2007－MPS－63 (14)
2007／3／4

電子マネーシステムの価値保存形式を考慮したモデル化

小山 健一郎 †, 稲永 俊介 ‡, 安浦 寛人 ‡
† 九州大学大学院システム情報科学府情報工学専攻
‡ 九州大学大学院システム情報科学研究院情報工学部門
〒819-0395 福岡市西区元岡 744
{k-oyama, yasuura}@c.csce.kyushu-u.ac.jp
shunsuke.inenaga@i.kyushu-u.ac.jp

近年，価値を表すデジタルデータをICチップに保存する**ストアバリュー型電子マネー**[1]と呼ばれる電子マネーシステムが注目されている．これまでに提案された電子マネーシステムの安定性に関する手法は，ほとんどが暗号技術や耐タンパー技術といったセキュリティ技術に基づいている[3]．では，仮にこれらのセキュリティー技術が破られたとすると，電子マネーシステムは即座に破綻してしまうのだろうか．
そこで，本稿では電子マネーシステムの「セキュリティ技術やプロトコルとは独立した」安定性について検証する．そのために，まず貨幣の集合論的なモデルを構築し，そのモデルに金銭の流通操作を加えた**貨幣システムモデル**を提案する．さらに，貨幣システムモデルを電子マネーに適用し，**紙幣型マネーシステムモデル**と**残高型マネーシステムモデル**という2つの価値保存形式の異なる電子マネーシステムモデルを提案する．最後に，紙幣型システムと残高型システムにおける「偽価値量」の検知可能性について考察する．ここで，「偽価値量」とは電子マネーシステム内に正規に追加されたものではない価値量のことをいい，現金通貨での偽札や偽硬貨に相当するものである．本稿では，残高型における三者間の偽価値量の譲渡操作ののちに，この偽価値量が検知できなくなってしまうことを示した．

Modeling Electronic Money System Considering Its Value Preservation Formats

Kenichirou Oyama, Shunsuke Inenaga, Hiroto Yasuura
Department of Computer Science and Communication Engineering,
Graduate School of Information Science and Electrical Engineering, Kyushu University
744 Moto'oka, Fukuoka 819-0395, Japan

Many attentions have recently been paid to the so-called value-storing type of electronic money. Since any money operating system requires extremely high stability, information security technologies such as Cryptography and tamper resistance have been developed for maintenance of the stability of the system. But, what happens if those securities are attacked and broken? In this paper, we study the stability of electronic money systems which is *independent* of the security technologies and the protocols used. In so doing, we firstly develop a set-theory-based model for general money systems, and extend it to a *general money system model* by adding to the set-theory-based model some operations for circulation of money. Then, we propose a model for electronic money systems modifying the above general money system model. In particular, two different types of electronic money system, a *note-type money system model* and a *balance-type money system model*, are proposed in this paper. Lastly, we study possibilities of detecting a "fake value" that has been circulated in the note-type and balance-type money system models. Here, a "fake value" applies to a value which was *not* issued by the originator (or issuer) of the system, and thus it corresponds to a counterfeit of cash currencies. As a key feature of this work, we show that a fake value becomes *impossible to be detected* after it is transferred between at least three users.

1 準備

- **価値量（*Right*）集合** $R := \{0, 1, 2, \ldots, n\}$.
  価値を表す0以上n以下の自然数の集合．時刻によらず一定．
- **媒体（*Vehicle*）集合** $V^t := \{v_1, v_2, ..., v_m\}$.
  媒体とは貨幣のことであり，価値量を媒介するものである．
- **ホルダ（*Holder*）集合** $H := \{h_1, h_2, ..., h_l\}$.
  媒体を保持するもの．時刻によらず一定．
- **価値量関数** $I^t : V^t \to R$.
  時刻tにおいて媒体が媒介する価値量を表す関数（図1参照）．
- **保持者関数** $K^t : V^t \to H$.
  時刻tにおいて媒体を保持するホルダを表す関数（図1参照）．

上記で示した集合と関数からなるものを**貨幣集合モデル**と呼ぶ．図1に貨幣集合モデルを示す．

1.1 価値総量保存則

貨幣集合モデルは以下の式を満たすものとする．

$$\forall t \sum_{v \in V^t} I^t(v) = \sum_{v \in V^{t+1}} I^{t+1}(v) \quad (1)$$

つまり，任意の時刻において，全媒体が保持する価値の総量は変化しない．これを，**価値総量保存則**と呼ぶ．

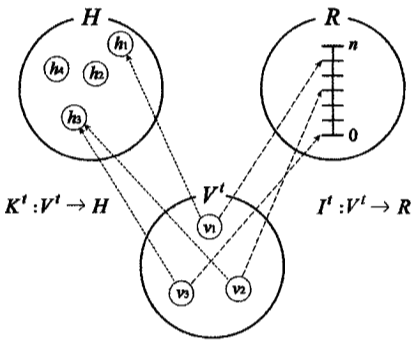

図 1: 貨幣集合モデル

1.2 近似価値量関数と媒体の種類

各ホルダ $h \in H$ は，関数 I の近似関数 I_h を持つ．I_h を**近似価値量関数**と呼ぶ．

任意の時刻 t において，任意のホルダ h は $K^t(v) = h$ である媒体 v にのみ近似価値量関数 I_h^t を行使できると仮定する．

任意の時刻 t において，$F_{I_h^t}(v) = |I_h^t(v) - I^t(v)|$ を媒体 v の I_h^t による時刻 t での**偽価値量**と呼ぶ．これに対し，$I^t(v)$ を媒体 v の時刻 t での**真価値量**と呼ぶ．

F を用いて媒体を以下の 3 つに分類する．

$^\forall t, {}^\forall I_h^t,\ F_{I_h^t}(v_\ell) = 0$ を満たすとき，媒体 v_ℓ を *legitimate* という．$^\exists t, {}^\exists I_h^t,\ F_{I_h^t}(v_f) > 0$ を満たすとき，媒体 v_ℓ を *fake* という．$^\forall t, {}^\forall I_h^t,\ F_{I_h^t}(v_c) > 0$ を満たすとき，媒体 v_ℓ を *copy* という．

2 貨幣システムのモデル

本章では，貨幣集合モデル上の以下の操作を考える．

2.1 譲渡

任意の異なる 2 つのホルダ $h_i, h_j \in H$ を考える $(i \neq j)$．時刻 t から $t+1$ においてホルダ h_i から価値量 r をホルダ h_j に**譲渡**するとは，以下の式が成り立つことをいう．

$$\begin{aligned}
\sum_{K^t(v)=h_i} I^t(v) &\geq r, \\
\sum_{K^t(v)=h_i} I^t(v) - r &= \sum_{K^{t+1}(v)=h_i} I^{t+1}(v), \\
\sum_{K^t(v)=h_j} I^t(v) + r &= \sum_{K^{t+1}(v)=h_j} I^{t+1}(v), \\
{}^\forall x \neq i,j,\ \sum_{K^t(v)=h_x} I^t(v) &= \sum_{K^{t+1}(v_x)=h_x} I^{t+1}(v).
\end{aligned}$$

2.2 システムの安定性

ε を 0 以上の実定数とする．時刻 t において次式が成り立つとき，マネーシステムは時刻 t において ε-**安定**しているという．

$$\sum_{v \in V^t} F_{I_h^t}(v) \leq \varepsilon \sum_{v \in V^t} I^t(v),$$

ただし，$K^t(v) = h \in H$.

3 電子マネーシステムのモデル化

本章では，2 章で示した貨幣システムモデル上の価値保持形式を考察し，ストアバリュー型電子マネー [1] と呼ばれる，ホルダ自身が価値量を保持する形式の電子マネーシステムのモデル化を行う．複数の媒体を保存する形式の**紙幣型マネーシステムモデル**と，残高額のみを保存する**残高型マネーシステムモデル**の二種類のモデルを提案する．

3.1 紙幣型マネーシステムモデル

ある定まった価値量を媒介する媒体をホルダが複数保持する形式の貨幣システムモデルを，**紙幣型マネーシステムモデル**という [4, 5]．

紙幣型マネーシステムモデルでは，任意の媒体が媒介する価値量は時刻によらず変化しない．すなわち，

$$^\forall t\ {}^\forall v \in V^t,\ I^t(v) = I^{t+1}(v)$$

なる式が第 2 章の貨幣システムモデルに加わる．

3.1.1 譲渡

任意の異なる 2 つのホルダ $h_i, h_j \in H$ を考える $(i \neq j)$．紙幣型マネーシステムモデルにおいて，時刻 t から $t+1$ においてホルダ h_i から価値量 $r \in R$ をホルダ h_j に譲渡するとは，第 2.1 章の式と以下の式が成り立つことをいう．

$$\begin{aligned}
{}^\exists v_r,\ I^t(v_r) &= r, \\
K^t(v_r) = h_i \quad \text{かつ} \quad K^{t+1}(v_r) &= h_j, \\
V^t &= V^{t+1}, \\
{}^\forall v \neq v_r,\ K^t(v) &= K^{t+1}(v), \\
{}^\forall v,\ I^t(v) &= I^{t+1}(v).
\end{aligned}$$

3.2 残高型マネーシステムモデル

ホルダが，残高額を表す価値量を媒介する媒体を一つだけ保持する形式の貨幣システムモデルを，**残高型マネーシステムモデル**という．実用化されている電子マネーシステムの多くは残高型である．

残高型マネーシステムモデルにおいて，次式が成り立つ．

$$\begin{aligned}
{}^\forall t,\ V^t &= V^{t+1}, \\
{}^\forall t,\ |V^t| &= |H|, \\
{}^\forall t {}^\forall v_i \neq {}^\forall v_j,\ K^t(v_i) &\neq K^t(v_j), \\
{}^\forall t {}^\forall v,\ K^t(v) &= K^{t+1}(v).
\end{aligned}$$

任意のホルダ h_i が保持する唯一の媒体を v_i と表す．

3.2.1 譲渡

任意の異なる2つのホルダ $h_i, h_j \in H$ を考える $(i \neq j)$. 残高型マネーシステムモデルにおいて，時刻 t から $t+1$ においてホルダ h_i から価値量 r をホルダ h_j に譲渡するとは，第 2.1 章の式と以下の式が成り立つことをいう．

$$\begin{aligned} I^t(v_i) &\geq r, \\ I^t(v_i) - r &= I^{t+1}(v_i), \\ I^t(v_j) + r &= I^{t+1}(v_j), \\ {}^\forall v \neq v_i, v_j,\ I^t(v) &= I^{t+1}(v). \end{aligned}$$

ここで，譲渡の前後でホルダと媒体の一対一対応に変化がないことに注意する．

4 局所的な価値量譲渡

本章では，価値量の**局所的な譲渡**について考察する．価値量の局所的な譲渡とは，譲渡を行う2ホルダが価値量関数 I ではなく各々の持つ近似価値量関数に基づいて行う価値量の譲渡のことである．局所的な譲渡を行うことにより，システム内の価値流通の匿名性 [2] が保たれる．

4.1 貨幣システム上の局所的譲渡

貨幣システム上でホルダ h_i がホルダ h_j へ価値量 r を局所的に譲渡するとは，以下の式が成り立つことをいう．

$$\begin{aligned} \sum_{K^t(v)=h_i} I^t_{h_i}(v) &\geq r, \\ \sum_{K^t(v)=h_i} I^t_{h_i}(v) - r &= \sum_{K^{t+1}(v)=h_i} I^{t+1}_{h_i}(v), \\ \sum_{K^t(v)=h_j} I^t_{h_j}(v) + r &= \sum_{K^{t+1}(v)=h_j} I^{t+1}_{h_j}(v), \qquad (2) \\ {}^\forall x \neq i,j,\ \sum_{K^t(v)=h_x} I^t_{h_x}(v) &= \sum_{K^{t+1}(v_x)=h_x} I^{t+1}_{h_x}(v). \end{aligned}$$

4.2 紙幣型マネーシステム上の局所的譲渡

紙幣型マネーシステム上で，ホルダ h_i がホルダ h_j へ価値量 r を局所的に譲渡するとは，第 4.1 章の式と以下の式が成り立つことをいう．

$$\begin{aligned} {}^\exists v_r,\ I^t_{h_i}(v_r) &= r, \qquad (3) \\ K^t(v_r) = h_i \ \text{かつ}\ & K^{t+1}(v_r) = h_j, \\ V^t &= V^{t+1}, \\ {}^\forall v \neq v_r,\ K^t(v) &= K^{t+1}(v), \\ {}^\forall v,\ I^t_{h_x}(v) &= I^{t+1}_{h_y}(v), \end{aligned}$$

ただし，$h_x = K^t(v)$ かつ $h_y = K^{t+1}(v)$.

4.3 残高型マネーシステム上の局所的譲渡

残高型マネーシステム上で，ホルダ h_i がホルダ h_j へ価値量 r を局所的に譲渡するとは，第 4.1 章の式と以下の式が成り立つことをいう．

$$\begin{aligned} I^t_{h_i}(v_i) &\geq r, \qquad (4) \\ I^t_{h_i}(v_i) - r &= I^{t+1}_{h_i}(v_i), \\ I^t_{h_j}(v_j) + r &= I^{t+1}_{h_j}(v_j), \qquad (5) \\ V^t &= V^{t+1}, \\ {}^\forall v,\ K^t(v) &= K^{t+1}(v), \\ {}^\forall v \neq v_i, v_j,\ I^t_{h_x}(v) &= I^{t+1}_{h_x}(v), \end{aligned}$$

ただし，$h_x = K^t(v) = K^{t+1}(v)$.

5 偽価値量の譲渡と検知可能性

本章では，紙幣型マネーシステムモデルと残高型マネーシステムモデルにおける偽価値量の局所的な譲渡を取り扱う．

3つのホルダ $h_i, h_j, h_k \in H$ を考える（ただし，$i \neq j \neq k$）．任意の時刻において，ホルダ h_i, h_j, h_k はそれぞれ $I_{h_i}, I_{h_j}, I_{h_k}$ という近似価値量関数を使用するとする．

任意の Fake 媒体 v_f に対し，${}^\forall t,\ I^t(v_f) = 0$ と仮定する．また，$K^t(v_f) = h_i$ かつ $I^t_{h_i}(v_f) = r > 0$ を満たす時刻 t を考える．ここで，$F_{I^t_{h_i}}(v_f) = r > 0$ であることに注意する．

本章では，以下の価値量の局所的な譲渡を考える．

時刻 t から時刻 $t+1$：ホルダ h_i からホルダ h_j への価値量 r の譲渡．

時刻 $t+1$ から時刻 $t+2$：ホルダ h_j からホルダ h_k への価値量 r の譲渡．

5.1 紙幣型における Fake 媒体の局所的譲渡

時刻 t から時刻 $t+1$.

$K^t(v_f) = h_i$ かつ $I^t_{h_i}(v_f) = r$ より式 3 が成り立つので，媒体 v_f を用いて価値量 r を局所的に譲渡することを試みる．このとき，ホルダ h_j の近似価値量関数 $I^{t+1}_{h_j}$ の出力によって以下の2つの場合がある．

(1) $I^{t+1}_{h_j}(v_f) = r$ のとき．
式 2 が成り立ち，価値量 r の局所的譲渡が成立する．

(2) $I^{t+1}_{h_j}(v_f) = 0$ のとき．
式 2 が成り立たず，v_f による価値量 r の局所的譲渡が成立しない．つまり，偽価値量 $F_{I^t_{h_i}}(v_f) = r$ が，より精度の高い近似価値量関数 $I^{t+1}_{h_j}$ によって検知された．

時刻 $t+1$ から時刻 $t+2$.

ここでは，場合 (1) でホルダ h_i からホルダ h_j への媒体 v_f による価値量 r の局所的譲渡が成立したときを考える．次にホルダ h_j からホルダ h_k への価値量 r の譲渡を考える．$K^{t+1}(v_f) = h_j$ かつ $I^{t+1}_{h_j}(v_f) = r$ であるので，式 3 が成り立ち，媒体 v_f を用いて価値量 r を局所的に譲渡することを試みる．

(1-1) $I^{t+2}_{h_k}(v_f) = r$ のとき．
式 2 が成り立ち，価値量 r の局所的譲渡が成立する．

(1-2) $I_{h_k}^{t+2}(v_f)=0$ のとき．
式 2 が成り立たず，v_f による価値量 r の局所的譲渡が成立しない．また，偽価値量 $F_{I_{h_j}^{t+1}}(v_f)=r$ が，より精度の高い近似価値量関数，$I_{h_k}^{t+2}$ によって検知された．

以上の議論を一般化することにより，次の定理がいえる．

定理 1 (偽価値量の検知可能性) 紙幣型マネーシステム上において，ある時刻 t で $K^t(v_f)=h_i$，$I^t(v_f)=0$ かつ $I_{h_i}^t(v_f)=r>0$ とする．任意の時刻 $t+d$ (ただし $d\geq 1$) で $K^{t+d}(v_f)=h_\ell$ のとき，もし $I_{h_\ell}^{t+d}(v_f)=I^{t+d}(v_f)=0$ ならば，偽価値量 r は近似価値量関数 $I_{h_\ell}^{t+d}$ により検知可能である．

5.2 残高型における Fake 媒体の局所的譲渡

時刻 t から時刻 $t+1$.

$K^t(v_f)=h_i$ かつ $I_{h_i}^t(v_f)=r$ より式 4 が成り立つので，価値量 r を局所的に譲渡することを試みる．v_j を $K(v_j)=h_j$ を満たす媒体とし，$I_{h_j}^t(v_j)=r_j^t>0$ とする．

このとき，ホルダ h_j の近似価値量関数 $I_{h_j}^{t+1}$ の出力によって以下の 2 つの場合がある．

(i) $I_{h_j}^{t+1}(v_f)=r_j^t+r$ のとき．
式 2 と式 5 が成り立ち，価値量 r の局所的譲渡が成立する．このとき，$r_j^{t+1}=r_j^t+r$ となる．

(ii) $I_{h_j}^{t+1}(v_f)=r_j^t$ のとき．
式 2 と式 5 が成り立たず，価値量 r の局所的譲渡は成立しない．このとき，偽価値量 $F_{I_{h_i}^t}(v_f)=r$ が，より精度の高い近似価値量関数 $I_{h_j}^{t+1}$ によって検知された．

時刻 $t+1$ から時刻 $t+2$.

ここでは，場合 (i) でホルダ h_i からホルダ h_j への価値量 r の局所的譲渡が成立したときを考える．次にホルダ h_j からホルダ h_k への価値量 r の譲渡を考える．$K^{t+1}(v_j)=h_j$ かつ $I_{h_j}^{t+1}(v_j)=r_j^{t+1}>r$ より式 3 が成り立つので，価値量 r を局所的に譲渡することを考える．v_k を $K(v_k)=h_k$ を満たす媒体とし，$I_{h_k}^{t+1}(v_k)=r_k$ とする．

ここで，$r_j^{t+1}>r$ であるので，ホルダ h_j からホルダ h_k に局所的に譲渡される価値量 r は，**真価値量と偽価値量の両方を含みうる**．しかしながら，受け手側のホルダ h_k はその割合を調べることはできない．なぜならば，ホルダ h_k はホルダ h_j が持つ媒体 v_j に自らの近似価値量関数 $I_{h_k}^{t+2}$ を行使することはできないからである (第 1.2 章参照)．したがって，価値量 r の譲渡に際して以下の 2 つの場合がある．

(i-i) $I_{h_k}^{t+2}(v_k)=r_k^{t+2}+r$ のとき．
式 2 が成り立ち，価値量 r の局所的譲渡が成立する．

(i-ii) $I_{h_k}^{t+2}(v_k)=r_k^{t+2}$ のとき．
式 2 が成り立たず，価値量 r の局所的譲渡が成立しない．

すなわち，**r が含む真価値量と偽価値量の割合にかかわらず，r の譲渡が成立してしまうか，ホルダ h_k は価値量 r の譲渡を拒否するかのどちらかしかない．**

以上の議論を一般化することにより，次の定理がいえる．

定理 2 (偽価値量の検知不可能性) 残高型マネーシステム上において，ある時刻 t で $K^t(v_f)=h_i$，$I^t(v_f)=0$ かつ $I_{h_i}^t(v_f)=r>0$ とする．任意の時刻 $t+d$ (ただし $d\geq 1$) において，ホルダ h_i が任意のホルダ h_j (ただし $i\neq j$) に偽価値量 r' (ただし $1\leq r'\leq r$) を局所的に譲渡したとき，任意の時刻 $t+d'$ (ただし $d'>d$) において偽価値量 r' は検知不可能である．

5.2.1 考察

残高型マネーシステムを安定させるためには，

(a) 価値量の譲渡に信頼できる第三者の介入を許す，もしくは

(b) 偽価値量が混入しないセキュリティシステムを構築する

という方法が考えられる．しかしながら，(a) は価値流通の匿名性 [2] を残高型マネーシステムから失わせることとなり，また (b) はシステムの安定性を暗号技術や IC チップの耐タンパー性に委ねることとなる．

謝辞

本研究において貴重なご意見をいただく九州大学大学院システム情報科学研究院 池田大輔助教授に感謝します．ならびに，安浦研究室の諸氏に感謝します．なお，本研究は平成 14-18 年度科学研究費補助金 (学術創成研究費 (2))・課題番号 14GS0218 によるものである．

参考文献

[1] 国際決済銀行, "電子マネーのセキュリティ", ときわ総合サービス株式会社出版調査部, 1998.

[2] J.D.Tygar, "Atomicity in Electronic Commerce", Proceedings of the 15th Annual ACM Symposium on Principles of Distributed Computing (PODC'96)", pp8–26, 1996.

[3] FIPS PUB 140-2, "Security Requirements for Cryptographic Modules", National Institute of Standards and Technology, 2001.

[4] David Chaum, "Build signaures for untraceable payments", Crypto 82, pp.199–203, 1982.

[5] Stefan Brands, "Untraceable off-line cash in wallet with observers", Crypto 93, pp.302–318, 1993.