インターネット上での通貨に関する研究

三輪 信介

北陸先端科学技術大学院大学 情報科学研究科

1997年2月14日

キーワード： 電子通貨, インターネット, 電子署名, 暗号化, 最終的決済.

近年利用者を増やしているインターネットにおいて、様々な商取引をする機会が増えてきている。インターネットの性質上、この商取引は24時間かつ国際的に行われるため、24時間決済や国際決済を可能とする決済システムへの要求が高まってきており、現在、様々な方式が提案／実装されている。しかし、現在のインターネット上での決済システムには、全ての決済に何らかのサーバが介在しなければならないという欠点や、最終的決済が行えないので必ずしも24時間決済や国際決済の要求を満たすことができないといった欠点がある。また、最終的決済を行うために決済コストがかかり、利用者や決済機関の負担が増大するという問題もある。

これらの欠点を克服するために、本研究ではインターネット上での電子通貨システムとして、「裏書譲渡可能な銀行券」方式を提案した。本方式は、サーバを介することなく転々譲渡することが可能で、決済は譲渡によって行う。このようにすることで、サーバが介在しなければならないのは銀行券の「振出」と「検証」、「引換」のみとなり、利用者同士の決済にはサーバが介在する必要はなくなる。これによって、サーバへの通信負荷の集中を避けることができる。また、譲渡によって決済がなされるため、システム全体の社会的信用が向上すれば、「引換」されることなく「検証」のみで利用されるインターネット上での最終的決済可能な通貨となりうる可能性がある。

提案方式では、銀行券本体の中にその使用者の電子署名の連鎖を記録することで、不正を事後検出できるようにした。ただし、この電子署名の連鎖は検証を行う発行局以外が内容を知ることがないように暗号化する。このようにすることで、使用者が他の使用者について知ることができなくなると同時に、内容を再現できないので改ざんできなくなる。本方式は、不正を事後検出することができるために、犯罪への利用やマネー・ロンダリングへの利用を抑止すると同時に、事後に証拠を提出することができる。

本研究では、この提案方式についての実装を行なった。大規模な運用実験は行なっていないが、実際に各トランザクションを実行することができた。

評価は、他の決済方式との比較によって行った。比較は、実現されているかどうか、匿名性が提供されているか、暗号化されているか、専用のハードウェア／ソフトウェアを必要とするか、決済すべてにサーバが介在する必要があるかなどの観点から行った。比較の対象としては、安全なクレジットカード番号の提示法として FIRST VIRTUAL と CyberCash 、電子通貨方式として ecash 、電子小切手方式として NetCheque 、インターネット上の方式ではないが現実社会での決済システムとして実験段階にある MONDEX 、今後主流となると考えられている供託電子マネー方式を取り上げた。比較の結果、提案方式は実現すれば、匿名性に関して不利である一方、取引に常にサーバが介在する必要がないという優位点があることが解った。

提案方式では発行局に対する匿名性が提供できないことや、不正が事後にしか検出できないため、銀行券の社会的信用を維持することが困難であるなどの問題が指摘されている。本研究ではこれらについて解決法の一つを提示するが、完全な解決が行えたわけではなく、これらの問題については今後の課題としている。これらの問題の他に、到達の確認の問題や最終的決済の可能性の問題などインターネット上での決済システムすべてに関わる議論も存在し、本研究では解決には至っていない。

インターネットが一つのコミュニティであると考えると、その内部で最終的決済が可能な通貨が存在することは、その内部に独立した経済が存在することを意味する。これは、現実社会における経済や国家の枠組みを超えて、インターネットが存在し、活動しうることを示唆する。現実の経済や国家の枠組みが 21 世紀に向けて昏迷を続ける中、インターネットが最終的決済可能な通貨を手にすることで、新しい経済的枠組みのあり方を示すことが可能となる。