

Peer-to-Peer Electronic-Payment System

Field of the Invention

- 5 The present invention relates to a peer-to-peer electronic-payment system and refers particularly, though not exclusively, to such a payment system wherein digital money is generated in a distributed manner.

Background to the Invention

- 10 A significant factor in the growth of the Internet has been, and still is, electronic commerce - the ability to advertise goods and services, search for suppliers, compare prices and make payments, all being conducted at a few clicks of a computer mouse button. One of the challenges facing electronic commerce is how payments can be made efficiently, reliably, and securely. During the past several years, many electronic payment systems have been
15 proposed, and some of them have been implemented and deployed.

- Electronic payment systems can be broadly classified into two categories: cash-like systems and bank-account-based systems. In cash-like or electronic cash systems the payer/customer withdraws electronic cash tokens through an account established with a
20 bank before purchases are made. The electronic cash tokens have denomination values and may be spent with a payee/shop who in turn deposits the tokens in its own account established with the same or another bank.

- Bank-account-based electronic payment systems include pay-now systems and pay-later
25 systems. In pay-now system, the payer's account is debited at the time of payment. In pay-later systems, the payee's bank account is credited the amount of sale before the payer's account is debited.

- The two most basis requirements for electronic cash systems are preserving payer
30 anonymity and preventing double spending. In most electronic cash systems, electronic cash tokens have fixed denomination values and therefore one needs the right combination of tokens to make a payment. This is necessary so that the bank cannot trace the payer by looking at the value of the purchase. However, maintaining payer anonymity is a double-edged sword. While user anonymity prevents someone from compiling dossiers on the
35 spending patterns and whereabouts of individuals, criminals can also exploit it for, by way of example, blackmailing or money laundering. It is this concern that has recently lead to the study of anonymity revocation techniques.

Double spending in electronic cash systems is dealt with by "after-the-fact-detection" in the sense that the ID of a double-spending payer can be recovered. However, financial businesses are reluctant to accept such security mechanisms since they are subject to attacks by an enemy. "Prevention-before-the-fact" solutions are more welcome. Another
5 drawback of some electronic cash systems is that they are based on operations of public key cryptosystems and, therefore, are computation intensive.

In bank-account-based payment systems, a payment is conducted by sending an information object, whether it is a cheque or a credit card slip, from the payer to the payee. The object
10 should be self-contained with all information needed to complete the payment. In bank-account-based systems, the information object issued by the payer carries the exact amount of payment. Since payer anonymity is not a concern in bank-account-based payment systems, such systems are naturally suited for home billing, electronic ordering, and medium-to-high value payments for electronic shopping. An important problem in the design
15 of bank-account-based payment systems is how to prevent a payer from over drawing their bank account. When the payee accepts to cheque from the payer, the payee should be assured that the payer's account has sufficient funds available to meet the payment. One approach suggested in is analogous to that of a certified check. The payer draws a check and provides the details (the cheque number, the payee and the amount) to his bank. The
20 bank places a hold on the amount of money and returns an authorization token to the payer certifying that the payer has sufficient funds to cover the check. The payer presents the authorization token and the cheque to the payee. While this method works in preventing overdrawing of payer's account, it may not be suitable for on-line transactions where the amount of the payment may be negotiated in real time.

25 Peer-to-peer (P2P) systems are distributed systems where all nodes are peers in the sense that they have equal roles and responsibilities. Peer-to-peer systems presently available are mostly for free sharing of files and computation resources amongst a community of peers, such as Napster, Gnutella and Freenet. Much research has been done on peer-to-peer
30 systems in recent years.

In a peer-to-peer commerce environment, every peer can be both a merchant – to sell something - and a customer – to buy something. In a particular transaction, a peer who sells something is called a merchant peer while the peer who buys something is called a customer
35 peer. An example of such a peer-to-peer commerce environment could be a community of video enthusiasts, who shoot their own videos on various topics and trade the videos with each other for entertainment. The attractive feature of peer-to-peer commerce is that a person can make money provided the person has something other people want.

Summary of the Invention

5 The present invention provides a peer-to-peer payment system that is similar in operation to an electronic cash system in that payers need to withdraw money (digital tokens) from a bank in advance and the tokens have fixed denomination values. The system is for macro-payments catering mainly to low-to-medium value payments. However, the system does not support full anonymity (unlinkability) for the customer, which can only be achieved using public key cryptosystems.

10 The system uses relatively lightweight computation, and avoids public key operations. The system prevents double spending in a "prevention-before-the-fact" manner, where there is no need for payees to check online with banks. The payee authenticates the payment directly.

15 Moreover, it allows peers to become merchants while at the same time protecting the interests of customers and banks. Merchant servers are attractive to attackers. With the present invention, compromise of a merchant is time-limited since digital money has expiry dates. If digital money is stolen from the merchant, it will be no use to an attacker.

20 The payment system of the present invention has a trusted party that is required to play the role of a bank. Although the nature of peer-to-peer systems is to exclude a central party, a trusted bank is always necessary and must be involved whenever a payment system is created. However, the trusted party of the present invention doesn't know what the merchant peer is selling and the merchant peer doesn't require any sensitive personal information from the customer. The trusted party is not the party that produces the digital money. Instead, the money is generated by every merchant peer in a distributed manner and is validated by the trusted party by adding a stamp. However, digital signatures are normally not used for stamping the money to keep computational requirements as low as possible. Hence, public key cryptography operations are normally not used.

30 There are three main entities in this payment protocol. The broker is the most trusted entity. A bank or a credit card authority may be the broker role. The peers involved are customer peers and merchant peers, depending on their role during a transaction. As already mentioned, these two roles are interchangeable. A customer peer can be a merchant peer and vice versa.

35 A merchant peer generates digital notes in several fixed denomination values, which reflect the prices of the goods/services it is selling. Each peer has only a finite set of fixed prices for its goods. This is a reasonable assumption for a peer-to-peer commerce environment where

peers mainly trade digital goods such as pictures, e-books, video/audio files etc. The generated digital notes are submitted to the broker by the merchant peer for validation and stamping. The notes are preferably spent only at the particular merchant peer. The broker validates the notes by generating stamps for the notes, but the broker will not give the stamps to the merchant peer. Instead, the broker returns a stamp verification code to the merchant peer so that the merchant peer is able to check whether a stamp verification code from a customer peer is valid during an electronic purchase. Preferably, no peer can generate other peer's notes. More preferably, the broker cannot generate merchant peer's notes.

A customer peer withdraws the digital cash of a merchant peer - from whom an electronic purchase is desired - from the broker. The customer peer purchases digital cash or notes from the broker using macro payment mechanisms such as for example, credit card payment schemes. The broker gives not only the notes but also the broker stamps to the customer peer. The customer peer will spend the notes at the merchant peer by giving both the notes and the stamp. Upon receiving the payment, the merchant peer checks both the received note with its own database, and the stamp by checking it with the stamp verification code received from the broker. The merchant peer need not check online with the broker to prevent double spending.

A merchant peer can claim money from the broker by giving the broker stamps it received (from the customer peer) to the broker. A customer peer is allowed to refund the notes and the associated stamps from the broker if the customer has not spent the money. To prevent the customer cheating by refunding spent notes, there may be specified time limits for both merchant redemption and customer refund.

All the previous e-payment systems adopt at least one of the following three approaches, public key cryptography, secret sharing between bank and merchant, or online checking with a trusted bank to prevent double spending. The present invention does not use any of the above three approaches. Public key cryptographic operations consume much computation, while online checking always decreases efficiency and introduces operational delay. Sharing of secrets between bank and merchant could lead to some advantages during the verification of digital money, however it jeopardizes the security and reliability of the system.

Preferably the broker is always online. Merchant and customer peers are not necessarily always online. Notes submission from merchant peer to broker can be done in batches. Notes can be obtained from the broker at any time, either in batches or individually. The merchant peer may redeem money from the broker at any time before the deadline for redemption. The customer peer can only refund notes that have not been spent after the

refund starting time and before the expiry time. Refund should preferably be processed in batches to make the process more efficient.

Description of the Drawings

5

In order that the invention may be better understood and readily put into practical effect, there shall now be described by way of non-limitative example only preferred embodiments of the present invention, the description being with reference to the accompanying illustrative drawings in which:

10

Figure 1 is a schematic arrangement of the relationship between the parties when the merchant peer generates digital notes;

15

Figure 2 is a view similar to Figure 1 when the merchant peer transfers the notes to the broker for stamping;

Figure 3 is a view similar to Figure 2 when the customer peer purchases digital money;

20

Figure 4 is a view similar to Figure 3 when a customer peer purchases from a merchant peer;

Figure 5 is a view similar to Figure 4 when a merchant peer obtains a redemption from the broker; and

25

Figure 6 is a view similar to Figure 5 when a customer peer refunds un-spent money.

Description of the Preferred Embodiments

In this description the following apply:

30

- X, Y means the concatenation of X with Y
- $\text{KeyedHash}_{K_A}(X)$ means that X is hashed using a secret key K_A . A Keyed-hashing algorithm is also referred to as MAC (message authentication code) algorithm
- $\text{Hash}(X)$ means that X is hashed with a one-way hash algorithm

35

In any peer-to-peer payment systems there are many variables. The present invention includes the following variables:

1. $K_{\text{MerchantPeer}}$ is the secret key used by the merchant peer (and known only to the merchant peer) to key hash the digital notes.

2. K_{Broker} is the secret key used by the broker (and known only to the broker) to key hash the digital notes.
3. $ID_{\text{MerchantPeer}}$ is the identification of the merchant peer.
4. ID_{Broker} is the identification of the broker.
5. ID_{Customer} is the identification of the customer.
6. $SerNum$ is the unique serial number associated with every digital note. The merchant peer generates this serial number.
7. $Value$ refers to the denomination value of the digital note. There can be multiple denomination values but it may be necessary to have notes with reasonably low denomination values since the protocol does not support the concept of change. The exact amount has to be supplied during a purchase.
8. T_0 is the time of issue of the digital note.
9. T_1 is the expiry time for the merchant peer to seek redemption from the broker.
10. T_2 is the start time for the customer peer to seek refund from the broker.
11. T_3 is the expiry time for the digital note.
12. SVC is the stamp verification code explained in the next section.

The preparation of digital notes by a Merchant Peer is shown in Figure 1:

$ID_{\text{Material}} = ID_{\text{MerchantPeer}}, Value, SerNum, T_0, T_1, T_2, T_3$

$Digital\ Note = ID_{\text{Material}}, KeyedHash_{K_{\text{MerchantPeer}}}(ID_{\text{Material}})$

As shown in Figure 2, the Merchant Peer then transfers the created digital notes to a broker, and the broker adds a broker stamp.

$Broker\ Stamp = ID_{\text{Broker}}, KeyedHash_{K_{\text{Broker}}} (Digital\ Note, ID_{\text{Broker}})$

Stamp verification code ("SVC") = Hash (Broker Stamp)

Stamped digital note = {Digital Note, Broker Stamp, Stamp Verification Code}

- The broker then transfer the SVC to the merchant peer and the stamped digital note is ready for circulation. The stamped unspent digital note should be kept secret and protected by the entity possessing it, either by the broker or customer

As shown in Figure 3, customer peers may have a long-term relationship with the broker. When a customer peer wants to purchase goods/services from a particular merchant peer, they approach the broker, obtain a required amount of digital cash (issued by the merchant peer and stamped and stored by the broker) using macro payment mechanisms such as credit card payment schemes.

Referring now to Figure 4, once a customer peer has obtained digital cash from the broker they can purchase goods/services from the merchant peer. During a transaction process the customer peer reveals the stamped digital note, excluding the broker stamp. Before approving a transaction, the merchant peer checks:

1. That current time $< T1$;
2. That the digital cash has not been spent yet; and
3. The SVC matches with the SVC provided by the broker for that particular note

The merchant peer then approves the transaction and transfers the goods/services purchased to the customer peer. In return the customer peer transfers the broker stamp (whose hash should be equal to the SVC).

To now refer to Figure 5, a merchant peer can redeem the value of digital cash before time $T1$ associated with the digital cash. The merchant peer has to reveal the broker stamp to the broker, the broker stamp having been transferred to the merchant peer by customer peer during the transaction. The broker checks for validity of the broker stamp, and if valid, credits the merchant peer's account.

In Figure 6 there is shown the process by which a customer peer can seek refund of any unused digital cash. After time $T2$ has elapsed and before time $T3$ (expiry time), a customer peer can approach the broker for a refund. A customer peer cannot seek refund of digital cash already spent because the merchant peer would have redeemed real money in lieu for spent digital cash transferred to it by the customer. The broker checks for the validity of the unspent digital cash (especially the broker stamp) and refunds the customer peer.

After time $T3$, the digital cash is considered invalid. The merchant peer should have redeemed real money for any digital cash spent by a customer peer at its site by time $T1$.

As the clocks of the entities involved may not be synchronized, so a time delay may be allowed. This is Δ , where Δ specifies the maximum tolerable difference in time between the clock of the broker (assumed to have a reliable clock) and a peer. The creation of digital cash and its purchase by customer peers remains the same.

A merchant peer should seek redemption before T1. The broker should however entertain redemption requests up to $T1 + \Delta$, according to the broker's clock.

A customer peer should seek refund from the broker between time T2 and time T3.

5 However, the request should be made (according to the broker's clock) any time after $T2 - \Delta$, but before $T3 + \Delta$. Hence

$$2\Delta < T2 - T1$$

and

10 $2\Delta < T3 - T2.$

The broker may eliminate notes after expiry at $T3 + \Delta$.

As is clear, the system of the present invention, does not use a public key operation.

15 Moreover, double spending does not require verification with a centralized server. As such the system can be highly efficient. The customer peer, the most vulnerable entity, has sufficient safeguards to protect against fraud by the merchant peer (which should be considered less trustworthy than a established web commerce site). Moreover this scheme also ensures that the merchant peer does not have to obtain sensitive customer information
20 to complete a transaction. As such, a compromise of a merchant peer is not severe, and damage can be easily localized.

It is preferred for all the computer systems involved and to be secure, and all secrets to be well protected. All network communications are preferably secured using mechanisms such
25 as HTTPS.

The system can prevent and deter wrongdoing on the part of any of the entities involved, especially the peers, in a peer-to-peer environment. The digital notes generated by the merchant peer are protected by the keyed hash of the merchant peer. So it is impossible for
30 any other party to create the digital notes. The digital notes are stamped (keyed hash of the broker) by the broker and the SVC transferred to the merchant peer. The merchant peer does not know the broker stamp at that time and cannot create broker stamps of its own. Only the customer peer and the broker know the broker stamp as well as the SVC.

35 When a customer peer uses digital cash, the merchant peer removes the particular digital stamped note from its database. This prevents double spending. The customer peer cannot spend the digital money at any other merchant peer. The customer peer cannot seek refund

for digital money before time T2. This prevents the customer peer from spending money and still seeking refund from the broker.

5 The merchant peer cannot seek redemption of spent digital cash from the broker unless it can provide the correct broker stamp for each digital note. So the merchant peer cannot seek redemption for fraudulent money it creates on its own.

10 Each stamped digital note has an expiry date. So compromises are time limited. Compromise of the merchant peer's secret key will not compromise the system since the attacker also needs the broker's secret key to create valid digital money.

15 The main module used by the customer peer will be a wallet software. The wallet software is preferably capable of securely communicating with the broker as well as various merchant peers. It also preferably maintain an audit log of all transactions and manage digital notes from various merchant peers. The wallet preferably has the customer peer's machine inform the customer peer of impending refund expiry times of digital cash stored in it the customer's machine.

20 Digital money that is stored in the wallet should be protected against compromises as stolen money can easily be misused and spent.

Alternatively, the digital money of the various customer peers may be stored on a central server, possibly by the broker.

25 A merchant peer is an entity that is interested in selling goods/services on-line. They may not be a well-established e-merchant, and might not have the resources to be a full-time e-merchant. It is possible that they can be students or amateurs. Hence, they may not be meticulous in managing their on-line site. Moreover they might not be on-line all the time.

30 The merchant peer may have a payment gateway and a "digital money creation" module. Since the broker stamps the digital notes created by the merchant peer, even if an attacker compromises the merchant peer server and steals digital notes (even with the SVCs), they will not be able to be use because when a customer peer makes a purchase, the customer peer has to reveal the broker stamp (whose hash is the original SVC). Only the broker and
35 the relevant customer peer know the broker stamp. So even if the merchant peer database is stolen, it cannot be misused.

The broker is preferably the most trusted entity and may be operated by a bank or a credit card institution, or a similar organization. Advantageously, the broker has secure facilities to

house servers to which merchant and customer peers make connections. The broker is preferably on-line all the time.

5 The relationship between the broker and a customer peer may be long-term. Hence, the broker may be the guarantor for the customer peers. In a P2P environment, it may be difficult to trust a merchant peer. The broker redeems stamped digital notes from the merchant peer only when it receives the correct broker stamps before time T1. The merchant peer should possess valid broker stamps only if a customer peer has transferred them to the merchant. Hence, real money is transferred to the merchant peer only when the
10 broker is fully satisfied that the customer peer has transferred the broker stamps to the merchant peer.

15 The three main entities, broker, merchant peer and customer peer need to communicate with each other. They may use standard network security protocols such as SSL over HTTP (HTTPS).

It is common human behavior not to trust strangers especially in financial transactions. The natural tendency when having to deal with unfamiliar people is to involve an intermediary, known to all the interested parties involved in the transaction. The broker in this protocol
20 plays that role. The broker may use traditional risk management strategies used by banks, and other financial institutions to associate risk with a peer. Merchant peers as well as customers peers, may be rated according to their credit history. A customer peer can become a merchant peer and credit histories of one kind can be used to determining risk category of another. For example, a new merchant peer might fall into a "very risky" category
25 while a long-standing merchant peer might fall into a "reliable" category. The evaluation of "risk" should be done by the broker, and can be determined not only on the credit history of the merchant peer but also based on factors such as reliability and load handling capabilities of the merchant peer servers, merchant peer's management practices, whether the merchant peer servers have been compromised earlier, and so forth.

30 Depending upon the risk category of the merchant peer, the broker may charge a transaction fee on each digital note transacted. The broker may request for a deposit from the merchant peer, especially for a new merchant peer. Risk categories can change with time. In this way, the broker can not only protect its own interests but also the interests of other peers. Brokers
35 may reveal ratings of merchant peers to a requesting customer peer to enable the customer peer to evaluate the risk involved in a transaction.

Customer peers may also be rated. A new customer peer may be considered unreliable with regard to a longstanding customer. Customer peer rating can be used to determine the

liability the broker is willing to accept if there is a purchase dispute between the customer peer and merchant peer. For example, if a long standing customer peer complains about a transaction with an unreliable merchant peer, the broker might be willing to compensate the customer peer and deduct an equivalent amount from the deposit submitted by the merchant peer.

The broker may be a computer system of a financial or other organization, and both the merchant and customer peers may be computers of a merchant and customer respectively.

10 The present invention also extends to a computer usable medium comprising a computer program code configured to cause a processor to execute one or more functions to perform the methods described herein.

15 Whilst there has been described in the foregoing description preferred embodiments of the present invention, it will be understood by those skilled in the technology that many variations or modifications in details of the system may be made without departing from the present invention.

20 The present invention extends to all features disclosed and claimed both individually and in all possible permutations and combination.

The claims:

1. A peer-to-peer financial transaction method to be conducted over a telecommunications network, the method including the steps of:
 - 5 a. a first peer generating at least one digital note and submitting the at least one digital note to a broker for validation and stamping;
 - b. the broker generating a broker stamp for the at least one digital note and a stamp verification code; and sending the stamp verification code to the first peer;
 - 10 c. a second peer purchasing the at least one digital note from the broker;
 - d. the broker providing the at least one digital note and the broker stamp to the second peer;
 - e. the second peer providing to the first peer the at least one stamped digital note and the stamp verification code, but without the broker stamp, in return for goods/services;
 - 15 f. the first peer checking the at least one digital note and the stamp verification code; and
 - g. the second peer transferring to the first peer the broker stamp.
- 20 2. A peer-to-peer financial transaction method to be conducted over a telecommunications network, the method including the steps of:
 - a. a first peer generating at least one digital note;
 - b. submitting the at least one digital note to a broker for verification;
 - c. receiving from the broker a stamp verification code for the at least one digital
 - 25 note;
 - d. receiving from a second peer a request for goods/services in return for a payment;
 - e. receiving the at least one digital note with the stamp verification code from the second peer;
 - 30 f. checking the at least one digital note and the stamp verification code; and
 - g. supplying the requested goods/services to the second peer and receiving from the second peer a stamp of the broker.
3. A peer-to-peer financial transaction method to be conducted over a telecommunications network, the method including the steps of:
 - 35 a. receiving from a first peer at least one digital note for verification;
 - b. generating a stamp for verifying the at least one digital note;
 - c. generating a stamp verification code for the stamp ;
 - d. sending the stamp verification code to the first peer;

- 5 e. receiving from a second peer a request to purchase the at least one digital note; and
- f. sending the at least one digital note; the stamp, and the stamp verification code to the second peer as a result of the purchase thereof by the second peer.
4. A peer-to-peer financial transaction methods to be conducted over a telecommunications network, the method including the steps of:
- 10 a. a second peer making a request to a broker to purchase at least one digital note;
- b. making a payment for the at least one digital note;
- c. receiving from the broker the at least one digital note, a broker stamp, and a stamp verification code;
- 15 d. making a request of a first peer to purchase goods/services using the at least one digital note;
- e. sending to the first peer the at least one digital note and the stamp verification code in payment for the goods/services; and
- f. sending the broker stamp with the at least one digital note to enable the first peer to verify the at least one digital note.
- 20 5. A method as claimed in anyone of claims 1 to 4, wherein in step (f) the first peer also checks the at least one digital note with a database of digital notes of the first peer.
6. A method as claimed in claim 5, wherein the database of digital notes includes a field indicating those digital notes the first peer has submitted to the broker for stamping.
- 25 7. A method as claimed in any one of claims 1 to 6, wherein there is included a final step of the first peer forwarding the stamp to the broker to obtain a redemption.
- 30 8. A method as claimed in claim 7, wherein the first peer has a first predetermined time from a time of issue of the at least one digital note in which to forward the stamp to the broker for the redemption.
- 35 9. A method as claimed in any one of claims 1 to 8, wherein the second peer can present the at least one digital note and the stamp to the broker for a refund within predetermined time but not thereafter.

10. A method as claimed in claim 9 when appended to claim 8, wherein the refund cannot take place before the expiry of the first predetermined time.
- 5 11. A method as claimed in any one of claims 1 to 10, wherein the second peer cannot use the at least one digital note and the stamp for a purchase after expiry of a third predetermined time.
12. A method as claimed in claim 11, wherein the at least one digital note expires at the end of the third predetermined time.
- 10 13. A method as claimed in claim 11 or claim 12, wherein the third predetermined time is the same as the first predetermined time.
- 15 14. A method as claimed in any one of claims 1 to 13, wherein the at least one digital note includes a plurality of digital notes of different values, each of the plurality of digital notes having a unique serial number.
- 20 15. A method as claimed in any one of claims 1 to 14, wherein there are a plurality of first peers, each of the plurality of first peers being able to issue digital notes, the digital notes of one first peer being able to be used by the second peer to effect a transaction with the one first peer but no other of the plurality of first peers.
- 25 16. A method as claimed in any one of claims 1 to 15, wherein the first peer is a merchant peer and the second peer is a customer peer.
- 30 17. A method as claimed in any one of claims 1 to 16, including allowing a time delay due to lack of clock synchronization.
18. A method as claimed in any one of claims 1 to 17, wherein the at least one digital note is protected by a keyed hash of the first peer.
- 35 19. A method as claimed in any one of claims 1 to 18, wherein the broker stamp includes a keyed hash.
20. A method as claimed in any one of claims 1 to 19, wherein the stamp verification code is a cryptographic hash of the broker stamp.

21. A computer usable medium comprising a computer program code configured to cause a processor to execute one or more functions to perform the method as claimed in any one of claims 1 to 20.