社団法人　電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

信学技報
TECHNICAL REPORT OF IEICE.

中央銀行の発行に適した電子マネー

木下　宏揚†　　森住　哲也††

† 神奈川大学
†† 東洋通信機

あらまし　電子マネーは電子商取引の基本的な要素となる。電子マネーが従来の現金に取って代わるためには、通貨の供給量をコントロール可能でなければならない。現金には情報、証拠、象徴の 3 つの機能がある。このうち、象徴的機能は二重使用を防止するために重要な要因となる。本研究は電子マネー発行者を中央銀行とし、中央銀行が管理する分散データベースと匿名通信路を利用することによりプライバシー保護と安全性を両立させるシステムを提案する。発行の権限を中央銀行に持たせることによりマネーサプライの制御が可能となる。電子マネーとユーザは一対の公開鍵暗号で関連付けられる。データベースは口座ではなく発行した電子マネーの価値を管理するために用いられる。ユーザは匿名で電子マネーを所有することができる。

キーワード　電子商取引、電子マネー、情報セキュリティ

An electronic money system suitable for the central bank

KINOSHITA HIROTSUGU† and MORIZUMI TETSUYA††

† Kanagawa University
†† Toyo Communication Equipment Co., Ltd.

Abstract　Electronic cash may be the most fundamental elements on the electronic commerce. The control of memory flow by the finance administration authorities must be considered to alter from conventional cash. The central bank coordinates a quantity of publication of a currency and coordinates money supply so that inflation does not occur. The money has three function of the information, the evidence and symbol. The function of symbol is important factor to prevent duplicate reuse of money. We propose an electronic cash system using distributed database of a central bank as new settlement method. In this system, the money is issued by the central bank and the value of money is not stored in users hardware such as IC cards. A money and a user are linked by public key cryptography. The database of the central bank is not a bank account, but manages the value of the issued cash. The user can possess the cash anonymously. Furthermore, the money supply could be controlled by the central bank.

Key words　Electronic-Commerce, Electronic Money, Security

1. まえがき

インターネットを利用したビジネスを支えるインフラとして効率的で安全な決済システムが必要とされている。電子マネーはこの要求に答えて発展してきた。[5] [6] [7] [8] [9] しかし、電子マネーの「価値」を記録する形態によっていくつか問題が発生する。従来の電子マネーシステムの多くが「価値」を IC カードに記録している。したがって、耐水性、耐火性、耐衝撃性などが要求される。さらに、一度支払いに用いた電子マネーの再使用など不正使用や現在の現金でも対策が必要な偽造といった問題に対処しなくてはならない。また、現金の発行機関である中央銀行による通過の供給量すなわちマネーフローの管理が可能でなければならない。中央銀行が市場に流通している現金の発行量を調整できないとインフレやデフレを引き起こす原因となる。一方、現金の匿名性と電子決済の利便性の組合わせが犯罪を助長する恐れがある。

本稿では、新しい決済手段として、中央銀行の分散化されたデータベースを用いた電子マネーシステムを提案する。このシステムでは、現金は中央銀行によって発行されその価値は IC カードのようなユーザの所持するハードウェアに蓄積されない。その代わりに電子マネーとユーザは一対の公開鍵暗号の鍵で結び付けられる。中央銀行のデータベースは通常の意味での銀行の預金口座とは異なり、発行された現金の価値の管理のみを行う。ユーザは電子マネーを匿名で所持できる。さらに、中央銀行によるマネーサプライも可能となっている。

2. 現金と電子マネーの性質

2.1 貨幣の必要性

貨幣の必要性は次のものがあると考えられている。

- 価値の交換

物々交換である場合を除いて、企業や個人の間で取引をおこなうと債権と債務が発生する。したがってこれを解消するためには、同等の価値があるものを債権者から債務者へと移動する必要がある。この価値があるものとして貨幣が用いられる。

- 価値の基準

ある物がある物に対してどのくらい価値があるかを決定することは経済活動で基本的な事項である。貨幣は物の価値に対する比較基準となる。

- 価値の保蔵

債権を回収したあと直ちに債務の解消に充当する当てがなければ価値を何らかの形で保存する必要がある。貨幣はこの目的にも使用される。

電子マネーが完全に現金と置き換わるもしくは現金と固定したレートで双方向に交換可能であることが保証されない限りは、交換媒体としての決済手段の機能を完全に果たすことは困難である。また価値尺度や価値保存として利用することも困難である。

2.2 現金の備えている性質

貨幣の必要性を満たすため現状では中央銀行の信用創造に基づく現金が発行されている。一般に現金は次のような性質を持っている。[2][13][14]

- 全国どこでも使える流通性
- 受け取った現金を別の支払に使用できる連続譲渡性
- どのような用途の支払でもできる汎用性
- 取引と同時に決済が完了する完了性
- 偽造が困難な安全性
- 誰がどこで使用したかがわからない匿名性

しかし、現状の紙や金属の現金には次のような問題点がある。現金書留の利用など遠隔地への送金が不便である。1 万円札の価値を二つに分割したり、統合したりすることができない。仕訳、保管、紛失、盗難など取り扱いが不便である。貴重な紙の資源を消費している。

2.3 換金可能証書の機能

上述の現金の性質以外にも、決済手段として用いるための現金や小切手など換金可能証書には 3 つの機能がある。

- 情報

情報の機能はデータとしての貨幣価値を示す。この機能は電子マネーとして簡単に実装できる。

- 証拠

証拠の機能は貨幣の発行者の正当性を示す。この機能は電子マネーではデジタル署名として実装される。

- 象徴

象徴的機能は誰が貨幣の価値を行使することができるかを示すものである。紙幣の場合を考えてみると紙幣を所有しているという事実に意味があり、紙幣の所有者がその価値を所有権の移転とともに交換できる。

2.4 電子マネーに必要な条件

以上の現金の性質を踏まえて、電子マネーシステムを実装するにあたってはいくつか要求される条件がある。

（1） 独立性

電子マネーは物理的なメディアに依存していないことが望ましい。ハードウェアに依存する限り偽造の可能性は否定できない。この条件は電子マネーをネットワーク上のデータとして扱うことを可能にする。

（2） 安全性

電子マネーの不正なコピーと偽造が防止されている。これには電子マネーの二重使用も含まれる。二重使用を防止する手法としては、使用済の電子マネーのデータベースを利用刷る手法や二重使用時に匿名性が破れる仕組みを設けペナルティーを科す手法が考えられているがデータベース維持のコストが高いことや食い逃げなどペナルティーが必ずしも有効でない場合もある。

（3） 匿名性と追跡不可能性

匿名性とは電子マネーの発行者の決済の記録とユーザの対応関係を識別できないことである。追跡不可能性とは電子マネーの流通の履歴を追跡できないことである。これら匿名性と追跡不可能性はユーザのプライバシーを守るために必須となる。例えば、誰がどこのお店で買い物を行ったとか、二つの企業の間で取引があったなどの情報は保護されなければならない。追跡可能性と関連した項目としてはリンク可能性がある。リンク可能性とは誰のものかはわからないが、特定の電子マネーの流通を補足可能なケースである。匿名性が保たれていればリンク可能性から有益な情報は得られない場合が多い。

（4） オフライン性

オフライン性とは支払いのプロセスは第三者とのオンラインでの通信なしに、電子マネーの正当性の検査を行うことができる性質である。この要求は、今後のユビキタスなネットワークの普及を考えると必ずしも重要とは言えない。

（5） 譲渡制と流通性

電子マネーはその発行者に直ちに還流するのではなく、ユーザの間を転々と流通する。

（6） 分割性

電子マネーの額面が使用時に分割して使用することが可能な性質である。ただし、合計金額を減額していくタイプの場合は分割性は意味がない。

これら以外にも電子マネーを普及させるためには、取り引きの規模がある程度大きくなりコストは低減させる必要がある。さらに店舗や顧客が簡単に利用でき店舗にとってコスト削減につながらなくてはならない。[1]

2.5 従来の電子マネー

電子マネーはいくつかの観点から分類できる。[3][4] まず、電子マネーで使用するハードウェアなどの媒体からは以下のように分類できる。

- IC カードに蓄積する電子マネー

電子マネーの価値は IC カードに充填される。システムのセキュリティは IC カードの物理的な耐改竄性に依存する。

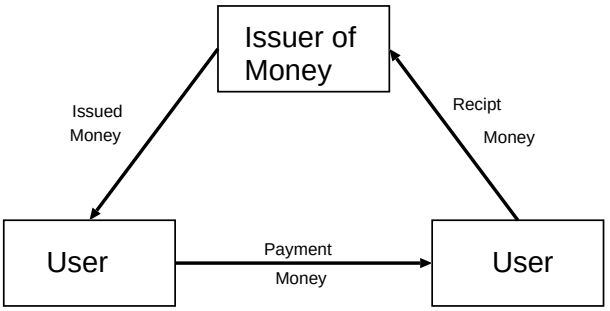

図 1　Closed loop type

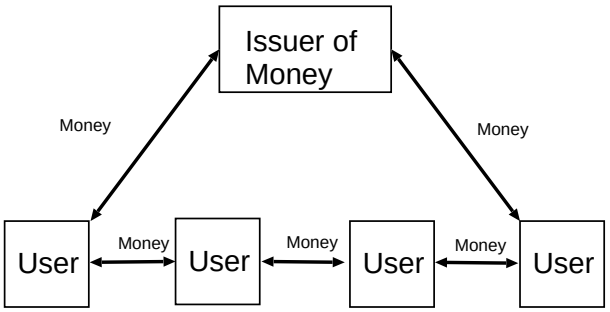

図 2　Open loop type

- ネットワーク上の電子マネー

システムのセキュリティは暗号に基づいたアルゴリズムとと認証機関の信用に依存している。ネットワーク上の電子マネーでは匿名性の確保が問題となるが匿名口座 [13] [14] を用いることによって解決する方法がある。

- ハイブリッド型

IC カードとネットワークの組合わせで両者の利点を持ち合わせている。

決済の柔軟性と偽造防止の観点からは IC カードに依存しない方式が望ましい。もう一つの分類法は図 1 と図 2 にしめすように、電子マネーの流通によるものがある。

- クローズドループタイプ

電子マネーの受領者は、受け取った電子マネーを第三者に転送できない。受け取った電子マネーは決済の度にその発行者に還流する必要がある。

- オープンループタイプ

電子マネーは、発行者に還流することなくユーザからユーザへの流通が可能である。

次の分類は決済の完了するタイミングによるものである。

- 後払い

決済は取引のあとに完了する。クレジットカードは典型的な後払いの決済である。

- 同時払い

決済は取引とほぼ同時に行われる。現金や出ビッドガードはこの分類に属していると考えられる。

- 先払い

決済は取り引きの前に完了している。プリペイドカードはこの分類に属している。

典型的なプリペイドカードは銀行の預金口座から IC カードへ電子マネーの価値が充填される。そのあと店舗での支払いが行われる。クレジットカードは取り扱わなければいけない現金の量を減らし取り引きの機会を失うことを防ぐまた顧客情報の蓄積や資金の流れの捕捉を容易にする。言い換えれば、匿名性は低いと言える。このため、決済は電子マネーでは決済は直ちに終了することが望ましい。

データ保管場所	ローカル	TFM	リモート
所有者のメタアクセス権	有り	無し	無し
情報のフロー	無し	無し	有り
通信	不要	不要	必要
情報紛失責任	自己	自己	相手

表 1　データ保管場所

3. 電子マネーのあるべき形態

3.1 データの存在場所の意味

電子マネーの価値の実体をどこに保管するかという問題について考えてみる。保管場所の形態は 3 つあると考えられる。これらの相違点は、システムの特権ユーザの権限のおよぶ範囲と関連がある。表 1 にデータ保管場所の特徴をまとめる。メタアクセス権とはアクセス権の設定に対するアクセス権である。メタアクセス権があれば無制限のアクセス権を持つことになる。情報のフローとはプライバシーに関する情報など所有者の意図に反して情報が流出する可能性を示す。

（1） ユーザが保管する場合 (ローカルな保管)

ユーザは保管するデータに関してあらゆるアクセス権を行使できる。したがって、システム外部への情報のコピーが可能となる。このことの副作用としてデータの消去が保証できなくなる。すなわち電子マネーをユーザがローカルに保管すると二重使用が可能となり、これを防止するための枠組みが別途必要となる。

（2） ユーザが発行者の耐改竄モジュールに保管する場合

耐改竄モジュール (TFM) に対しては所有者はメタアクセス権を持たないと考えられる。なぜなら、モジュールに対して改竄を試みればデータが破壊される可能性が極めて高いからである。したがって、情報の外部へのフローを発行者がコントロール可能であり、データの消去も保証される。したがって、 二重使用を単体で防止可能となる。

（3） 電子マネーの発行者などユーザ以外が保管する場合 (リモートな保管)

保管場所に対してユーザ側の特権ユーザの権限が及ばないためメタアクセス権はない。したがって TFM の場合と同様、二重使用の問題は発生しない。

リモートによる保管の場合、情報紛失責任を問題にする場合があるが、一般に事故などにより情報が失われる可能性はユーザの保管による場合の方が高いと考えられる。また、通信にかかるコストは将来的には十分低くなると考えられるのでこれも問題にはならない。

耐改竄モジュールを利用すればメタアクセス権で有利なように見えるがローカルに情報を維持する以上、偽造改竄の可能性がゼロとは言えない。これらの特徴をふまえると、電子マネー

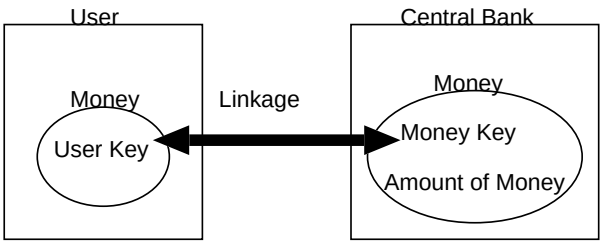

図 3　Linkage of user and money

のように情報のコピーに起因した二重使用などの問題が発生する用途ではローカルな保管は適当とは言えない。

3.2　中央銀行が貨幣を発行する意義

中央銀行が発行する貨幣は、中央銀行の債務であると考えられる。貨幣はその債務に対する請求権となる。電子マネーが新しい通貨として通用するためには、必要な信用力を既存の通貨に依存するのではなく、独自に信用力を創造させる必要がある。また、一般に物の価値はその希少性とリンクしている。現金に価値があると誰もが信じるためには、現金に希少性が確保されていなければならない。すなわち、有限であり発行者以外は作ることができないという保証が必要となる。

一方、通貨の供給量をコントロールすることは経済政策上重要な機能と考えられる。つまり、電子マネーの発行者は十分な信頼性と経済政策に対する責任を持つ必要がある。

以上の観点から、電子マネーが補助的な決済手段ではなく紙幣や硬貨に取って代わるためには中央銀行が発行する形態が望ましい。

4.　提 案 方 式

4.1　システムの概要

従来の電子マネーシステムにはいくつか問題点がある。ほとんどの電子マネーは銀行あるいは発行会社が発行する。これはプリペイドカードか地域通貨に似た側面がある。

またマネーサプライの管理ととセキュリティの観点からこれらの電子マネーは主に少額の決済に適している。したがって、現行の現金をこれらの電子マネーで置き換えることは困難である。

本システムではプライバシーと匿名性は匿名通信路 [10] [11] [12] により実現される。さらに、ユーザと結び付けられる口座や識別番号は一切用いない。

現金の二重使用を防止するために象徴的機能と情報の機能は分離される。情報の機能は中央銀行の管理下にあるデータベースに蓄積される。証拠の機能はデジタル署名により実装する。象徴的機能は、ユーザとマネーを結合する鍵の所有により実現する。公開鍵暗号系の秘密鍵がユーザに割り当てられる。もう一方の公開鍵が電子マネーに割り当てられる。ユーザは複数の電子マネーを好きなだけ所有できる。図 3 は暗号によるユーザと電子マネーの結合を示す。

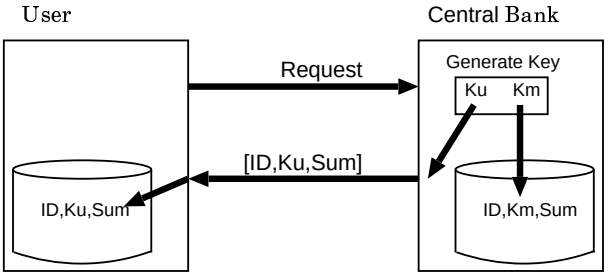

図 4　Registration

5.　プロトコル

5.1　概　　要

この章では、システムのプロトコルについて説明する。まず電子マネーは登録プロトコルにより発行される。そして、支払いは支払いプロトコルによって実行される。

5.2　登録プロトコル

ユーザは電子マネーの中央銀行への登録をリクエストし、電子マネーの識別子と鍵を得る。

（1）　ユーザは追跡不可能な匿名通信路を通して中央銀行に電子マネーの登録の要求を行う。

（2）　中央銀行は鍵のペアと電子マネーの識別番号 ID を生成する。公開鍵暗号系をユーザと電子マネーを結び付けるために使用する。ペアの公開鍵と秘密鍵のうち、ひとつはユーザ鍵 K_u でもうひとつの鍵はマネー鍵 K_m となる。ユーザ鍵を持っているユーザは、そのユーザ鍵と対になるマネー鍵が割り当てられた電子マネーの所有者となる。

$$M_{cu} = [ID, K_u, Sum]$$

がユーザに送られる。ここで $[x, y]$ は x と y の連結を示す。Sum は電子マネーの金額を示し、初期値として 0 が設定される。

（3）　ユーザはこれらの情報を IC カードやパソコンなどに蓄積する。

図 4 は登録プロトコルの概略を示す。ユーザは複数の電子マネーを所有することができる。次の節で説明する支払いプロトコルを利用することにより、それらの間でユーザは価値を自由に移動できる。

5.3　支払いプロトコル

支払いプロトコルの参加者は支払者と受領者である。このプロトコルは支払者から受領者への支払いを示している。

（1）　ユーザ鍵 K_p を用いて支払者は認証子 A_{pb} を計算する。

$$A_{pb} = E([ID_p, Transaction], K_p),$$

電子マネーの識別子 ID_p と認証子 A_{pb} を中央銀行の鍵 K_b で暗号化する。

$$M_{pb} = E([ID_p, Transaction, A_{pb}], K_b).$$

支払者は M_{pb} とともに $Transaction$ を受領者に送信する。

$$M_{pr} = E([Transaction, M_{pb}], P_r)$$

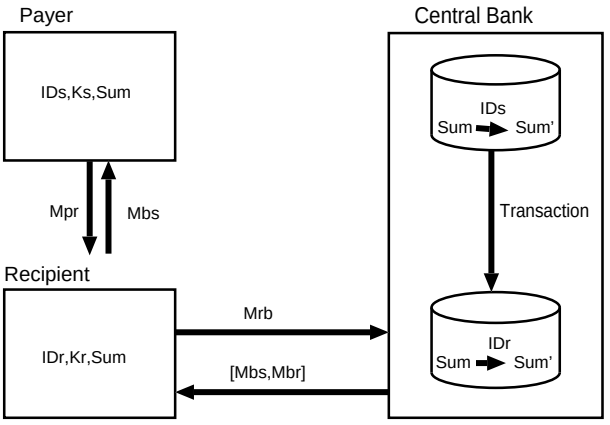

図 5　Payment

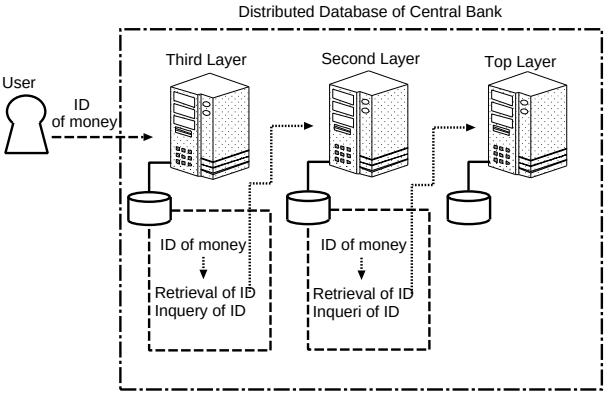

図 6　Hierarchy of database

ここで $h(x)$ は一方向性ハッシュ関数とする。$E(x, y)$ はデータ x を鍵 y で暗号化する関数を示す。P_r は受信者と通信に用いる公開鍵を示す。$Transaction$ は支払者から受領者へ移動する金額を示している。

（2） 受領者は $Transaction$ の正当性を検査する。次に受領者は受領者のユーザ鍵 K_r を用いて認証子 A_{rb} を生成する。

$$A_{rb} = E([ID_b, Transaction], K_r)$$

そして、中央銀行の鍵 K_b を用いて暗号化を行う。

$$M_{rb} = E([ID_r, Transaction, A_{rb}], K_b)$$

最後に受領者は M_{pb} と M_{rb} を中央銀行に送信する。

（3） 中央銀行は M_{pb} と M_{rb} を復号化する。次に中央銀行は M_{pb} と M_{rb} の間の取り引き内容 $Transaction$ に矛盾のないことを検査する。さらに A_{pb} と A_{rb} の正当性を検査する。次に中央銀行は支払者の電子マネーの金額を検査し取り引き内容に応じてデータベースを更新する。最後に、中央銀行は支払者と受領者へ領収書を送信する。支払者に対する領収書は

$$M_{bs} = E([ID_s, Amount], K_s)$$

となり、受領者に対する領収書は

$$M_{br} = E([ID_r, Amount], K_r).$$

となる。

図 5 に支払プロトコルの概略を示す。

6. 電子マネーのための分散データベース

中央銀行のデータベースは分散化され階層構造をなす。これにより、トラフィックと処理が集中することを避ける。またトラフィックは可能な限り局在化させる必要がある。

電子マネーの識別子 ID は、該当する電子マネーがどこのデータベースに蓄積されているか容易に見つけ出すことができるように割り当てられる。ID は $XX\$AA.BB.CC.centralbank.YY.ZZ$ のような形式で記述する。$AA.BB.CC.centralbank.YY.ZZ$ はデータベースを保持するサーバの Fully qualified domain name (FQDN) を示す。AA, BB, CC はデータベースの階層構造を示している。XX は電子マネーのシリアル番号を示す。$ はシリアル番号と FQDN の間の区切り文字を示す。特定の電子マネーの蓄積されているデータベースの位置を解決する手順を以下に示す。

（1） 支払いの受領者は最寄りの中央銀行のデータベースにアクセスする。

（2） 中央銀行のデータベースシステムは支払者と受領者の電子マネーを識別子を手がかりに検索する。

（3） 支払者と受領者の電子マネーが存在するデータベースの間でトランザクションが行われる。

図 6 はデータベースの階層構造を表す。

7. システムの評価

7.1 安全性とプライバシー

安全性の条件は以下のような観点から考える。

- 第三者が電子マネーを盗難できないこと。これは、通信路が暗号化されていることで実現されている。
- 第三者がトランザクションを妨害できないこと。トランザクションの完了は中央銀行から発行された領収書により確認される。何者かによって取引が妨害されて領収書が確認されなかったとしても、プロトコルを最初からやり直せば良い。
- 支払者は電子マネーを不正な二重の支払に用いることはできない。電子マネーの金額は中央銀行の管理下にあるので一度使用すると確実にこれが反映される。
- 受領者はトランザクションを改変することはできない。支払人から受け取ったデータは暗号化され電子マネーに割り当てられた鍵で暗号化されている。もし、支払者と受領者から送られた取引内容 $transaction$ が異なっていたとしても、中央銀行は承認できないと判断できる。

プライバシーと匿名性が以下の観点から保たれている。

- 中央銀行は取引の通信相手が誰だか特定できない。
- 中央銀行は電子現金の流れを追跡できない。

中央銀行と受領者の間の通信は追跡不可能な匿名通信路を用いて行われる。そして、電子マネーとユーザを結び付けるのはそれぞれに割り当てられた公開鍵暗号のみである。

7.2 利 便 性

多くの電子マネーが持つ利便性は提案方式にも受け継がれて

いる。

• 電子マネーの分割は 2 通りの方法で実現されている。本方式では、電子マネーの額面金額は変更可能である。さらに、ユーザは電子マネーを以下の手順で分割可能である。

（1） 新しい電子マネーを中央銀行に登録する。

（2） ユーザの既存の電子マネーから新しい電子マネーへ自分自身が支払者と受領者になって支払の処理を行う。

• 店頭などでの支払とネットワーク上の決済両方に使用することができる。

7.3 物理的な現金との比較

以下に示すように、従来の紙や金属の現金の利点が提案方式に受け継がれている。

• 電子マネーの流通は追跡できない。

• 電子マネーはユーザの間を流通する。電子マネーそのものが流通するわけではないが、電子マネーの価値は直接電子マネーから電子マネーに移動する。

• 提案方式は可搬性にも優れている。提案方式は IC カードなどの耐改竄性モジュールを必要としないので、ユーザは電子マネーを IC カードでもパソコンでも携帯電話などにも蓄積可能である。

• 中央銀行はマネーサプライをコントロール可能である。電子マネーの価値を創造できるのは中央銀行のみである。

8. む す び

本稿では、新しい電子マネーシステムを提案した。ユーザと電子マネーは公開鍵暗号鍵を用いて関連づけられるので匿名性やプライバシーが保護される。さらに、電子マネーの発行者はマネーサプライをコントロール可能で、決済は取引と同時に終了するので、信用の創造を伴わない。今後の課題としては、不正な送金などを防止するために鍵の供託の実装などがある。

文　　献

[1] 岡田仁志:" サイバー社会の商取引–コマーす&マネーの方と経済–", ,ISBN4-621-07019-3, 丸善 (2002)

[2] 青木:“電子マネーが社会に与える影響と問題点” http://cobweb.tamacc.chuo-u.ac.jp/semi/aoki/sotupage.htm

[3] 村松 郁夫:“経営と情報 1 第 6 回” http://serv532.biwako.shiga-u.ac.jp/staff/muramatz/doc/keijo06.pdf

[4] 竹村彰通:“電子マネープロトコル研究の動向” http://www.e.u-tokyo.ac.jp/itme/dp/dp36.pdf(2000)

[5] A.Chan,Y.Frankel,Y.Tsiounis,“Easy Come Easy Go Divisible Cash”, Advances in Cryptology EUROCRYPT'98, LNCS1403, Springer-Verlag, pp.561-575 (1998).

[6] D'Amiano S.,Di Cresceanzo G.:"Methodology for Digital Money based on General Cryptographic Tools",,Proc.of Eurocrypt '94,pp.156-170(1995).

[7] Brands S.:"Untraceable off-line cash in wallets with observers",Proc.of CRYPTO'93,pp.302-318(1994).

[8] D.Chaum,A.FIat,M.Naor,"Untraceable Electronic Cash", Lecture Notes in Computer Science 403,Advances in Cryptology - CRYPTO'88,Springer-Verlag,pp.319-327(1990).

[9] T.Okamoto, K.Ohta:"Universal Electronic Cash" Proc. of CRYPTO'91,LNCS 576,pp.324-337,Springer-Verlag(1991).

[10] D.Charum,"Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms", Communications of the ACM, Vol.24, No.2, pp.84-88(1981).

[11] W.Ogata, K.Kurosawa,K.Sako and K.Takatani,"Fault Tolerant Anonymous Channel",LNCS1334, Proc. of ICICS'97, Springer–Verlag, pp.440-444 (1997).

[12] M.Abe:"Universally Verifiable Mix-net with Verification Work Independent of the Number of Mix-centers", LNCS1403,Advances in Cryptology EUROCRYPT'98, Springer-Verlag, pp.437-444 (1998).

[13] D.R.Simon, “Anonymous communication and anonymous cash",Advances in Cryptology - CRYPTO'96,pp.61-73(1996).

[14] M.Jakobsson,"Mini-Cash: a minimalistic approach to E-commerce",Public Key Cryptography'99,H.Imai and Y.Zheng eds.LNCS 1560,pp.122-135(1999).