AN ELECTRONIC MONEY MODEL FOR MICROPAYMENTS

A THESIS SUBMITTED TO

THE GRADUATE SCHOOL OF INFORMATICS

OF

THE MIDDLE EAST TECHNICAL UNIVERSITY

BY

OUMOUT CHOUSEINOGLOU

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF

MASTER OF SCIENCE

IN

THE DEPARTMENT OF INFORMATION SYSTEMS

JANUARY 2004

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

_____

Oumout Chouseinoglou

Approval of the Graduate School of Informatics

_____

Prof. Dr. Neşe Yalabık
Director

I certify that this thesis satisfies all the requirements as a thesis for the degree of Master of Science.

_____

Assoc. Prof. Dr. Onur Demirörs
Head of Department

This is to certify that we have read this and that in our opinion it is fully adequate, in scope and quality, as a thesis for the degree of Master of Science.

_____

Assist. Prof. Dr. Adil Oran
Supervisor

Examining Committee Members

Prof. Dr. Semih Bilgen _____

Assoc. Prof. Dr. Onur Demirörs _____

Assist. Prof. Dr. Y. Murat Erten _____

Assoc. Prof. Dr. Zeynep Onay _____

Assist. Prof. Dr. Adil Oran _____

ABSTRACT

AN ELECTRONIC MONEY MODEL FOR MICROPAYMENTS

Chouseinoglou, Oumout

M.S., Department of Information Systems

Supervisor: Assist. Prof. Dr. Adil Oran

January 2004, 147 pages

This research first defines money and lists its functions and properties. Among these properties, the anonymity and off-line capability of money are pointed out. Then the history of money is briefly discussed, to show that money has evolved similarly to the Lamarckian evolution of species. The examination of the history of money helps us justify why electronic money is necessary, and to point out that money will continuously evolve towards Pure Money. The definition of electronic money conducted afterwards, draws the lines within which the model will be proposed. The proposed model is formally constructed and evaluated accordingly with the use of micropayment evaluation frameworks.

The model is a hardware based model considering as baseline smart cards with secure co-processors, and allows transactions with cross-challenging. The

model is evaluated with respect to technologic, social and economic dimensions, and taking into account the associated computational and storage costs.

Keywords: Electronic Money, Micropayments, Pure Money, Anonymous Electronic Money, Off-Line Capability, Secure Co-processors.

ÖZ

MİKRO ÖDEMELERE UYGUN ELEKTRONİK PARA UYGULAMASI

Chouseinoglou, Oumout

Yüksek Lisans, Bilişim Sistemleri Bölümü

Tez Yöneticisi: Yrd. Doç. Dr. Adil Oran

Ocak 2004, 147 sayfa

Bu çalışmada paranın kısa tarihçesi sunulmuştur ve bu tarihçe para evriminin Lamarck'ın türlerin evrimine benzer şekilde ilerlediğini, elektronik paranın gerekli bir adım olduğunu ve Saf Para geliştirilene kadar da paranın evrim geçirmeye devam edeceğini ortaya koymuştur. Elektronik paranın tanımı yapılmıştır ve geliştirilen modelin sınırları çizilmiştir. Elektronik para modeli biçimsel olarak tasarlanmış ve mikroödeme modelleri için geliştirilmiş olan değerlendirme çerçeveleri doğrultusunda değerlendirilmiştir.

Geliştirilen model donanıma dayalı bir model olup temel olarak güvenli ek-işlemcili akıllı kartları ve karşılıklı 'meydan okuma' yaklaşımını benimsemektedir. Model, teknolojik, sosyal ve ekonomik boyutları ve ilintili işlem ve saklama maliyetlerini göz önüne alarak değerlendirilmiştir.

.

Anahtar Kelimeler: Elektronik Para, Mikroödemeler, Saf Para, Anonim Elektronik Para, Çevrimdışı Olabilme, Güvenli Ek-İşlemciler

To my Immortal Beloved,

For the nest, the compass and the wings

ACKNOWLEDGMENTS

I can only express my gratitude to my supervisor Assist. Prof. Dr. Adil Oran with the words of Alexander the Great, to Aristoteles; "Εις τον πατέραν μου οφείλω το ζείν καί εις τον διδασκαλόν μου το ευ ζείν"[i].

I wish to thank Assoc. Prof. Dr. Zeynep Onay for her invaluable guidance, and corrections but above all these, her encouragement, because "Correction does much, but encouragement does more. Encouragement after censure is as the sun after a shower"[ii]

My thanks also go to Prof. Dr. Semih Bilgen and Assist. Prof. Dr. Murat Erten, for always offering their priceless help and knowledge.

I wish to thank Yüksel Görmez for his guidance and inspiration.

I want to thank Cüneyt Sevgi for being my Socrates, when I was decaying like the city of Athens, "προσκείμενον τῇ πόλει ὑπὸ τοῦ θεοῦ ὥσπερ ἵππῳ μεγάλῳ μὲν καὶ γενναίῳ, ὑπὸ μεγέθους δὲ νωθεστέρῳ καὶ δεομένῳ ἐγείρεσθαι ὑπὸ μύωπός τινος, οἷον δή μοι δοκεῖ ὁ θεὸς ἐμὲ τῇ πόλει προστεθηκέναι τοιοῦτόν τινα, ὃς ὑμᾶς ἐγείρων καὶ πείθων καὶ ὀνειδίζων ἕνα ἕκαστον οὐδὲν παύομαι τὴν ἡμέραν ὅλην πανταχοῦ προσκαθίζων"[iii]

---

[i] "I owe my life to my father, but my soul and knowledge to my tutor"

[ii] Johann Wolfgang Von Goethe

[iii] "am a sort of gadfly, given to the state by the god; and the state is like a great and noble steed who is tardy in his motions owing to his very size, and requires to be stirred into life.", Plato, "*Apology of Socrates*"

I also want to thank Emre Doğruel for being my Prometheus and offering me the light of joy and happiness whenever I lost it and Alpay K. Ertürkmen for being my Daedalus and guiding me in the labyrinth of Java.

This thesis would never have been completed without the precious friendships of Resim Alioğlu, Yasemin Salihoğlu, Çiğdem Gencel, Murat Yakıcı, Pınar Onay, Duygu Apak, Tevfik Aytekin, Hasan Malkoç, Elif Küçükçiftçi and Ufuk Genç.

Finally, I would like to thank my family for their understanding, patience, and unshakable faith in me.

TABLE OF CONTENTS

LIST OF TABLES

TABLE

LIST OF FIGURES

FIGURE

LIST OF ABBREVIATIONS AND ACRONYMS

ACID	:	Atomicity, Consistency, Isolation, Durability
ACH	:	Automated Clearing House
AES	:	Advanced Encryption Standard
ATM	:	Automated Teller Machine
B	:	Broker or Bank
CD	:	Central Database
CHIPS	:	Clearing House Interbank Payment System
CPU	:	Central Processing Unit
CSK	:	Customer Shared Key
Cu	:	Customer Certificate
DoI	:	Date of Issue
ECB	:	European Central Bank
EDI	:	Electronic Data Interchange
EFT	:	Electronic Fund Transfer
EFTPOS	:	Electronic Fund Transfer at Point of Sale
ER	:	Entity Relationship Diagram
eW	:	Electronic Wallet
eWAK	:	Electronic Wallet Authentication Key

eWID	:	Electronic Wallet Identification Number
FIPS	:	Federal Information Processing Standards
GHz	:	Gigahertz
GRN	:	Generic Random Number
IA	:	Issuing Authority
IC	:	Integrated Circuit
IDE	:	AT Bus Interface
I/O	:	Input/Output
ISP	:	Internet Service Provider
JDK	:	Java Development Kit
JVMPI	:	Java Virtual Machine Profile Interface
Kbit/s	:	Kilobit per second
Kcycles	:	Kilocycles
LETS	:	Local Employment-Trading System
Mb	:	Megabyte
MHz	:	Megahertz
MICR	:	Magnetic ink character recognition
msec	:	Milliseconds
NIST	:	National Institute of Standards and Technology
NVM	:	Non-Volatile Memory
O_{cr}	:	Current Owner
O_{int}	:	Initial Owner
O_{pr}	:	Previous Owner
P	:	penny

P_r	:	Payer
P_e	:	Payee
PCMCIA	:	Personal Computer Memory Card International Association
PID	:	Personal Identification
PIN	:	Personal Identification Number
PRNG	:	Pseudo Random Number Generator
ROM	:	Read Only Memory
SCK	:	Secure Communication Key
SET	:	Secure Electronic Transaction
SHA	:	Secure Hash Algorithm
SVP	:	Small Value Payments
t	:	Electronic Token
*t*AK	:	Electronic Token Authentication Key
TFV	:	Token Face Value
TL	:	Turkish Lira
U	:	User
U.S.	:	United States of America
UTSN	:	Unique Token Serial Number
UTSNCV	:	Unique Token Serial Number Control Value
V	:	Vendor
VTS	:	Vertical Time Sequence

CHAPTER 1

INTRODUCTION

"*At the very heart of nearly all economic relationships in communities that have attained any considerable degree of economic development lies the institution of money.*"

(Day, Beza, 1996)

1.1. The Importance of Money

The evolution of human societies from the very first primitive ones to the modern societies of today relies on different inventions of humans. Each of these inventions would alter the way human societies were interacting with each other and within, easing the different problems of life and providing welfare. It can be argued that money is one of man's most important inventions, without which civilised society would be unthinkable.

"Money is an invention. It expedites the transfer of goods and services among persons." (Kaufman, 1981)

In separate geographical places and locations, under different cultural influences, traditions and beliefs, all over the world, humans have created economies, to better

employ and exploit nature and the world they were living within, and to trade with other economies. From the self-sufficient primitive economies, more advanced economies have emerged which relied on trade. The further development of these economies, has by itself led to the growth of the concept of a "medium of exchange", in order for trade to function. As "necessity is the mother of invention", people used the media of exchange to overcome the obstacles of the problematic and highly inefficient initial economies.

"Money is almost everywhere in the economic system where the production and exchange of goods and services are involved." (Cochran, 1979)

The development of a medium of exchange is highly related with the important invention of trade. People noticed that some goods were easier to trade than others and that these goods had similar properties. These goods were durable, easily divisible into smaller amounts, relatively scarce, that procuring and producing them required effort, and that they were homogeneous, and convenient to use. These commodities were used mainly in trade and exchange, and these commodities had become money.

The importance of money by itself as a variable of the economy is explained by Kaufman (1981) as:

"A substantial body of evidence – generated over the course of history – indicates that money is related more closely to aggregate levels of spending, prices, income, production, and employment than any other single economic variable."

There are basic foundation stones, which an economy is based upon. In an advanced and sophisticated economy, the level to which individuals can trade, work, and produce determines the potential and capacity of that economy, whereas the confidence with which persons can invest long term determines the current and future prosperity of

that economy. This is what money actually does. Money allows people and economies to produce what they produce best, to work, exchange, and trade, to gather and preserve their effort, and to make the necessary savings for the future.

It can be argued that the evolution of any civilized society depends on the discovery of the idea of money, and on the discovery of something that can be used as money. Without something to facilitate trade and allow specialization, societies would not be able to develop. Moreover, the future of any civilized society depends on the quality of what is used as money. Societies and economies are transforming money to different shapes (coins, banknotes) to better meet the needs, and to overcome the obstacles. This by itself is a quest for Perfect Money, or in other words, Pure Money.

Today, money and economies depend substantially on information systems, products and services. The advance in information systems changes the way modern economies are shaped and the way money is issued, stored and circulated within these economies. Economies and monetary systems have started to rely extensively on information systems, and information systems are designed and developed accordingly to serve and better fit these newly emerging forms of economies and monetary systems. Today, economies, monetary systems, payment and financial technologies heavily rely on information systems. That is why emerging types of payment such as electronic money are built upon the overall science of information systems and technologies. Such new and emerging forms of money need to be investigated, designed and implemented with respect not only to the classical economic science but also with respect to the information systems science.

1.2. Scope and Objective of the Study

Electronic money was introduced as a concept early in the development of e-commerce applications, and several pioneers have invented different schemes and techniques in order to use them as electronic money. However, the future of these electronic money schemes and techniques has proved less than successful. Within the very first few years of their introduction, either the issuers of electronic money went bankrupt like in the DigiCash example, dropped the product like in the CyberCash example, or moved into another business like in the First Virtual example (Chou, et al., 2002).

The main scope of this research is to develop an electronic money scheme appropriate for micropayments, considering the design methodologies that scholars have undertaken in previous researches, but also approaching the subject from the viewpoint of what money is and whether it is necessary to develop electronic money models.

The first discussion conducted in this research is related to the question of what money is actually and how it should be treated in order to develop a model for electronic payments. The classic definitions of money by economists which focus on the functions of money are considered not to be appropriate when developing a payment model. Therefore the first objective of this study is to provide an abstract definition of money, based on the properties of the money rather than the functions of money, which can act as a guideline while developing the overall model. Thus, the gathering and evaluation of the properties of different types of money becomes an important point to focus on. The list of properties provided is the outcome of a detailed literature survey

and an important groundwork for both this study but also for studies to follow focusing on electronic payment models.

Currently conducted studies on electronic payment models do not answer satisfactorily why the development of electronic money is necessary at all. Therefore, the proposed models lack justification of development. This study however, aims to provide the reasons why electronic money appears as a necessary step in the money evolution ladder. This approach requires the clarification of three main points, how money originated and evolved, how long it will continue to evolve and how this evolution will continue. This study attempts to provide an accurate and well established description of the money evolution, the significant steps undertaken, the route followed, the principles that lie beneath this evolution, and most importantly the final destination node that this evolution is heading to. The properties of Lamarckian evolution of species are evident in the evolution of money and the according parallelisms and similarities are provided. The concept of Pure Money, the final destination point in the money evolution, is a concept introduced by this research and is described abstractly. All these subjects are covered in detail in this study, to provide the rationale why electronic money is necessary not only for the sake of this study but for all studies focusing on electronic money models.

Not only the definition of money but also the accurate and acceptable definition of electronic money is a main objective of this study as existing studies have shown that each scholar tries to define electronic money in order to suit the model that their research proposes. In this study however, a vast list of definitions of electronic money are given, the definition chosen is accepted by most scholars and is the definition that is close to the perception of this study. Moreover, the assessment of each definition is

included, as no of the definitions are complete and each has its own shortcomings and points that fail to cover. The definition of electronic money would be another important guideline in the model to be developed.

The existing electronic money schemes and models are briefly covered, in order to distinguish the properties of money that electronic money models primarily distinguish. Two important debates stand out, the off-line vs. on-line capability and the anonymity vs. traceability properties. The developed model is built upon this debate and promotes the off-line capability and the anonymity of the transactions. Moreover, the scope of the developed model is not to satisfy every existing payment, but to focus on a particular area of payments with respect to the size of transactions, namely micro-payments and nano-payments. This distinction between payments based on the monetary volume of each, the related discussion, and the definition of micropayments are covered in detail. The developed model aims to satisfy payments for business areas such as newspapers, magazines, search engines, micro-gambling, personal essays, etc.

The foundation of the developed model is two studies, the secure coprocessors and tamper resistant smart cards by Tygar and Yee (1993) and the Small Value Payments by Stern and Vaudenay (1997). The design objectives of the model, the target market, the methodology, the details of the transaction, the possible cryptography and the considerations to be taken into account while selecting the cryptography are covered in detail. Moreover, the developed model is evaluated in detail with respect to three major considerations: the computational cost of the model, the VTS evaluation and Chi frameworks. The results of these three considerations are included and discussed in order to better understand the developed model in its completeness.

1.3. Outline

The main body of this thesis report consists of two sections, where the first section addresses the money related issues whilst the second section is discussing electronic money and the proposed model for micropayments. Furthermore, this study consists of 6 chapters.

Chapter 1 provides a broad introduction to the subject and the importance of money, and gives the scope and objective of this study.

Chapter 2 covers the classical definition of money. The functions and attributes of money are listed, described and discussed thoroughly. However, this study proposes that money should be defined and classified not with respect to its functions, but with respect to its attributes and properties, thus providing a new insight.

Chapter 3 presents the history and detailed evolution of money, providing different views on how money was first initiated. Moreover, the new notion of Pure Money is first introduced in Chapter 3.

Chapter 4 presents and discusses the existing definitions of electronic money and compares them. An attempt is made to select the best and most appropriate definition, but also the shortcomings of this definition are discussed. The properties that electronic money should possess are described in detail. Moreover, the notion of micropayments is introduced.

Chapter 5 proposes a new electronic money model for micropayments. The model is described in detail and is evaluated with respect to its computational cost and two frameworks proposed by scholars. The results of these evaluations are favourable compared with other existing payment methods proposed for micropayments, and the

model proposed of this study shows superiority with respect to the attributes of anonymity and offline capability.

Chapter 6 concludes the research with the discussion of the findings in the previous Chapters and lists the planned future work to follow this study.

CHAPTER 2

DEFINITION OF MONEY

"It is in this manner that money has become in all civilized nations the universal instrument of commerce, by the intervention of which goods of all kinds are bought and sold, or exchanged for one another."

(Smith, 1776)

2.1. Definition of Money

As money itself has evolved during the course of time from barter to plastic money, based on this evolution the definition of money has also evolved. It is difficult to distinguish the abstract idea of money from the actual money circulating in the daily life economies. Moreover, most economics scholars differentiate between money and means of payment, and do not accept as money the credit cards, cheques and etc. However, in this research the terms money and means of payment will be used interchangeably.

The very first definition of money we encounter was made by Plato, who states that "Money is a 'symbol' devised for facilitating exchange" and that the value of money is independent of the material it is made of (EconJournal, 2003). Plato's student

Aristotle on the other hand defines money by involving the exchange of goods and services (EconJournal, 2003). This exchange at first naturally takes the form of barter; but the coincidence of wants is not always present, obvious convenience will then induce people to choose tacitly or through legislative action, a single commodity as a medium of exchange. Moreover, the requirements of Aristotle's rule of equivalence in exchange naturally led him to observe that the medium of exchange will also be used as a measure of value and implicitly as a store of value. For Aristotle, money serves as a medium of exchange, and in order to serve as a medium of exchange in the market of commodities, money itself must be one of these commodities (EconJournal, 2003).

For Adam Smith (1776), money acts as a unit of account; money is not by its nature, a valuable object; the significance of money is only to express the value relations between other objects.

For Cochran (1979), money can be defined as anything which is generally acceptable in payment for goods, services, and debts, primarily focusing on the general acceptability of the article or medium to serve as money. He argues that for money to be money, it must be generally acceptable. However, he further includes in his primary definition the facts that money is the most liquid asset by which the market value of all goods and services may be determined, mainly a medium of exchange and a measure of debt and contracts.

There are more definitions of money, each focusing on a particular area or specific philosophic idea of money, narrowing the definition of money. However, as with any object, money can be analyzed either with respect to what it does (functions) or with respect to its characteristics (properties). This research will focus on both aspects, functions as well as the properties of money. By analyzing both the functions

and properties of money it is possible to derive a more general, healthy and up-to-date understanding of money.

2.1.1. Functions of Money

Walker (1883) argues that "Money is what money does", indicating that it is impossible to distinguish money from its functions. Furthermore, as Friedman (1994) says anything can be money: stones, iron, gold, tobacco, silver, shells, cigarettes, copper, paper, nickel, etc. What makes these things money is not what they are, but what they are used for. They may have value in themselves, like gold, or they may not, like banknotes and bank deposits; but their value as money is separate from their intrinsic value. As Einzig (1966) claims "Money does not exist in a vacuum. It is not a mere lifeless object, but a social institution. Without its background it has as little meaning as a verb divorced from its context".

Therefore it is important to list the functions of money. Listing the functions of money may help us to distinguish between different money forms. These functions, according to Davies (1994), are:

- Standard unit of account
- Common measure of value
- Medium of exchange
- Means of payment
- Standard and means of deferred payments
- Store of value

Each of these functions are covered in detail in the following paragraphs.

- **Standard Unit of account**: Money is an agreed-upon measure for stating the prices of goods and services. As a unit of account money allows for easy comparison of

relative prices of goods or services by allowing commodities to be labelled with a price using a common denominator. In other words, unit of account is the unit in which values are stated, recorded and settled. Cochran (1979) describes this function of money as:

> Goods and services can be priced in terms of money, and this price is understandable to the would-be buyer as well as to the seller. The use of money as a measure of value eliminates the necessity to quote the price of apples in terms of nuts, the price of nuts in terms of oranges, and so on. Furthermore, we can add the market values of goods, once they are expressed in monetary terms.

- **Common measure of value**: Money is a commonly agreed metric used to measure the value of different items. The value of an item measured should be understandable by other parties so that an idea regarding the measured item is delivered. The difference between the function of common measure of value from the function of standard unit of account is subtle. Einzig (1966) names the function of common measure of value as standard of value and describes it as:

> Standard of value is a common denominator or unit of account in terms of which the prices of goods and services are regularly measured and expressed. Magnitudes of value can be compared by expressing them as a fraction or a multiple of the units concerned. Prices are figures expressing the numbers of these units representing the equivalents of various goods and services. Every exchange implies a price. … The standard of value must be, however, a unit that is used regularly for measuring and expressing exchange values of goods and services.

- **Medium of exchange**: Money is an accepted way to facilitate transactions as people accept money in trade for goods and services. By avoiding the need for barter, money improves the efficiency of making transactions. Einzig (1966) defines the term of medium of exchange as an object conforming to certain standards of uniformity that is widely accepted in payment for goods and services, because the recipient can easily use it for making similar payments.

Cochran (1979) summarizes the medium of exchange function of money stating that we can work for money, knowing that the money we secure from selling our labour services can be used to acquire useful goods and services, which is the real economic justification for our work in the first place. We do not want money for its own sake, but we have learned from experience that the possession of money gives us a good deal of economic independence. Money makes it possible for us to extend our economic capacities, so that we can enjoy an assorted bundle of goods and services, which it would be impossible for us to produce single-handedly.

- **Means of payment**: Money can be used to pay for an item or service that is being purchased, as both the purchaser and seller agree in using money as a mean of payment. However, it differs slightly from the function of being a medium of exchange, as money can be used to make payments without necessitating an exchange. This is closely related to the first fundamental characteristic of money as stated by De Grauwe (1997):

> A first fundamental characteristic of money is that it is very much like a collective good. That is, the benefit of money to an individual derives exclusively from the fact that others also use it. Contrary to a private good which has a utility to an individual whether or not others also consume it, money has no utility whatsoever when used by only one person. In order to have value to an individual, it is necessary that others also use it. And the larger the group of people using the same money the greater the utility to that individual.

- **Standard and means for deferred payments**: No matter what is considered money, debts have to be quoted in terms of it. Money is used to enable people to borrow and lend agreed amounts. Einzig (1966) summarizes this function of money as "Standard of deferred payments is a monetary unit in which liabilities maturing at some future date are expressed. For the purposes of this definition, "liabilities"

include payments of every description under long contracts, debts, rents, interest etc."

According to Cochran (1979) money is a standard of deferred payments just because

> Just as money is used to measure the market value of goods or services at a given point in time, so it serves to indicate the sum of purchasing power that is being lent and borrowed. Although a specific, useful commodity can be lent with the same commodity or one similar to it due in repayment, different interpretations about the quality of the two commodities being exchanged over time may occur, as we have mentioned. With money being lent there is no difficulty about the amount due in return.

- **Store of value**: Money is used to hold wealth, and is used as a form of savings in order to store value over time although not all of savings is kept in the form of money. According to Einzig (1966):

> A store of value is an object in which wealth is held exclusively, or at any rate primarily, for the purpose of preserving the value it represents. In a broader sense every medium of exchange must necessarily be suitable also to serve as store of value, since the recipient accepts it because it is capable of preserving his purchasing power until he is prepared to spend it. If, however, the period that elapses between receiving the medium of exchange and spending is brief – or rather if the recipient does not intend it to be long – the medium of exchange is not considered to constitute also a store of value in the more generally accepted narrower sense of the term.

Cochran (1979) exemplifies the store of value function of money by stating that:

> Sometime individuals and institutions do not wish to spend all today's income today. Acquiring an amount of money today makes available purchasing power tomorrow, or at any future time. The amount of purchasing power available tomorrow is the same as the purchasing power saved today, however, only if tomorrow's prices of commodities and services are the same as they are today.

It can be argued that, for a commodity or item to qualify as money, it should serve almost all the functions listed above. However, it is crucial to point out that a form of money that does not satisfy some of these functions, may have serious problems surviving as a generally accepted form of money.

An important economist conduct research in the area of denationalization of money, Hayek (1976), defines the importance of each function of money as:

> To serve as a widely accepted medium of exchange is the only function which an object must perform to qualify as money, though a generally accepted medium of exchange will generally acquire also the further functions of unit of account, store of value, standard of deferred payment, etc.

Actually, some argue that the other characteristics may reduce the "moneyness" of some monies. Weighted monetary aggregates like "divisia" index are based on the idea that monetary aggregates (M1, M2, M3 and M4) that simply add up different types of money may not be appropriate. They argue that if some types earn interest, then they are less money.

No function of money is more important or significant with respect to other functions. However, communities and societies have attributed certain significance to some functions and even not used one or more functions of money. Based on the functions listed above, Davies (1994) concludes that:

> What is now the prime or main function in a particular community or country may not have been the first or original function in time, while what may well have been a secondary or derived function in one place may have been in some other region the original which gave rise to a related secondary function... The logical listing of functions in the table therefore implies no priority in either time or importance, for those which may be both first and foremost reflect only their particular time and place.

The definition of Davies (1994) for money is: "Money is anything that is widely used for making payments and accounting for debts and credits". This simple but general definition of money summarizes all functions of money previously described.

Concluding on the analysis of the functions of money it can be argued that a specific form of money would serve for any function of money, as long as users of that money use it for these particular functions. However, the users will employ that form of

money for any function, with respect to the embedded properties and attributes of the money in question; these properties would be the criteria to choose what monies to use for a specific function and which not to. Therefore it may be more appropriate to place importance on the attributes of money rather than the functions of money.

2.1.2. Attributes of Money

The functions of money previously listed describe how money dictates the way economies transact and work. However, different forms of money currently coexist within the same economies, just as different forms of money have coexisted throughout the historical development of money. This history of money will be further discussed in CHAPTER 3.

Characterizing and comparing different forms of money with respect to the functions they perform would not be possible as each form of money can accomplish every function, if used by the society for that particular function.

Therefore the reason that a form of money is not used for a specific function is not the money itself but a choice of the users of money. This research argues that, monies should be characterized not with respect to their functions but with respect to their attributes. These different monies circulating within the same economic system and coexisting is due to the fact that each form of money, is distinct from other forms of money with respect to some attributes. Therefore, the list of attributes given below has been developed as a first step in this research, and is the result of empirical approach and an extensive research within studies focusing on the nature of money. These attributes can be listed as:

- Security
- User friendliness

- Portability
- Divisibility
- Anonymity
- Durability
- Acceptability
- Recognisability
- Latency
- Reliability
- Nonrepudiation

Each of these attributes is defined in the following paragraphs.

- **Security (Unforgeability)**: Money should be secure; counterfeiting should be difficult if not impossible. A form of money easily counterfeited would eventually be wiped out.
- **User Friendliness**: Money should be easy to use in any of the previously described functions of money. Moreover, the transactions and functions related to that money should also be user friendly.
- **Portability**: Money should be easy to carry and store physically, without any significant inconvenience to the carrier.
- **Divisibility**: Money should be divisible into smaller amounts, so that no loss should occur in any transaction. Furthermore, it should also be possible for small amounts of money to be added up to a more convenient larger amount, to ease the transactions to be conducted.
- **Anonymity**: Many users of money may argue that money should be anonymous; there should be no trace of the previous transactions committed and of the persons

who committed them. However, others may argue that by having a fully traceable form of money, crime and felonies committed and related with some amount of money would be traced to its committers.

- **Durability**: Money should be durable over time; money should not be spoiled, destroyed or damaged with its usage or storage.
- **Acceptability**: Money should be acceptable by some (preferably all) parties involved in that economy, in order to be considered as money. Otherwise no transactions will occur.
- **Recognisability**: Money should be easily recognisable, especially regarding the amount it denotes.
- **Latency (with respect to Clearing Time and Frequency)**: If the payment requires to be settled and cleared by a third authorizing party, then even during peak load periods, the payment information and details should be transmitted at a steady pace (Schmidt, Muller, 1997).
- **Reliability:** Money must be available continuously whenever necessary, 24 hours a day. That is, the operation system of the payment should not present failures at anytime (Neuman, Medvinsky, 1995a).
- **Nonrepudiation:** Acknowledging the payment made with money and producing receipts are the basic properties required for any payment system, to provide proof of payment. (Neuman, Medvinsky, 1995a).

Different forms of money will focus on different attributes of money and will be used particularly by some distinct users, in some distinct transactions due to their unique attribute combinations. A person will prefer to use cash and banknotes while purchasing bread because of the excessive ease of use it provides, but will prefer credit card while

purchasing a book from the Internet due to its international acceptability, portability and sophisticated security. Each form of money is a distinct combination of different attributes in different ratios. These attributes differentiate a given form or type of money from the other existing monies.

CHAPTER 3

HISTORY AND EVOLUTION TIMELINE OF MONEY

"*The use of coin, which has been handed down to us from remote antiquity, has powerfully aided the progress of commercial organization, as the art of making glass helped many discoveries in astronomy and physics; but commercial organization is not essentially bound to the use of the monetary metals. All means are good which tend to facilitate exchange, to fix value in exchange; and there is reason to believe in the further development of this organization the monetary metals will play a part of gradually diminishing importance.*"

Augustin Cournot, 1838
(Evans, Schmalensee, 1999)

3.1. Introduction

History, as in all subjects is an important metric and the basis on which civilization evolves. Society itself is constantly changing and so everything that lies within is subject to this change. A review of history is essential to any study examining the future of a subject. The history of money therefore is significant for any study focusing on the future of money, like this is. As a result this study will review the history of money in order to allow us to look into the future of money. It can be argued that one of the most valuable allies of this study, is the history of money, because by

demonstrating the continuous evolution of money this study aims to show that the evolution will continue. Davies (1994) argues that

> Because of the difficulties of conducting experiments in the ordinary business of economic life, at the centre of which is money, it is most fortunate that history generously provides us with a proxy laboratory, a guidebook of more or less relevant alternatives. Around the next corner there may be lying in wait apparently quite novel monetary problems which in all probability bear a basic similarity to those that have already been tackled with varying degrees of success or failure in other times and places.

Throughout history, an evolution of money can be seen. Economies have evolved, and so has money. Rogers (1974) states that every society that has existed above a subsistence level has developed money in some form, a fact that is not accidental. Cowry shells that have been used as money between exchanging parties at the very first, now are worthless as a financial instrument. Instead, new forms of money have evolved throughout, coexisted and the best suited were selected to continue their existence. Whenever there are any costs associated with the use of an exchange medium, there is an opportunity for further development. Between these different forms of money a "natural selection" process took place: the most costly forms of money were abandoned and the ones costing less were selected for further use. In other words, monies meeting as many needs as possible at the lowest cost and price would be selected. The selected form of money however would evolve within itself to minimize this usage cost and better meet the needs of exchanging parties, similar to a Lamarckian evolution, as shown in Figure 1. According to the Lamarckian evolution, more complex forms of life have originated from simpler forms (Encarta), and this form of evolution can be traced in the evolution of money also (Lockard, 1997). A further parallelism between the Lamarckian evolution and the evolution of money is that, as different

monies acquired new attributes (such as security, divisibility, etc.), these attributes would be inherited to newer monies to follow, thus creating a link between the generations.

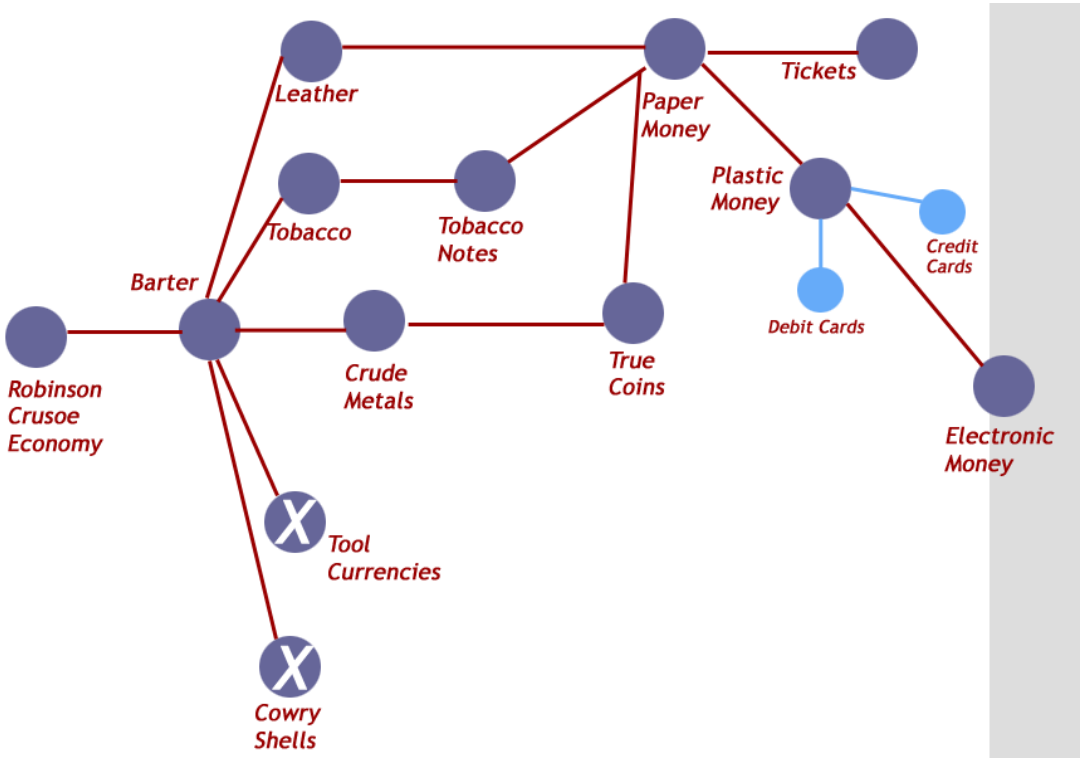

Figure 1 The Lamarckian evolution of money

A sample drawing showing the Lamarckian evolution of money is Figure 1 where different types and forms of money have coexisted together and eventually some of them have evolved to better fit the increasing needs of the economic society in order to diminish the associated costs, whereas other forms have been wiped out. Moreover, the newer monies originate from older monies, and the attributes are inherited.

3.2. Robinson Crusoe Economies

At first there was no money. Although there was no money, economies still existed. People, living in very small family based societies, would produce only the necessary commodities for their survival and existence. Nitsche (1970), describing these

people, states that they worked together and were entirely self-supporting, they did not need money. These economies are sometimes referred to as "Robinson Crusoe" economies. The Robinson Crusoe economies consisted of a small society, possibly a family, which was both the producer and consumer and in no way was there trade. There was a complete autarky and no need for accounting and no intermediation cost. As Rogers (1974) defines, in an utopist Robinson Crusoe economy there are almost no scarce alternatives, there is nothing to economize, goods abound in such quantity as to make them free and nothing need be given up to get another wanted thing, therefore there is no need to trade or specialize. This is due to the fact that each economy would produce the vital things for survival; there was no specialization of work force. From an economics point of view this case is not interesting as there are no problems in such economies as there are no scarce resources. However, it can be considered that this was not the case in the first Robinson Crusoe economies: The resources were scarce, and those resources would not be used efficiently, the production would be limited and any surpluses of the produced goods would be lost as there would be no exchange of the surpluses for scarce goods. In most cases, whenever a natural problem occurred people would fail even to produce the very vital items for their survival.

Einzig (1966) characterizes these primitive economies as a phase of food-gathering by isolated individuals or families. Kaufman (1981) on the other hand describes these primitive economies as:

> In the early days of world history, money did not exist. Man was totally self-sufficient. He raised his own food, prepared his own clothing, constructed his own shelter, and provided for his own security. He engaged in no trade and had no use for money.

The lack of trade implies lack of specialization and low productivity. However, even without any change in production trade would make the parties better off. Once

trade established between parties, the changes in production and the specialization to follow, truly large benefits could be obtained.

3.3. Barter Economies

Due to the disadvantages of the Robinson Crusoe economies previously stated, people started to exchange commodities in surplus for scarce commodities. This process of exchange is barter. Barter can be defined as the direct exchange of resources or services for mutual advantage. More precisely dictionaries define barter as the "direct exchange of goods or services--without an intervening medium of exchange or money--either according to established rates of exchange or by bargaining" (Merriam-Webster). It is important to distinguish that barter is the direct exchange of goods, and no indirect exchange is accepted, as indirect exchange would imply the use of an exchange medium, which in turn would be considered a form of money. As Von Mises (1953) states:

> Indirect exchange is distinguished from direct exchange according to whether a medium is involved or not.
> Suppose that A and B exchange with each other a number of units of the commodities *m* and *n*. A acquires the commodity *n* because of the use-value that it has for him. He intends to consume it. The same is true of B, who acquires the commodity *m* for his immediate use. This is a case of direct exchange.

Economists agree that gradually, division of labour led to the barter economy, in which items were produced for exchange. This specialization process is described by Kaufman (1981) as:

> In time, self-sufficient man discovered that he was not equally good at all tasks and neither were his neighbours. He observed that he consistently outperformed others at some types of work but was, in turn, outperformed by others at different tasks. He soon realized that he and everyone else in his community would be better off in terms of greater output if everyone concentrated on doing that at which he was best and pooled their resources. The sum of the outputs generated by specialists, exceeds the sum of the outputs generated by generalists.

Rogers (1974) in his simple example from Robinson Crusoe economies to barter explains the reasons that initiated barter as:

> …economizing has taken place in the resource of human time and energy. The economizing has been accomplished by specialization. But for the specialization to be practical, trade *must* take place between the specialists. Otherwise, surpluses and shortages of desired goods and services will occur immediately.

Although nobody actually knows how the first barter was conducted, it can be imagined that two people, owners of two different items, each needing the item of the other one agreed to exchange those items for the sake of mutual advantage. However, barter existed before that and it was not a human activity; but an activity of the natural environment humans are living within; plants and animals have been bartering with each other and living a symbiotic life for mutual advantage.

Einzig (1966) states that although many textbooks argue that barter came as a result of the development of division of labour and of private ownership, it is difficult to distinguish which came first. He claims that indeed a certain degree of barter can exist not only before the development of division of labour but even before the development of private property in the generally accepted sense of term, which is the individual ownership of means of production.

Economies trading with each other using barter were able to directly exchange goods and commodities. The items in surplus would be exchanged for scarce items, people would specialize regarding their works and there would be no need for everyone to produce the vitals for survival. However, compared to the economies that followed, (money economies), barter economies had significant disadvantages. Instead, barter economies have proven to humans that exchange of goods is advantageous for both exchanging parties, but the exchange should be conducted with more efficient methods

than barter. What is called as the "meet of needs" (or coincidence of needs) is very important in barter. Unless the needs of people meet there is no opportunity for barter. Moreover, most commodities are neither divisible, nor can be transferred or carried easily. The disadvantages of barter are pinpointed by Kaufman (1981) as:

> Although such trade increased everyone's welfare, it was highly inefficient and absorbed time and energy that could well have been put to better use. Not only did traders have to find others who wanted what they had to offer and who, in turn, had to offer what the first person wanted, but they had to find individuals who had the correct quantities of the particular items.

In large scale economies like today's economies, purchasing goods with the use of barter is by no means applicable or acceptable. Rogers (1974) concludes that

> *Direct* trade of goods and services is probably the best (most efficient) way of organizing things, as long as there are (a) few people, (b) few products, (c) small distances, and (d) simple production processes involved.

On the same subject Von Mises (1953) states that "Indirect exchange becomes more necessary as division of labour increases and wants become more refined".

3.4. Money Economies

3.4.1. Initiation of Money

In separate places, under different cultures, all over the world, the concept of a medium of exchange grew. Kaufman (1981) argues that money was invented to overcome the limitations of a barter system. The trade based on barter was not at all efficient. Menger (1871) has argued that barter was significantly complicated because of lack of coincidence of wants and needs. In barter economies people noticed that some goods and commodities were easier to trade than others, and they were durable, were easily divisible into larger or smaller amounts, were comparatively scarce and procuring

them required effort, and above all they were convenient. Kaufman (1981) lists these properties as scarcity, durability and divisibility. Those goods that possessed these properties were useful and commanded an exchange value in their own right but because they were easier to trade than any other goods, they came to be perceived as having a value over and above their basic utility. They came to have a value as an easily tradeable good. They came to have a value as a medium of exchange. Kaufman (1981) points:

"Money was demanded not only for its own sake, but for its exchange value or value in current or future trade."

Von Mises (1953) on the same subject states that:

> Thus along with the demand in a market for goods for direct consumption there is a demand for goods that the purchaser does not wish to consume but to dispose of by further exchange. It is clearer that not all goods are subject to this sort of demand. An individual obviously has no motive for an indirect exchange if he does not expect that it will bring him nearer to his ultimate objective, the acquisition of goods for his own use.

Once this value became widely recognized, the commodity in question was no longer consumed for anything else but the most vital purposes. Instead, it was used in exchange. It had become money. However, Kaufman (1981) remarks on a very important point regarding the use of commodities as money:

> Primitive monies consisted of items for which the exchange or monetary value was shared with the intrinsic or market value of the commodity for its own sake. This provided holders with protection against deep declines in exchange value. The intrinsic value served as a floor for the exchange value. If at times the exchange value threatened to decline below the intrinsic value, the commodity could always be sold for its own sake. On the other hand, at times the intrinsic value climbed above the exchange value, the commodity stopped serving as money, and was used for its own sake.

It is debatable however how money was first generated. As forms of money were developed in different periods of time in different places, it can be concluded that the process of money initiation was different in each case. Davies (1994) hypothesizes that money originated very largely from non-economic causes: from tribute as well as from trade, from blood-money and bride-money as well as from barter, from ceremonial and religious rites as well as from commerce, from ostentatious ornamentation as well as from acting as the common drudge between economic men.

On the other hand, other economists are stricter on the subject. As Von Mises (1953) says, whenever a direct exchange seemed out of the question, each of the parties to a transaction would naturally endeavor to exchange his superfluous commodities not merely for more marketable commodities in general, but for the most marketable commodities; and among these again he would naturally prefer whichever commodity was the most marketable of all.

Whatever the real cause of the money initiation was, it is obvious that money by its invention resolved the various problems of barter. Barter was no longer a sufficient medium of exchange for the societies; the economies were developing and changing. Menger (1871) summarizes the use of money as:

"Precisely because money is a natural product of human economy, the specific forms in which it has appeared were everywhere and at all times the result of specific and changing economic conditions."

Furthermore, one can assume that barter was incapable of easing the trade process; the items to be used in barter were usually neither **portable** nor **divisible**. People would prefer to trade with items that would be easily divided into smaller parts and would be easily carried to the market place. The attributes of portability and

divisibility were some of the complementary reasons that people would prefer to use certain commodities as medium of exchange rather than other commodities. The attributes of portability and divisibility moreover would accompany from that time on, in some extent, all items serving as money so that in economies following this advance, a surviving scheme of money or a proposed model should be both portable and divisible.

Einzig, (1966) describing the evolution from moneyless economies to money, identifies more than one cause of origination. He lists these causes of origination as different theories, which are:

- the medium of exchange theory; where money arose from the realization of the inconveniences of barter, as Menger (1871) and Von Mises (1953) argue
- the origin through external trade; where the money of each individual economy is either the imported objects which have in general non-monetary use within the importing community and have a relative scarcity value, or imported objects which are imported with the specific purpose of their monetary use, and which have no non-monetary use in the importing community, or exportable staple products which are in strong and systematic monetary or non-monetary demand outside the exporting community, or imported objects which have in general monetary or non-monetary use in third communities
- the origin through internal trade; where non-professional barter between producers and consumers gave rise to currency
- the standard of value theory; where money arose from the need for a common denominator

- the store of value theory; where money originated from articles or objects used as an insurance against the uncertainties of future
- the origin from standard of deferred payments; where money arose from the need to ease the repayment of loans or credits back to the lender
- the origin through non-commercial factors such as ornamental and ceremonial functions, religious origin, political origin, matrimonial origin, and origin through status symbol function (Einzig, 1966).

Whatever the origin is, different societies have invented money in different periods by different necessities, and societies continue to invent new forms of money.

3.4.2. Evolution of Money

Quite a few researchers argue that cattle was the first money ever used. Lockard (1997) states that cattle is often cited as the earliest of commodities to establish itself as general medium of exchange. The selection of cattle according to Menger (1871) was because as early people passed from a nomadic to agricultural system, cattle were familiar to and used by everyone, prior to the existence of roads, the transportation of cattle was virtually costless, cows are durable, where there is open pasture and water, the costs of maintenance are low, and trade involving cattle would have been widespread and continuous. Davies (1994) furthermore states that:

> Subsequently both livestock, particularly cattle, and plant products such as grain, came to be used as money in many different societies at different periods. Cattle are probably the oldest of all forms of money, as domestication of animals tended to precede the cultivation of crops, and were still used for that purpose in parts of Africa in the middle of the 20th century.

Although cattle is considered to be the first form of money used, according to Lockard (1997) other commodities which have served a monetary function in primitive

societies include oxen, sheep, skins, grain, shells, tobacco, rice, wheat, beef, pork, cocoa, cotton, copper, tin, wax, cod, slaves and ivory. For salt, it is known that the word "salary" originates from the Latin word "salarum", which means salt. More commodities can be added to the list. However, Lockard (1997) pinpoints an important characteristic of all those commodities used as money in the very beginning: **marketability**.

> Any commodity with superior marketability may be pressed into service as a money, and, in the final analysis, marketability is the defining characteristic. Other characteristics of various goods will, however, determine the acceptability of a particular good as a medium of indirect exchange, which is what provides any good with the sought after acceptability in exchange.

However, it is important to distinguish that the economic environments by themselves and the social conditions usually have played a significant role in the selection process of the money forms to be used. For example, during World War II, due to hyperinflation in Germany, Germans would use cigarettes as money, despite the fact that cigarettes were particularly primitive when compared to coins and banknotes. By this example the ability of economies to select a more appropriate form of money in case of social emergency can also be shown.

As in economies of today, it is expected that in primitive economies different forms of money and different items serving as money coexisted at the same time. However, people would tend to use the most marketable commodity as money in determining the values of the items to be sold. Lockard (1997) parallels this selection between the items used as money with the natural selection process of Lamarck:

> Although several common goods may perform reasonably well as money, there is an additional advantage to minimizing the number of goods utilized as money. If a single good can be identified as money, then the market specialists need only be familiar with the valuation of one commodity in addition to their own area of expertise; the money commodity, which has been selected, in part, for the relative ease of evaluating it in this regard. In the case of a single medium of

> exchange, its role as a unit of account is automatic, and there is never a need to translate prices into some other value scale. Thus we can expect a natural process of selection to narrow in on a minimum number of commodities that are best suited to function in the role of money.

This natural selection between the different items used as money has also attracted the interest of Von Mises (1953) who summarizes the evolution from cattle towards the precious metals by stating that the natural selection process resulted in the broad variety of commodities, that had enjoyed some use as exchange media in different places, to eventually become lessened down to include just two commodities; the precious metals silver and gold.

Precious metals such as silver and gold, in weighed quantities, were a common form of money in ancient times. The weighting of these metals was procuring risk costs in their use, as the parties exchanging the metals were unaware of the exact weight and purity or quality of the metal. The lack of information on the purity and exact weight of the metal can be called the security cost of the metal. This cost was later eliminated by using coins, which could be counted. The transition to metal quantities that could be counted rather than weighed came gradually. According to Davies (1994) , Lydians were the first to use coinage as Herodotus criticises the gross commercialism of the Lydians who are the first people to coin money. Therefore true coinage developed in Asia Minor as a result of the practice of the Lydians, of stamping small round pieces of precious metals as a guarantee of their purity. Later, when their metallurgical skills improved and these pieces became more regular in form and weight, the seals served as a symbol of both purity and weight.

Lockard (1997) comments on the use of coins rather than crude metal as:

> Here we see that at this stage of development there are still considerable costs involved in the monetary use of precious metals,

> including the need for a market specialist for the metals, in the case of large transactions. These problems can, however, be addressed by the process of coinage. Metal of a known quality and quantity can be pressed into coins by a trusted agent, and marked as to their content. The information costs associated with using the coins as money is then reduced to the process of determining if a particular coin that has been presented is, or is not, counterfeit.

By the use of metals, one of the most significant attributes of money; which every commodity serving as money should meet, was realized; the attribute of **security**. With the use of metal coins, counterfeited and debased coins would circulate in the market, resulting in what is called Gresham's Law; that the bad money would drive out the good money. According to Gresham's Law, in a situation where two media of exchange come into circulation together and if they trade for the same value, the more valuable will tend to disappear from circulation as the less valuable will tend to be spent first. This assumes that the community will accept the bad money and not demand the good money as a medium of exchange. The first historic record of what later became known as Gresham's Law comes from Aristophanes in 405 BC. who in The Frogs wrote "the full-bodied coins that are the pride of Athens are never used while the mean brass coins pass hand to hand" in order to criticize the hoarding of silver coins by the Athenian public which, as a result, quickly disappear from circulation, leaving only the inferior bronze ones (Lockard, 1997). With coins becoming popular the security of purity and genuinity of money circulating on the market becomes of vital importance, as witnessed in the Trial of the Pyx, conducted in 1282, and was a public test of the purity of gold and silver coins, which continues in Britain to this day (Lockard, 1997).

Moreover, another aspect of money to be realized with the use of coins is **durability**. As primitive forms of money such as cattle or grain would be durable only

for a particular period of time, the use of metal as a medium of exchange has introduced the idea of almost infinite duration. Lockard (1997) argues that:

> With the development of coinage, the precious metals are especially well suited to serve as media of exchange. They are durable and divisible, and in the form of coins or bullion, fungible, and determination of the value of any particular coin is virtually costless.

Furthermore, coins would be homogeneous and identical with each other, resulting in what is called money **anonymity**. A coin used in a particular event of trade would be undistinguishable from a coin of similar weight and purity used in some other trade event. The anonymity of a money form would increase its related popularity, as some people would prefer their activities not to be monitored or traced. On the other hand, other people want to have their payments to be traceable, in order to be able to prove that they have actually conducted that payment (e.g. credit cards, checks). In economies of today, the anonymity or traceability of money is one of the most important aspects of any form of money. This debate is further discussed in detail in section 4.3.2.

The coins would be minted usually by kings or governments, resulting in the nationalization of money, although in some extraordinary cases special mintmasters would mint their own money. The primitive forms of money were not related to a particular nation, government or king. The sign of a central authority on the coin would declare that the metal the coin was made of was pure and of appropriate weight.

The evolution of money continues even though today gold coins are still used as a means of payment or exchange. The next most important step in the evolution of money is the invention of banknotes, or paper money. Lockard (1997) tells the story of the transition from coinage to banknotes as:

> At this point a critical stage in monetary evolution has been reached; an optimum monetary commodity has been selected. The process of monetary evolution is not over, however. Whenever there are costs associated with the use of an exchange medium, there is an opportunity for further development. Additional problems remained regarding storage and transportation of coins and bullion. At this point we see that further innovation in exchange media change from a question of what will serve as a medium to how it will be exchanged. Initially, coins and bullion are transferred by delivery. Possession of coins and bullion involves some risk of theft, however. When not actually needed for commerce, owners of coins and bullion will likely prefer that those items be deposited with people with a reputation for trustworthiness accustomed to protecting valuable property. Bill brokers, moneychangers, scriveners, goldsmith and mintmasters come to hold the commodity money of others. Transfers of money, early on, will take place at theses tradespeople's places of business. As coins from one individual are transferred to another and immediately redeposited with the tradesman, the benefits of transfer by assignment rather than transfer by delivery become apparent. Selgin points out that transfer by booking entry was first practiced by English goldsmiths during the 17th century.

It is important to distinguish that people have preferred to trade not with actual metal coins but instead with notes, which would state the actual value of metal stored at the blacksmith or bank. These notes would be popular only if the issuing party is respected and trusted by the common public, and the notes by themselves are *secure*. Related to the use and issuance of notes as money, Von Mises (1953) states that "When an indirect exchange is transacted with the aid of money, it is not necessary for the money to change hands physically; a perfectly secure claim to an equivalent sum, payable on demand, may be transferred instead of the actual coins."

Davies (1994) states that the first banknotes were issued in 1660 in England by goldsmiths:

> Because goldsmiths' notes are accepted as evidence of ability to pay they are a convenient alternative to handling coins or bullion. The realization by goldsmiths that borrowers would find them just as convenient as depositors marks the start of the use of banknotes in England.

In 1698, just 38 years after the introduction of banknotes in the economy, Davenant estimates that the total value of coins in circulation is less than that of tallies, bills, banknotes etc. (Davies, 1994). This analysis is a proof of the popularity that notes have gained. Due to this popularity, the power of money creation is passing from the King, who is in charge of the mint, to the London money market and provincial banks. Political and constitutional power is also affected by this transfer of financial power. The financial power of issuing money is referred to as the power of seignorage. The ancient concept of seignorage as a government's profit from issuing coinage that costs less to mint than its face value is essentially the same with paper currencies: abstracting from the minor cost of printing paper money, seignorage is simply the increase in the volume of domestic currency less any loss due to inflation. This incident is the first return on a denationalized form of money after the introduction of coins.

It is important at this point to distinguish the advantages that note claims have with respect to metal coins. The claims are as fungible and interchangeable as metal coins; they are definitely more divisible with respect to coins and more portable.

Paper money found an important ally in the face of Adam Smith who in his Wealth of Nations in 1776 draws attention to the benefits of paper money in stimulating business both in Scotland and in the American colonies (Smith, 1776). The paper money therefore was widely accepted and supported by most economics scholars.

The evolution of money with the issuance and spreading use of banknotes continued but with an important change. As banknotes and other papers were claims of money and not a monetary commodity by themselves and the popularity in use of those claims was continuously increasing due to their convenience, these claims were the

subject of evolution and not the money by itself. Lockard (1997) pinpoints this change of focus in the evolution of money as:

> From this point forward, monetary evolution is centered on innovations regarding claims to the monetary commodity, rather than changes in the monetary commodity itself. In a sense, the medium of exchange becomes separate from the unit of account (and medium of redemption).

Although paper money and banknotes obviously have no intrinsic value, their acceptability originally depended on their being backed or redeemed by some commodity, normally precious metals, what was known as the Gold Standard. Currently none national currencies does have a link with the amount of gold that it is being held. Therefore these currencies are referred to as fiat currencies or fiduciary money, money that the government declares to be legal tender although it cannot be converted into standard specie.

The initiation of checks and credit payments followed paper money. However, both with respect to technological and payment innovation, the next significant development in the money evolution ladder was the invention of credit cards. Credit cards were developed to serve two main functions; to be a convenient means of paying for goods and services and at the same time to be a convenient way for consumers to obtain unsecured credit. Lockard (1997) summarizes the initiation of credit cards as:

> The risk of default is low when lending to known individuals of integrity with high incomes or established wealth. As travel became more frequent, an exploitable opportunity arose in being able to identify these creditworthy individuals to merchants to whom they were not personally known. In the 1950s, the travel and entertainment (T&E) card was developed to exploit this opportunity.

Individual stores and gasoline companies issued cards that could be used to charge merchandise at their own businesses in the early decades of the 20th century. The independent credit card, usable at many establishments, began with Diner's Club in

1950. Banks began issuing their own cards later in the 1950s, but the geographical fragmentation of the banking industry limited the scope of their networks. In order to provide nationwide, then worldwide markets for their credit cards, banks joined together in the 1960s to form two main cooperative ventures to administer processing networks. These evolved into today's Visa and MasterCard organizations (Web Ref1).

Lockard (1997) identifies information cost constraint on exchange as an important reason of the credit card development:

> The market specialists can easily determine the quality of goods in which they specialize, but they cannot so easily evaluate the quality of the credit-worthiness of their potential customer, if he is unknown to them. Intermediaries (card issuing banks) can target themselves to the elimination of those information costs, with the potential to charge either the customer, merchant, or both for the service. Banking institutions saw the benefits of selective extension of credit to facilitate exchange, and the now familiar four-party (purchaser, purchaser bank, merchant, merchant bank) bank credit card emerged. This process was facilitated by relatively rapid growth in real income in conjunction with technological advances in the areas of data processing and electronic communications, reducing the costs of maintaining accessible documentation on creditworthiness and of billing and collection.

It can be seen in the historical evolution of money described; that forms of money evolve in order to minimize the costs associated with them. As Lockard (1997) states, whenever there are costs associated with the use of an exchange medium, there is an opportunity for further development. It is important to distinguish that this development will continue until no costs are any longer associated with the use of an exchange medium or a minimum level is attained.

The Table 1, adopted from Kalakota and Whinston (1996) provides a very informative summary of the innovations in money and payment systems.

Table 1 Timeline of innovations in payment systems

Period	Innovation
700 BC	Earliest coins produced in western Turkey to pay mercenaries or taxes.
1400	First bank opens, in Italy and Catalonia, honoring cheques against cash reserves.
1694	The Bank of England opens, creating deposits on the principle that not all deposit receipts will be presented for redemption simultaneously. The bank monopolizes the issuing of bank notes.
1865	A sample of payments into British banks shows that 97 percent are made by cheque.
1887	The phrase credit card is coined in Looking Backward, a novel by Edward Bellamy.
1880-1914	Heyday of the gold standard as major currencies are pegged to gold at fixed rates.
1945	Bretton Woods agreement links currencies to gold via their fixed parities with the U.S. dollar.
1947	Flatbush National Bank issues first general-purpose credit card, for use in select New York shops.
1950	Diner's Club Charge Card introduced.
Mid 1950's	The development of magnetic ink character recognition (MICR), facilitating more timely processing of cheques, sealed the cheques standing as preferred noncash payment option.
1958	BankAmerica, in Fresco, California, executes the first mass mailing of credit cards.
1967	Westminster Bank installs first automated teller machine at Victoria, London, branch.
1970	The New York Clearing House launches CHIPS - Clearing House Interbank Payment System which provides U.S. dollar funds-transfer and transaction settlements on-line and in real-time.
Late 1970's	Chemical Bank launches its Pronto system providing 3000 computer terminals to customers homes linked to its central computers by telephone. It offers a range of facilities: balance inquires, money, transfers between Chemical Bank accounts, and bill payments to selected local stores. The stumbling block for first-generation home-banking systems in general was who is to pay for the terminals at home.
1985	Electronic data interchange (EDI) extensively used in bank-to-bank payment systems.
1994	Digital cash trails by Digi-Cash of Holland conducted on-line.
1995	Mondex electronic currency trials begin in Swindon, England.
Source (Kalakota, Whinston, 1996)	

3.5. Pure Money

The evolution of money that has started with barter, will potentially continue until a medium of exchange is invented that will serve as Pure Money. At this point of the research, there is a need to define an exchange medium that can be used as money, but without any costs associated with it. Therefore we define Pure or Perfect Money as the exchange medium without any transaction costs associated with respect to the properties of security, user-friendliness, portability, divisibility, anonymity, durability, acceptability, recognizability, latency, reliability and repudiation, in other words an exchange medium which is perfectly secure, perfectly user-friendly, perfectly portable, perfectly divisible, perfectly untraceable (anonymous) and perfectly traceable when necessary, infinitely durable, perfectly acceptable, perfectly recognizable, with no latency, perfectly reliable and providing perfect nonrepudiation.

In economics theory, the concept of perfection is widely used as a reference point which then allows imperfections and costs associated with real life objects to be defined. Economists prefer to derive the imperfections of financial markets and markets in general, by describing firstly the Perfect Market concept. Perfect Markets are the markets where:

- Perfect competition (infinitely many buyers and sellers) exists
- There are no transaction costs (frictionless transactions)
- Perfect information (information which is costless, immediate, complete and available to everybody) exists
- The products are perfectly divisible, homogeneous and fungible.

Under these conditions, money is unnecessary. However, in the presence of some imperfections, trade would be greatly aided by the introduction of money and if it

was Pure Money, a significant portion of the costs due to transaction costs and some of the costs due to information problems could be eliminated. Further information on Perfect markets can be obtained from sources like Fabozzi, Modigliani, Ferri, (1998), and Madura, (2003).

3.5.1. A Sample Model for Pure Money

It is important to describe in this part of the study a possible sample model for Pure Money. The proposed sample model will be developed for a simplified imaginary economy, not for a real scale economy. This is due to the difficulties of proposing a model as stated by Day (1996) "immense number of facts and relationships that would have to be described; the impossibility (to describe fully the important relationships in a complicated monetary and economic system) might derive from our inadequate knowledge of these things." Due to these difficulties, Day (1996) concludes that:

"A way in which these difficulties can be avoided is to imagine an economic and monetary system that is much simpler than the real one in which we live, but which approximates to it as nearly as possible."

Let us visualize a small town with very few citizens and assume that no cash and no credit cards exist any longer in this town. Instead all payments are made using pure money. This payment scheme will be called the Pure System. People store their money on electronic purses, which can hold an infinite amount of money with perfect security, (no counterfeiting or duplication of this money is possible). Money can be stored and can be transferred with no cost to any medium like electronic purses, computers, bank accounts, etc. therefore being perfectly portable. The amount of money stored in these electronic purses is perfectly divisible; the smallest amount possible can be transferred from one electronic purse to another. At the same time, the complete amount stored in

the electronic purse can be transferred as a lump sum. All electronic purses accept money from any electronic purse. No connection to a central authority is necessary to authenticate the money transfer from one electronic purse to another, contrary to the case of credit or debit cards. Therefore, pure money circulates freely without any control within the market between all transacting parties, but securely and safely, so that no one can doubt or question the genuineness of the pure money. Figure 2 depicts the circulation of pure money between individuals and institutions. It ought to be distinguished that institutions in the Pure System are no different than individuals.

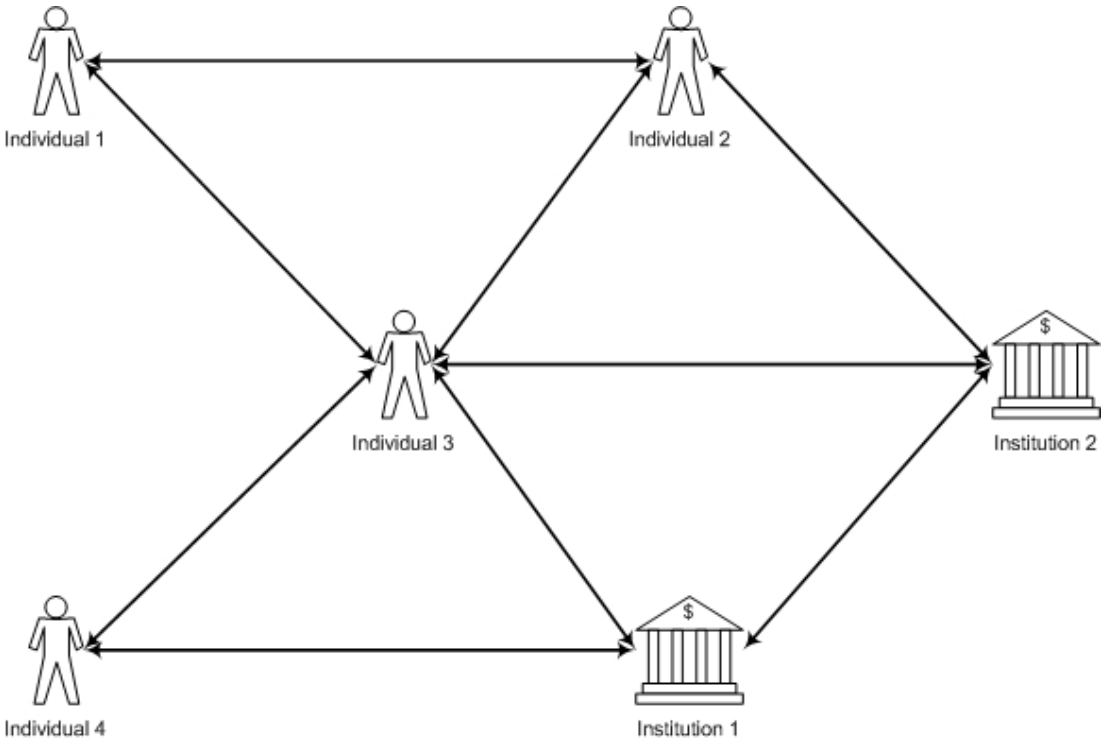

Figure 2 The Pure Money system

CHAPTER 4

ELECTRONIC MONEY

"It was necessary to reconceive, in the most fundamental sense, the nature of bank, money, and credit card; even beyond that to the essential elements of each and how they might change in a microelectronics environment. Several conclusions emerged: First: Money had become nothing but guaranteed, alphanumeric data recorded in valueless paper and metal. It would eventually become guaranteed dots in the form of arranged electronics and photons which would move around the world at the speed of light.

Dee Hock, former CEO of Visa
(Evans, Schmalensee, 1999)

4.1. Introduction

This research, puts forward the understanding that money is evolving continuously in shape, and form, in order to better meet and fit the needs of the evolving economy, and as it changes, it approaches continuously the Pure Money. Pure Money, is probably utopic, possibly an unreachable peak in economic development and evolution. However, as we can analyze and recognize our current position in the "Money Evolution Ladder", and as we know our destination point in this journey, which is Pure Money, it may be possible to identify the next possible steps on this ladder.

Timelines are important tools that may be used to predict and forecast the next step on the evolution process. The timeline of money evolution therefore can be used to try to foresee the next step that money will follow. If we consider the evolution of money previously described, we can draw a simple timeline. At the very right end of this timeline, Pure Money is placed. At the very left of this timeline, the first form of exchange, Barter is placed. The timeline between Barter and Today, is almost known, and important points in this historical evolution are identified. However, the area between Today and Pure Money is intentionally left blank. The values that each sample payment type scores in the properties scale, are own evaluations and are subjective.

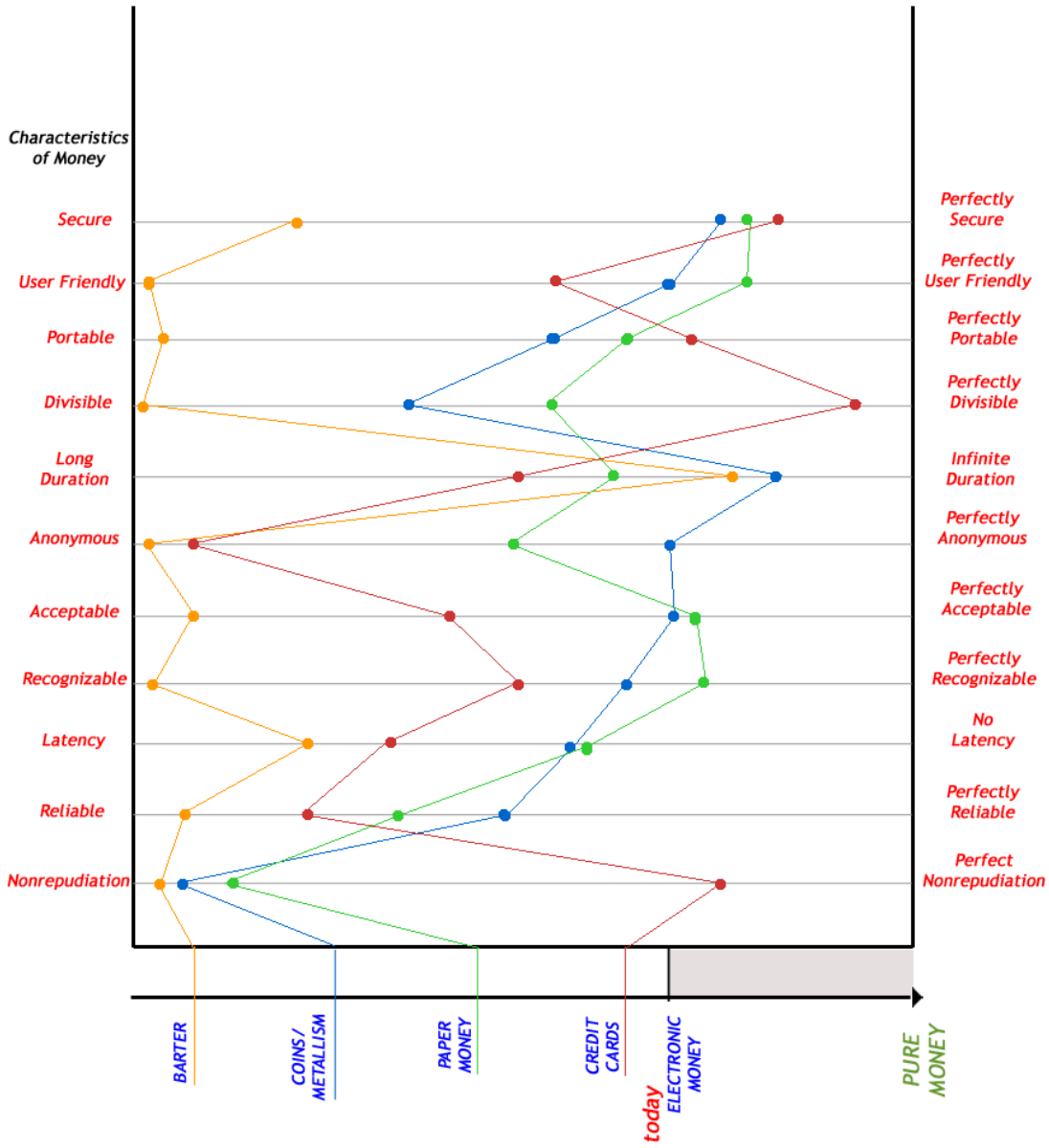

Figure 3 Evolution timeline of money

Between Today and the day that people will possibly develop Pure Money, lies an unknown area. It is possible that people and economies will invent, develop and employ different media, methodologies and technologies to further reach a state that will resemble Pure Money in one or more on the attributes of money listed. We argue

that it is possible, if not necessary, that electronic money shall be one of those steps to be taken to reach from Today towards Pure Money.

Electronic money can be accepted as a necessary step towards Pure Money, it can be argued that some or all of the attributes of electronic money, should be closer to the attributes of Pure Money than the attributes of any other money form currently existing and in use in the economies. However, it is debatable whether all attributes of electronic money should be or can be closer to Pure Money. For example, if a form of electronic money to be developed is perfectly secure, an attribute we assigned to Pure Money during this research, but with respect to other monies currently coexisting, this form of electronic money lacks in some other properties, can we argue that this form of electronic money is a step towards Pure Money? We argue that to become the next step, electronic money should be closer to Pure Money in at least one attribute. One of our tasks should be to determine which attributes electronic money will focus on and surpass the present day. At the same time we can identify attributes which may be especially problematic.

4.2. Existing Definitions of Electronic Money

Previously conducted researches are far from providing a single answer to the question "what is electronic money?" As Capie, Gormez and Stojanovic (2001) state:

> There is no generally agreed definition of e-money in the literature. In recent discussions, it has been defined in different ways and gone under different names such as, smart money, digital money, electronic money, cyber-money, electronic currency, electronic purse, virtual money, internet money and electronic script. Money and cash are sometimes assumed to be the same and some writers call e-money smart cash, digital cash, virtual cash, cyber cash or electronic cash. Additionally, there is a general confusion about money and payment instruments such as debit and credit cards. In some analyses, anything from cheques to point of sales electronic fund transfers have been included in the definition of e-money, and in

> other cases it is strictly limited to the electronic representation of purchasing power.

In this quote many important points are described. First of all, it is obvious that there is no common agreed upon name for electronic money: for example digital money and electronic currency may point to identical payment instruments, although the names used obviously imply different instruments. Therefore it can be concluded that different names point to the same payment instrument which in this study for convenience was and will be named as Electronic Money. This confusion between different names is described also by Capie, Gormez and Stojanovic (2001).

One more important point of discussion pointed in the above quote is the difference between electronic payment instruments and payment methods. In this research we will not consider credit and debit cards to be electronic money. Credit and debit cards will be treated as electronic payment methods and not electronic money. As Camp, Sirbu and Tygar (1995) define, money can be defined as token or as notational. Token money is the physical money used, banknotes, paper currency and coins, whereas notational money is notations in the ledgers of depository institutions such as banks. Debit and credit cards are used not to transfer or pay with token money but with notational money, thus they are electronic transfers of notational currency, also known as EFTPOS (Electronic Fund Transfer at Point of Sale). Physical transfers of notational currency are the checks. (Camp, et al., 1995) However, electronic money should be the electronic transfer of token money or currency. This is an important distinction between credit cards and electronic money.

The work of Capie, Gormez and Stojanovic (2001) continues with a list of different definitions for electronic money, while they conclude on the best definition within the listed definitions.

Goldfinger (2001) points that these vast definitions for electronic money are due to the fact that academic, business and regulatory experts appear deeply divided over the question. However, he also tries to derive the best definition for electronic money within a list of previously given definitions and concludes with a definition of his own.

For the sake of traceability in this study it is important that we should conduct a similar list of definitions for electronic money, before we conclude to the currently best definition. Goldfinger (2001) starts the list of definitions of electronic money with the definition of Megabyte money by Kurtzman:

> Some analysts define electronic money as any form of money that is stored and moved over computer systems and data networks. This implies that the bulk of scriptural money is now by and large electronic. One example here is Kurtzmann's "megabyte money", which are nothing else than large-amount of cross-border interbank payments.

The definition of Kurtzman fails to distinguish and identify explicitly the phenomenon called electronic money, circulating between individuals in the Internet, used to transact and pay for very small amounts in the daily life. These very small amounts will be described in detail in section 4.3.6.

Ely (1996) defines electronic money as:

> E-money, which is the money balance recorded electronically on a "stored-value" card; also is credit, for the balance on the card is a liability of its issuer. As with a depository institution, the card issuer uses funds paid by the card holder to acquire assets. The legal evidence of the issuer's liability to the cardholder consists of electronic bits and bytes recorded on the card. Similarly, the legal evidence of a government's liability to a currency holder is the piece of currency itself. For deposits, though, liability is evidenced by the records of the depository institution. For a long time, that liability was recorded on paper ledger cards; today, it almost always is accounted for in a computer.

However, Capie, Gormez and Stojanovic (2001) comment on this definition as, "The author argued that specie is the only form of money that is not a form of credit

and concluded that fundamentally, e-money is no different from any other form of money in use today." In this study we have previously accepted that electronic money as the next step towards Pure Money should be different than the currently existing monies and moreover resemble more to Pure Money than any other model of money currently co-existing.

Singh (1999) very broadly speaking defines electronic money as:

> Electronic money includes all non-cash and non-paper payments instruments such as plastic cards and direct transfer and all money transactions via electronic channels such as ATMs, EFTPOS, the telephone, fax and the Internet. However, when policymakers talk of electronic money in the context of electronic commerce, it is the plastic card over the Internet which is at the centre of debate.

However, her definition accepts methods of payment and payment instruments that are widely used today and merely are money by themselves, they could be accepted more as money transfer methods. Her definition resembles the definition of Ely (1996), and fails to define the newly emerging forms of electronic money.

Duisenberg (2003) defines electronic money as that which consists of values that are stored in digital form on an information storage device. Smant (2002) states that digital money is a very special variant of an electronic wallet and network money, where money value is not stored as a balance (receipts less payments), but as an electronic representation of single digital coins/notes of predetermined value units.

On the other hand White (1996) defines the emerging forms of electronic money as:

> A second form of digital money--an alternative to the deposit-transfer method of payment--has recently appeared on the horizon. Developments in cryptography are said to be bringing us what we can call "digital currency". The currency balance information, an encoded string of digits, can be carried on a "smart" plastic card with an implanted microchip, or kept on a computer hard drive. Like a traveler's check, a digital currency balance is a floating claim on a

> bank or other financial institution that is not linked to any particular account. One cardholder can make a payment to another without bank involvement, by placing both cards in a "digital wallet" that writes down the card balance on one card and writes up the balance on the other by the same amount. Desktop electronic currency transfers can similarly be made by electronic mail. A card's digital currency balance can be "topped up" by placing it in an ATM (a PC's balance by getting on-line with the bank) and downloading funds from one's account. Like paper currency and coins (which we can conveniently call "analog currency"), digital currency balances are circulating bearer media. If personal information is omitted from the balance transfer information (unlike current practice in debit- and credit-card transactions), the bearer can remain anonymous. An issuing bank need only know the total of its outstanding currency liabilities, not who holds them at any moment.

Furthermore, Capie, Gormez and Stojanovic (2001) list a vast number of definitions as:

> Lynch and Lundquist (1996) viewed digital money as an electronic replacement for cash, which is storable, transferable, and unforgeable. For Boeschoten and Hebbink (1996) e-money included multi-purpose prepaid cards as well as other electronic transactions used in internet-payments (e-cash) and EFTPOS payments and argued that such as prepaid card payments, electronic transfers replace cash and consequently currency demand. A similar line was adopted by Solomon (1997) who concluded that developments in the electronic delivery channels (through EFT) might lead to fast money flows and eventually virtual money.

Capie, Gormez and Stojanovic (2001) conclude on the definitions listed and follow the definition by the European Central Bank which is:

> …as an electronic store of monetary value on a technical device that may be widely used for making payments to undertakings other than the issuer without necessarily involving bank accounts in the transaction, but acting as a prepaid bearer instrument.

They (Capie, et al., 2001) break up this definition and argue that it covers:

> E-money is a prepaid bearer instrument excluding all kind of electronic payment instruments such as credit and debit cards and EFT payments. Obviously, the word 'prepaid' should be treated cautiously as e-money may also be earned directly or be owned as a credit.

> It covers payments to undertakings other than the issuer which is a required aspect to differentiate e-money products from single purpose prepaid cards such as telephone cards.
> Transactions do not necessarily require a bank account or any other financial service providers' authorisation. This excludes all kind of account-based (debit or credit) payment instruments.
> E-money stores monetary value on a technical device with a capacity to be used widely for making payments. It does not specify the type of technical device, which may be accepted as a superior definition of e-money as it is in an emerging stage and the technical potential of proposed devices are not fully clear yet..

However, they (Capie, et al., 2001) conclude that this definition is incomplete and does not cover all electronic money forms and proposals that circulate:

> Technological developments relating to e-money products need to be monitored carefully, and they may influence the above definition if an unexpected innovation changes some basic features of e-money. Another caution is that as the definition stands it seems to cover just representative issue of e-money. It limits the definition to prepaid instruments, which means that e-money may be used only as a medium of exchange that has the backing of an existing monetary system. In order to make a purchase, for example, first electronic value should be paid for so that it can be owned and transferred to complete the transaction. As a result, e-money for euro-zone becomes e-euro and e-money for the US becomes e-dollar.
> Unfortunately, this definition does not cover all types of e-money proposals that currently exist. To give just one example, Beenz can only be earned on the Internet and it can not be paid for by the end-users. Consequently, the definition does not cover the electronic issue of independent e-money. It is possible for monetary value to be held by an electronic device that does not represent any national currency. In this case, any kind of backing can be used. Such developments are already available in different parts of the world through LETS but not limited to locality only. At least one company at the moment has been trying to circulate gold digitally as a medium of exchange. To conclude, it is better to be cautious on the definition of e-money as prepaid instruments as it is not only limited to representation of a given national money. It may be an independent part of a competitive monetary arrangement.

Goldfinger (2001) comments on the same definition by the ECB and states that:

> In the directive proposal, the EC defines e-money as a multi-purpose instrument. In other words, e-money is construed as a payment instrument that can be used to settle more than one kind of transaction, while the traditional definition of money stresses its

> universal dimension. The new definition leads to a broader and more ambiguous definition of the issuer of electronic money. A non-financial institution, a retailer or an ISP (Internet Service Provider) that issues an electronic instrument, which can be used in several types of transactions (buying physical goods with selected merchants, buying intangible goods such as information, participating in an auction, etc.) can thus be considered as an electronic money issuer. The proposed directive explicitly acknowledges the possibility of non-banking e-money issuers and defines a specific regulatory and prudential framework for them.
>
> The proposed directive is still under discussion. It is highly controversial and afflicted by the middle-of-the-road syndrome. For e-commerce enthusiasts, it may create an additional burden and deter innovation. For regulators such as Central Banks, it may be too light. Thus the ECB would prefer that the issuance of electronic money be limited to credit institutions and that the definition of credit institution be enlarged to include all issuers of electronic money. Under this approach, electronic money is assimilated to scriptural money on an electronic support and as such does not require a fundamental overhaul of the regulatory and institutional framework of monetary systems. According to many central banks within the European Union such as Banque de France, e-purse or e-cash are prepaid instrument that resemble in substance traveller checks, except that the latter are not divisible. No new status or regulations were required for traveller checks, and therefore no new status is necessary for e-money.
>
> As for loyalty schemes, their use is restricted and they are not broadly redeemable (except with the designated set of merchants). Therefore, they cannot be considered as money.

As the purpose of this research is not to define what electronic money is, but to propose an electronic money model, the definition of ECB on electronic money will be considered as the most relevant and acceptable definition up to date, but the questions and points proposed by Capie, Gormez, and Stojanovic (2001), and Goldfinger (2001) will be accepted as guidelines for a future more complete definition on electronic money. The electronic money model will be considered and developed with accordance to the ECB definition.

4.3. Existing Electronic Money Schemes and Techniques

The existing electronic money schemes and techniques are described briefly and analyzed in order to distinguish which inherit attributes of money should be emphasized while developing an electronic money model. Electronic money, in order to be accepted as money from every transacting party, should function in accordance to the functions of ordinary money and moreover should contain all the attributes of ordinary money previously described in Sections 2.1.1 and 2.1.2. Therefore, electronic money should function as a standard unit of account, common measure of value, medium of exchange, means of payment, standard and means for deferred payments and finally store of value. Furthermore, electronic money should be with respect to the attributes of ordinary money secure, user friendly, portable, divisible, anonymous, durable, widely acceptable, recognizable, with acceptable amount of latency related to the clearing and settlement, reliable, and should provide an acceptable degree of nonrepudiation.

4.3.1. Off-Line vs. On-Line Capability

Electronic money due to its unique nature with respect to other forms of money contains the additional attribute of being off-line and on-line. Off-line money can be defined as the money that can be authenticated to be genuine and not-counterfeited without the authentication of a central authority such as a bank or issuing company. On-line money on the other hand can be defined as the money that cannot be authenticated for being genuine without the confirmation of a central authority. The ordinary cash that we use today is perfectly off-line; the merchant who accepts the banknote for payment can check whether it is genuine or fake without communicating with a central authority. However, on the other hand the payments conducted with credit or debit

cards are perfectly on-line, the issuing bank or credit company needs to authenticate both the card and the credit or amount of money to be transferred. Different proposed electronic money schemes are employing either an on-line or off-line approach. Definitely the approach developed in this study is a consequence of the technology, hardware and software limitations. With respect to the approach employed, the technology, hardware and software media to be employed are decided upon.

With respect to the variable of being on-line or off-line, and considering that there are only two transacting parties, a payer and a payee, and that the authentication authority is used by the on-line party in each case, currently employed payment methods can be grouped into four categories, as shown in Table 2:

Table 2 Online and offline cases

Status of Payer	Status of Payee	Example
Off-line	Off-line	Cash payments
Off-line	On-line	Credit card/debit card payments
On-line	Off-line	Electronic money transfer by the payer and the submission of the receipt to the off-line payee.
On-line	On-line	Payments over the Internet with the immediate generation of electronic coins by the payer before the transaction, communicating with the central issuing company

As can be seen from Table 2, only the first case where both the payer and the payee are in off-line status is a truly off-line situation. The following three cases are all related to an on-line case, as the payer or the payee is in an on-line status.

On-line money can be identified as a tripolar system which can be described as a closed circulation system (Pifaretti, 1998), where the payer, the payee and the issuer or

authenticator constitute the three poles. However, everyday payments conducted with cash are not at all closed systems, as banknotes circulate almost freely within the economy and are bipolar systems, where the payer and the payee constitute the two poles, and they are both off-line. An on-line electronic money scheme therefore would only substitute payments with credit or debit cards, merchants or transacting parties with no on-line capability would therefore be left out. With respect to the fact that on-line electronic money schemes are closed circulation systems, it can be argued that with respect to the limitations that such a system provides, on-line electronic money is less efficient and less desirable with respect to off-line electronic money. However, no electronic money scheme can be disregarded due to the fact that it is not off-line capable, but it is a necessary approach to distinguish electronic money schemes with respect to the authentication process they are employing.

This research adds that electronic money schemes should be defined in an **on-line/off-line scale**. In more detail, each electronic money proposal should be classified with respect to the amount of off-line capability it provides to the transacting parties, considering that the off-line capability is a more desired attribute with respect to on-line capability. However, it must be noted that a perfectly off-line system, can be simultaneously a perfectly on-line system, but a perfectly on-line system may not work in an off-line environment. For example, consider an electronic money system that authenticates whether an electronic coin is genuine or not without connecting to a central authentication centre. The same system would work whether the party that is accepting the electronic coins is online and connected to a central authenticating party.

4.3.2. Traceability vs. Anonymity

A further classifier of electronic money is the attribute of **traceability**, an attribute inherited from ordinary money. As Bootle (2000) states, people have a substantial demand for a medium in which they can make *anonymous* payments – i.e. ordinary currency, where anonymity is clearly important for people pursuing criminal activities, but it is also important when trying to evade paying tax, gambling, or spending money on some immoral, or irresponsible purpose, or simply wanting to keep activities, and how much is paid for them, private, away from prying eyes, not only at the bank or the authorities, but in your own family.

However, the property of being traceable or not is a more significant attribute in electronic money due to the advanced tracing capabilities that electronic media provide. It is debatable whether **anonymity** is better than traceability, the trade-off within the two extremes is important. As Gemmell (1997) argues, for electronic money to be widely acceptable and therefore successful, electronic money systems need to obtain a balance between anonymity and traceability.

In either case, anonymous or traceable, problems do exist. In completely anonymous payment systems problems such as money laundering and counterfeiting would be untraceable, threats that would not allow governments and financial institutions to employ a perfectly anonymous electronic money scheme, until a perfect security system is designed. On the other hand, a traceable system would not provide the necessary protection on the privacy of users, and would keep all off the record (underground) economy out of the system, something that could eventually result in the collapse of the system. The perfect combination would be a system that would allow the

central authorities, such as governments and financial institutions to prevent and control crime or suspicious transactions while providing protection for the privacy of users (Gemmell, 1997).

The property of anonymity can be further analyzed by examining the amount of information available for each party participating in the transaction. In other words, the two parties transacting with electronic money may have complete information on each other, however, a third party observing the transaction may not be able to retrieve any information on these parties. Camp, Sirbu and Tygar (1995) identify that the amount of information available to different parties should be classified with respect to the type of information and the party receiving that information. Table 3,

Table 4 and Table 5 (Camp, et al., 1995) are generated based on this assumption, each analyzing the amount of information made available to parties in classical payment schemes; cash, checks and credit and debit card systems.

Table 3 Information available to the parties in a cash transaction

Information / Party	Seller	Buyer	Date	Amount	Item
Seller	Full	Partial	Full	Full	Full
Buyer	Full	Full	Full	Full	Full
Law Enf.	None	None	None	None	None
Bank	None	None	None	None	None

Physical Observer	Full	Partial	Full	Full	Full

Table 4 Information available to the parties in a check transaction

Information / Party	Seller	Buyer	Date	Amount	Item
Seller	Full	**Full**	Full	Full	Full
Buyer	Full	Full	Full	Full	Full
Law Enf.	**Full**	**Full**	**Full**	**Full**	None
Bank	**Full**	**Full**	**Full**	**Full**	None
Physical Observer	Full	**Full**	Full	Full	Full

Table 5 Information available to the parties in a POS transaction

Information / Party	Seller	Buyer	Date	Amount	Item
Seller	Full	Full	Full	Full	Full
Buyer	Full	Full	Full	Full	Full
Law Enf.	Full	Full	Full	Full	**Full**
Bank	Full	Full	Full	Full	None
Physical Observer	Full	**Partial**	Full	Full	Full
Electronic Observer	**Partial**	**Partial**	**Full**	**None**	**None**

It is evident that any payment scheme or payment system should be categorized based on Table 3,

Table 4, and Table 5, with respect to the amount of anonymity available and provided by that system. It can be seen that even one of the most anonymous payment methods invented, cash, is not fully anonymous with respect to the information that is made available to the transacting parties. However, the most important anonymity metric while classifying a payment scheme which is not mentioned in the above tables should definitely be whether the payment system allows the identification of individuals who use counterfeited money.

Therefore, another important classifier after the off-line capability is the **anonymity or traceability** of electronic money. In this study it is argued that electronic money schemes proposed should be compared with respect to the amount of anonymity they do provide to the individual users, but also the traceability of any criminal activities or attacks that the proposed scheme may suffer.

4.3.3. ACID Properties

Transactions to be conducted with electronic money should be considered to be computerized transaction systems. In describing computerized transaction systems several properties are applicable with respect to the characteristics of the computerized transaction, the property of **Atomicity**, the property of **Consistency**, the property of **Isolation** and the property of **Durability** (which differs from the durability property of money), and these properties are referred to as the ACID properties (Gray, Reuter, 1993). Each of the ACID properties is described by Camp, Sirbu and Tygar (1995) as:

- **Atomicity:** Either a transaction occurs completely or it does not occur at all. For example, consider what happens when a person transfers funds from a savings account to a checking account. Both the checking account is credited and the savings account is debited or neither account balance changes. The atomicity property requires that a transaction is executed to completion.
- **Consistency:** All relevant parties must agree on critical facts of the exchange. Moreover, the transaction should preserve consistency, the execution of the transaction should take the related parties from one consistent state to the other consistent state.
- **Isolation:** Transactions should not interfere with each other, and the result of a set of overlapping transactions must be equivalent to some sequence of those transactions executed in non-concurrent serial order, in other words a transaction should appear as though it is being executed in isolation from other transactions.
- **Durability:** The changes applied to a stored data by a committed transaction must persist, these changes must not be lost because of any failure.

4.3.4. Security on Electronic Payments

At this point of the study, it would be appropriate to briefly point the importance of security in electronic payments. Although all monies and payment types need to be secure at great extent, electronic payments', due to their nature, are more prone to attacks. Therefore, even the possibility that the security of the electronic payment system may suffer attacks and not be able to overcome them is possible to result in the collapse of the whole system. Thus, the importance of the security of

electronic payment systems steps forward with respect to the importance of the security in other monies.

4.3.5. Classification of Electronic Payments

It would be appropriate to break down the existing electronic payment types and schemes with respect to the value that they involve. Such a study has been conducted by Birch (1997) in a very useful analysis. He has broken down the online payments sector into four subsections as macro-payments, mini-payments, micropayments and nano-payments (Birch, 1997). Birch (1997) has defined the amounts related to each payment subsection as: Macro-payments are those payments in excess of £10,000; mini-payments, from £10 to £10,000; micro-payments, which are payments from 1p to £10 and nano-payments which, are payments that can not be made using any existing payment means. The payment subsections and the corresponding amounts are shown in Table 6.

Table 6 The classification of electronic payments

Payment Subsection	Corresponding Amount
Macro-payments	>£10,000
Mini-payments	£10-£10,000
Micro-payments	1p-£10
Nano-payments	<1p

The **micro-payments** will be discussed further in detail in CHAPTER 5 because the model developed by this study focuses on this category of payments.

4.3.6. Classification of Electronic Payment Types and Schemes

Different electronic payment types and schemes exist and have been implemented for each of these specified payment subsections. The most detailed survey on the field has been conducted by Lipton and Ostrovsky (1998), and although others exist, Micali and Rivest (2002) have concluded that this paper is an excellent survey. Lipton and Ostrovsky (1998) classify the most well-known existing payment types and schemes under these 5 major headings, as shown in Table 7:

Table 7 Existing payment types and schemes

Online Protocols	Hardware-Based Schemes	Subscription Schemes	Coupon-Based Schemes	Probabilistic Schemes
Credit Card Setting	Mondex (Web Ref2)	Chrg-http Protocol (Tang, Low, 1996)	Millicent (Glassman, et al., 1995)	Agora Protocol (Gabber, Silberschatz, 1996)
SET (Web Ref1)	Small-Value-Payment (Stern, Vaudenay, 1997)		PayWord (Rivest, Shamir, 1996)	Probabilistic Polling (Jarecki, Adlyzko, 1997)
NetBill (Cox, et al., 1995)	MicroMint (Rivest, Shamir, 1996)		NetCard (Anderson, et al., 1996)	MicroCash (Rivest, 1997)
DigiCash (Chaum, 1993)			PayTree (Jutla, Yung, 1996)	Transactions Using Bets (Wheeler, 1996)
NetCash (Medvinsky, Neuman, 1994)	Yacobi's e-war (Yacobi, 1997)		Micro-iKP (Hauser, et al., 1996)	
NetCheque (Neuman, Medvinsky, 1995b)				

Further details and information regarding each payment type and scheme can be obtained from the respective references. The most important aspect of Table 7 and the reason that is included in this study is the fact that Lipton and Ostrovsky (1998) after

surveying in detail the existing electronic money payment types and schemes have classified these under 5 major headings: the online protocols, hardware-based schemes, subscription schemes, coupon-based schemes and probabilistic schemes. This classification shall be a major guideline in the electronic money model to be proposed in CHAPTER 5.

Further electronic money schemes currently existing but are not enlisted on Table 7 are the First Virtual (Web Ref4), and Wenbo Mao's Simple Payment Scheme (Mao, 96).

CHAPTER 5

THE MODEL

"Progress, sometimes called evolution, is a natural part of life. Perhaps it is the trial-and-error of life. To play the game, we have to allow ourselves to be moved by our curiosity to try new things, knowing that our next trial may result in error."

Jürgen Dethloff, 1996
(Rankl, Effing, 2000)

5.1. Introduction

In this part of this study, the proposed model is described. As stated previously in CHAPTER 4, this study proposes a payment scheme appropriate for both micro-payments and nano-payments, operating on off-line basis, designed both for real life and world-wide web applications. The model tries to avoid many shortcomings of previous similar schemes. In particular, at the very heart of this constructed model lie two main ideas: the Small Value Payments (SVP) scheme of Stern and Vaudenay (1997) and the tamper resistant smart cards (Dyad) proposed by Tygar and Yee (1993).

5.2. Design Principles and Parameters

5.2.1. The Participants

In the simple electronic money case, the system consists of the Issuing Authority (**IA**), a payer (**P*r***) and a payee (**P*e***). The IA, issues the electronic monies, or electronic tokens (*t*) in this model, which are distributed to all the parties requesting electronic money. The P*r* carries the *t*'s in his electronic wallet (eW). The P*r* obtains issued *t*'s and while transacting with the P*e*, pays with these *t*'s, the payment occurs by the physical transfer of *t*'s from the eW of the P*r* to the eW of the P*e*. While each *t* is token money and not notational money, the clearing and settlement takes place immediately at the moment of transaction. Moreover, three of the most important characteristics of cash payments do exist in the described system: the P*r* and the P*e* both recognize the payment, neither party can deny that specified amount of electronic money was transferred from the P*r* to the P*e*, and the P*e* can use the same *t*'s received by the P*r* to pay a third person, without depositing or renewing the *t*'s (reusability of coins), as shown in Figure 4.

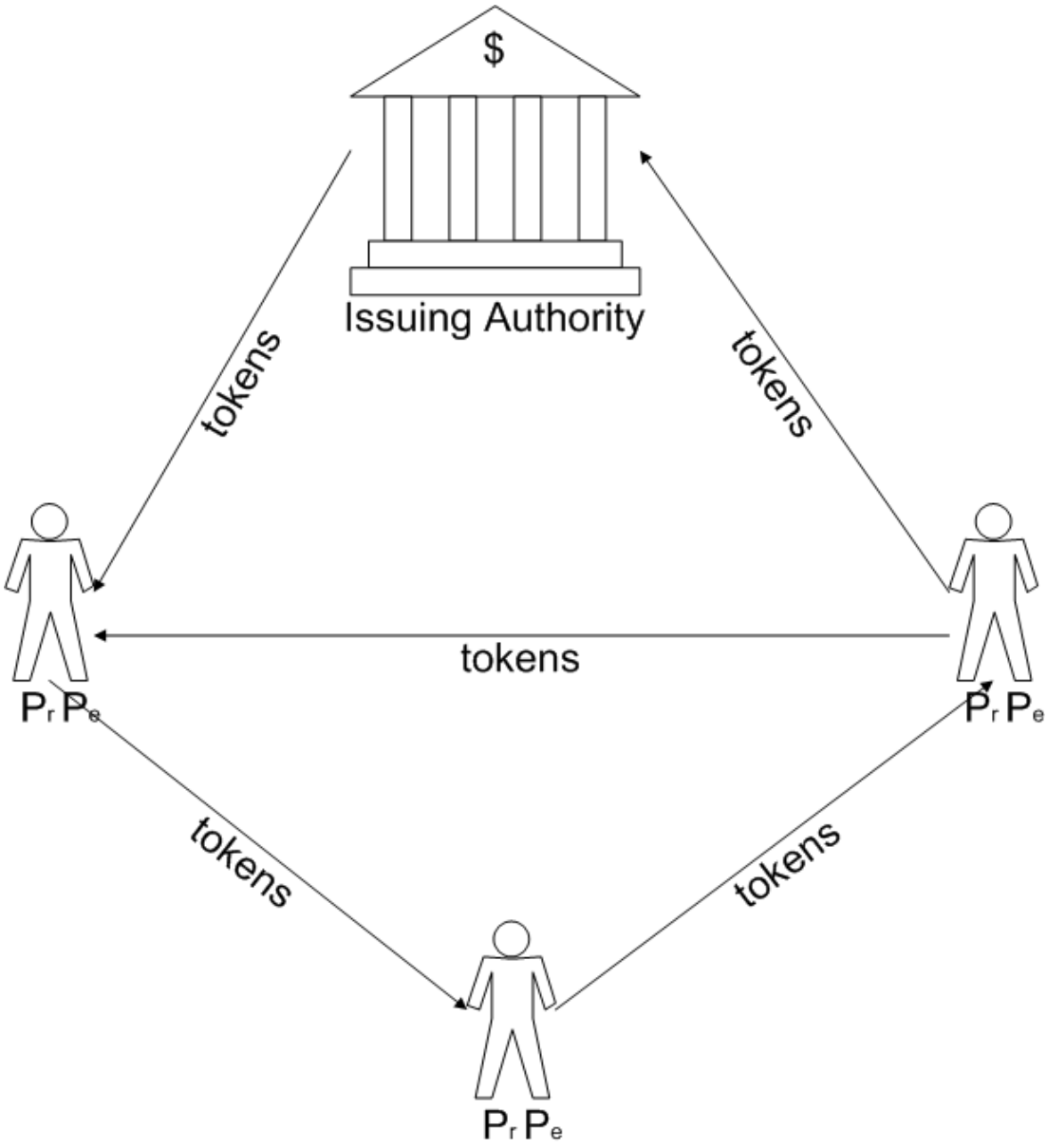

Figure 4 The participants and their interactions

5.2.2. Design Objectives

In order to develop a more accurate and realistic model, we have established some design objectives and goals. The most important design objective is the off-line capability; the token transfer, clearing and settlement processes should be conducted on off-line basis, as previously described in detail in section 4.3.1. Moreover, the electronic

money model should ensure the anonymity of both the payers and payees, and all transactions should be able to be conducted anonymously. Further design objectives have been proposed by researchers and the appropriate ones are included in this section. Therefore, the proposed model aims to minimize public-key cryptography in favour of faster private-key and hash-function based schemes as pointed out by Lipton and Ostrovsky (1998). Additionally, one other design objective is to minimize the communication, both the number of rounds and the number of bits transmitted, per transaction, between all the parties, as well as computational requirements of the scheme and memory requirements for all the participants (Lipton, Ostrovsky, 1998). Another important objective is to minimize the potential of fraud and forgery.

5.2.3. Target Market

The ideal case for an electronic money scheme or any money scheme would be to apply for any type of payment, involving infinitely large sums or the smallest amounts of money thinkable, and to be able to be used in all payment media currently existing (such as Internet, card payments, everyday cash and etc.). However, currently this is impossible, unless a medium such as Pure Money is invented, because different payment types and sums, and environments require different attributes of money in different scales, so satisfying each requirement, would be only possible with Pure Money.

The model proposed in this research aims to address and satisfy micro and nano-payments which have been previously mentioned in section 4.3.5. Micropayments have been defined as the amounts ranging from 1 penny to 10 £, whereas nano-payments have been defined as all amounts smaller than micro-payments. From this point on, both micro and nano-payments will be referred to as micropayments.

Other researchers have defined micropayments quite similarly: Tang (1995) defines Micropayments as low-value financial transactions ranging from several pennies to a few dollars whilst Economist (2000) refers to micropayments as purchases costing from a tenth of a cent to $10. Further extending the amount that can be denominated, RSA argues that micropayments are payments of small sums of money, generally smaller than those in which physical currency is available and is envisioned that sums of as little as US$0.00001 may someday be used to pay for content access or for small quantities of network resources (RSA). Furthermore, Rivest (2002) defines micropayments as a payment small enough that processing it is relatively costly. Schubert and Zimmermann (1998) define micropayments as **anonymous** payments of amounts smaller than approximately 10$. In the definition by Schubert and Zimmermann (1998) is very important the reference to the fact that micropayments should be anonymous. Lawrence defines micropayments as fractions of a cent or a very small amount that may be charged for on-line usage or connection time (Lawrence et al., 1998). It is obvious that there is no definite agreed upon definition of micropayments, but they are successfully utilized in practice, as stated by Sefton (2001), who defines the use of the mobile phone accounts to deduct value to pay for logos, ringtones etc. as a successful electronic micropayment. In this research, we will define micropayments as any payment equal or less than 10$, however, the lower boundary is not defined so that every small amount, such that the smallest amount that can be paid in consideration for value received is payable. Therefore, this definition includes such payments:

- Everyday cash transactions and payments less than 10$.
- Payments done for public transport, parking, pay phones, kiosks etc. (Such payments are mostly done today by disposable cards, such as Akbil in Istanbul)

- Payments not currently realized because of the impossibility of denominating such a payment with the currently existing methodologies (Payments such as 0,1 cent)

It is the third point in the above list that makes the subject of micropayments such an interesting topic. Services and items not currently charged would be chargeable with respect to amounts denoted with micropayments. Rivest (2002) lists these as:

- "Pay-per-click" purchases on Web, to include streaming music and video, and information services, so that the consumer pays for the pages visited on the Web or the seconds of a music clip watched.
- Mobile commerce, to include geographically based information services, gaming and small "real world" purchases.
- Infrastructure accounting, such as paying for bandwidth used.

Table 8 adopted from Jones (1997) is listing some possible microcommerce content providers where micropayments seem to form an ideal way to pay for this kind of content.

Table 8 The intangible goods offered by the content providers of the microcommerce

Traditional Content Providers	New Content Providers	Individual Content Providers
• Newspapers • Magazines • Directories • Book publishers • Newsletters • Photo libraries • Music publishers • Clip-art • Stock Quotes	• Applet developers • Search engines • Rating services • Micro-gambling • Interactive games • Software add-ons • Shopping agents • Buyer or Seller brokering • Currency conversion	• e-zines • Personal essays • Subject indexes • How-To Guides • Cookbooks • Annotated bookmark files • Personalized filtering • Other access to some shared resource
Source: (Jones, 1997)		

However, the concept of micropayments is more interesting in countries such as Turkey, where the smallest coin in circulation is the 25,000 TL (2003) and any value below that cannot be paid for exactly in cash without a loss for the payer or the payee, or if this amount is paid with debit and credit cards, the related transaction cost exceeds any possible gains from that transaction.

Moreover, micropayments should be differentiated from low-value payments, as these two notions usually are misunderstood and wrongly used interchangeably. Low-value payments can be defined as transactions slightly above the profitability threshold; they may be affordable but net receipts after costs do not justify the issuers' marketing expense and effort, especially for businesses characterized by large volumes of transactions in this range (Cardis). Transactions in the range of $10–$25 can be classified as low-value payments, which leave transactions below $10 to be micropayments (Cardis).

The associated costs of each payment type to the payee, are shown in the Table 9 (Hancock, Humphrey, 1998).

Table 9 Payee costs of receiving different payment instruments by transaction and sales value (for US supermarkets)

	By transaction volume		By 100$ of sales value	
	Unit Cost	**Percent (%)**	**Cost**	**Percent (%)**
Cash	$0.07	57	$0.52	36
Debit Card [a]	$0.30	2	$0.94	3
Check [b]	$0.43	33	$1.20	49
Credit Card	$0.81	3	$2.27	5
Other [c]	---	5	---	7

Source: (Hancock, Humphrey, 1998)

[a] Refers to an on-line debit, with settlement through the ACH.

[b] A verified check reduces fraud losses and it's cost per transaction (per $100 of sales) is somewhat lower at $0.37 ($1.05).

[c] Primarily food stamps, a government-sponsored food welfare program.

Further researchers on the subject of what micropayments are and how they can be defined are included on the "Evaluation of Micropayment Schemes" by Chi (1997), which provides an excellent literature survey on the currently existing Micropayment schemes, and the "Framework for Micropayment Evaluation" by Schmidt and Müller (1997).

5.2.4. The Methodology

Based on the desired properties that an electronic money system should contain, an electronic money model is proposed that meets those previously described properties. Ideally, if electronic money is to replace existing payment methods and schemes, it should be working in similar environments with the replaced models. In

other words, in order for electronic money to replace ordinary cash, the proposed electronic money should work in an off-line basis, whereas in order to replace credit cards, the proposed electronic money should work in an on-line basis. However, it can be argued that the on-line capability is a subset of the off-line capability, there is no obstacle for an electronic money model working off-line not to work on-line, but the opposite is not true. Therefore we can list the aimed attributes of the proposed electronic money such as:

- Ability to work on both off-line and on-line basis
- Appropriate mainly for micropayments
- Embodying all properties and attributes of money
- Reusability of coins

The first consideration regarding the above mentioned attributes is what the electronic coins consist of. Think of the normal paper currency, a banknote which consists of a unique serial number, a face value and a set of security attributes. Initially let the electronic coins contain only the unique serial number and the face value. Therefore an electronic coin is distinguished by all other coins with respect to its own serial number and communicates to other parties the value it denominates with its face value. The payee therefore knows the value that the electronic coin denominates by just checking the face value of that coin. However, several problems arise from the very nature of the characteristics described above:

1. How does the payee know that the electronic coins presented by the payer for payment are issued electronic coins by the issuing authority and not counterfeited?

2. How does the payee know that the electronic coins presented by the payer for payment are unique electronic coins and that they were not copied? (the double-spending problem)
3. How does the payee know that the face value of the presented electronic coin was not altered?
4. How does the payer know that the payee received the correct electronic coins within a vast amount of presented coins? (In other words, how it can be guaranteed that coins in the exact value were transferred?)
5. How does the issuing authority know that nobody is counterfeiting electronic coins?

Such an electronic money system is prone to several attacks from different parties. Holders and non-holders of electronic money will want to counterfeit electronic money either by generating new electronic coins using the electronic coin generation technique of the issuing authority, or duplicate the already existing electronic coins. Therefore, the proposed electronic money model should try to resolve all these questions based on the methodology that it shall adopt.

As previously explained in Table 7, five different methodologies exist while implementing an electronic money scheme: the *Online Protocols*, the *Hardware-Based Schemes*, the *Subscription Schemes*, the *Coupon-Based Schemes* and the *Probabilistic Schemes*. The design methodology implemented in this electronic money scheme in this study is the Hardware-Based scheme.

The above mentioned considerations arise from the fact that the owner of the electronic money, if he desires, can easily copy the electronic coin and duplicate it in infinite numbers because of the nature of the electronic coin: electronic coins consist of

data, ensuring the security and the unforgeability of the electronic coins is almost impossible considering the fact that all data if read, can be copied. Encrypting the data is not a solution in an off-line electronic money scheme, as the holder of electronic money has also the knowledge to authenticate its legitimacy and also to access and read the data those electronic coins consists of. Considering the paper currency, the banknotes are almost impossible to be copied because of their nature, which is paper, and the extremely detailed printing process. The paradox is evident; an off-line electronic money scheme requires the owner of an electronic coin to safeguard it from its owner, himself. Therefore the solution is also evident; if the electronic coins need to be protected from their owner, and then another physical entity needs to be placed between the coins and their owner. The most ideal candidate for protecting electronic coins from their owner would be the item within which the electronic coins are carried on, the eW.

In the proposed electronic money model, any given party that wants to transact using electronic money is actually composed of the P*r*, the eW and the *t*'s. The P*r* carries the eW and the eW carries the *t*'s. Both the eW and the *t*'s are developed and issued by the IA. The *t*'s can only be transferred with the use of the eW and can only be stored in eW, or in the central repository of the IA.

In the proposed electronic money model, the eW's are realized by using Smart Cards. Smart cards are portable, tamper-resistant computers with a programmable data store (Guthery, Jurgensen, 2002). The reason that smart cards are appropriate as electronic wallets, is based on the predictions of Rankl and Effing (2000), who state that the functionality and applications of the new integrated circuit cards will reach far beyond the currently envisaged, eventually perhaps influencing us in our behaviour as

citizens. But for our proposed electronic money model, an electronic wallet built upon a normal smart card would not be appropriate, as it will be explained below.

The required and necessary electronic wallet is similar to the physically secure coprocessors as described by Tygar and Yee (1993). A secure coprocessor is described as a hardware module containing a Central Processing Unit (CPU), Read Only Memory (ROM), and non-volatile memory (NVM), which hardware module is physically shielded from penetration, and the I/O (Input/Output) interface to this module is the only means by which access to the internal state of the module can be achieved. According to Smith (1996) such hardware modules can be in the form of IC (Integrated Circuit) Chip cards (the smartcards), PCMCIA (Personal Computer Memory Card International Association) Tokens, Smart Disks, Bus Cards and other card tokens such as SecureID and ActivCard.

Tygar and Yee (1993) argue that such a hardware module can store cryptographic keys without risk of release. In the proposed system of secure coprocessors by Tygar and Yee (1993), the CPU can perform arbitrary computations (under control of the operating system) and thus the hardware module, when added to a computer, becomes a true coprocessor, but often, the secure coprocessor will contain special-purpose hardware in addition to the CPU and memory; for example, high speed encryption/decryption hardware may be.

Tygar and Yee (1993) conclude that:

> Secure coprocessors must be packaged so that physical attempts to gain access to the internal state of the coprocessor will result in resetting the state of the secure coprocessor (i.e., erasure of the NVM contents and CPU registers). An intruder might be able to break into a secure coprocessor and see how it is constructed; the intruder cannot, however, learn or change the internal state of the secure coprocessor except through normal I/O channels or by forcibly resetting the entire secure coprocessor. The guarantees about the

privacy and integrity of non-volatile memory provide the foundations needed to build security systems.

Smart cards with secure co-processors have not yet been developed, however the research continues. Therefore, in this study, we shall assume that the necessary hardware technology of smartcards with secure coprocessors to implement the proposed model has been achieved and we shall construct the model on this base.

5.2.5. The Detailed Model

5.2.5.1. The Issuing Authority (IA)

The IA is the central authority that issues both the *t*'s and eW's, and owns and controls the Central Database (CD). The duty of the IA is not to authorize each single transaction, but to provide the means, techniques and tools necessary for the transactions to be conducted with respect to the properties described previously in Section 4.3, namely the off-line capability and anonymity of transactions.

5.2.5.2. The Payer (P_r) and the Payee (P_e)

The proposed electronic money transaction model is a bipolar system, consisting only of the P_r and the P_e. Although the *t* issuance requires and necessitates the existence of the third pole of IA, the transaction of the *t*'s requires only the existence of the P_r and P_e. In the proposed model, the P_r and the P_e are exactly identical users, each owning a valid eW with valid *t*'s deposited on. A P_r, at any given time and circumstance can be a P_e and vice versa. Each P_r and P_e are registered with a unique Personal Identification (PID) to the central IA database.

5.2.5.3. The Electronic Wallet (eW)

The eW is the smartcard embodying a physically secure co-processor as described previously in Section 5.2.4. P_r and P_e carry eW's in order to conduct transactions. Each eW is identified with a unique eW identification number (eWID). eW's, as ordinary credit and debit cards do have a validity period, which is decided by the IA. The security of eW's is provided by three different cryptographic algorithms, where each algorithm can be viewed as a *security barrier*. For an attacker or eavesdropper, breaking two of the three security barriers will not be enough to forge, cheat or duplicate a transaction. Therefore, each eW contains 3 main cryptographic algorithms necessary to conduct and conclude a transaction:

- A Secure Communication Key (SCK)
- An eW Authentication Key (eWAK)
- An Electronic Token Authentication Key (*t*AK)

The SCK, eWAK and *t*AK keys are shared by all users in the system and are common for all users. Therefore, the SCK, eWAK and *t*AK keys are of vital importance for the system to function, and as described in Section 5.2.4, all these keys should be stored in the NVM, to avoid any possibility of release to attackers.

5.2.5.3.1. Secure Communication Key (SCK)

The SCK is a key necessary to secure the communication between the P*e* and the P*r*, to ensure that any possible eavesdroppers do not understand the communication that takes place. The proposed SCK for the model is a ***Symmetric Algorithm***, sometimes called conventional algorithm, where the encryption key can be calculated from the decryption key and vice versa (Schneier, 1996).

All communicated data between the P*e* and the P*r* is encrypted and decrypted with the use of SCK. The P*e* when is sending a message to the P*r*, or when the P*r* is sending a message or *t*'s to the P*e*, before the transmission, the data to be sent is encrypted with the SCK. The same SCK is used by the receiver of the data to decrypt the message or the *t*'s.

Examples of symmetric algorithms can be given from the well celebrated symmetric key competition by NIST. NIST started to select a symmetric-key encryption algorithm that is to be used to protect sensitive Federal Information. In 1998, there were 15 candidate algorithms accepted by NIST and NIST requested the assistance of the cryptographic research community in analyzing the candidates. According to the results of the analysis, NIST selected MARS, RC6, Rijndael, Serpent, and Twofish as finalists in 1999. Having reviewed further public analysis of the finalists, NIST judged Rijndael to be the best overall algorithm for the AES.

The number of rounds and the key size that SCK should employ are far beyond the scope of this research and will have to be decided with respect to the computational power and limits of the microprocessors to be utilized.

5.2.5.3.2. Electronic Wallet Authentication Key (eWAK)

The eWAK is the necessary key that enables P*e* to authenticate P*r*, and vice versa. The function of the eWAK is to authorize the opposite transacting party. As defined by Knudsen (1998), *authentication* assures to the transacting parties, that the parties they deal with are not imposters. The proposed eWAK for the model is a ***one-way Hash Function.*** A one-way Hash function, **H(M)**, as described by Schneier (1996), operates on an arbitrary-length pre-image message, **M**, and it returns a fixed-length hash value, **h**.

h = H(M), where h is of length m

One-way hash functions have these characteristics that make them one-way:

- Given M, it is easy to compute h.
- Given h, it is hard to compute M such that H(M)= h.
- Given M, it is hard to find another message, M', such that H(M) =H(M') (Schneier, 1996).

Currently existing one-way Hash functions are HAVAL, MD2, MD4, MD5, RIPE-MD, N-HASH, SHA and SNEFRU. However, as stated by Schneier (1996), only MD5 and SHA are contenders if a question of which one-way Hash function to choose would arise.

The work principle of the eWAK is simple: both the P*e* and P*r* generate a Generic Random Number (***GRN)*** each and calculate the ***h*** by the one-way Hash function of ***h=H(GRN).*** Then they challenge the other party by sending the generated random numbers ***GRN*** to each other to hash, expecting the reply to be equal to the ***h*** they calculated in the first place. If both parties authenticate each other, then all messages to be sent are hashed using the same algorithm and both the message and then the resulting hash value are sent to the receiver. Each message is authenticated, so that no intruder intercepts the communication.

As stated previously for the SCK case, the number of rounds and the key size that eWAK should employ are far beyond the scope of this research and should be decided with respect to the computational power and limits of the microprocessors to be utilized.

5.2.5.3.3. Token Authentication Key (*t*AK)

*t*AK, is the key necessary to authenticate a given *t*. Similar to the eWAK, *t*AK is a one-way Hash function, but is not the same function with eWAK. As it will be discussed in Section 0, each *t,* has a Unique Token Serial Number (UTSN) and a UTSN Control Value (UTSNCV). The P*e*, after receiving the $t_{(i)}$ from the P*r*, authenticates the $t_{(i)}$ by hashing the UTSN to the *t*AK function. If the outcome of the function is equal to the UTSNCV, then the $t_{(i)}$ is a valid *t*. Else, the $t_{(i)}$ is not a valid *t*, and therefore the transaction is not authorized.

The number of rounds and the key size that *t*AK should employ are far beyond the scope of this research and should be decided with respect to the computational power and limits of the microprocessors to be utilized.

5.2.5.4. The Electronic Token (*t*)

At the very heart of all Electronic money models, lies the money itself. In the proposed model of this study, we shall refer to the monies in question as **Electronic Tokens** (***t***). The *t*'s are generated by the IA, and no one else, not even the P*r* and the P*e*, do have the authority to issue new *t*'s. *t*'s consist of a set of necessary and critical data. Specifically, a given $\boldsymbol{t_{(i)}}$ (where ***i*** denotes the unique *t* serial number (UTSN) of that given *t*) consists of the following fields, as shown in Table 10:

Table 10 The electronic token (*t*)

$t_{(i)}$
UTSN: Unique Token Serial Number
UTSNCV: UTSN Control Value
TFV: Token Face Value
DoI: Date of Issue
O*pr*: Previous Owner
O*cr*: Current Owner
O*int:* Initial Owner

The UTSN, as the name implies, is a serial number assigned to each token by the IA, in order to distinguish every token. Therefore, the UTSN's are all unique. The size of the UTSN depends on the amount of *t*'s issued by the IA; the more *t*'s, the larger the UTSN should be.

The Token UTSNCV is a generated output value, with inputting the UTSN to the *t*AK function. UTSNCV is necessary to understand whether the given $t_{(i)}$ is a valid *t*.

The TFV refers to the value amount that each *t* represents. Each token may have different TFV's or all *t*'s may have the same TFV.

The DOI denotes the date that the *t* was issued by the IA. DOI is a necessary field to check the transaction validity of each issued *t*.

The O_{pr} is the eWID of the P_r who transferred this given $t_{(i)}$ to the O_{cr}. The O_{int} is the eWID of the P_r who first received this $t_{(i)}$ from the IA. The O_{cr} is the eWID of the current owner of the $t_{(i)}$.

5.2.5.5. The Central Database (CD)

The Central Database (CD) is the database operating in the IA and keeps track and information on each P_r and P_e, eW, and *t*. The CD is designed in order to ensure the anonymity of each P_r and P_e, but also to enable tracking of any possible double-spenders or cheaters. The design considerations of the CD are:

- Each user (P_r and P_e) can have more than one eW's.
- A given eW can have only one owner.
- eW's can store more than one *t*'s.
- *t*'s can be transferred from eW's and therefore a single *t*(i) can be stored by more than one eW.

The Entity Relationship (ER) diagram of the CD is given in Figure 5.

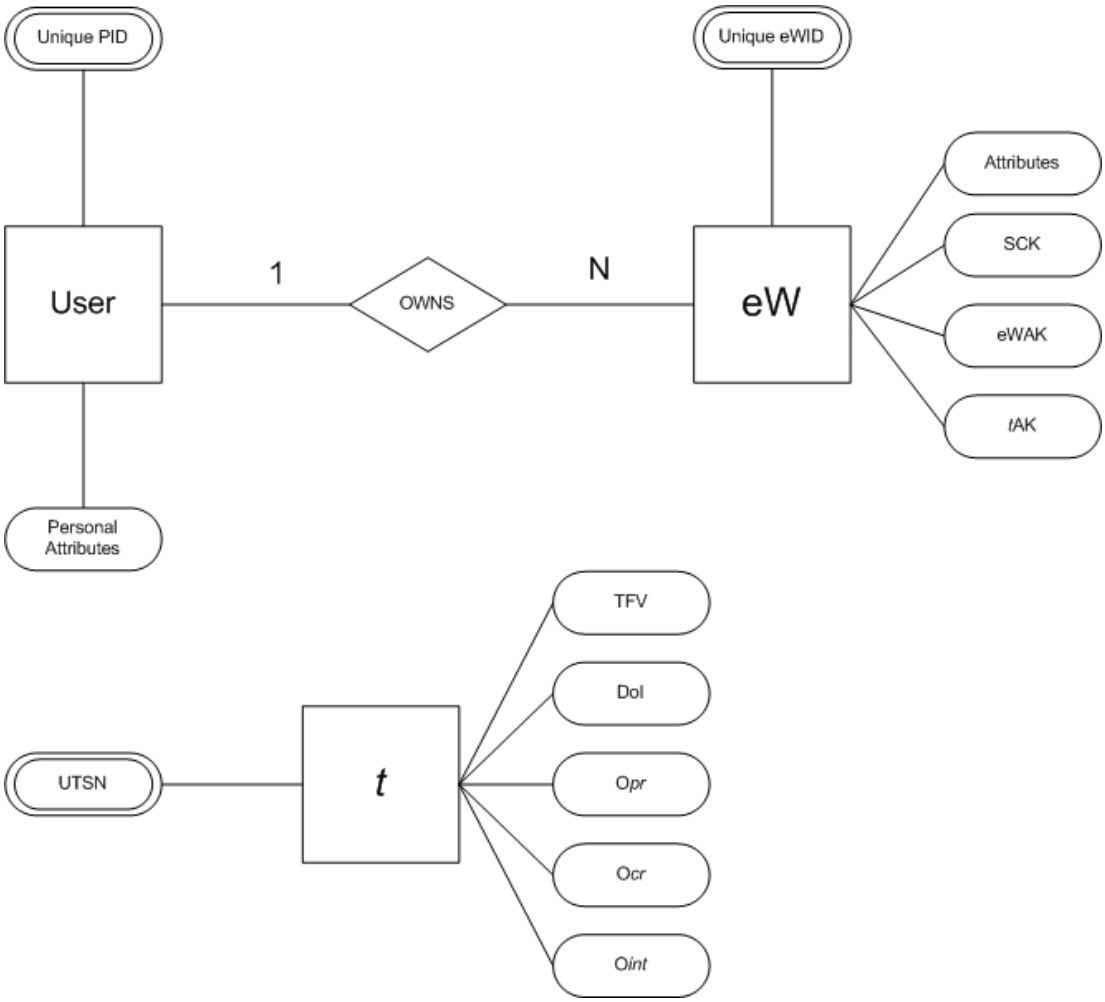

Figure 5 The ER diagram of CD

The separation of the information of t's from the User and eW entities in the ER diagram of the CD, is to ensure that no tracking of the usage history of each t can be executed, thus ensuring complete usage anonymity.

5.2.5.6. The Protocol

Before describing in detail the proposed protocol, the notation to be used is briefly introduced. The notation is the conventional notation utilized for security protocols, as described also by Hubbers, Oostdijk and Poll (2002) This notation reads as follows:

SCK(eWID$_{(Pr)}$): The agent is encrypting eWID$_{(Pr)}$ using the SCK key

{eWID$_{(Pr)}$}$_{SCK}$: The eWID$_{(Pr)}$ data encrypted using the SCK key

P*r*→ P*e* : {eWID$_{(Pr)}$}$_{SCK}$: The P*r* sends to P*e* the {eWID$_{(Pr)}$}$_{SCK}$

SCK{eWID$_{(Pr)}$}$_{SCK}$: The agent is decrypting {eWID$_{(Pr)}$}$_{SCK}$ using the SCK key

The protocol, for ease of reading and understanding, is divided in further subsections. Several assumptions have been made regarding the proposed protocol. These assumptions are:

- The protocol is notated for the transfer of a **single** *t* from the P*r* to P*e*. However, by repeating the "*t* Transfer Step", further *t*'s can be transferred from the P*r* to P*e*.
- The face value of the transferred *t* is considered to be fixed to a predetermined value; therefore the face value is not negotiated, checked and informed between the P*e* and P*r*.
- The protocol only includes the steps/operations that are undertaken only in smooth/normal operation: that is, in case of a problem, attack or eavesdropping, the steps to be undertaken are not enlisted.
- No frauds or fraud attempts are discovered in the verification and authentication processes.
- Cases of macropayment and doublespending are excluded.

The protocol consists of seven steps which are namely:

- Initialization step
- User authentication step
- Identification step
- P*r* and P*e* authentication step

- *t* transfer step
- Clearing and settlement step
- Termination step

5.2.5.6.1. Initialization step

The initialization step starts by physically placing the eW to a simple dummy data transfer device, such as an ATM or a Smart Card reader, which restores the inserted cards to the Initial State necessary to start the *t* transaction.

1. Initialize($eW_{(Pr)}$) **1. Initialize($eW_{(Pe)}$)**

5.2.5.6.2. User authentication step

The purpose of the user authentication step is to authenticate that the user presenting the eW does have the privilege to transact with that given eW (in other words is the owner of that given eW). The User Authentication is possible with the use of Personal Identification Numbers (PIN), similar to those used in Debit Cards.

2. P*r* → P*r*: $PIN_{(Pr)}$ **2. P*e* → P*e*: $PIN_{(Pe)}$**

The flowchart of the User Authentication process is given in Figure 6.

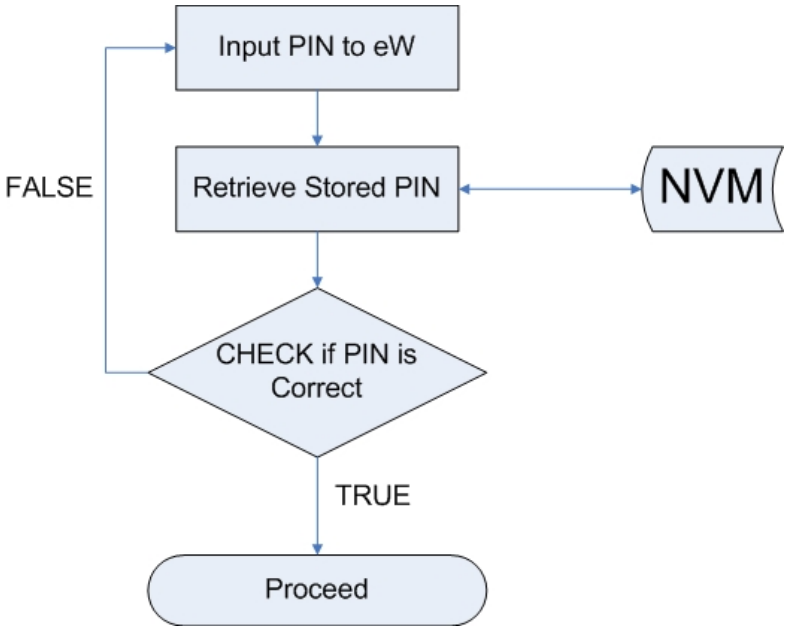

Figure 6 Flowchart of user authentication step

5.2.5.6.3. Identification step.

The purpose of the identification step is the exchange of credentials between the P*e* and P*r*. The exchanged credentials consist of the eWID's of each eW. The credentials are exchanged after they have been encrypted with the SCK.

3. SCK(eWID$_{(Pr)}$)

4. P*r*→ P*e*: {eWID$_{(Pr)}$}$_{SCK}$

5. SCK{eWID$_{(Pr)}$}$_{SCK}$

6. SCK(eWID$_{(Pe)}$)

7. P*e*→ P*r*: {eWID$_{(Pe)}$}$_{SCK}$

8. SCK{eWID$_{(Pe)}$}$_{SCK}$

5.2.5.6.4. P*r* and P*e* authentication step

The P*r* and P*e* authentication step is required to authenticate that the transacting parties are using valid eW's issued and distributed by the IA. This step is realized with the use of the eWAK key. The operation details of the eWAK key were previously briefly described in Section 5.2.5.3.2.The input for the eWAK hash function is the GRN. The length of the GRN should be predefined by the IA. It is important that the P*e* and P*r* should not challenge each other with the same GRN's. If both parties challenge each other with the same GRN, then the transaction should immediately terminate.

9. Randomize(GRN)

10. SCK(GRN)

11. P*e* → P*r*: $\{GRN\}_{SCK}$

12. SCK$\{GRN\}_{SCK}$

13. eWAK(GRN)

14. SCK(eWAK(GRN))

15. P*r* → P*e*: $\{eWAK(GRN)\}_{SCK}$

16. SCK$\{eWAK(GRN)\}_{SCK}$

17. eWAK(GRN)′

18. [eWAK(GRN)′= eWAK(GRN)]

19. SCK(Reply)

20. P*e* → P*r*: $\{Reply\}_{SCK}$

21. SCK$\{Reply\}_{SCK}$

22. Randomize(GRN′)

23. [(GRN′) = (GRN)]

24. SCK(GRN′)

25. P*r*→ P*e*: {GRN′}$_{SCK}$

26. SCK{GRN′}$_{SCK}$

27. [(GRN′) = (GRN)]

28. eWAK(GRN′)

29. SCK(eWAK(GRN′))

30. P*e*→ P*r*: {eWAK(GRN′)}$_{SCK}$

31. SCK{eWAK(GRN′)}$_{SCK}$

32. eWAK(GRN′)′

33. [eWAK(GRN′)′= eWAK(GRN′)]

34. SCK(Reply)

35. P*r*→ P*e*: {Reply}$_{SCK}$

36. SCK{Reply}$_{SCK}$

The flowchart of the Pr and Pe authentication step is given in Figure 7.

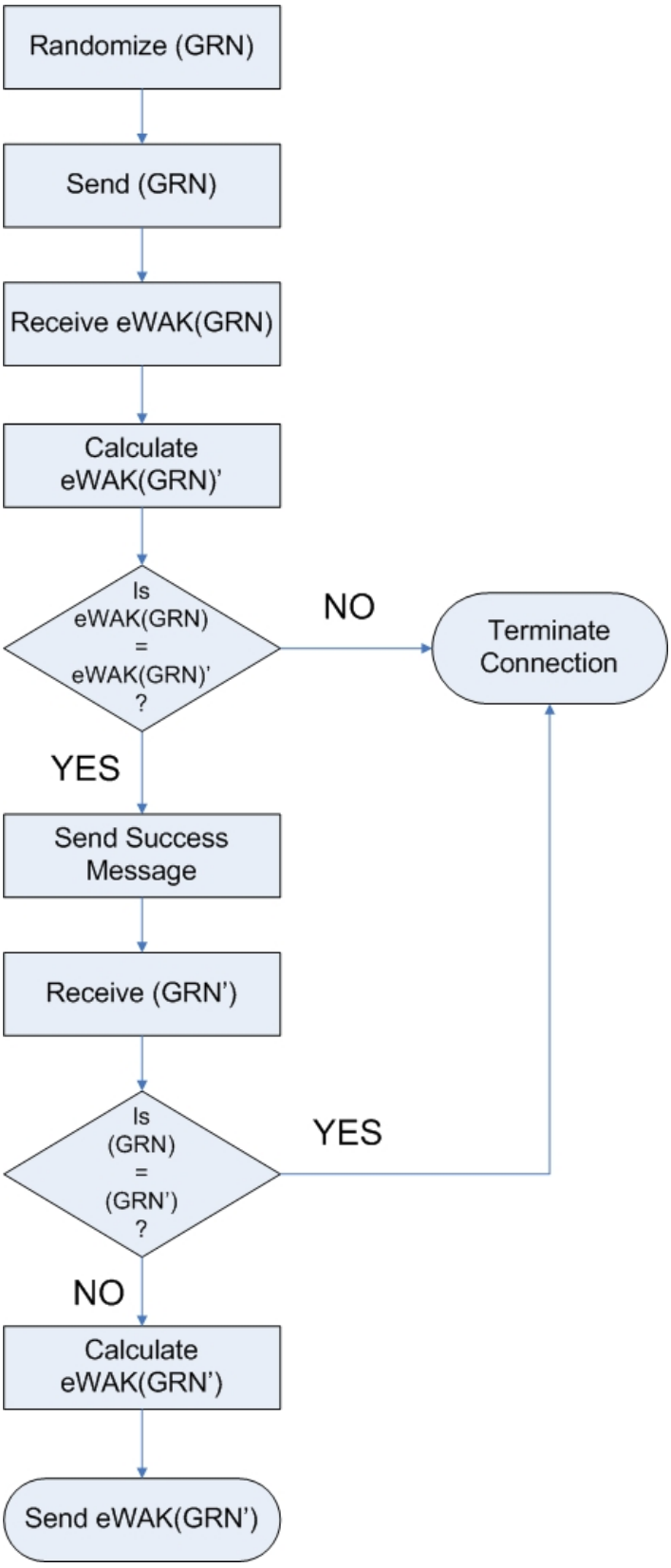

Figure 7 Flowchart of the P*r* and P*e* authentication step

5.2.5.6.5. *t* transfer step

The *t* transfer step is required to transfer the *t*'s from P*r* to P*e*. The following protocol step describes the transfer of a single $t_{(i)}$, however, for further transfers in a single transaction, this step should be repeated.

37. eWAK($UTSN_{(i)}$)

38. SCK(eWAK($UTSN_{(i)}$))

39. P*r*→ P*e*: {eWAK($UTSN_{(i)}$)}$_{SCK}$

40. SCK($t_{(i)}$)

41. P*r*→ P*e*: {($t_{(i)}$)}$_{SCK}$

42. SCK{eWAK($UTSN_{(i)}$)}$_{SCK}$

43. SCK{($t_{(i)}$)}$_{SCK}$

44. eWAK($UTSN_{(i)}$)′

45. [eWAK($UTSN_{(i)}$)′= eWAK($UTSN_{(i)}$)]

46. *t*AK($UTSN_{(i)}$)

47. [UTSNCV= *t*AK($UTSN_{(i)}$)]

48. SCK(Reply)

49. P*e*→ P*r*: {Reply}$_{SCK}$

50. SCK{Reply}$_{SCK}$

The flowchart of the *t* Transfer Step is given in Figure 8.

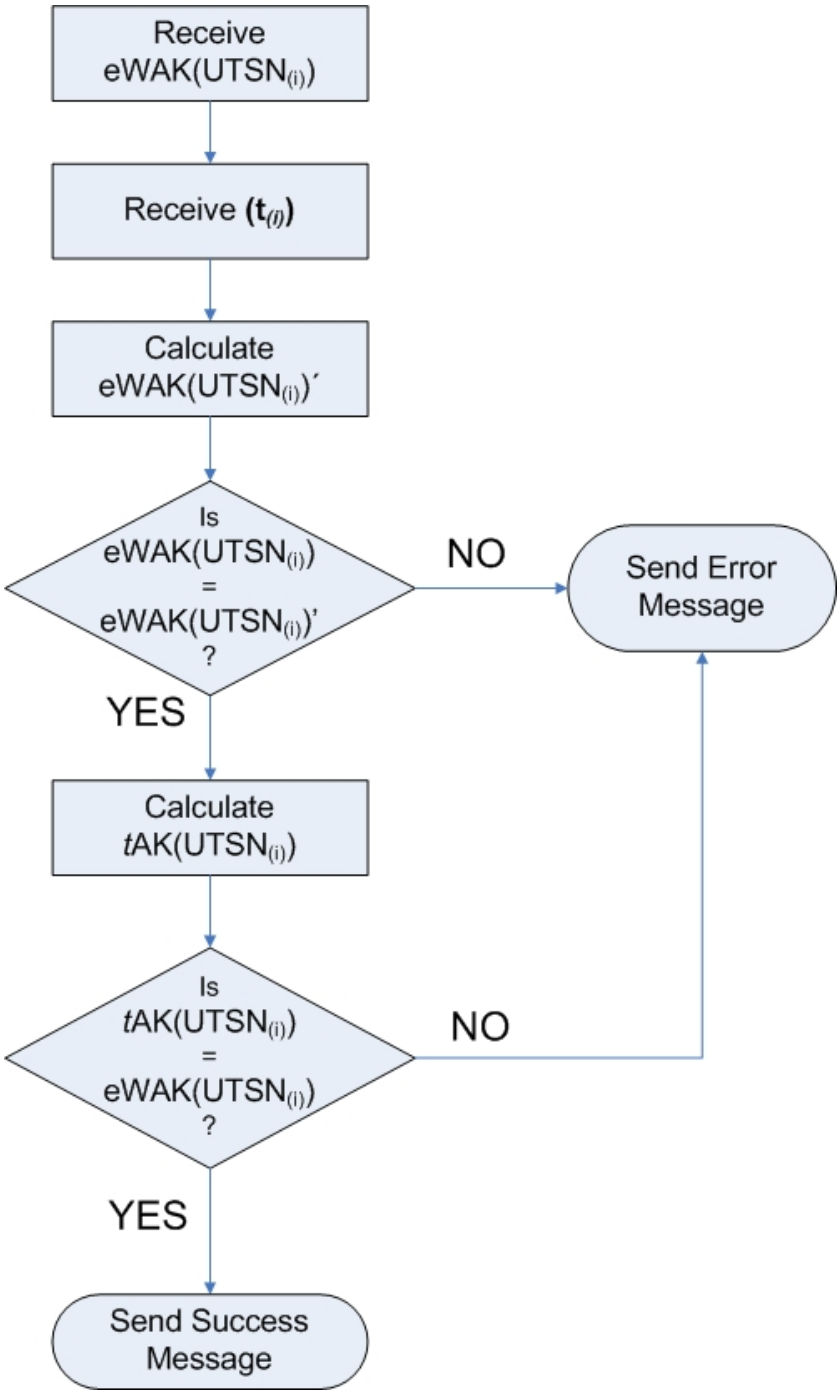

Figure 8 Flowchart of the *t* transfer step

5.2.5.6.6. Clearing and settlement step

The clearing and settlement step is necessary to ensure that the transfer of $t_{(i)}$ is completed accordingly. The P*e*, after receiving the $t_{(i)}$ informs the P*r* that the $t_{(i)}$ was received and authenticated with a receipt, and the P*r* deletes the $t_{(i)}$. The P*e* further alters accordingly the O*pr* and O*cr* fields of the $t_{(i)}$. It is important to note that the P*r* does not erase the $t_{(i)}$ from its storage until the receipt is received from the P*e,* and the P*e* does not alter the O*pr* and O*cr* fields of the $t_{(i)}$ until the receipt is prepared and sent.

51. SCK(Receipt)

52. P*e*→ P*r*: {Receipt}$_{SCK}$

53. SCK{Receipt}$_{SCK}$

54. Delete($t_{(i)}$)

55. $t_{(i)}[O_{pr}]=t_{(i)}[O_{cr}]$

56. $t_{(i)}[O_{cr}]$=P*e*[eWID]

5.2.5.6.7. Termination step

At the termination step the transaction between the P*e* and the P*r* is terminated by issuing a "Goodbye" message.

57. P*e*→ P*r*: {Goodbye}

58. P*r*→ P*e*: {Goodbye}

59. Terminate($eW_{(Pr)}$) **59. Terminate($eW_{(Pe)}$)**

5.3. Evaluation of the Proposed Micropayment Scheme

As stated previously in section 4.3.5 currently there exist many micropayment proposals, schemes and methodologies. Therefore it is very important to evaluate these micropayment schemes based upon some standardized frameworks. Such two frameworks have previously been proposed, the VTS framework by Schmidt and Müler (1997), and the Chi framework by Chi (1997). Therefore, the model developed in this study is evaluated using the VTS and Chi frameworks in sections 5.3.2 and 5.3.3 respectively. The computation cost of the proposed model is estimated by developing a computer code that runs accordingly to the proposed model, and the findings are presented in section 5.3.1.

5.3.1. Estimation of the Computation Costs for the Proposed Model

In order to estimate the computation cost of the proposed model, the explicit model previously provided was coded. The programming language used was Java. The reason for employing the Java programming language mainly is the fact that the most common smartcards are the JavaCards which do use programs written in Java. The Java code of the main program is given in Appendix A.

Several assumptions were undertaken while developing the code. These assumptions are:

- The proposed model runs not in two different clients (P*r* and P*e*) but in a single client. This is done in order to avoid any communication costs that could occur while transmitting data from the P*e* to P*r*.
- The cryptography keys, the GRN, and the token fields are assumed to be of 1024 bytes.

- The assumptions made in The Protocol section previously do apply in the developed code also.

Further assumptions were regarding the cryptography to be utilized. In these assumptions, the cryptography to be used for the SCK, eWAK and *t*AK keys were selected according to the proposals and evaluations by Schneier (1996). Therefore, Table 11 provides the list of the selected cryptography algorithms used in the estimation of the computation costs.

Table 11 The selected cryptographic algorithms

Key	Cryptography Algorithm Selected
SCK	Rijndael
eWAK	SHA-1
*t*AK	SHA-1

The SHA-1 algorithm utilized does exist within the Java API specification, and is the Secure Hash Algorithm, as defined in Secure Hash Standard, NIST FIPS 180-1 (Web Ref3).

The Table 12 provides the performance figures of the SHA-1 algorithm with respect to other currently existing hash algorithms, on a Pentium® processor. Further details on the architecture specification can be found on (Bosselaers, et al., 1996).

Table 12 Performance figures of Hash algorithms on a Pentium®

Algorithm	MD4	MD5	SHA-1	RMD	RMD-128	RMD-160
Instructions	397	573	**1247**	795	985	1566
% V Pipe use	43.32	41.19	**42.82**	43.65	41.73	37.55
% Paired simple instr.	98.57	92.73	**99.72**	99.57	95.92	94.38
%Memory ref's.	14.61	12.91	**35.85**	14.72	15.13	11.88
Cycles	275	403	**943**	556	718	1153
Cycles per instr.	0.69	0.70	**0.76**	0.70	0.73	0.74
Speed-up factor	1.63	1.59	**1.64**	1.62	1.57	1.51
Source (Bosselaers, et al., 1996)						

Rijndael (AES) algorithm utilized was obtained by Paulo Barreto (Barreto) who developed the Optimised Java implementation of the Rijndael (AES) block cipher in May 2001. The code is given in Appendix B.

Table 13 by Daemen and Rijmen, (2003) provides the performance figures of Rijndael (AES) algorithm for a Intel 8051 microprocessor, using 8051 Development tools of Keil Elektronik: uVision IDE for Windows and dScope Debugger/Simulator for Windows; whilst Table 14 (Daemen, Rijmen, 2003) provides the performance figures of the Rijndael (AES) algorithm for a Java implementation based on the execution time of the KAT and MCT code on a 200 MHz Pentium®, running Linux, and using the JDK1.1.1 Java compiler.

Table 13 Execution time and code size for Rijndael in Intel 8051 assembler

Key/Block Length	Number of Cycles	Code length
(128,128) a)	4065 cycles	768 bytes
(128,128) b)	3744 cycles	826 bytes
(128,128) c)	3168 cycles	1016 bytes
(192,128)	4512 cycles	1125 bytes
(256,128)	5221 cycles	1041 bytes
Source (Daemen, Rijmen, 2003)		

Table 14 Execution time for Rijndael in Java

Key/Block length	Speed	# cycles for Rijndael
(128,128)	1100 Kbit/s	23.0 Kcycles
(192,128)	930 Kbit/s	27.6 Kcycles
(256,128)	790 Kbit/s	32.3 Kcycles
Source (Daemen, Rijmen, 2003)		

The Random numbers necessary for the eWAK key to function in the proposed model, were generated with the use of the SecureRandom public class provided with Java. The SecureRandom class provides a cryptographically strong pseudo-random number generator (PRNG). A cryptographically strong pseudo-random number minimally complies with the statistical random number generator tests specified in FIPS 140-2, Security Requirements for Cryptographic Modules (Web Ref5), section 4.9.1. Additionally, SecureRandom must produce non-deterministic output and therefore it is required that the seed material be unpredictable and that output of SecureRandom be cryptographically strong sequences as described in RFC 1750, Randomness Recommendations for Security (Web Ref6).

Finally, the *t* (electronic tokens) were not embodied within the main code of the model but instead were generated with an independent Java code, which is provided in Appendix C.

The generated codes were run on a PC with a 1 GHz Pentium ® III, and a 512 MB memory and the runtime environment was the Java 2 Runtime Environment. The computational time of the code was calculated using the GetCurrentThreadCpuTime() function of the JVMPI. The related discussion on how to measure CPU time in Java and which is the best methodology is thoroughly covered by Bıçakçı (2003). The calculated computation times are given on Table 15.

Table 15 Calculated computation times

Executed Part of Code	Execution Time
SCK Encrypt	10 msec.
SCK Decrypt	12 msec.
eWAK	10 msec.
Identification Step	24 msec.
Authentication Step	21 msec.
t Transfer Step	20 msec.
Total Execution Time	511 msec.

5.3.2. VTS Evaluation Framework

The VTS micropayment evaluation framework proposed by Schmidt and Muller (1997) is based upon the 30 attributes proposed by scholars to describe electronic payment systems and the VTS diagrams (Rumbough et al. 1991) from the field of object oriented analysis. The framework combines and groups the 30 electronic payments attributes under three major dimensions: the technological, the economic and the social dimension. The attributes listed below these three major dimensions are given in Table 16:

Table 16 The three dimensions and relative attributes

Technological Dimension	Economic Dimension	Social Dimension
• Security • Reliability • Scalability • Latency	• Low Transaction costs • Atomic Exchange • Customer Base	• Anonymity • Peer-to-peer Payments

The details of each attribute are given in detail in (Schmidt, Muller, 1997).

VTS diagrams are a graphical method from object oriented analysis and design to describe interaction between a set of objects in a system. Briefly, the participating objects are displayed by vertical arrows representing the time scale. Communication between these objects is displayed by horizontal arrows, which are labeled by the content of a message. Additional the vertical object arrow may have descriptions of the action the object takes in response to a message from another object. Schmidt and Muller propose that VTS diagrams can be used to describe business transactions, which include the payment process and the transmission of the information good. The objects can be the customers client software, the merchants server, and one or more payment system servers. Each horizontal arrow represents a complete session of Internet communication between a client and a server. Further details of the VTS diagrams are given in (Schmidt, Muller, 1997).

Schmidt and Muller perform the VTS analysis on DigiCash, SET and First Virtual payment schemes (Schmidt, Muller, 1997), therefore we shall proceed directly to the evaluation of our proposed method. Furthermore, we shall not use the notation of Schmidt and Muller but continue with the notation previously described in The Protocol section.

The VTS Micropayment Evaluation framework is particularly applicable to the proposed model in this research due to the fact that there is intense exchange of data between the P*r* and the P*e* and features that were taken as design objectives while developing this model are evaluation criteria in the framework. Thus, the VTS Micropayment Evaluation framework will show whether the intense data exchange has any effects in the transactions based on the proposed model, and how good the design criteria were met.

The verbal description of the developed model on the VTS diagram is shown on Figure 9 and Figure 10.

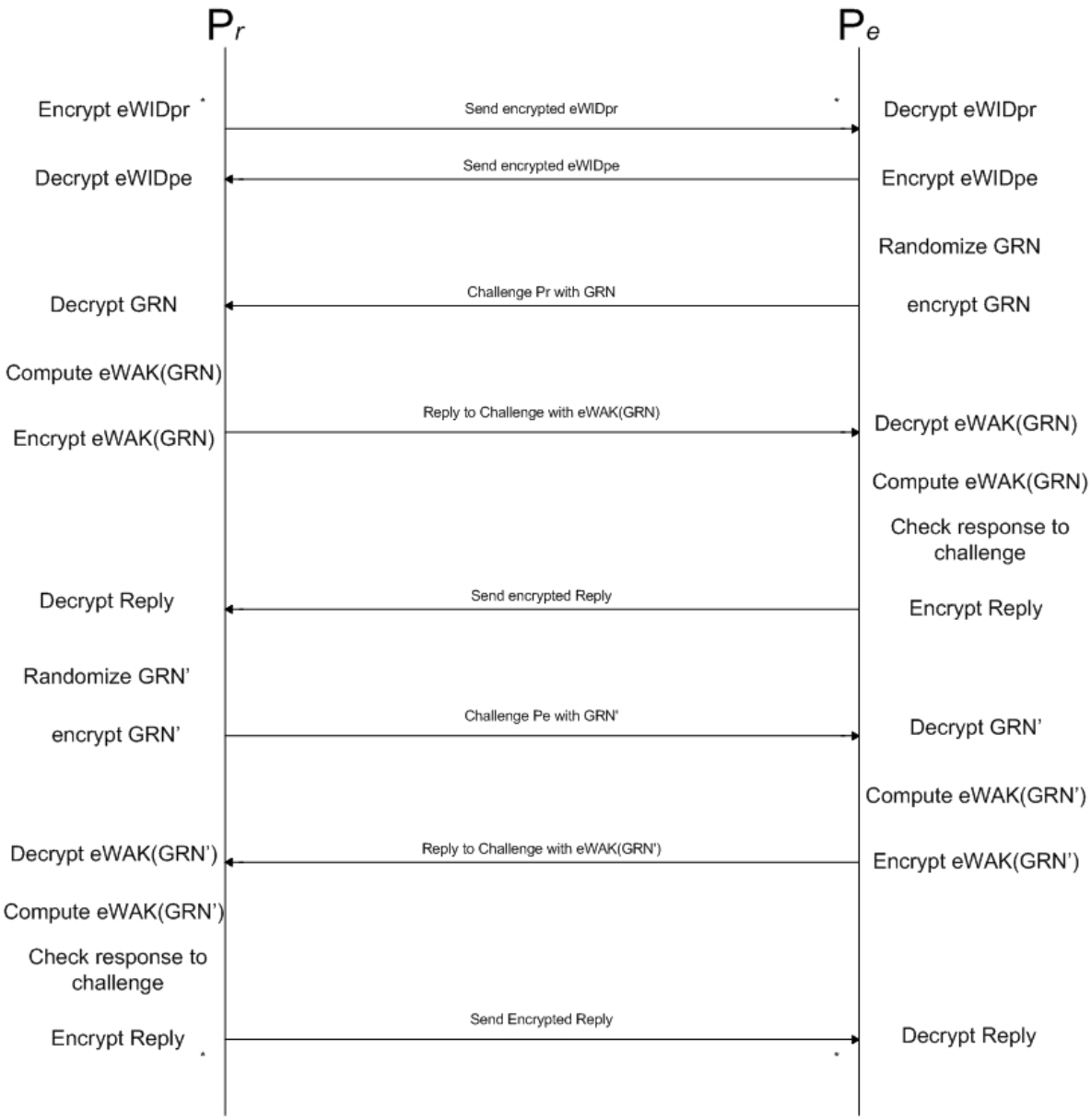

Figure 9 Verbal description of the proposed model on the VTS diagram

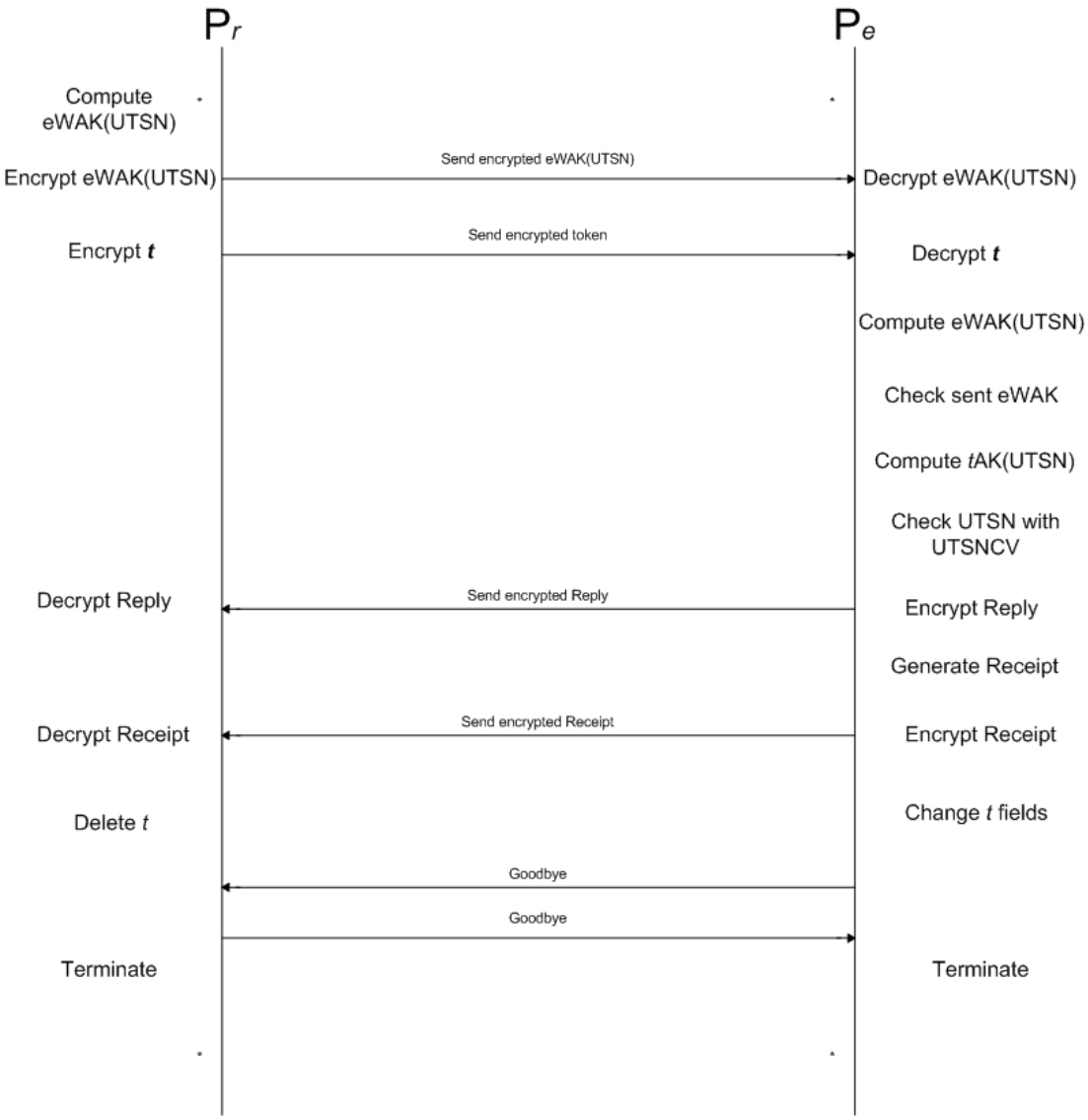

Figure 10 Verbal description of the proposed model on the VTS diagram (contd.)

The detailed formal description of the developed model on the VTS diagram is shown on Figure 11 and Figure 12.

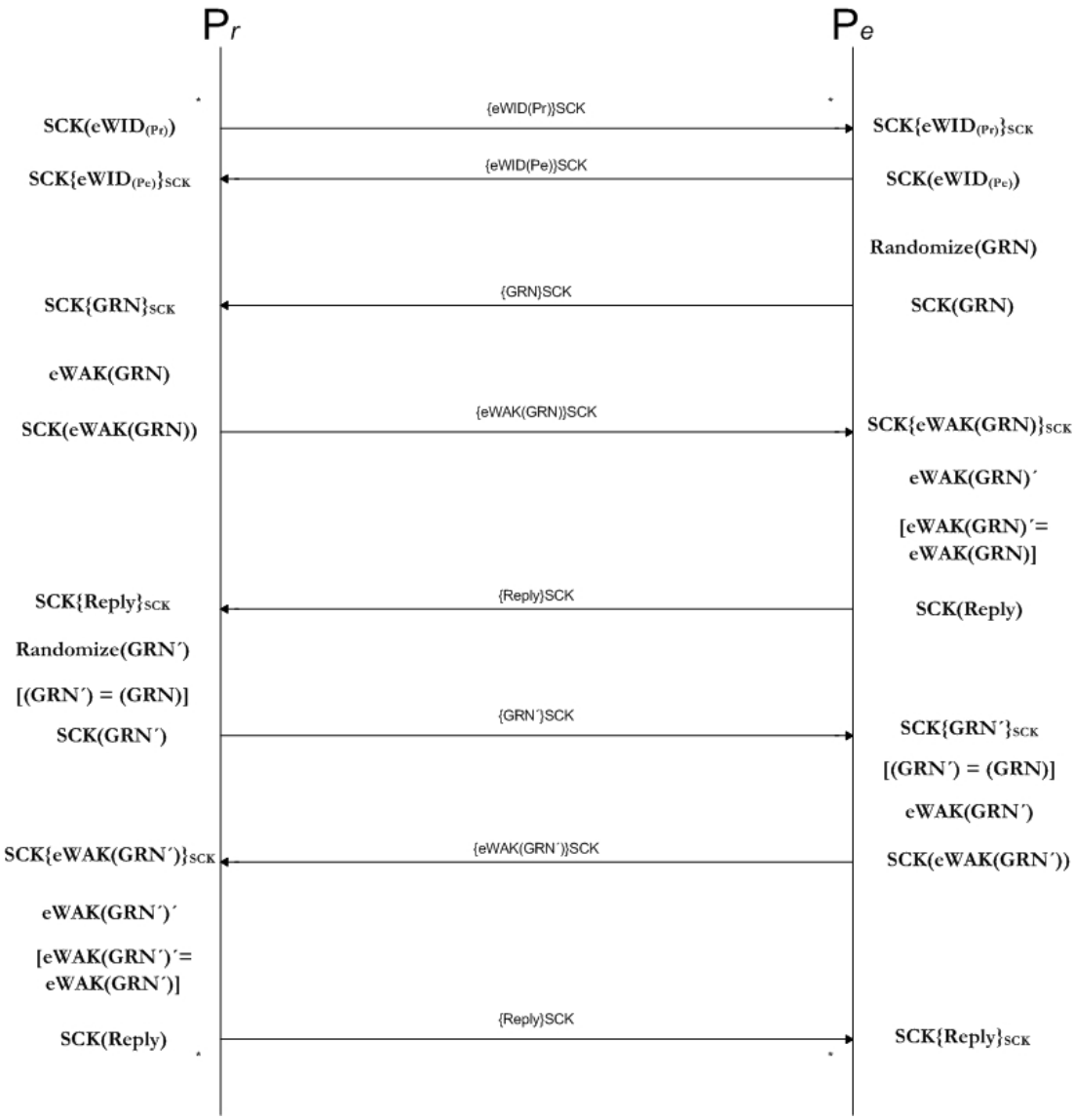

Figure 11 Detailed formal description of the proposed model on the VTS diagram

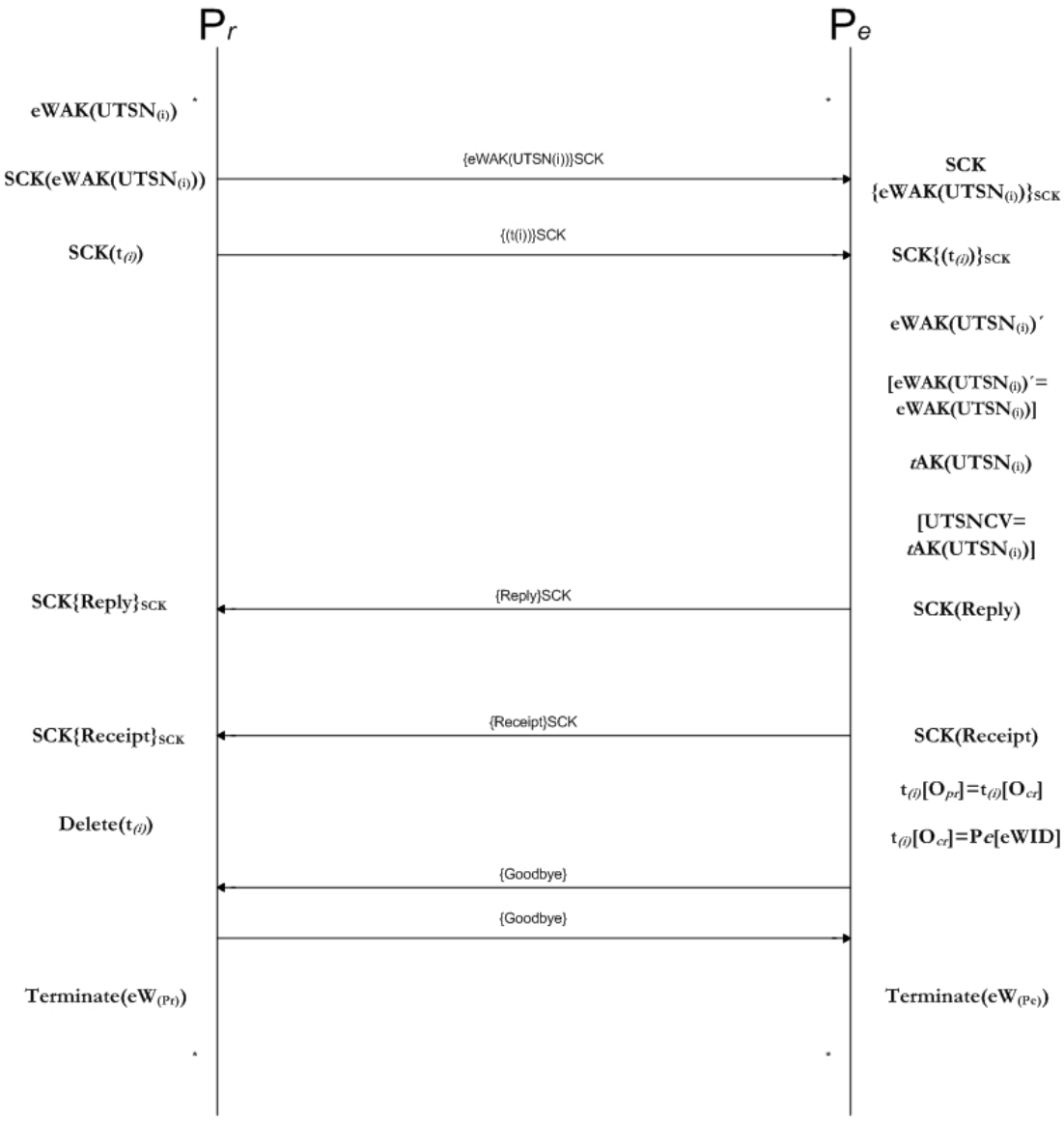

Figure 12 Detailed formal description of the proposed model on the VTS diagram (contd.)

5.3.2.1. Results of the VTS Diagram Analysis

Examining the VTS diagrams in Figure 11 and Figure 12 drawn for the Proposed Model, based on the guidelines described by Schmidt and Muller (1997), it is possible to obtain the results regarding the microeconomic, social and technological main headings. Table 17 gives these results combined with the results that Schmidt and Muller (1997) have obtained for DigiCash, First Virtual and SET. The findings of

Schmidt and Muller (1997) are included in this study to provide a comparison with respect to the obtained values of the developed model.

Table 17 Results according to the analysis in the VTS diagrams

	Requirements	DigiCash	FirstVirtual	SET	Proposed Model
		(electronic currency)	(third-party processing)	(secure credit Card transaction)	(Secure Co-Processors based)
Microeconomic	Low transaction costs	-	+	+	o
	Atomic exchange	-	-	-	+
	Customer base	-	-	o	o
Technological	Security	++	-	+	++
	Reliability	++	+	+	++
	Scalability	--	++	++	++
	Latency	+	-	--	++
Social	Peer-to-peer payments	**yes**	**Not implemented**	**no**	**yes**
	Grade of Anonymity	**full**	**some**	**some**	**full**

The qualitative evaluation is done by assigning the following values:
++ for best fulfillment of the requirement,
+ for good fulfillment of the requirement,
o for undecided,
- for bad fulfillment of the requirement,
-- for not meeting the requirement at all

Based on the findings in Table 17 we can conclude that the design objectives of the developed model, namely anonymity and off-line capability, have been satisfied in

extent, and due to its off-line capability, the proposed model does not face any technological costs such as latency, scalability or reliability. Regarding security, the developed model depends heavily upon hardware and cryptography security. If implemented correctly, then it also scores high in the security field. Finally, regarding the peer-to-peer payment and grade of anonymity features, it is obvious the similarity in scores regarding the DigiCash.

5.3.3. The Chi Evaluation Framework

The micropayment evaluation framework of Chi (1997), although not formally structured and described, is based upon three evaluation spectrums: the social features, the computation costs and the storage costs. This evaluation framework is particularly applicable to the proposed micropayment model, due to the fact that some comparisons can be made regarding the computational and storage costs of the proposed model with respect to other micropayment models, but also social aspects utilized by the proposed model, such as anonymity and off-line capability, can be evaluated.

Chi (1997) has examined four different micropayment schemes with respect to the proposed framework. These schemes are the Millicent (Glassman, et al., 1995), MicroMint (Rivest, Shamir, 1996), PayWord (Rivest, Shamir, 1996) and Wenbo Mao's simple cash (Mao, 96) payment technique. The findings of Chi are included in this study to provide a comparison with respect to the obtained values of the developed model.

5.3.3.1. Summary of the Features

The summary of the features of the four micropayment schemes by Chi (1997), plus the summary of the features of proposed model are given in Table 18. The

abbreviations of the table are: U: User (Pr), V: Vendor (Pe), B: Broker or Bank (IA), Cu: Customer Certificate, CSK: Customer Shared Key.

Table 18 Summary of the features of the five payment schemes

	Denomination	Produced by	Anonymity	Credit- or Debit-Based?
Millicent	V- or B-specific scrip	V and/or B	No	Debit to U, V and B
Micro-Mint	Coins satisfying monthly criterion, U_id, and V_id	B	No	Debit to U and B, credit to V
Payword	U-V-specific chains of paywords	U	No	Credit
Wenbo Scheme	Chains of coins	U, certified by B	Yes, if no double spending	Debit to U and B, credit to V
Proposed Model	i's with unique UTSN's and face value	B (IA)	Yes	Debit C (Pr)

As seen in Table 18, the proposed model is the only model within the five examined that ensures full anonymity without any risk of double-spending. This is a significant point, as anonymity had been a design objective while constructing the proposed model. Moreover, it should also be noted that the proposed model is a debit based model, as the micropayments, in our understanding, by nature are not economic for the utilization of credit payments.

5.3.3.2. Computation Costs

The Table 19 provides the summary of computational costs regarding each model. It is obvious that the proposed model is the most costly one with respect to

computation, as requires the execution of 7 hash functions, 12 message encryptions with symmetric key, 12 message decryptions with symmetric key and 2 randomizations only for the transfer of a single token. If more tokens are transferred, then the associated cost increases proportionally to the number of tokens to be transferred. Therefore, with respect to the other four micropayment methods, the proposed model definitely embodies higher computational costs.

Table 19 Summary of computation costs.

	Before Payment	For U, During Payment	V Verification	Redemption
Millicent	(assume C has V's scrip for payment already)	1 hash/request	1 hash/request verification 1 hash/V's scrip verification 1 hash/change generation 1 hash/reply generation	None
MicroMint (Assumes a coin is a U-V-specific k-tuple	1 hash and storage/valid x-value generated k-1 subtraction to locate the groups of x-values satisfying U_id k searches to get the groups of x-values	1 hash/V_id k-1 subtraction k searches/coin built	**For each coin:** k hashes of x-values k comparison for monthly criterion 2(k-1) subtraction 1 hash/ U_id 1 hash/V_id	Same as V's
Payword	1 request for Cu 1 verification for Cu 1 user signature generation/ commitment 1 hash/payword generation	(optional if not stored in advance) 1 hash/ payword generation	1 signature verification/ commitment 1 signature verification/ Cu #(paywords-paid) hashes	commitment verification Cu verification #(paywords-redeemed) hashes
Wenbo Scheme	1 request for Cu 1 blind signature for bank signature generation/chain 1 hash/coin generation 1 key/payment for using Schnorr's scheme	1 spending signature generation/ payment (optional if not stored in advance) 1 hash/ coin generation	1 bank signature verification 1 spending signature verification using Schnorr's signature scheme 1 verification for change from Vlast 1 signature generation or change #(coins-paid) hashes	1 bank signature verification previous V signature verification 1 change signature verification #(coins-paid) hashes
Proposed Model	4 hash operations (2 for Pr and 2 for Pe), 8 message encryptions with symmetric key, 8 message decryptions with the same symmetric key, 2 randomizations	**For each coin:** 1 hash operation, 2 message encryptions with symmetric key, 2 decryptions with symmetric key	**For each coin:** 2 hash operations, 2 message encryptions with symmetric key, 2 message decryptions with symmetric key	none
(Macropayment and double spending are excluded. Assume no frauds discovered during verification.)				

5.3.3.3. Storage Requirements

The Table 20 provides the storage requirements of the five micropayment models. Due to the off-line nature of the proposed model, all cryptographic keys (such as symmetric keys and hash functions) must exist in each eW, therefore requiring significant storage capacity. Furthermore, all tokens debited currently to that particular eW, must be stored on that eW, until they are transferred to the eW of the Pe. However, this also requires significant storage requirements in each eW, and therefore limits the maximum number of t's a eW can carry simultaneously. With respect to the other four models, the storage requirement of the proposed model is higher, and therefore requires thorough and careful storage planning and design.

Table 20 Summary of storage requirements

	Customer	Vendor	Broker
Millicent	Scrip purchased CSK	All V's valid scrip (CSK)	All B's valid scrip (V's scrip) CSK
MicroMint	Coins purchased	Valid received coins	All valid coins Customer purchase record
Payword	(Payword chain, commit-ments) CU **For each chain:** n, i, wn	All valid Plast's and M's received	All valid Plast's and M's redeemed
Wenbo Scheme	(coin chain) CU **For each chain:** bank signature, last coin, n, i, change from Vlast, and parameters for Schnorr's scheme	All valid signatures (and certificates)	All valid signatures (and certificates)
Proposed Model	All valid signatures (2 hash functions and 1 symmetric algorithm) Tokens currently debited to eW.	All valid signatures (2 hash functions and 1 symmetric algorithm) Tokens currently debited eW.	All valid signatures

CHAPTER 6

DISCUSSION AND CONCLUSION

"The killer application for electronic networks isn't video-on-demand. It's going to hit you where it really matters - in your wallet. It's, not only going to revolutionize the Net, it will change the global economy.

… At the worst, a faulty or crackable system of electronic money could lead to an economic Chernobyl."
(Levy, 1994)

6.1. Discussion

Today, money is almost everywhere and depends heavily on information systems, products and services, which shape the way money is issued, stored and circulated. New forms of money and payment types emerge under the overall heading of electronic money. Therefore, it is important to distinguish these new emerging monies, and while developing new electronic money models to focus on which properties are vital and should be exploited. This study has not only proposed an electronic money model, but has also given a framework that should be considered while new models for electronic payments are being developed.

Electronic money, no matter how much it relies on information systems, nevertheless is still money, and in order to be understood, first the notion of money should be defined. Classical definitions of money focus on the functions of money, promoting the fact that money is what money does. However, while selecting a medium to act as money, the properties of that medium become important, and need to be considered. Each money scores different with respect to these properties, and these properties differentiate a given form or type of money from the other existing monies. This study concludes that attributing importance to the properties of money rather than its functions will provide the necessary groundwork. However, not all properties of money are important at the same extent and each should be given a weight of importance while being considered. The developed model by this study has promoted the properties of security, anonymity and off-line capability.

Although much research exists on electronic money, most fail to justify the need for electronic money. This study argues that electronic money is a next step in the money evolution ladder, an evolution that has started with barter, displays similarities with the Lamarckian evolution of species and will continue until Pure Money is realized. Pure Money is a genuine idea of this research originally proposed to explain the extreme that the evolution of money will continue until no cost is associated any longer. However, Pure Money is not discussed in the necessary extent because the discussion is mainly economic, and is beyond the scope of this subject. The discussion of Pure Money in this research is based on a simple economy, so that further considerations such as exchange rates, tariffs, intermediary costs and etc. should not arise. A complete discussion of Pure Money should address all possible economic issues. Even though the described evolution of money in this study is a brief history, nevertheless it provides a

significant insight on how and why money has evolved over time. Although different views exist on how money was initiated and evolved, all views emphasize the similar main underlying motives, to improve the existing monies, and to minimize the existing costs. It should not be forgotten that as long as there is a cost associated with a money scheme, then there is always an opportunity for further development. Successful new monies fit better the requirements of the transacting parties with respect to previous monies, and eventually the satisfaction of the requirements determines the success of these monies. Similarly, the electronic money model in this study is developed to satisfy emerging unsatisfied needs of transacting parties.

Moreover, the electronic money model in this study was developed considering currently existing monies, the Pure Money and the gap existing between. The proposed model is intended to be a step forward in the money evolution ladder, not only with the transaction principles it proposes, but also with the overall underlying design methodologies and points of consideration.

The similarities of money evolution to Lamarckian evolution of species are meaningful. Not only a natural selection process has taken place between coexisting forms of money, also every new property introduced by a money, has been inherited by monies to follow. Thus, the properties of money today listed on this research, were not realized immediately with the very first monies, but have been introduced and developed over time. The Lamarckian evolution of money and the natural selection process that it embodies, should not be a debacle. On the contrary, the natural selection of the fittest and best among all monies to survive, may result to some individual monies to diminish, but will benefit the *race* (the money concept) in the long run.

However, the details of the Lamarckian evolution on the overall money evolution yet need to be clarified and discussed in the extent.

Money evolves, and it evolves to electronic money. However, the definitions of electronic money not only are many, but also differ significantly, resulting in confusion. The definition of electronic money is important because it provides another framework for developing electronic money schemes, but also points out the properties of money that need to be focused. In this research, credit cards and debit cards have not been considered as electronic money, but as electronic means of payment. In credit and debit cards the transacting parties do not exchange money, but information and credentials. The transfer of money from one account to another occurs in the Credit Card Company or Bank's computer centre. However, the concept of electronic money accepted in this study requires the physical transfer of electronic tokens that embody a value in themselves, from one transacting party to another, thus resulting to immediate clearing and settlement.

An ideal electronic money model would satisfy all possible payments, ranging from fractions of cent to amounts of thousands of dollars, or maybe higher. However, this is not the case in real life, we use cash for small payments, credit cards for larger purchases, and EFT or checks for amounts that are over the credit limit of the cards. Therefore, a decision was made regarding the payment category to be focused in this research. The electronic money proposed in this study has been developed mainly for micro and nano-payments. The rationale in this selection has been the fact that a significant volume of transactions are not being realized because they lack of the appropriate payment method. This method would provide almost no transactions costs,

so that payments small as a fraction of a cent would still be economically feasible and provide gains.

The definition of electronic money in this study requires two subjects to be covered, the on-line vs. off-line capability and anonymity vs. traceability. The developed model is an off-line capable payment model which honours anonymity and does not allow tracing to occur. Therefore, the model is not appropriate for payments larger than micropayments for several reasons. Although it provides acceptable security and satisfies the security requirements and considerations, allowing larger amounts to be transferred, would eventually attract more attacks. Moreover, as the amount carried in electronic wallets consists of tokens with predetermined face values, the ability to carry larger amounts would mean to carry more tokens, which would eventually require bigger storage. Finally, larger amounts than micropayments are currently satisfied in extent by credit and debit cards, and checks, thus diminishing any need for new payment types.

However, the increasing storage capacity of smart cards parallel to the future introduction of optical cards which can store extremely vast amount of data, the increasing bad credit history of individuals and the tendency to have one payment instrument to satisfy all payments, may require the proposed model to either satisfy larger payments or to eventually be wiped out, as the natural selection of species dictates.

The model in this study relies on two previous researches, the first one providing the possible hardware of the electronic wallets (Tygar, Yee, 1993) and the second one which has given the insight that payments can be conducted on tamper resistant devices with the use of counter-challenging (Stern, Vaudenay, 1997). The applicability of the model is highly dependent on the fact whether such tamper resistant

devices will be developed, and unless such devices are manufactured the model is very difficult to be utilized. All money schemes and payment types rely heavily on security and on the public notion that they provide unbreakable security, and if there is even a slight suspicion that the money in question fails in security aspects, then this money type will eventually lose public acceptability and will be wiped out. The security of the model in this study depends on cryptographic keys that are securely stored in the co-processors of tamper resistant devices. If such devices are not utilized, then the vital cryptographic keys would never be safeguarded in the required extent.

The developed model because of the small storage capacity of the media considered to be used as electronic wallets and the insignificant costs related to each transaction, is extremely appropriate for micropayments. This is displayed on the evaluation of the model with respect to two evaluation frameworks by Schmidt and Muller (1997) and Chi (1997). These two frameworks have been selected mainly because they address and evaluate electronic moneys with respect to properties that have been focused by the proposed model, namely anonymity and off-line capability. As previously displayed in section 5.3, the model scores high with respect to these evaluation frameworks. These frameworks draw attention on more abstract dimensions, such as the technological dimension, economic dimension and social dimension, rather than evaluating single computational complexities and costs. Therefore, the evaluation results with respect to these frameworks provide more understandable and brief conclusions. These conclusions can be summarized as that the proposed model, if implemented accordingly and providing the necessary hardware requirements should result in a real life payment instrument that with respect to the considerations of these evaluation frameworks would be a successful electronic payment scheme. The rationale in this

statement is that these two frameworks heavily depend and focus on the driving forces for the development of electronic payments.

This study provides further researchers in the area of electronic payments and money with a bunch of helpful approaches, tools, methodologies, development and evaluation frameworks, but most importantly than all these, ideas and insights, combining the disciplines of information technologies, economics and management.

Electronic money satisfying micropayments is a necessity and an undeniable fact. However, what needs to be questioned and discussed is, how these payments will be realized and satisfied, so that no party, neither the issuer nor the payer and payee is subject to costs exceeding their benefits. It is evident that, more models, similar to the one developed for the sake of this study, have been proposed and will continue. Some of these schemes will be materialized and will be undertaken. However, the markets and the overall economies in general will decide which should survive and which shall be doomed. Considering individual payment instruments, this natural selection process will be tough and merciless, but for the overall race of money, it shall be beneficial.

6.2. Future Work

A major future work to follow this study is the development of the complete and detailed payment protocol, which was briefly introduced in this research. The protocol to be developed should address the hardware issues of secure co-processors in detail, as the software to run upon this hardware, needs to utilize in maximum that hardware. Moreover, the model in this research describes the transfer of a single token, with any failure or attack cases discussed. A complete protocol should embody all alternative actions to be undertaken when abnormal situations, such as power loss, intrusions or attacks, early card removals etc., arise. Briefly, the model introduced in this

research should be exploited to its very detail, in order to obtain a complete model and protocol which can be developed.

While developing the model in its extent, possible mergers with existing payment types can be proposed and developed. An interesting approach could be the symbiosis of a credit instrument, debit instrument and micropayment instrument in a single electronic wallet (similar to a credit card built upon a smart card).

The economics and the business model of the proposed electronic money is an interesting research issue that was not covered in this research. As the proposed model addresses a part of the economy currently not realized, it turns out to be significant how such a model would affect the established economies and commerce, namely electronic commerce. Points to be covered can be the demand and supply, and the overall volume of electronic money appropriate for micropayments. Moreover, with very small benefits in question, but with high entry and fixed costs, the business viewpoint of this study provides an interesting subject to be covered.

Further research areas can be, as previously stated in this section, the analysis of Pure Money within the economics science and related considerations, such as the role of intermediaries and agents, the differentiation of the market, and etc.. The study can be carried out to define in its full extent the concept of Pure Money, taking as baseline the brief description provided by this study.

REFERENCES

(Anderson, et al., 1996) R. Anderson, C. Manifavas, C. Sutherland "Netcard - a practical electronic cash system", In Fourth Cambridge Workshop on Security Protocols. Springer Verlag, Lecture Notes in Computer Science, April 1996, available online URL http://www.cl.cam.ac.uk/users/rja14/

(Barreto) P. Barreto, "Cryptography Page", last seen online at 29 January 2004, available online URL http://planeta.terra.com.br/informatica/paulobarreto/

(Bıçakçı, 2003) K. Bıçakçı, "On the efficiency of authentication protocols, digital signatures and their applications in e-health: a top-down approach", PhD. Thesis, Informatics Institute, METU, September 2003.

(Birch, 1997) B. Dave; "The emerging cyberspace payments sectors: early experience and future predictions", Hyperion Systems Ltd., October 1997.

(Bootle, 2000) R. Bootle, "The Future of Electronic Money - Why the Nok will not replace the Dollar", Society of Business Economists, Business Economist Volume, Volume 32 No 1, 2000.

(Bosselaers, et al., 1996) A. Bosselaers, R. Govaerts, and J. Vandewalle, "Fast Hashing on the Pentium", Advances in Cryptology, Proceedings Crypto'96, LNCS 1109, N. Koblitz, Ed., Springer-Verlag, 1996, pp. 298-312.

(Camp, et al., 1995) L. J. Camp, M. Sirbu, and J. D. Tygar, "Token and Notational Money in Electronic Commerce", Proceedings of the First USENIX Workshop on Electronic Commerce, New York, New York, July 1995.

(Capie, et al., 2001) F. Capie, Y. Gormez and A. Stojanovic, "Emerging Electronic Money: Policy Issues & Relevance to Payment Systems in Emerging Economies", Draft, May 2001.

(Cardis) "Business issues related to buffered micropayments", Cardis Enterprises International B.V., last seen on 29 January 2003, available online URL: http://www.cardis-international.com/pdf/BusinessIssues.pdf

(Chaum, 1993) D. Chaum, "Achieving Electronic Privacy", Scientific American, pp. 96-101, August 1992.

(Chi, 1997) E. Chi, "Evaluation of Micropayment Schemes", HP Labs Technical Reports, 1997, available online URL http://www.hpl.hp.com/techreports/97/HPL-97-14.html

(Chou, et al., 2002) Y. Chou, C. Lee, J. Chung, "Understanding m-commerce payment systems through the analytic hierarchy process", Journal of Business Research, Published by Elsevier Science, 2002.

(Cochran, 1979) J. A. Cochran, "Money, banking and the economy", 4th ed., New York: Macmillan, c1979.

(Cox, et al., 1995) B. Cox, D. Tygar, M. Sirbu "NetBill security and transaction protocol" First USENIX Workshop on Electronic Commerce, New York, July 1995 available online URL http://www.ini.cmu/NETBILL/home.html

(Daemen, Rijmen, 2003) J. Daemen, V. Rijmen, "AES Proposal: Rijndael", The Advanced Encryption Standard, Springer-Verlag, 2003.

(Davies, 1994) G. Davies. "A history of money: from ancient times to the present day" Cardiff: University of Wales Press, 1994.

(Day, Beza, 1996) A. C. L. Day, S. T. Beza, "Money and income; an outline of monetary economics", New York, Oxford University Press, 1960.

(De Grauwe, 1997) P. de Grauwe, "The economics of monetary integration", 3rd rev. ed., Oxford; New York: Oxford University Press, 1997.

(Duisenberg, 2003) W. F. Duisenberg, "New economy, financial markets and monetary policy", Speech by Dr. Willem F. Duisenberg President of the European Central Bank, at the meeting of the Zürcher Volkswirtschaftliche Gesellschaft, Zurich, 19 May 2003.

(EconJournal, 2003) "Evolution of the conventional theory of money", EconJournal, available online URL http://www.econjournal.netfirms.com/finance/moneyevolution.htm, last updated April 25, 2003.

(Economist, 2000) "E-CASH 2.0", Economist, 00130613, 02/19/2000, Vol. 354, Issue 8158.

(Einzig, 1966) P. Einzig, "Primitive Money in its ethnological, historical, and economic aspects", 2nd ed., rev. and enl., Oxford, New York, Pergamon Press, 1966.

(Ely, 1996) B. Ely, "Electronic money and monetary policy: separating fact from fiction", Prepared for the Cato Institute's 14th Annual Monetary Conference, May 23, 1996, Washington, D.C.

(Encarta) Encyclopaedia Encarta, available online URL: http://encarta.msn.com/.

(Evans, Schmalensee, 1999) D. S. Evans, R. Schmalensee, "Paying with plastic: the digital revolution in buying and borrowing", Cambridge, Mass.: MIT Press, c1999.

(Fabozzi, et al., 1998) F. J. Fabozzi, F. Modigliani, M. G. Ferri, "Foundations of financial markets and institutions", 2nd ed., Upper Saddle River, N.J.: Prentice Hall, c1998.

(Friedman, 1994) M. Friedman, "Money mischief: episodes in monetary history", 1st Harvest ed. San Diego: Harcourt Brace & Co., 1994.

(Gabber, Silberschatz, 1996) E. Gabber, A. Silberschatz "Agora: A Minimal Distributed Protocol for Electronic Commerce" USENIX Workshop on E-Commerce, Oakland CA Nov. 1996.

(Gemmell, 1997) P. S. Gemmell, "Traceable e-cash", IEEE Spectrum, Volume: 34, Issue: 2, Feb. 1997, pp.35-37.

(Glassman, et al., 1995) S. Glassman, M. Manasse, M. Abadai, P. Gauthier, and P. Sobalvarro "The milicent protocol for inexpensive electronic commerce" In Proc. of the forth International World Wide Web Conference", 1995. available online URL http://www.research.digital.com/SRC/milicent

(Goldfinger, 2001) C. Goldfinger, "Money and economy: Electronic Money and intangible economy", e-article, last updated on: 23/07/2001 available online URL: http://www.fininter.net/OECD%20Money%20and%20economy.htm

(Gray, Reuter, 1993) J. Gray, A. Reuter, "Transaction Processing: Concepts and Techniques", Morgan Kaufmann Publishers; San Francisco, CA, 1993.

(Guthery, Jurgensen, 2002) S. B. Guthery, T. M. Jurgensen, "Smart cards: the developer's toolkit", Upper Saddle River, N.J.: Prentice Hall, 2002.

(Hancock, Humphrey, 1998) D. Hancock, D. B. Humphrey, "Payment transactions, instruments, and systems: A survey", Journal of Banking & Finance 21, 1998, pp. 1573-1624

(Hauser, et al., 1996) R. Hauser, M. Steiner, M. Waidner "Micropayments based on ikp" in 14th Worldwide Congress on Computer and Communication Security Protection, CNIT Paris La defense France, June 1996. available online URL

http://www.zurich.ibm.com./Technology/Security/publications/1996/HSW96-new.ps.gz

(Hayek, 1976) F. A. von Hayek, "Choice in currency: a way to stop inflation by F. A. Hayek; with commentaries by Ivor F. Pearce… [and others]", London: Institute of Economic Affairs, 1976.

(Hubbers, et al., 2002) E. Hubbers, M. Oostdijk, E. Poll, "Implementing a Formally Verifiable Security Protocol in Java Card", Nijmegen Institute for Information and Computing Sciences, 2002.

(Jarecki, Adlyzko, 1997) S. Jarecki, A. Adlyzko "An efficient micropayment system based on probabilistic polling" Conference proceedings of Financial Cryptography'97, Anguilla, BWI, February 1997

(Jones, 1997) R. Jones, "MilliCent Update – Presentation", MilliCent Marketing, Digital Equipment Corporation, 1997. Presented at the Electronic Payments Forum held March 2-3, 1998, in San Francisco.

(Jutla, Yung, 1996) C. Jutla, M. Yung "Paytree: amortized signature for flexible micropayments" In Second USENIX workshop on Electronic Commerce, November 1996.

(Kalakota, Whinston, 1996) R. Kalakota, A. B. Whinston, "Frontiers of the electronic commerce", Reading, Massachusetts: Addison-Wesley Publishing Company, Inc., 1996.

(Kaufman, 1981) G. G. Kaufman, "Money, the financial system, and the economy", 3rd ed., Boston: Houghton Mifflin, c1981

(Knudsen, 1998) J. B. Knudsen, "Java Cryptography", Sebastopol, Calif.: O'Reilly, c1998.

(Lawrence et al., 1998) E. Lawrence, et al. "Internet Commerce: Digital Models for Business", John Wiley & Sons Australia, 1998.

(Levy, 1994) Steven Levy, "E-Money (that's what I want)", Wired magazine, Issue 2-12, Dec. 1994, available online URL: http://www.wired.com/wired/archive/2.12/emoney_pr.html

(Lipton, Ostrovsky, 1998) R. J. Lipton and R. Ostrovsky, "Micro-Payments via efficient coin-flipping", in Proceedings of Second Financial Cryptography Conference '98, volume 1465 of Lecture Notes in Computer Science LNCS, February 1998

(Lockard, 1997) A. A. Lockard, "The Evolution of Money: The effects of Legal Restrictions and Technological Innovation", a research paper in partial

fulfilment of the requirements for the degree of Master of Arts in Economics, Trinity College Hartford, Connecticut, May 1997

(Madura, 2003) J. Madura, "Financial markets & institutions", 6th. Ed., Mason, Ohio: South-Western/Thomson Learning, c2003.

(Mao, 96) W. Mao, "A Simple Cash Payment Technique for the Internet", Proceedings of 1996 European Symposium on Research in Computer Science (ESORICS'96), Springer-Verlag, September 1996, available online URL: http://wenbomao.hpl.hp.com/esorics96.ps.

(Medvinsky, Neuman, 1994) G. Medvinsky, C. Neuman "NetCash: A design for practical electronic currency on the internet", in Proceeding sof the Second ACM Conference on Computer and Communcation Security Novemeber 1994.

(Menger, 1871) C. Menger, "Grundsätze der volkswirthschaftslehre", Wien, W. Braumüller, 1871.

(Merriam-Webster) Merriam-Webster Online dictionary, available online URL: http://www.webster.com/

(Micali, Rivest, 2002) S. Micali and R. L. Rivest, "Micropayments Revisited", Proceedings of the Cryptographer's Track at the RSA Conference 2002, Bart Preneel (ed.), Springer Verlag CT-RSA 2002, LNCS 2271, pages 149—163.

(Neuman, Medvinsky, 1995a) C. B. Neuman, G. Medvinsky, "NetCheque, NetCash, and the Characteristics of Internet Payment Services", paper presented at MIT workshop on Internet Economics, March 1995, University of Michigan Press.

(Neuman, Medvinsky, 1995b) C. Neuman, G. Medvinsky "Requirements for network payment: The Netcheque prospective" in Proc. of IEEE COMCON, March 1995 available online FTP ftp://prospero.isi/edu/pub/papers/security/

(Nitsche, 1970) R. Nitsche, "Money", London, Collins; New York, McGraw-Hill, 1970.

(Pifaretti, 1998) N. Pifaretti, "A theoretical approach to electronic money", Working papers, N. 302, February 1998, Faculty of Economic and Social Sciences, University of Fribourg, Switzerland.

(Rankl, Effing, 2000) W. Rankl, W. Effing, "Smart Card Handbook", translated by Kenneth Cox, 2nd ed., Chichester, England; New York: Wiley, c2000.

(Rivest, Shamir, 1996) R. L. Rivest, A. Shamir "Payword and micromint: Two simple micropayment schemes", In fourth Cambridge workshop on security protocols, Springer Verlag, lecture Notes in Computer Science, April 1996. available online URL http://theory.lcs.mit.edu/rivest/publications.html

(Rivest, 1997) R. L. Rivest "Lottery tickets as Micro-Cash", rump session talk at Financial Cryptography'97, February 1997, Anguilla, BWI.

(Rivest, 2002) R. L. Rivest, S. Micali, "Micropayments Revisited", Presentation for the RSA Conference 2002.

(Rogers, 1974) A. J. Rogers, "Choice, an introduction to economics", 2nd ed., Englewood Cliffs, N.J., Prentice-Hall, 1974.

(RSA) RSA Security. "What are micropayments", RSA Security Crypto FAQ, available online URL: http://www.rsasecurity.com/rsalabs/4-2-5000.htm.

(Rumbough et al. 1991) J. Rumbaugh, M. Blaha, W. Premerlani, F. Eddy, W. Lorenson, "Object Oriented Modelling and Design", Prentice Hall, 1991.

(Schmidt, Muller, 1997) C. Schmidt, R. Muller, "A framework for micropayment evaluation", Netnomics, 1999, 1, S. 187-200.

(Schneier, 1996) B. Schneier, "Applied Cryptography, Second Edition: Protocols, Algorthms, and Source Code in C (cloth)", John Wiley and Sons, Inc. 1996.

(Schubert, Zimmermann, 1998) P. Schubert, H-D. Zimmermann, "Electronic Commerce transactions: The deployment of chip cards for micropayment settlements", Institute for Information Management, University of St. Gallen, Switzerland, p.2, 1998.

(Sefton, 2001) Personal correspondence, Kevin Sefton, Director, Smartcreds Limited. Tue, 6 Nov 2001

(Smant, 2002) D. J. C. Smant, "Lectures notes on Credit and Banking", EUR A1604, October 2002, available online URL: http://www.few.eur.nl/few/people/smant/a1604/notes/c1_money1-paym.pdf

(Smith, 1776) A. Smith, "An inquiry into the nature and causes of the wealth of nations", London, Printed for W. Strahan and T. Cadell, 1776.

(Smith, 1996) S. W. Smith, "Secure Coprocessing Applications and Research Issues", Computer Research and Applications Group (CIC-3), Los Alamos National Laboratory, Los Alamos Unclassified Release LA-UR-96-2805, August 1996.

(Singh, 1999) S. Singh, "Electronic money: understanding its use to increase the effectiveness of policy", Telecommunications Policy 23, pp. 753-773, 1999.

(Stern, Vaudenay, 1997) J. Stern, S. Vaudenay "Small-Value-Payment: a Flexible Micropayment Scheme", Conference proceedings of Financial Cryptography'97, February 1997, Anguilla, BWI.

(Tang, Low, 1996) L. Tang, S. Low "Chrg-http: A Tool for Micropayments on the World Wide Web", 6th USENIX Security Symposium, San Jose, CA July 1996.

(Tang, 1995) L. Tang, "A Set of Protocols for Micropayments in Distributed Systems" Proceedings of the First USENIX Workshop on Electronic Commerce New York, New York, July 1995

(Tygar, Yee, 1993) J. D.Tygar and B. S.Yee. "Dyad: A System for Using Physically Secure Coprocessors." Proceedings of the Joint Harvard-MIT Workshop on Technological Strategies for the Protection of Intellectual Property in the Network Multimedia Environment, April 1993.

(Von Mises, 1953) L. Von Mises, "The theory of money and credit", (translated from the German by H. E. Batson), New ed., New Haven, Yale University Press, 1953.

(Walker, 1883) F. A. Walker, "Money in its relations to trade and industry", New York: Henry Holt and Co., 1883.

(Web Ref1) VISA and MASTERCARD "Secure Electronic Transactions (SET) specification", available online URL http://www.mastercard.com/set

(Web Ref2) Mondex USA, available online URL http://www2.mondexusa.com/

(Web Ref3) "Secure Hash Standard", NIST FIPS 180-1, available online URL http://www.itl.nist.gov/fipspubs/fip180-1.htm

(Web Ref4) Virtual PIN of First Virtual, available online URL http://www.fv.com

(Web Ref5) FIPS 140-2, "Security Requirements for Cryptographic Modules", available online URL: http://csrc.nist.gov/cryptval/140-2.htm

(Web Ref6) RFC 1750, "Randomness Recommendations for Security", available online URL: http://www.ietf.org/rfc/rfc1750.txt

(Wheeler, 1996) D. Wheeler "Transactions using bets", in security protocols Int.Workshop, Cambridge, UK April 1996. In LNCS 1189 pp. 89-92 available online URL http://www.cl.cam.ac.uk/users/cm213/Project/project publ.html

(White, 1996) L. H. White, "The Technology Revolution and Monetary Evolution", in The Future of Money in the Information Age, Cato Institute's 14th Annual Monetary Conference, May 23, 1996, Washington, D.C.

(Yacobi, 1997) Y. Yacobi "On the continuum between on-line and off-line e-cash systems – I", Conference proceedings of Financial Cryptography'97, Anguilla, February 1997

APPENDIX A

MAIN PROGRAM

The code segment (UhusThesis.java) which is the main program representing the structure of the proposed model and controls and calls the eWAK, SCK and *t*AK keys is given below:

```
import javax.crypto.*;
import java.security.*;

public class uhusThesis{
	static Rijndael rijn;
	public byte[] SCKencrypt(byte[] message, byte[] key) {
		byte[] cipherText = cropByteArray((new String("")).getBytes(),1024);
		rijn.encrypt(cropByteArray(message,1024), cipherText);
		return cipherText;
	}
	public byte[] SCKdecrypt(byte[] message, byte[] key) {
		byte[] plainText = cropByteArray((new String("")).getBytes(), 1024);
		rijn.decrypt(message, plainText);
		return plainText;
	}
	public byte[] randomize(int size) {
		SecureRandom sr = null;
		try {
			sr = SecureRandom.getInstance("SHA1PRNG", "SUN");
		} catch(Exception e) {
			e.printStackTrace();
			System.out.println("No such algorithm...");
		}
		byte bytes[] = new byte[size/8];
```

```
		sr.nextBytes(bytes);
		return bytes;
	}

	public byte[] eWAK(byte[] message) {
		MessageDigest messageDigest = null;
		try {
			messageDigest = MessageDigest.getInstance("SHA-1");
		} catch(Exception e) {
			e.printStackTrace();
			System.out.println("No such algorithm...");
		}
		messageDigest.update(message);
		message = messageDigest.digest();
		return message;
	}

	public byte[] tAK(byte[] message) {
		return eWAK(message);
	}
	public byte[] cropByteArray(byte[] input, int size) {
		byte[] returnArray = new byte[size];
		for (int i=0; i<returnArray.length; i++) {
			returnArray[i] = (new Byte("5")).byteValue();
		}
		for (int i=0; i<input.length; i++) {
			returnArray[i] = input[i];
		}
		return returnArray;
	}
	public void uhusThesis() {
	}

	public void executecode() {

		//instantiate Rijndael
		rijn = new Rijndael();
		Token token = new Token();
		token.initialize();

		//define IDs named eWIDpr and eWIDpe
		byte[] eWIDpr, eWIDpe;
		eWIDpr = cropByteArray((new String("0")).getBytes(), 1024);
		eWIDpe = cropByteArray((new String("1")).getBytes(), 1024);

		//common SCK key
		byte[] key  = randomize(1024);
		//initialize Rijndael key
```

```
rijn.makeKey(key, key.length);


//define storage for temporary cipher/plain text
byte[] message = new byte[1024];
byte[] hashRandomNumberPe = new byte[1024];
byte[] hashRandomNumberPePrime = new byte[1024];
byte[] hashRandomNumberPr = new byte[1024];
byte[] hashRandomNumberPrPrime = new byte[1024];
byte[] hashUTSN = new byte[1024];
byte[] hashUTSNPrime = new byte[1024];

//define storage for random number
byte[] randomNumberPe = new byte[1024];
byte[] randomNumberPr = new byte[1024];

byte[] reply = new byte[1024];
byte[] receipt = new byte[1024];

receipt = cropByteArray((new String("")).getBytes(), 1024);
//encrypt eWIDpr using SCK

message = SCKencrypt(eWIDpr, key);

//decrypt eWIDpr using SCK
SCKdecrypt(message, key);

//encrypt eWIDpe using SCK
message = SCKencrypt(eWIDpe, key);

//decrypt eWIDpe using SCK
SCKdecrypt(message, key);

//generate GRNpe (a random number for pe)
randomNumberPe = randomize(1024);

//encrypt GRNpe using SCK
message = SCKencrypt(randomNumberPe, key);

//decrypt GRNpe using SCK
randomNumberPe = SCKdecrypt(message, key);

//hash GRNpe using eWAK -->eWAK(GRNpe)
hashRandomNumberPe = eWAK(randomNumberPe);

//encrypt GRNpe using SCK
message = SCKencrypt(hashRandomNumberPe, key);
```

```
//descrypt GRNpe using SCK
hashRandomNumberPe = SCKdecrypt(message, key);

//hash GRNpe using eWAK -->eWAK(GRNpe')
hashRandomNumberPePrime = eWAK(randomNumberPe);

//compare (eWAK(GRNpe)) with (eWAK(GRNpe')
if (hashRandomNumberPePrime.equals(hashRandomNumberPe)) {
        reply = cropByteArray((new String("true")).getBytes(), 1024);
} else {
        reply = cropByteArray((new String("false")).getBytes(), 1024);
}

//encrypt Reply
message = SCKencrypt(reply, key);

//decrypt Reply
SCKdecrypt(message, key);



//generate GRNpr (a random number for pr)
randomNumberPr = randomize(1024);

//Compare (GRNpr) with (GRNpe)
if (randomNumberPe == randomNumberPr) {
}

//encrypt GRNpr using SCK
message = SCKencrypt(randomNumberPr, key);

//decrypt GRNpr using SCK
randomNumberPr = SCKdecrypt(message, key);

//Compare (GRNpr) with (GRNpe)
if (randomNumberPe == randomNumberPr) {
}

//hash GRNpr using eWAK -->eWAK(GRNpr)
hashRandomNumberPr = eWAK(randomNumberPr);

//encrypt GRNpr using SCK
message = SCKencrypt(hashRandomNumberPr, key);

//descrypt GRNpr using SCK
hashRandomNumberPr = SCKdecrypt(message, key);

//hash GRNpr using eWAK -->eWAK(GRNpr')
```

```
hashRandomNumberPrPrime = eWAK(randomNumberPr);

//compare (eWAK(GRNpr)) with (eWAK(GRNpr')
if (hashRandomNumberPrPrime.equals(hashRandomNumberPr)) {
        reply = cropByteArray((new String("true")).getBytes(), 1024);
} else {
        reply = cropByteArray((new String("false")).getBytes(), 1024);
}

//encrypt Reply
message = SCKencrypt(reply, key);

//decrypt Reply
SCKdecrypt(message, key);

//hash UTSN(i) using eWAK -->eWAK(UTSN(i))
hashUTSN = eWAK(token.getUTSN());

//encrypt eWAK(UTSN(i)) using SCK
message = SCKencrypt(hashUTSN, key);

//decrypt eWAK(UTSN(i)) using SCK
hashUTSN = SCKdecrypt(message, key);

//encrypt token(i) using SCK
message = SCKencrypt(token.getAll(), key);

//decrypt token(i) using SCK
SCKdecrypt(message, key);

//hash UTSN(i) using eWAK -->eWAK(UTSN(i))'
hashUTSNPrime = eWAK(token.getUTSN());

//compare (eWAK(UTSN(i))) with (eWAK(UTSN(i))')
if (hashUTSN == hashUTSNPrime) {
}

//hash UTSN(i) usin tAK -->tAK(UTSN(i))
hashUTSN = tAK(token.getUTSN());

//compare tAK(UTSN(i)) with UTSNCV
if (hashUTSN.equals(token.getUTSNCV())) {
        reply = cropByteArray((new String("true")).getBytes(), 1024);
} else {
        reply = cropByteArray((new String("false")).getBytes(), 1024);
}

//encrypt Reply using SCK
```

```
                message = SCKencrypt(reply, key);

                //decrypt Reply using SCK
                SCKdecrypt(message, key);

                //encrypt Receipt using SCK
                message = SCKencrypt(receipt, key);

                //decrypt Receipt using SCK
                SCKdecrypt(message, key);



        }

        public static void main(String args[]) {
                time1 = new int[256];
                time1 = GetCurrentThreadCpuTime();
                uhusThesis ut = new uhusThesis();
                ut.executecode();

        }

}
```

APPENDIX B

CODE FOR SCK

The code segment (Rijndael.java) of the Optimised Java implementation of the Rijndael (AES) block cipher, written by Paulo Barreto, is given below:

```
/**
 * Rijndael.java
 *
 * @version 1.0 (May 2001)
 *
 * Optimised Java implementation of the Rijndael (AES) block cipher.
 *
 * @author Paulo Barreto <paulo.barreto@terra.com.br>
 *
 * This software is hereby placed in the public domain.
 *
 * THIS SOFTWARE IS PROVIDED BY THE AUTHOR "AS IS" AND ANY EXPRESS
 * OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED
 * WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
 * ARE DISCLAIMED.  IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE
 * LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
 * CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF
 * SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR
```

```
 * BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY,
 * WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE
 * OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE,
 * EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
 */
public final class Rijndael {

    public Rijndael() {
    }

    /**
     * Flag to setup the encryption key schedule.
     */
    public static final int DIR_ENCRYPT = 1;

    /**
     * Flag to setup the decryption key schedule.
     */
    public static final int DIR_DECRYPT = 2;

    /**
     * Flag to setup both key schedules (encryption/decryption).
     */
    public static final int DIR_BOTH    = (DIR_ENCRYPT|DIR_DECRYPT);

    /**
     * AES block size in bits
     * (N.B. the Rijndael algorithm itself allows for other sizes).
     */
    public static final int BLOCK_BITS  = 128;

    /**
     * AES block size in bytes
     * (N.B. the Rijndael algorithm itself allows for other sizes).
     */
    public static final int BLOCK_SIZE  = (BLOCK_BITS >>> 3);

    /**
     * Substitution table (S-box).
     */
    private static final String SS =
        "\u637C\u777B\uF26B\u6FC5\u3001\u672B\uFED7\uAB76" +
        "\uCA82\uC97D\uFA59\u47F0\uADD4\uA2AF\u9CA4\u72C0" +
        "\uB7FD\u9326\u363F\uF7CC\u34A5\uE5F1\u71D8\u3115" +
        "\u04C7\u23C3\u1896\u059A\u0712\u80E2\uEB27\uB275" +
```

```
        "\u0983\u2C1A\u1B6E\u5AA0\u523B\uD6B3\u29E3\u2F84" +
        "\u53D1\u00ED\u20FC\uB15B\u6ACB\uBE39\u4A4C\u58CF" +
        "\uD0EF\uAAFB\u434D\u3385\u45F9\u027F\u503C\u9FA8" +
        "\u51A3\u408F\u929D\u38F5\uBCB6\uDA21\u10FF\uF3D2" +
        "\uCD0C\u13EC\u5F97\u4417\uC4A7\u7E3D\u645D\u1973" +
        "\u6081\u4FDC\u222A\u9088\u46EE\uB814\uDE5E\u0BDB" +
        "\uE032\u3A0A\u4906\u245C\uC2D3\uAC62\u9195\uE479" +
        "\uE7C8\u376D\u8DD5\u4EA9\u6C56\uF4EA\u657A\uAE08" +
        "\uBA78\u252E\u1CA6\uB4C6\uE8DD\u741F\u4BBD\u8B8A" +
        "\u703E\uB566\u4803\uF60E\u6135\u57B9\u86C1\u1D9E" +
        "\uE1F8\u9811\u69D9\u8E94\u9B1E\u87E9\uCE55\u28DF" +
        "\u8CA1\u890D\uBFE6\u4268\u4199\u2D0F\uB054\uBB16";

    private static final byte[]
        Se = new byte[256];

    private static final int[]
        Te0 = new int[256],
        Te1 = new int[256],
        Te2 = new int[256],
        Te3 = new int[256];

    private static final byte[]
        Sd = new byte[256];

    private static final int[]
        Td0 = new int[256],
        Td1 = new int[256],
        Td2 = new int[256],
        Td3 = new int[256];

    /**
     * Round constants
     */
    private static final int[]
        rcon = new int[10]; /* for 128-bit blocks, Rijndael never uses more than 10 rcon
values */

    /**
     * Number of rounds (depends on key size).
     */
    private int Nr = 0;

    private int Nk = 0;

    private int Nw = 0;

    /**
```

```
 * Encryption key schedule
 */
private int rek[] = null;

/**
 * Decryption key schedule
 */
private int rdk[] = null;

static {
   /*
      Te0[x] = Se[x].[02, 01, 01, 03];
      Te1[x] = Se[x].[03, 02, 01, 01];
      Te2[x] = Se[x].[01, 03, 02, 01];
      Te3[x] = Se[x].[01, 01, 03, 02];

      Td0[x] = Sd[x].[0e, 09, 0d, 0b];
      Td1[x] = Sd[x].[0b, 0e, 09, 0d];
      Td2[x] = Sd[x].[0d, 0b, 0e, 09];
      Td3[x] = Sd[x].[09, 0d, 0b, 0e];
   */
   int ROOT = 0x11B;
   int s1, s2, s3, i1, i2, i4, i8, i9, ib, id, ie, t;
   for (i1 = 0; i1 < 256; i1++) {
      char c = SS.charAt(i1 >>> 1);
      s1 = (byte)((i1 & 1) == 0 ? c >>> 8 : c) & 0xff;
      s2 = s1 << 1;
      if (s2 >= 0x100) {
         s2 ^= ROOT;
      }
      s3 = s2 ^ s1;
      i2 = i1 << 1;
      if (i2 >= 0x100) {
         i2 ^= ROOT;
      }
      i4 = i2 << 1;
      if (i4 >= 0x100) {
         i4 ^= ROOT;
      }
      i8 = i4 << 1;
      if (i8 >= 0x100) {
         i8 ^= ROOT;
      }
      i9 = i8 ^ i1;
      ib = i9 ^ i2;
      id = i9 ^ i4;
      ie = i8 ^ i4 ^ i2;
```

```
            Se[i1] = (byte)s1;
            Te0[i1] = t = (s2 << 24) | (s1 << 16) | (s1 << 8) | s3;
            Te1[i1] = (t >>>  8) | (t  << 24);
            Te2[i1] = (t >>> 16) | (t  << 16);
            Te3[i1] = (t >>> 24) | (t  <<  8);

            Sd[s1] = (byte)i1;
            Td0[s1] = t = (ie << 24) | (i9 << 16) | (id << 8) | ib;
            Td1[s1] = (t >>>  8) | (t  << 24);
            Td2[s1] = (t >>> 16) | (t  << 16);
            Td3[s1] = (t >>> 24) | (t  <<  8);
                    }
        /*
         * round constants
         */
        int r = 1;
        rcon[0] = r << 24;
        for (int i = 1; i < 10; i++) {
            r <<= 1;
            if (r >= 0x100) {
                r ^= ROOT;
            }
            rcon[i] = r << 24;
        }
    }

    /**
     * Expand a cipher key into a full encryption key schedule.
     *
     * @param   cipherKey   the cipher key (128, 192, or 256 bits).
     */
    private void expandKey(byte[] cipherKey) {
        int temp, r = 0;
        for (int i = 0, k = 0; i < Nk; i++, k += 4) {
            rek[i] =
                ((cipherKey[k    ]       ) << 24) |
                ((cipherKey[k + 1] & 0xff) << 16) |
                ((cipherKey[k + 2] & 0xff) <<  8) |
                ((cipherKey[k + 3] & 0xff));
        }
        for (int i = Nk, n = 0; i < Nw; i++, n--) {
            temp = rek[i - 1];
            if (n == 0) {
                    n = Nk;
                temp =
                    ((Se[(temp >>> 16) & 0xff]       ) << 24) |
                    ((Se[(temp >>>  8) & 0xff] & 0xff) << 16) |
                    ((Se[(temp       ) & 0xff] & 0xff) <<  8) |
```

```
                ((Se[(temp >>> 24)       ] & 0xff));
            temp ^= rcon[r++];
        } else if (Nk == 8 && n == 4) {
            temp =
                ((Se[(temp >>> 24)       ]       ) << 24) |
                ((Se[(temp >>> 16) & 0xff] & 0xff) << 16) |
                ((Se[(temp >>>  8) & 0xff] & 0xff) <<  8) |
                ((Se[(temp       ) & 0xff] & 0xff));
        }
        rek[i] = rek[i - Nk] ^ temp;
    }
    temp = 0;
}

        /*
         * Faster implementation of the key expansion
         * (only worthwhile in Rijndael is used in a hashing function mode).
         */
        /*
private void expandKey(byte[] cipherKey) {
    int keyOffset = 0;
            int i = 0;
            int temp;

    rek[0] =
        (cipherKey[ 0]       ) << 24 |
        (cipherKey[ 1] & 0xff) << 16 |
        (cipherKey[ 2] & 0xff) <<  8 |
        (cipherKey[ 3] & 0xff);
            rek[1] =
        (cipherKey[ 4]       ) << 24 |
        (cipherKey[ 5] & 0xff) << 16 |
        (cipherKey[ 6] & 0xff) <<  8 |
        (cipherKey[ 7] & 0xff);
            rek[2] =
        (cipherKey[ 8]       ) << 24 |
        (cipherKey[ 9] & 0xff) << 16 |
        (cipherKey[10] & 0xff) <<  8 |
        (cipherKey[11] & 0xff);
            rek[3] =
        (cipherKey[12]       ) << 24 |
        (cipherKey[13] & 0xff) << 16 |
        (cipherKey[14] & 0xff) <<  8 |
        (cipherKey[15] & 0xff);
            if (Nk == 4) {
                for (;;) {
                        temp = rek[keyOffset + 3];
                        rek[keyOffset + 4] = rek[keyOffset] ^
```

```
                        ((Se[(temp >>> 16) & 0xff]       ) << 24) ^
                        ((Se[(temp >>>  8) & 0xff] & 0xff) << 16) ^
            ((Se[(temp       ) & 0xff] & 0xff) <<  8) ^
            ((Se[(temp >>> 24)       ] & 0xff)      ) ^
                        rcon[i];
                rek[keyOffset + 5] = rek[keyOffset + 1] ^ rek[keyOffset + 4];
                rek[keyOffset + 6] = rek[keyOffset + 2] ^ rek[keyOffset + 5];
                rek[keyOffset + 7] = rek[keyOffset + 3] ^ rek[keyOffset + 6];
                if (++i == 10) {
                        return;
                }
                keyOffset += 4;
            }
        }
rek[keyOffset + 4] =
    (cipherKey[16]       ) << 24 |
    (cipherKey[17] & 0xff) << 16 |
    (cipherKey[18] & 0xff) <<  8 |
    (cipherKey[19] & 0xff);
        rek[keyOffset + 5] =
    (cipherKey[20]       ) << 24 |
    (cipherKey[21] & 0xff) << 16 |
    (cipherKey[22] & 0xff) <<  8 |
    (cipherKey[23] & 0xff);
        if (Nk == 6) {
            for (;;) {
                temp = rek[keyOffset + 5];
                rek[keyOffset +  6] = rek[keyOffset] ^
            ((Se[(temp >>> 16) & 0xff]       ) << 24) ^
            ((Se[(temp >>>  8) & 0xff] & 0xff) << 16) ^
            ((Se[(temp       ) & 0xff] & 0xff) <<  8) ^
            ((Se[(temp >>> 24)       ] & 0xff)      ) ^
            rcon[i];
                rek[keyOffset +  7] = rek[keyOffset +  1] ^ rek[keyOffset +  6];
                rek[keyOffset +  8] = rek[keyOffset +  2] ^ rek[keyOffset +  7];
                rek[keyOffset +  9] = rek[keyOffset +  3] ^ rek[keyOffset +  8];
                if (++i == 8) {
                        return;
                }
                rek[keyOffset + 10] = rek[keyOffset +  4] ^ rek[keyOffset +  9];
                rek[keyOffset + 11] = rek[keyOffset +  5] ^ rek[keyOffset + 10];
                keyOffset += 6;
            }
        }
rek[keyOffset + 6] =
    (cipherKey[24]       ) << 24 |
    (cipherKey[25] & 0xff) << 16 |
    (cipherKey[26] & 0xff) <<  8 |
```

```
        (cipherKey[27] & 0xff);
           rek[keyOffset + 7] =
        (cipherKey[28]      ) << 24 |
        (cipherKey[29] & 0xff) << 16 |
        (cipherKey[30] & 0xff) <<  8 |
        (cipherKey[31] & 0xff);
           if (Nk == 8) {
        for (;;) {
                temp = rek[keyOffset +  7];
                rek[keyOffset +  8] = rek[keyOffset] ^
              ((Se[(temp >>> 16) & 0xff]      ) << 24) ^
              ((Se[(temp >>>  8) & 0xff] & 0xff) << 16) ^
              ((Se[(temp       ) & 0xff] & 0xff) <<  8) ^
              ((Se[(temp >>> 24)       ] & 0xff)      ) ^
              rcon[i];
                rek[keyOffset +  9] = rek[keyOffset +  1] ^ rek[keyOffset +  8];
                rek[keyOffset + 10] = rek[keyOffset +  2] ^ rek[keyOffset +  9];
                rek[keyOffset + 11] = rek[keyOffset +  3] ^ rek[keyOffset + 10];
                        if (++i == 7) {
                                return;
                        }
                temp = rek[keyOffset + 11];
                rek[keyOffset + 12] = rek[keyOffset +  4] ^
                        ((Se[(temp >>> 24)       ]       ) << 24) ^
                        ((Se[(temp >>> 16) & 0xff] & 0xff) << 16) ^
                        ((Se[(temp >>>  8) & 0xff] & 0xff) <<  8) ^
                        ((Se[(temp       ) & 0xff] & 0xff));
                rek[keyOffset + 13] = rek[keyOffset +  5] ^ rek[keyOffset + 12];
                rek[keyOffset + 14] = rek[keyOffset +  6] ^ rek[keyOffset + 13];
                rek[keyOffset + 15] = rek[keyOffset +  7] ^ rek[keyOffset + 14];
                        keyOffset += 8;
        }
           }
}
*/

/**
 * Compute the decryption schedule from the encryption schedule .
 */
private void invertKey() {
   int d = 0, e = 4*Nr, w;
         /*
    * apply the inverse MixColumn transform to all round keys
    * but the first and the last:
    */
   rdk[d    ] = rek[e    ];
   rdk[d + 1] = rek[e + 1];
   rdk[d + 2] = rek[e + 2];
```

```
        rdk[d + 3] = rek[e + 3];
            d += 4;
            e -= 4;
            for (int r = 1; r < Nr; r++) {
        w = rek[e    ];
                rdk[d    ] =
                        Td0[Se[(w >>> 24)       ] & 0xff] ^
                        Td1[Se[(w >>> 16) & 0xff] & 0xff] ^
                        Td2[Se[(w >>>  8) & 0xff] & 0xff] ^
                        Td3[Se[(w       ) & 0xff] & 0xff];
        w = rek[e + 1];
                rdk[d + 1] =
                        Td0[Se[(w >>> 24)       ] & 0xff] ^
                        Td1[Se[(w >>> 16) & 0xff] & 0xff] ^
                        Td2[Se[(w >>>  8) & 0xff] & 0xff] ^
                        Td3[Se[(w       ) & 0xff] & 0xff];
        w = rek[e + 2];
                rdk[d + 2] =
                        Td0[Se[(w >>> 24)       ] & 0xff] ^
                        Td1[Se[(w >>> 16) & 0xff] & 0xff] ^
                        Td2[Se[(w >>>  8) & 0xff] & 0xff] ^
                        Td3[Se[(w       ) & 0xff] & 0xff];
        w = rek[e + 3];
                rdk[d + 3] =
                        Td0[Se[(w >>> 24)       ] & 0xff] ^
                        Td1[Se[(w >>> 16) & 0xff] & 0xff] ^
                        Td2[Se[(w >>>  8) & 0xff] & 0xff] ^
                        Td3[Se[(w       ) & 0xff] & 0xff];
        d += 4;
        e -= 4;
            }
      rdk[d    ] = rek[e    ];
      rdk[d + 1] = rek[e + 1];
      rdk[d + 2] = rek[e + 2];
      rdk[d + 3] = rek[e + 3];
    }

    /**
     * Setup the AES key schedule for encryption, decryption, or both.
     *
     * @param   cipherKey   the cipher key (128, 192, or 256 bits).
     * @param   keyBits     size of the cipher key in bits.
     * @param     direction     cipher direction (DIR_ENCRYPT, DIR_DECRYPT, or
DIR_BOTH).
     */
    public void makeKey(byte[] cipherKey, int keyBits, int direction)
            throws RuntimeException {
        // check key size:
```

```
    if (keyBits != 128 && keyBits != 192 && keyBits != 256) {
        throw new RuntimeException("Invalid AES key size (" + keyBits + " bits)");
    }
    Nk = keyBits >>> 5;
    Nr = Nk + 6;
    Nw = 4*(Nr + 1);
    rek = new int[Nw];
    rdk = new int[Nw];
    if ((direction & DIR_BOTH) != 0) {
        expandKey(cipherKey);
        /*
        for (int r = 0; r <= Nr; r++) {
                System.out.print("RK" + r + "=");
                for (int i = 0; i < 4; i++) {
                        int w = rek[4*r + i];
                        System.out.print(" " + Integer.toHexString(w));
                }
                System.out.println();
        }
        */
        if ((direction & DIR_DECRYPT) != 0) {
            invertKey();
        }
    }
}

/**
 * Setup the AES key schedule (any cipher direction).
 *
 * @param   cipherKey   the cipher key (128, 192, or 256 bits).
 * @param   keyBits     size of the cipher key in bits.
 */
public void makeKey(byte[] cipherKey, int keyBits)
        throws RuntimeException {
    makeKey(cipherKey, keyBits, DIR_BOTH);
}

/**
 * Encrypt exactly one block (BLOCK_SIZE bytes) of plaintext.
 *
 * @param   pt          plaintext block.
 * @param   ct          ciphertext block.
 */
public void encrypt(byte[] pt, byte[] ct) {
    /*
            * map byte array block to cipher state
            * and add initial round key:
            */
```

```
int k = 0, v;
int t0   = ((pt[ 0]       ) << 24 |
            (pt[ 1] & 0xff) << 16 |
            (pt[ 2] & 0xff) <<  8 |
            (pt[ 3] & 0xff)       ) ^ rek[0];
int t1   = ((pt[ 4]       ) << 24 |
            (pt[ 5] & 0xff) << 16 |
            (pt[ 6] & 0xff) <<  8 |
            (pt[ 7] & 0xff)       ) ^ rek[1];
int t2   = ((pt[ 8]       ) << 24 |
            (pt[ 9] & 0xff) << 16 |
            (pt[10] & 0xff) <<  8 |
            (pt[11] & 0xff)       ) ^ rek[2];
int t3   = ((pt[12]       ) << 24 |
            (pt[13] & 0xff) << 16 |
            (pt[14] & 0xff) <<  8 |
            (pt[15] & 0xff)       ) ^ rek[3];
/*
        * Nr - 1 full rounds:
        */
for (int r = 1; r < Nr; r++) {
   k += 4;
   int a0 =
      Te0[(t0 >>> 24)       ] ^
      Te1[(t1 >>> 16) & 0xff] ^
      Te2[(t2 >>>  8) & 0xff] ^
      Te3[(t3       ) & 0xff] ^
      rek[k    ];
   int a1 =
      Te0[(t1 >>> 24)       ] ^
      Te1[(t2 >>> 16) & 0xff] ^
      Te2[(t3 >>>  8) & 0xff] ^
      Te3[(t0       ) & 0xff] ^
      rek[k + 1];
   int a2 =
      Te0[(t2 >>> 24)       ] ^
      Te1[(t3 >>> 16) & 0xff] ^
      Te2[(t0 >>>  8) & 0xff] ^
      Te3[(t1       ) & 0xff] ^
      rek[k + 2];
   int a3 =
      Te0[(t3 >>> 24)       ] ^
      Te1[(t0 >>> 16) & 0xff] ^
      Te2[(t1 >>>  8) & 0xff] ^
      Te3[(t2       ) & 0xff] ^
      rek[k + 3];
   t0 = a0; t1 = a1; t2 = a2; t3 = a3;
}
```

```
    /*
     * last round lacks MixColumn:
     */
    k += 4;

    v = rek[k    ];
    ct[ 0] = (byte)(Se[(t0 >>> 24)       ] ^ (v >>> 24));
    ct[ 1] = (byte)(Se[(t1 >>> 16) & 0xff] ^ (v >>> 16));
    ct[ 2] = (byte)(Se[(t2 >>>  8) & 0xff] ^ (v >>>  8));
    ct[ 3] = (byte)(Se[(t3       ) & 0xff] ^ (v       ));

    v = rek[k + 1];
    ct[ 4] = (byte)(Se[(t1 >>> 24)       ] ^ (v >>> 24));
    ct[ 5] = (byte)(Se[(t2 >>> 16) & 0xff] ^ (v >>> 16));
    ct[ 6] = (byte)(Se[(t3 >>>  8) & 0xff] ^ (v >>>  8));
    ct[ 7] = (byte)(Se[(t0       ) & 0xff] ^ (v       ));

    v = rek[k + 2];
    ct[ 8] = (byte)(Se[(t2 >>> 24)       ] ^ (v >>> 24));
    ct[ 9] = (byte)(Se[(t3 >>> 16) & 0xff] ^ (v >>> 16));
    ct[10] = (byte)(Se[(t0 >>>  8) & 0xff] ^ (v >>>  8));
    ct[11] = (byte)(Se[(t1       ) & 0xff] ^ (v       ));

    v = rek[k + 3];
    ct[12] = (byte)(Se[(t3 >>> 24)       ] ^ (v >>> 24));
    ct[13] = (byte)(Se[(t0 >>> 16) & 0xff] ^ (v >>> 16));
    ct[14] = (byte)(Se[(t1 >>>  8) & 0xff] ^ (v >>>  8));
    ct[15] = (byte)(Se[(t2       ) & 0xff] ^ (v       ));
}

/**
 * Decrypt exactly one block (BLOCK_SIZE bytes) of ciphertext.
 *
 * @param   ct          ciphertext block.
 * @param   pt          plaintext block.
 */
public void decrypt(byte[] ct, byte[] pt) {
    /*
            * map byte array block to cipher state
            * and add initial round key:
            */
    int k = 0, v;
    int t0 =   ((ct[ 0]       ) << 24 |
               (ct[ 1] & 0xff) << 16 |
               (ct[ 2] & 0xff) <<  8 |
               (ct[ 3] & 0xff)       ) ^ rdk[0];
    int t1 =   ((ct[ 4]       ) << 24 |
               (ct[ 5] & 0xff) << 16 |
```

```
            (ct[ 6] & 0xff) <<  8 |
            (ct[ 7] & 0xff)       ) ^ rdk[1];
int t2 =   ((ct[ 8]       ) << 24 |
            (ct[ 9] & 0xff) << 16 |
            (ct[10] & 0xff) <<  8 |
            (ct[11] & 0xff)       ) ^ rdk[2];
int t3 =   ((ct[12]       ) << 24 |
            (ct[13] & 0xff) << 16 |
            (ct[14] & 0xff) <<  8 |
            (ct[15] & 0xff)       ) ^ rdk[3];
/*
        * Nr - 1 full rounds:
        */
for (int r = 1; r < Nr; r++) {
    k += 4;
    int a0 =
        Td0[(t0 >>> 24)       ] ^
        Td1[(t3 >>> 16) & 0xff] ^
        Td2[(t2 >>>  8) & 0xff] ^
        Td3[(t1       ) & 0xff] ^
        rdk[k    ];
    int a1 =
        Td0[(t1 >>> 24)       ] ^
        Td1[(t0 >>> 16) & 0xff] ^
        Td2[(t3 >>>  8) & 0xff] ^
        Td3[(t2       ) & 0xff] ^
        rdk[k + 1];
    int a2 =
        Td0[(t2 >>> 24)       ] ^
        Td1[(t1 >>> 16) & 0xff] ^
        Td2[(t0 >>>  8) & 0xff] ^
        Td3[(t3       ) & 0xff] ^
        rdk[k + 2];
    int a3 =
        Td0[(t3 >>> 24)       ] ^
        Td1[(t2 >>> 16) & 0xff] ^
        Td2[(t1 >>>  8) & 0xff] ^
        Td3[(t0       ) & 0xff] ^
        rdk[k + 3];
    t0 = a0; t1 = a1; t2 = a2; t3 = a3;
}
/*
 * last round lacks MixColumn:
 */
k += 4;

v = rdk[k    ];
pt[ 0] = (byte)(Sd[(t0 >>> 24)       ] ^ (v >>> 24));
```

```
        pt[ 1] = (byte)(Sd[(t3 >>> 16) & 0xff] ^ (v >>> 16));
        pt[ 2] = (byte)(Sd[(t2 >>>  8) & 0xff] ^ (v >>>  8));
        pt[ 3] = (byte)(Sd[(t1       ) & 0xff] ^ (v       ));

        v = rdk[k + 1];
        pt[ 4] = (byte)(Sd[(t1 >>> 24)       ] ^ (v >>> 24));
        pt[ 5] = (byte)(Sd[(t0 >>> 16) & 0xff] ^ (v >>> 16));
        pt[ 6] = (byte)(Sd[(t3 >>>  8) & 0xff] ^ (v >>>  8));
        pt[ 7] = (byte)(Sd[(t2       ) & 0xff] ^ (v       ));

        v = rdk[k + 2];
        pt[ 8] = (byte)(Sd[(t2 >>> 24)       ] ^ (v >>> 24));
        pt[ 9] = (byte)(Sd[(t1 >>> 16) & 0xff] ^ (v >>> 16));
        pt[10] = (byte)(Sd[(t0 >>>  8) & 0xff] ^ (v >>>  8));
        pt[11] = (byte)(Sd[(t3       ) & 0xff] ^ (v       ));

        v = rdk[k + 3];
        pt[12] = (byte)(Sd[(t3 >>> 24)       ] ^ (v >>> 24));
        pt[13] = (byte)(Sd[(t2 >>> 16) & 0xff] ^ (v >>> 16));
        pt[14] = (byte)(Sd[(t1 >>>  8) & 0xff] ^ (v >>>  8));
        pt[15] = (byte)(Sd[(t0       ) & 0xff] ^ (v       ));
    }

    /**
     * Destroy all sensitive information in this object.
     */
    protected final void finalize() {
        if (rek != null) {
            for (int i = 0; i < rek.length; i++) {
                rek[i] = 0;
            }
            rek = null;
        }
        if (rdk != null) {
            for (int i = 0; i < rdk.length; i++) {
                rdk[i] = 0;
            }
            rdk = null;
        }
    }
}
```

APPENDIX C

CODE FOR *t* GENERATION

The code segment (Token.java) that generates a sample Token is given below:

```
ublic class Token {


        private String UTSN;
        private String UTSNCV;
        private String TFV;
        private String DoI;
        private String Opr;
        private String Ocr;
        private String Oint;

        public byte[] getUTSN() {
                byte[] returnArray = UTSN.getBytes();

                return returnArray;
        }

        public byte[] getAll() {
                return (UTSN+" "+UTSNCV+" "+TFV+" "+DoI+" "+Opr+"
"+Ocr+" "+Oint).getBytes();
        }

        public byte[] getUTSNCV() {
                return UTSNCV.getBytes();
        }
        public void initialize() {
                //read fields from text file
```

```
                UTSN = "0";
                UTSNCV = "0";
                TFV = "0";
                DoI = "0";
                Opr = "0";
                Ocr = "0";
                Oint = "0";


        }

        public void Token() {
        }
}
```