AN INTRODUCTION TO DIGITAL CASH WORLD

Lusiana Citra Dewi

Jurusan Teknik Informatika, Fakultas Ilmu Komputer, Universitas Bina Nusantara
Jln. K.H. Syahdan No. 9, Palmerah, Jakarta Barat 11480
laboratory@binus.ac.id

ABSTRACT

Digital cash is one of the payment methods that is very easy to use, especially when someone is doing a transaction through the internet. Digital cash has many forms and systems, which are supposed to simplify and make the process of transaction easier. This paper will discuss about the definition of the digital cash itself, the important properties that it has, the problems which occur due to its existence, the examples of some key players who operate the digital cash from all around the world, along with how the digital cash works, and lastly, how the digital cash is put into the practical world. The purpose of this paper is to give a glimpse of view on the functions of the digital cash, the systems or protocols which are needed to implement it, and the problems faced by those who use it.

Keywords: *Digital Cash, electronic money, payment.*

ABSTRAK

Digital cash merupakan salah satu cara pembayaran yang sangat praktis, khususnya untuk transaksi pembayaran yang dilakukan via internet. Banyak bentuk dan sistem digital cash yang mempermudah terjadinya transaksi. Pada paper ini akan dibahas mengenai pengertian dari digital cash, properti penting dari digital cash, permasalahan yang muncul untuk digital cash, contoh beberapa pemain kunci dari digital cash dari seluruh dunia serta dengan pembahasan "How it works"-nya, dan praktek digital cash dalam dunia nyata. Penulisan paper ini bertujuan memberikan gambaran mengenai kegunaan digital cash, sistem atau protokol yang seperti apa yang ada untuk pengimplementasian digital cash ini dan apa permasalahan yang kerap kali dihadapi oleh para pemain dan pengguna digital cash ini.

Kata kunci: *Digital Cash, Uang Elektronik, Payment*

INTRODUCTION

"What is actually the digital cash? …Is it a substitution for currencies which, in the future, will be produced and issued legally by the government? Or is it the next generation of the Credit Card which, if it really is, will be under the regulations of Banks?"(Joshua B. Konvisser)

Electronic trade or more commonly known as e-commerce has been developing greatly all around the world. In 1995, the volume of trade by the internet was estimated to be over US$ 159 million. By the end of 1999, the numbers rose significantly, getting to over than US$ 400 billion. Not only the volume of the dollar value which increased, but also the volume of the internet itself.

The development which has been happening in the world of electronic trade practically makes the lives of people nowadays much easier. Nowadays, it is easier for people to make purchases, or do other financial transactions through the use of Digital cash.

The background of the writing of this paper is because the digital cash is a new method of payment which utilizes the information technology and computer networks. Digital cash is believed to be a replacement of the credit cards, because it is much easier to use than the credit cards.

The scope of this paper discusses about the definition and understanding of the digital cash itself, the properties of the digital cash, the problems which exists because of the digital cash, some key players who operate the digital cash from all around the world, along with the brief explanation concerning the systems, and also the use of digital cash in practical world. What will not be discussed on this paper are the arithmetic computation to encrypt the data for the safety of digital cash and other topics which are not mentioned above.

The purpose and use of this paper are to give a general view of the digital cash, and how it works. Beside that, this paper also gives information about the functions of the digital cash, the explanation of the system or protocols which are needed to implement the digital cash, and the problems which surfaces and faced by the players and users of the digital cash.

The method of research of this paper is by gathering all the information sources and summarize it into a one general, and yet very useful, information.

Theoretical Perspective

Money has wide variations of definitions, but through the economical perspective, money is defined as (Pustekkom, 2005):

1. According to Roberson in *Money*, money is something which is widely accepted in payments for goods.
2. According to R.S. Sayers in *Modern Banking*, money is something that is widely accepted for the settlement of debts.
3. According to A.C. Pigou in *The Viel of Money*, money are those things that are widely used as a media for exchange.
4. According to Albert Gailort Hart in *Money Debt and Economic Activity*, money is property with which the owner can pay off the debt with certainty and without delay.
5. According to Rollin G. Thomas in *Our Modern Banking and Monetary System*, money is something that is readily and generally accepted by the public in payment debt.

While the word "electronic" itself means to only use the computer system or electronic system. In other word, electronic money is a payment mechanism which is done through the use of the computer and internet technology

The utilities of money are: (1) A mean of exchange; (2) A unit of counting; (3) A depository of properties; (4) A mean of transfer of properties or capitals; and (5) A mean of debt record or withheld payments

RESULTS AND DISCUSSIONS

The Role of E-cash in the World of E-Commerce

a. Non-cash Payment System

All along the record of history, the development and advancement of economy has always been dependant on the monetary situation. In the past, currency, or simply, money, had replaced the non-cash payment system in our social lives. And recently, check in the form of paper, and plastic card has replaced the role of money in various contexts and situations. The same thing goes with the electronic payment. Soon, the benefit it gives in various contexts, especially in purchases done in trading transactions will be noticed.

b. The Three Categories in Non-cash Payment

Nowadays, there are three principals or system categories of payment (non-cash) which is used on the internet. The first one is e-cash (digital cash), the second one is a credit card based payment (e-credit), and the third one is digital checking (e-check). The focus of this paper is on the first form of the non-cash payment system and the author will discuss about that more thoroughly in the following chapters.

The second non-cash payment is a credit card based payment system, which is not a new thing in everyday lives. The growth of this system is very significant, along with the growth of the internet and the “electronic shopping malls”. Along with its development, very substantial risk occurs which involves the hijacking of the credit cards serial numbers. It is basically caused by the insecure sending of the serial numbers. In this kind of system, usually consumers will create an account at a “facilitator” (in this case, the facilitator is usually a bank) to get the credit card and the serial numbers. After that, the consumer will be able to make purchases from the seller through the internet. Then the seller will send the data of the purchase to the facilitator, so that the facilitator can send an email of confirmation to the consumer. After the consumer confirms the transaction, the facilitator will subtract the consumer’s account and transfer the money to the seller. The facilitator will benefit a small portion of the ongoing transaction. Lately, there are a lot of encryption techniques which have become available to use, which increases the feeling of security for the users, and it also makes the sending of encrypted credit cards serial numbers through the online facilities becomes a very useful payment system.

The third non-cash payment system is the digital checking, or more commonly known as electronic check (e-check). The e-check works the same way as normal checks. Firstly, the buyer writes an e-check by using one of many electronic tools, and then he sends the e-check to the seller electronically. The seller deposits the check afterwards, and will receive the credits in his account. The seller’s bank will then confirm the e-check with the buyer’s bank. After that, the buyer’s bank will validate the received e-check and deduct the fee of the transaction on the buyer’s account.

Digital Cash

Money was originally made in the form of coins. And through the development of trading, coins became less and less practical to use in various circumstances. Then human created a monetary

note, or it was simply called as bill. After those periods, now is the time for the digital cash. The digital cash is on the same position as the common paper bills, which is used as an exchange tools in doing purchases. In the digital cash system, the user keeps tokens, or a series of bits which are electronically saved in the computer. These tokens can be deducted by bank through the internet, the same process as when we take out paper bills (in physical form of paper) through the ATM. The user can also send those tokens through the internet to other users. User can also keep those tokens for other purposes, or deposits them in his bank account, just like the common money.

System Model of Digital Cash

This sub-chapter will explain about the basic model or the life-cycle mechanism of the value of the electronic money, based on each type of the electronic money. The life-cycle of this electronic money basically will go through the following process:

a) Initialization
b) Debiting of the electronic money values
c) Crediting of the electronic money values
d) Closing

While the types of transaction which exists on the electronic money system are: (a) *Loading*, installing the value of the electronic money to a certain device; (b) *Payment*, making a purchase for goods or service by spending the installed value of the electronic money; (c) *Refund*, making a cancellation of the purchase of goods or service; and (d) *Collection*, to produce the value of the electronic money resulted from the payment of goods or service.

General Model

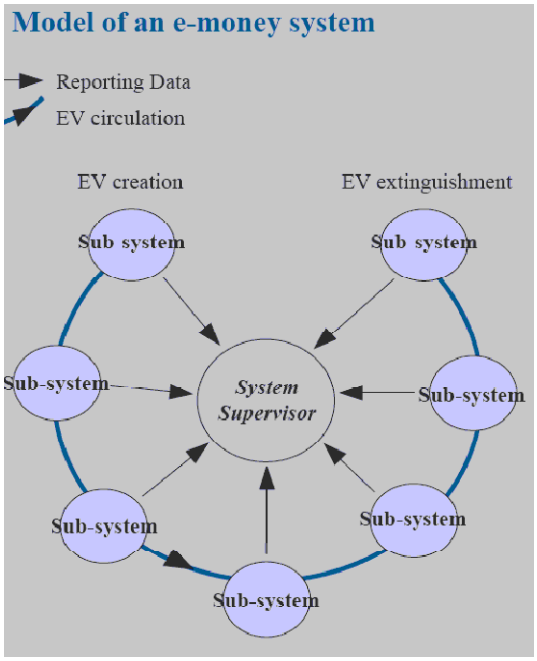

Figure 1. General systemic model of the electronic money

The above figure shows a systemic model of electronic money in general. An electronic money system generally consists of subsystems. Among the subsystems, there are two special

subsystems, which are EV Creation subsystem, and EV extinguishment subsystem. The EV creation subsystem functions as the creator of the electronic money value (create Electronic Value). While the EV extinguishment subsystem functions to delete the electronic money value (extinguish Electronic Value).

The movement of the electronic money value is clearly pictured on the above model. The value of electronic money moves from EV creation subsystem, through other subsystems. When the process goes through each of these interconnected subsystems, each subsystem will send a report to System Supervisor. The System supervisor will regulate and control the work of the subsystems around it. After that, the value of the electronic money will end at the EV extinguishment subsystem where the value of the electronic money will be deleted.

Stored-Value Model/Card Based

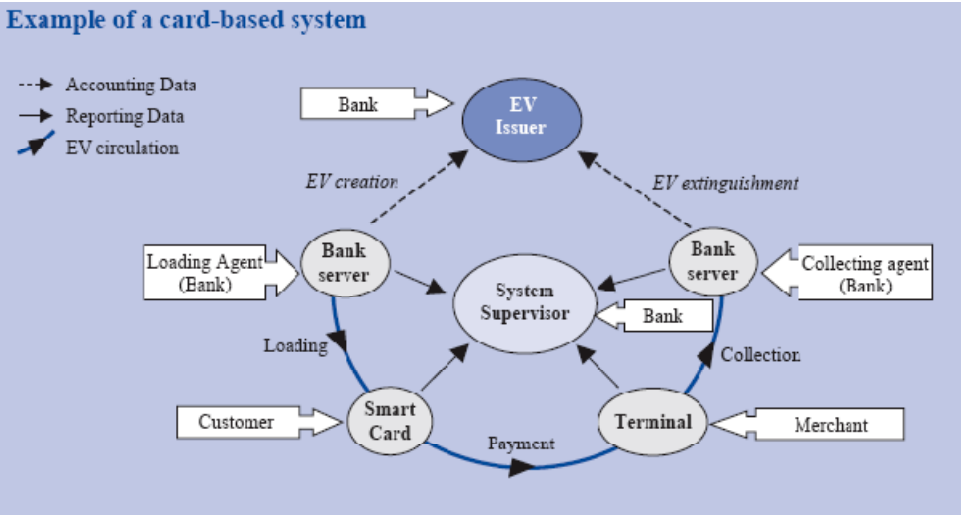

Figure 2. The model of Card based Electronic Money system (Stored-value)

The second model (Figure 2) is the stored-value electronic money system, or more commonly known as the card-based e-money. This system commonly uses prepaid payment method. The value of a user's money is installed to an electronic device, which is held by the user himself. The examples of the electronic devices are smart cards, RFID cards, or other devices. The value of the electronic money will be deducted or added, according to the transaction and purchases done by the user.

The model of this system can be seen on the image above. This model is based on the general model which was discussed in the previous sub-chapter, which sums up as the electronic value which moves through the existing subsystems, starting from EV creation and ending at EV extinguishment. The difference between the two models is the subsystems which exist in this model usually have four functions:

a) Loading Agent
   - The Loading Agent is commonly a Bank
   - The loading agent converts the value of money from other forms, such as paper bills or coins, to electronic value which is kept in an electronic device.

b) Collecting Agent
   - The collecting agent is commonly a bank
   - The collecting agent works in reverse of the loading agent, which is to convert the electronic value to real cash value in the form of paper bill or coins.

c) Customer
- The party who owns the electronic value (user).
- The user has the right to deduct or add his own electronic value according to his will.

d) Merchant
- The seller who receives the electronic value from the customer.
- The merchant side will have a terminal (the terminal looks approximately like the credit card terminal) with which the merchant can receive the electronic value according to the transaction value.

Access/Server-based

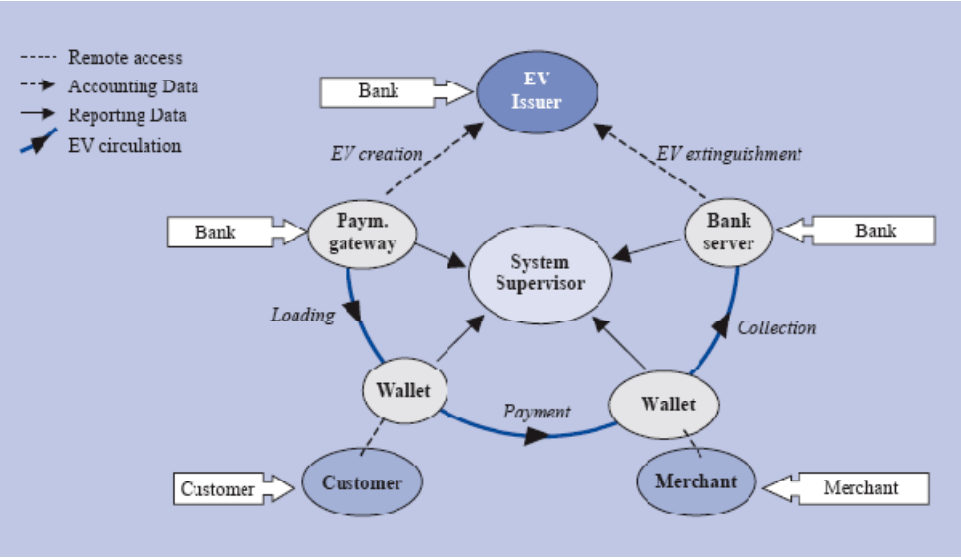

Figure 3. The model of access electronic money system.

The third model (Figure 3) is the system model of the access type of electronic money, or more commonly known as server-based electronic money system. In this system, our money value is saved in a database in a server. When the user wants to make a transaction, the server will be contacted, and then the electronic money value of the user, which is saved in the server, will be deducted or added, according to the value of the ongoing transaction.

The core difference which distinguishes the server-based model from the card-based one is the electronic value is not kept on the user's electronic device, but in the server's database instead. This electronic value can be accessed through a computer network such as the internet.

This difference can be clearly reviewed by comparing the model of the two systems. In the server-based one, Customer and Merchant are no longer a part of the model's subsystem. Instead, those two are just the external factor of the system. Even though they exist on the outside of the system, both of them have Remote Access to their own electronic money value, which is symbolized by the Wallet. It shows that they do not actually keep their electronic money value on their own, but rather they access the electronic value on the database of the legal bank.

Important Properties of Digital Cash

Digital cash is made to be a new payment system after paper bills. That is why the digital cash has to have the features which the physical money has, which are:

a) Easily recognized and accepted
b) Easy to transfer
c) Difficult to duplicate
d) Anonymous
e) Easily movable

The following are the detailed explanations of each important properties of the digital cash.

Security

The security property emphasizes the fact that the digital cash cannot be copied or reused. That is why the risk of duplication has to be minimized by creating a very good authentication system.

a) Fake duplication

The most obvious risk in every payment system is fake duplication. As it is with the paper bills, digital cash also has two types of fake duplication, which are:

- Fake tokens: an attempt to create tokens which look valid and not taken from a legal bank.
- Multiple spending: using the same tokens multiple times. Multiple spending is also called re-spending, double-spending, and repeat-spending.

To keep the creation of fake tokens, authentication system is what is commonly used, as it validates the identity of a user and it can also be used to prove the integrity of a message. In another case, to defend the system from the multiple spending case, the Bank maintains a database which records tokens which have been used previously. The tokens which are recorded in the database will be rejected if it is re-used. These course of action can be taken to anticipate the online purchase, but for offline purchases, the best way to overcome the problems is to detect the time when the multiple spending occurred. To protect the seller, the bank needs to identify the buyer.

b) Authentication

As the anticipation of the fake duplication risk, authentication on various levels needs to be done. The authentication can be categorized in 3 major levels, which are:

- User identification: a user has to know whom he is doing the transaction with.
- Message integrity: to ensure that the received message is valid.
- Non-repudiation: to avoid a transaction from being denied.

The authentication features can be achieved through a Key Management. Key management is achieved through a Certification Authority (CA), which is an agency which is trusted to take the responsibility of confirming the identity of a user. The CA functions the same way as the Indonesian SIM (Surat Izin Mengemudi) or a credit card. SIM, or a driver's license in general, identifies someone and validates that he/she is allowed to drive specific type of vehicle in a specific country. While credit card validates that someone is the rightful owner of a certain sum amount of money in a specific bank. Certification Authority works the same as the above, but only it is in a different form, which is a digital one. Digital certification can be used to validate someone's identity through the network. Without trusted Certification Authority and a secure infrastructure, the security feature for digital cash will not be very reliable, especially when it works on a insecure medium such as the internet.

Privacy

The definition of privacy itself is not really clear. Each side has their own definition of privacy. For example, for some people, privacy means protection of their personal interests. But this definition differs from the definition of David Chaum, the founder of DigiCash (a company which operates in the field of digital cash, this will be discussed more thoroughly in the following chapters). According to David Chaum, privacy is the anonymity to do payment in purchases and also un-

traceability for the transaction itself, so that the bank would not know whose money is used in one certain transaction.

The same thing goes with the anonymity of paper bills. Digital cash is also has the characteristic of anonymity, which makes it un-traceable to a specific person. This is what is called by "Unconditionally un-traceable". No matter what, the digital cash service providers have to ensure the authentication of the user who is going to do a transaction, so that one single token which are related to transaction can identify the user. But as one of the digital cash service provider, the system will protect the user's privacy.

Usually, the digital cash system does not bother with the user's privacy. Systems like those are called "Privacy Violation system". Virtually, every system which are commercially based, and are in the market nowadays, are Privacy Violation systems. They emphasize the security for the banks, but they do not pay attention on the security of their own customer (in terms of financial protection and supervision).

The anonymity in digital cash increases the risk of money laundering, illegal purchase, black mailing, and fake duplication, compared with the risk in using physical money. In other words, the higher the anonymity level is, the less secure the system becomes.

Portability

The security and usage of the digital cash do not depend on the physical location. The money can be transferred through computer networks to a safe depository.

Transferability

Transferability allows the user to use the received token as a payment in a transaction, without having to contact the related bank. The payment is a transfer if the receiver can use the token received in a purchase. A payment system is easily transferable if the system allows at least one token to be transferred. It is important to be fully aware that transferability is a very important thing in life. The life cycle of a token in a transferable system can be seen in the figure below:

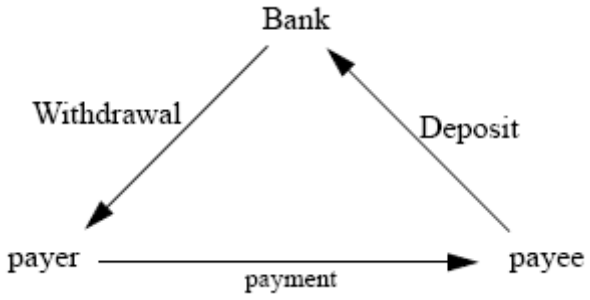

Figure 4. Token lifecycle

The problems which often surfaces in a transferable system:

a) In any electronic money system, a token must have a property which grows bigger each time the token is used. This is because the toke property keeps the information of each user who has used the token. This is done in order to catch those who commit multiple-spending crime. The problem is with the maximum numbers of transfer from the token, which is caused by the size of the property of the token.

b) Money laundering and tax avoidance, which is difficult to track because there is no record on such transactions.
c) The lateness or delay of transfer will cause the act of multiple-spending or token fraudulence. Multiple-spending cannot be detected unless there are two or more of the same token being deposited in the account, and it might be too late to retract.
d) The user may be able to recognize their own token if they see it in the next transaction.

Divisibility

What is meant by divisibility is the ability to make changes. In other words, the digital cash can be used in smaller units, so that it can be practically used in several internet transactions which require smaller value of cash.

The solution of divisible token is so that the token can be divided to several tokens with less value, but more in quantity, so that it sums up to the same value as one single previous token before it is divided. This is believed to be very practical to use, because user will not need to keep the token in different units. This is one feature which physical money does not have.

Off-line and On-line Payment

The protocol of electronic money can be implemented in two ways, which are off-line and on-line. And the ideal system is the one which goes with the off-line protocol. Both of the protocols will be discussed below:

Off-line Protocol

Off-line protocol means that the payer and the receiver can do the transaction without involving a third party (e.g. Bank). The case example would be: Mr. X verified and deposited token which he got from Ms. Y as the payment of several transactions, a while after the transaction was done. Even though the off-line protocol is more preferred than the on-line one, if you take a look from the practical perspective, the off-line protocol is very vulnerable of the multiple-spending crime, and for the exact same reason, the off-line protocol is more suitable only for transactions with small values. In the years of operation of the digital cash, the off-line protocol is designed not only to ensure the security for the banks and stores, but also to ensure the privacy of each user.

On-line Protocol

The on-line protocol means that the payer and the receiver have to do the transaction involving a third party, such as bank. The example of such case would be: Mr. X confirmed Ms. Y's token which would be used for the payment of several previous transaction before actually receiving the payment and delivering Ms. Y's order. This system is pretty similar with the transaction by using credit cards nowadays.

The on-line protocol is still needed for transactions with great value, which automatically requires high level of security. In on-line system, the payment and depository are inseparable steps which are similar with the off-line system. The on-line system requires communication with the bank in every purchase of any transaction. This causes the additional fees and time (communication fee, database maintenance fee, and when transfers need to be done). Basically, this protocol is a simplification of the off-line protocol.

Because the on-line protocol requires credibility checking of the payer's credibility, for the interest of the receiver, it is impossible to keep the anonymity intact, both for the sender as well as the receiver. This is also why the communication with a third party, which is bank, is needed.

The Problems in Digital Cash World

The system designers of the e-cash face two general problems. The first one is that there is no payment system model which will work if the third party does not have the right to read or to modify the messages which is being sent. This problem will head towards the protection of the integrity of a message. The second problem is the fraudulence. The same with fraudulence with financial notes or physical money (paper bills or coins), bank generally has taken precaution and certain course of action in order to overcome this problem. The depositor of e-cash has to go through several steps to overcome this problem, which of course will reduce the discomfort of the user. If this security issue is not taken care of promptly, then the e-cash system will not be able to grow.

Integrity

The method which has been used widely for quite some time to solve the problem of the integrity of a message which is sent through the internet as a medium (a considerably unsafe medium), is the encryption. Almost all encryption system uses key. What is meant by the key in this matter is an algorithm which changes the sent message into another form which is not understandable to human, and the key will be able to change it back to its original form when the message reaches its destination.

The traditional encryption method requires one key which is shared between the sender and the receiver of the message. There are two weakness of this system: the first one is, before the message is sent by the user, the user has to send the key to the receiver. This may allow a third party who is not related to the transaction at all, to actually steal the key. The second weakness is if the user often does transactions, then the key will have to be shared to more than one party, which automatically reduces the level of security of that certain key.

With those two weaknesses above, the most suitable solution for the problem of integrity of a message which is sent through the internet is by using the RSA encryption. The RSA encryption utilizes two kinds of keys, which are public key and private key. The public key is made to be shared among everyone, while private key is made to compute an equation from various arithmetical facts from the encoded public key. The fact itself is kept by the user. This mathematical system causes a condition which does not allow the public key to encode and described the sent message.

With this key, the sender can guarantee the receiver that the message is sent by the same person. And it also ensures that only certain parties who are actually involved in the same transaction can read that message.

For the simpler explanation, we will briefly discuss about the flow of a message from the sender to the receiver. The sender will encrypt the message which will be sent by using two keys, which are the private key of the sender and public key of the receiver. While the receiver will decrypt the message by using the two keys, which is the private key of the receiver, and the public key of the receiver. This procedure ensures that the message is sent by the specific sender, and read by the specific receiver.

Fraud Duplication

As it has been explained in the previous sub-chapter, the duplication case which often occurs in term of digital cash is the repeated uses of token or multiple-spending. This is done by someone who uses the same token over and over again.

One of the solution which overcomes this kind of problem is to make one-time-usage token only. How this solution works would be, both the buyer and seller make accounts in the same bank. After that, the buyer will deduct the token from the bank and keep the token in his computer, before he

choose and buy goods from the seller. After the buyer finish buying with the tokens, then the buyer send those tokens to the seller. Then the seller will confirm it and redeposit the token to the bank. after the bank clarifies the token, it will be destroyed along with its properties (serial number) and then generate new tokens with new properties. The bank will deposit the value to the seller's bank account according to the value of the token, and will send a confirmation message that the sent tokens are valid.

Government

There's a lack of participation of the government to adopt the system. Generally, governments of several countries choose to stay quiet and wait for the development to grow by itself. Some countries even choose to ignore the electronic computer networking system (internet). It is a drawback, since the government is the only party that can make regulations or rules in many forms, but there are still some governments who are still ignorance of these things and has not yet made the regulations to control the internet, computer networks, or the information technology.

Taxes Consideration

One of the problems with this system has something to do with the tax. Generally, trade process will get tax charged by the government of the country where the transaction is done. But the thing here is that the place of the transaction is not in a specific country, but rather in the digital world, the internet. Because most of the transactions done via the internet are international transactions. Considering this fact, which countries rules and regulations need to be applied? And which countries have the right to earn those taxes? These questions are still left unanswered in the digital cash world.

Besides that, the countries will actually benefit a lot if the digital cash system is actually applied as one of the tax payment system. It is simple and does not cost much to operate, and the government will no longer face difficulties in charging taxes from its people.

The Key Players in the World Payment System (Implementation)

a. DigiCash

DigiCash was invented and founded by David Chaum in 1990 and its main office is located in Amsterdam. The company has developed various products of payment technologies. One of the company's products is "ecash", a prototype of digital cash which had been developed since 1995. The system was designed to enable secured payment from any Personal Computer (PC) to any workstation, through the use of e-mail or the internet. Ecash was implemented on almost every digital cash systems which belong to Chaum. Ecash was a system which operates on on-line protocol.

Every people who use ecash, open an account in one of the digital banks on the internet, such as the EU bank which is located in Finland. By using the account, the user can withdraw or deposit the ecash. The security system of ecash is based on the RSA security system. When the ecash was first implemented on PC, the ecash software will automatically generate a couple of RSA encryption key.

When user makes ecash withdrawal, the user's PC will calculate the number of token needed to cover the value of withdrawal requested by the user. Then the PC will generate serial numbers randomly for those tokens. The results of the calculation will be sent to the digital bank in which the user has made an ecash account. The bank will firstly verify the message received and at almost the same time, debit the user's account with the requested value. The authenticated tokens are sent back to the user. Those tokens are insured by the bank.

Tokens will be recorded locally in the user's PC. Soon after the user wants to use those tokens, the PC will collect the necessary tokens, and then those tokens will be sent to the receiver. Then the receiver directly sends the tokens to the digital bank before he can receive the actual cash. The bank verifies the validity of the tokens and checks that the tokens have never been used before. After that, the digital bank will credit the account of the receiver. Each token can only be used once. When the receiver wants to withdraw his tokens, the bank will produce new tokens which have the same value and can only be used once.

The same with travel check, if the user loses his ecash tokens, then the user has to report to the bank and give the serial number of the lost tokens. The bank will check whether or not those tokens really lost. If they are really lost, then the bank will give back those tokens. User can also cancel a purchase if the user is not satisfied with the certain store. This can be done by showing the serial number of the tokens which are used to pay in the purchase, and asking the bank to cancel the purchase.

The benefit of this e-cash system is that the identity of the payer are kept private, it also has a low transaction cost, and it can deal with direct transaction without have a bank as the third party. Its drawbacks are that the buyer and seller have to have accounts at the same digital bank and the bank has to have a large database to record the serial numbers of the lots of tokens.

b. PayPal

Paypal is a cash transferring system which was founded to deal with C2C transaction (customer-to-customer). But lately, X.com, a company which operates behind PayPal, introduces a new product which can be used in B2C transaction (Business-to-customer), and offers accounts for the business owners. Paypal works as a medium which offers secured transaction to both parties (seller and buyer).

PayPal uses e-mail to inform the receiver that payment has been done. PayPal benefits from one of the three ways: (a) PayPal charges a fee from the users who use the credit cards to pay in each purchase; (b) Debiting from each user account for every purchase; and (c) The buyer sends a check to deposit the value in his account on PayPal, and all the transaction will deduct the account. Seller who uses the cash in his account can also receive payment through PayPal in the form of check, or PayPal can directly deposit the amount of cash to his account.

PayPal is one of the easiest ways for the buyers to do the purchases. The registration steps are even simpler than making email account. As buyer (payer), the information needed to register is only name, email address, credit card information, and postal address of the buyer's credit card.

For users who has the PayPal regular account, the payment has to be done through PayPal website. For the business and premier account, the purchase and payment can be done and received through their own websites by using the "Web Accept" button.

c. TradEnable

This service provider might be very familiar to those who operate auction website. Auction website has to have a fair credibility level. Credibility which insures that the auctioneers will provide the auctioned goods, and that the auction participants will pay the seller. However, credibility is one thing that is hard to find on the internet. This is where TradEnable comes in.

TradEnable allows the buyer and seller to reach an agreement. After both sides agreed, TradEnable sends an email to the seller, asking him to pay a specific amount of cash to TradEnable.

The payment can be done through the use of credit cards, checks, cash, or transfers. All the payment transaction has to be done by using US$ currency.

d. Mondex ®

Mondex is a product of smart card MasterCard, which allows the cardholder to carry, keep, and uses the cash value through the use of cards. This process is much faster compared with doing transaction using the physical cash, and it is safer in many ways. Mondex works like paper bills, offering the transfer of cash value without requiring any signatures, PIN, or authorization in a transaction. Mondex's platform allows the user to use Internet, mobile phone, and cable TV.

Mondex records the cash value as electronic information in a microchip, not in a note or token. The cash value will be securely transferred from the chip in the card, to the chip installed in a terminal or card reader. Mondex card can be bought from a franchise store and can be re-deposited easily by using telephone. The benefit of using Mondex are:

a) Security – Mondex is a safe way to carry your money. A locking function has been implanted in Mondex card, which enables the card holder to avoid unwanted access. The code is selected by the card holder and can be changed at any time.
b) Comfort – Mondex provides the card holder a safe and fast payment method.
c) Flexibility – Mondex can be used for purchase in any amount of cash.
d) Control – with Mondex, the card holder can only use the value which is stored in the card, so there will be no worries of getting in a pile of debt.

e. InternetCash™

InternetCash™ is perfect for people who do not have credit cards, or choose to not to use credit cards when making purchases through the internet (which may be caused by the lack of security factor on the internet). A lot of people purchase InternetCash™ and use it. It's because InternetCash™ is easy to get. InternetCash™ is sold in many stores, vending machine, and ATM machine. The next step is the customer visits the InternetCash™ website and activate their cards by inputting the 20 digits serial number from the back of the card, and then create a personal identification number.

The customer who uses the card can choose to pay by using InternetCash™ from the online shopping website. The customer will be redirected to a page which has already been secured by InternetCash™, and the customer will be asked to input the card's serial number. The value of the card will be automatically deducted from the ongoing transaction. Customer does not pay when using InternetCash™, but when the customer is doing a C2C transaction, he will be charged a considerably small amount of fee as the transfer fee to the receiver.

InternetCash™ is one of the payment solutions which has the significant role as the alternative online currency. Everyone can use InternetCash™ easily because it does not require the ownership of a credit card to make purchase. The customer's cash is recorded on a server, not on the customer's device which needs to be carried anywhere, or the customer has to sit in front of which when doing a transaction.

Digital Cash in Practice

Implementation Aspect

The problem with the storage will usually occur after a withdrawal is made. A customer wants the token which he deposits can be withdrawn anytime he needs it. And of course the information which is related with the tokens withdrawal will have to go along with it, since the tokens will be reused in another transaction.

An important problem in implementing a system is the safety of communication channel between the parties involved. We need to be sure that the communication channels are secured. If it is not secured, then we have to use algorithm to encrypt a data packet or information when we send it, so that it can be safely delivered through unsafe medium.

The receiver will be charged an amount of fee by bank each time a transaction is done. And if the receiver keeps the tokens on his PC for a while before depositing them to the bank, he will not get the interest fund. But if the PC of the receiver has the right to access the database, the receiver can keep the tokens on his PC and still get the interest.

Acceptance of the User

Some questions that need to be answered before the user can actually accept the digital cash and use it, namely: (a) Responsibility: if the token is lost, who will be responsible to refund it?; (b) Which currency is used as the main currency? US$? IDRP? Or is it necessary to create a new Cyber Currency?; and (c) How about the fees charged? Is it charged on each transaction, or when a token is produced?

Smart Card

Smart card has an important role in the digital cash system because; (1) As it has been discussed and explained previously, one of the important properties of the digital cash is portability. It means that the most important problem in digital cash system is to find a storage device, which is compatible with the computer technology, easy to carry around, and has the ability to be connected with the computer network, so that it can do transfers through the internet. Smart card is easy to carry, computer compatible, and can be connected to the internet through the card reader; and (2) One of the biggest problems in the world of digital cash is multiple-spending. The solution is to use a special smart card which contains a very durable chip which is called as *observer*. The observer chip records a mini database which keeps all the digital transaction which has been done by using the smart card. If someone wants to use his digital cash more than once, the observer chip will detect it and will not allow the transaction to continue.

Smart card is a plastic card which contains 25mm2 (ISO standard) integrated circuit chip (IC Chip). This chip records the information and protects it from the unauthorized access. Smart card also enables high level of security, because IC chip of the smart card has the computerized architecture.

Smart card has 2 different types, which are: (a) Simple Memory Card – this card has the function of a storage. This card keeps the application code and the simple mechanism to specify the company which issues the card; and (b) Hard Wired Login Card – this card contains memory and processor, and it also has the ability of data processing which enables the data stored in it to be managed. The data processing ability is usually used to encrypt or decrypt the data.

Using Digital Signature in Smart Card System

The digital signature which is produced from the smart card in a purchase is the basis of the transaction which occurs between a seller and buyer. The digital signature ensures that both parties and their cash are authenticated. Several methods have been implemented, namely: (a) *Shared-key system – private key* in the chip enables the card to authenticate the communication between any devices which have the same key. The security depends on the master key, because this key has to be distributed among all users. All purchases done through this system is called linkable, because each card is given a unique key to increase the security; (b) *Public-key signature-creating system* – in this kind of system, for each card, the bank created a couple of key: private key and public key, and then record it in the card. The card will be installed with co-processor because to operate the public key

signature, it requires a lot of power. Every purchases made by the user will be linked with the identity of each card; and (c) *Public-key signature-transporting system* – the bank will create pre-signature for the card before the transaction is done by using the private key system and record it in the card's chip. During the transaction time, the system changes the pre—signature into a full-signature. The changing process does not require a lot of processor power. The terminal which is supposedly located in stores will verify the full-signature by using its public key. This kind of system is not linkable, because the card uses different signatures in every transactions.

Using Smart Card to Transfer the Digital Cash

There are two different techniques to transfer digital cash by using smart card, which are: (a) Coin-transporting Technique – this technique is based on the token production. The value of the smart card is shown by the deposited tokens. This system is much more secure, because the balance is not recorded in the smart card. The drawback of this system is that it requires a lot of memory to record the token; and (b) Balance-counter technique – the card is installed with a balance-counter. The bank adds the card's value by increasing its balance. When the card gives the signature which represent the value which is used in a transaction, the same value will be used to deduct the card's balance.

RFID Card

RFID is an acronym of Radio-Frequency Identification. RFID is a small sized electronic device which contains a small chip and antenna. The chip usually can only contain approximately 2000 bytes of data (Technovelgy.com, N. D.).

The RFID device provides the same utilities as the bar code or magnetic strip which is located on the back of every credit cards or ATM cards. Both of those things provide a unique identity for each card. And, the same with those cards, RFID card also has to be scanned in order to get the information contained in it.

In general, there are 3 types of RFID cards, which are Passive RFID, semi-passive RFID, and active RFID. Passive RFID does not need a specific power source, and it becomes active when the RFID reader is close by and radiates the electrical power. While the semi-passive and active RFID has its own power source, which is usually a small battery.

For the long term use, such as the ID card, attendance card, and goods security card, the Passive RFID is more preferable. Even though it does not have a battery in it, the electric wave which occurs when the card is close by the reader will be enough to operate it.

The RFID reader emits radio wave signal which inducts the antenna in the RFID card. The wave which results from this induction is enough to turn on the CMOS type integrated circuit (IC), so that it would response by emitting radio wave.

The simplicity of the passive RFID enables it to be made through the printing process, including the antenna part. Since there is no battery in it, the size can be made very small, so that it can be installed in a paper, sticker, or even under the skin of living creatures (including human).

Hitachi, a Japanese company, in February 2007, introduced the smallest RFID which has the dimension of 0.05mm x 0.05mm (without the antenna). This Hitachi U-chip can transmit 128bit of unique ID number. This achievement is and improvement of passive RFID with the dimension of 0.15mm x 0.15mm, with 7.5micrometer of thickness, which was produced in the previous year.

The weakness of all RFID is the size of the antenna which is approximately 80 times as big as the chip itself, while the antenna (and the choice of frequency) itself, decides on how far the RFID can

emit the radio frequency wave. Usually, the furthest wave range is only 10cm, even though there are some which can reach a few meters away (Subarkah, 2008).

CONCLUSION

The use of the digital cash is to make it easier for the people when they want to make purchases or other transactions through the use of the internet. Nowadays, because of the existence of the digital cash, almost all people can experience doing their shopping without having a credit card, or without having to give any information of their credit card, due to the insecurity of the internet.

There are two protocols with which the digital cash can be implemented, which are off-line protocol, and on-line protocol. Both have their own benefits and drawbacks. According to the discussion, the off-line protocol is suitable to use in small transaction, because it is simpler, cheaper, and it has considerably low risk for the small transaction. While the on-line protocol is more suitable to use for the transactions with large value, because both parties involved in the transaction would want the transaction to be more secured.

The problems faced by the players and users of the digital cash are quite a lot. This might be caused by the young age of the system itself, so that it still has many weaknesses and flaws. But the most concerning problem which exists is the security problem. It is because this security problem can be perceived as the cause of most other problems existing in the world of digital cash. Not to mention that this system works in insecure medium such as the internet.

Suggestions

It is suggested that digital cash can be used more widely among all the people in Indonesia, regardless of the people status and locations. It is simple and easy to use, and it can also give a lot of benefit to all parties involved in it (buyer, seller, and even the service provider).

REFERENCES

Pustekkom (2005). *Uang dan Inflasi.* Downloaded from http://175.106.19.29/diknas/file.php/1/PENGETAHUAN%20UMUM/edukasinet/www.e-dukasi.net/mapok/mp_fullf3bc.html?id=92

Technovelgy.com. (N. D.) *What is RFID?* Downloaded from http://www.technovelgy.com/ct/Technology-Article.asp?ArtNum=1

Subarkah, A.W. (2008) Uang Digital, dari Ponsel dan Kartu RFID. Kompas 4 Februari 2008. Jakarta: Kompas. http://m.kompas.com/xl/read/data/2008.02.04.20064550