URL http://mining.bitcoin.cz/

You could download the miner from this URL https://bitcointalk.org/?topic=3878.0 or from the above link.

Once you join the pool it will ask for your BitCoin address to make payments. You are advised to create new addresses every time. Once you give the pool this address you will get your miner username and password. Mining is solving hashes. For a technical description on what is mining and the cryptography behind BitCoin please see section 3.3.4 of the report.

You could use your Central Processing Unit (CPU) of your computer to mine but this is really inefficient. A better way is to use a Graphic Processing Unit (GPU) as this works extremely faster than CPU. In this walkthrough we attempt a simple mining using a Radeon HD 6700 GPU. The screenshot is shown below and a 128 Mhash/s (128 million hashes per second) is achieved.

Another recent popular and more efficient way of mining is by using Application Specific Integrated Circuit (ASIC) miners. These dedicated hardware devices work extremely fast and boasts of achieving 50+ Ghash/s.
Figure A-D2: BitCoin Mining, Screenshot.