九州大学学術情報リポジトリ
Kyushu University Institutional Repository

電子マネー実現に向けた現金通貨システムのモデル化

小山, 健一郎
九州大学大学院

野原, 康伸
九州大学大学院

安浦, 寛人
九州大学大学院

https://hdl.handle.net/2324/6312

出版情報：SLRC 論文データベース, 2006-03
バージョン：
権利関係：

電子マネー実現に向けた現金通貨システムのモデル化

A Model of Currency System for Electric Money System Design

小山 健一郎 *　野原 康伸 *　安浦 寛人 *
Ken'ichiro Oyama　Yasunobu Nohara　Hiroto Yasuura

九州大学大学院 *
Kyushu University

1 はじめに

近年，電子マネーが決済の手段として利用されつつある．電子マネーの実現手法として多くの方法が考えられる [1][2]．本稿では，電子マネーの実現に必要な性質を明らかにするために現在の現金通貨システムを情報科学的にモデル化する．

2 モデル化

2.1 基本要素の集合

本論文では貨幣を価値トークン，媒体，保持者の 3 つの要素でモデル化をする．

- $R := \{r_1, r_2, ..., r_n\}$. 価値トークン (Rights)．価値や権利などを証明するものでありそれ以下に分割できない最小要素．偽札に対応する価値トークンはない．
- $V := \{v_1, v_2, ..., v_m\}$. 媒体 (Vehicle)．現金の集合．紙幣や硬貨のことを指す．偽札も含まれる．
- $H := \{h_1, h_2, ..., h_l\}$. 保持者 (Holder)．人が持つ財布など．

2.2 集合間の関係

$I^t : R \to V$: 時刻 t における価値トークンが帰属する現金を表す．I は R から V への単写である．

$K^t : V \to H$: 時刻 t における現金の保有者を表す．K は V から H への写像である．

判別関数 D: 現金 $v \in V$ の真贋を判別するために以下のような条件式を表す関数 $D(v)$ が必要である．

$$D(v) = \begin{cases} \text{真札} & \exists r \in R\{v = I(r)\} \\ \text{偽札} & \text{otherwise} \end{cases}$$

2.3 集合の時間的な変化

現金の譲渡: ある $h_i, h_j \in H, v_i \in V$ について h_i, h_j がある時刻 t に保持する媒体の集合を $V_{h_i}^{(t)}, V_{h_j}^{(t)}$ とする．$h_i = K(v_i)$ のとき，保持者 h_i の持つ現金 v_i を h_j に譲渡するとは

$$V_{h_i}^{(t+1)} = V_{h_i}^{(t)} - \{v_i\}, V_{h_j}^{(t+1)} = V_{h_j}^{(t)} \cup \{v_i\}$$

$$\forall x \neq i, x \neq j, V_{h_x}^{(t)} = V_{h_x}^{(t+1)}$$

が成り立つような行為をいう．

現金の発行: 現金 v_i の発行とは，既存の現金の集合 $V^{(t)}$ に v_i が追加されることをいう．正規に現金を発行するとき，$v_i = I^{(t)}(r_i)$ となる $r_i \in R$ が既存の価値トークンの集合 $R^{(t)}$ に追加される．発行者でない者が，$v_i = I(r_i)$ となる v_i を発行することはない．

$$V^{(t+1)} = V^{(t)} \cup \{v_i\}, R^{(t+1)} = R^{(t)} \cup \{r_i\}$$

現金の回収: 現金 v_i の回収とは，既存の現金の集合 $V^{(t)}$ から v_i が削除されることをいう．正規に現金を回収するとき，$v_i = I^{(t)}(r_i)$ となる $r_i \in R^{(t)}$ が既存の価値トークンの集合 $R^{(t)}$ から削除される．

$$V^{(t+1)} = V^{(t)} - \{v_i\}, R^{(t+1)} = R^{(t)} - \{r_i\}$$

3 現金通貨の性質

本章では現金通貨の性質を挙げる．

判別関数 D の周知: 全保持者は，判別関数 D を知っている．また，全保持者は「全保持者が判別関数 D を知っていること」を知っている．

判別関数の利用: 現金の譲渡時に，譲受人ならびに譲渡人の双方が判別関数 D を使用する．

転々流通性: 第三者を介することなく当事者同士のみで現金の譲渡ができる．

価値トークンの総量の保存: 発行者による発行及び回収以外では価値トークンの総量は変化しない．h_i が h_j に v_i を譲渡した場合，

$$\sum_{k=1}^{n} R_{h_k}^{(t+1)} = \sum_{k=1}^{n} R_{h_k}^{(t)}$$

が成り立つ．

4 まとめ

本稿では，現在の現金通貨システムを情報科学的にモデル化した．現金通貨システムをそのまま置き換える形で電子マネーのシステムを作る場合には，本モデルを満たすように設計する必要がある．

参考文献

[1] 中山靖司, 太田和夫, 松本勉, "電子マネーを構成する情報セキュリティと安全性評価", 日本銀行金融研究所, 1999 年 4 月

[2] 岡本龍明, 太田和夫, "理想的電子現金方式の一方法", 信学誌, Vol.J76-D1, No.6, pp.315-323, 1993 年 6 月