Journal of Electronic Commerce Research, VOL. 5, NO.4, 2004

USING E-CASH IN THE NEW ECONOMY: AN ECONOMIC ANALYSIS OF MICROPAYMENT SYSTEMS

Michelle Baddeley
Gonville & Caius College and Faculty of Economics and Politics, Cambridge, UK
mb150@cam.ac.uk

ABSTRACT

The growth of electronic commerce is dependent upon the emergence of effective electronic payment systems. Whilst payments for large purchases can be made relatively easily using credit/debit cards, small-scale electronic commerce is constrained by the limited nature of existing e-cash (or 'micropayments') systems. This paper outlines the evolution of electronic payment systems, leading to an analysis of the essential characteristics of e-cash, and microeconomic / macroeconomic implications of the development of e-cash. Finally, the key characteristics of successful electronic payment innovations are analysed using binary dependent variable estimation techniques on data derived from the Electronic Payments Systems Observatory (ePSO) database.

Keywords: e-cash, micro-payment systems, e-commerce

1. Introduction

Electronic commerce is growing at an increasing pace and financial instruments are adapting to the increased volume of spending taking place over the Internet (Economides, 2001). Until now, most buyers have used credit arrangements or checking accounts as the principle means of paying for Internet purchases. There is however, a 'price umbrella' underneath credit-card transactions that makes them an excessively costly financial instrument for low-value purchases (Rivest, 1998). Given the transactions costs involved with card transactions, the opportunity gap that remains in terms of e-money products lies in developing a popular alternative to conventional cash as a convenient way to make small payments ('micropayments'[1]). For many Internet transactions, electronic cash (e-cash) could provide a potentially superior substitute for conventional monetary instruments.

Most existing electronic small payments schemes are in essence account-based systems mediated by middle-people, in practice in much the same way as a bank or credit institution acts as a financial intermediary. Accounts-based payment mechanisms lack some of the key characteristics of conventional cash, e.g. complete anonymity and low transactions costs. Financial cryptographers are attempting to harness the lower computational and/or administrative transactions costs of electronic payments schemes in order to devise an efficient electronic micro-payments scheme whilst retaining in electronic cash the virtues of conventional cash (e.g. in terms of security and anonymity) and some of the computational and technical difficulties have been overcome (van Someren, 2001, van Someren *et al.*, 2003). But attempts at a practical implementation of e-cash systems have met with limited success because logistical problems remain; to some, the widespread adoption of e-cash systems seems to be a distant prospect (Odlyzko, 2003).

This paper begins with an analysis of ideas about the evolution of money, applied to modern forms of electronic money systems. Then the characteristics of electronic cash relative to conventional money and other electronic payment systems are outlined followed by an examination of the potential microeconomic and macroeconomic implications of e-cash systems. The evolution of electronic payment systems within the real world is analysed using data derived from the Electronic Payments Systems Observatory (ePSO), which is run by the European Central Bank (ECB) as part of its monitoring role. These data are used in a binary dependent variable analysis of the characteristics of successful electronic payment services. The paper concludes with the observation that whilst e-cash systems have the potential to change monetary systems by directly matching buyers and sellers in exchange, there is still a long way to go in developing effective and extensive e-cash systems. And the further evolution of widely accepted systems will require the co-operation of governments, central banks and business.

[1] Micro-payments systems are defined as e-payment solutions that allow for payments up to 5 Euros (Carat, 2002).

2. Definitions of electronic money

In understanding the evolution of electronic money, it is useful first to define electronic money and then to examine some of the specific characteristics of e-money in general and e-cash in particular. Fullenkamp and Nsouli (2004) argue that one of the 'puzzles' surrounding the evolution of electronic money has emerged because of confusions over terminology and definitions. This point is recognised by the Basel Committee of the Bank for International Settlements (BIS): electronic money is difficult to define because it blends particular technological and economic characteristics (Basel Committee, 1998; BIS, 1996). In addition, different e-money schemes will vary according to their technical implementation, the institutional arrangements required to support them, the way in which value is transferred, the recording of transactions and the currency of denomination (BIS, 1996). This means that several definitions of electronic money have evolved over time.

In broad terms, electronic money can be defined as monetary value stored on an electronic device issued on receipt of funds or accepted as a means of payments (Carat, 2002, p. 11). This mirrors the official definitions published by ECB and BIS in focussing on the stored value aspect of electronic money (e.g. BIS 1996, Basel Committee, 1998). The ECB (1998, 2000), following the first official definition issued by the European Monetary Institute (EMI, 1996), define electronic money in the following terms:

> 'Electronic money is broadly defined as an electronic store of monetary value on a technical device that may be widely used for making payments to undertakings other than the issuer without necessarily involving bank accounts in the transactions, but acting as a prepaid bearer instrument.'

Again, the focus in this definition is on the pre-paid aspect of electronic money. The Basel Committee (1998) further divides types of electronic money into the categories of electronic purses (hardware or card based) and digital cash (software, network based). But whether these instruments are 'balance-based' (i.e. account based) or 'token-based' (i.e. involving the expenditure of electronic tokens), the essential characteristic is their pre-paid nature. For this reason, credit cards and debit cards are regarded as access products or electronic payment systems, rather than as electronic money (BIS, 1996; Basel Committee, 1998).

3. Characteristics of electronic money

3.1 The Evolution of Money[2]

In analysing whether or not electronic cash can evolve as an efficient and flexible facilitator of exchange in the Internet economy, it is useful to revise theories about why and how conventional money has evolved over time. Money plays a number of roles in economic activity: it is a unit of account, a means of deferred payment, a store of value and a medium of exchange. According to a Mengerian view, the evolution of money has taken place in a context of economising on time, effort and scarce resources (Menger, 1892; Alvarez, 2002). All economic exchanges, including the exchange of money for goods and services, involve transaction costs and these hinder the trading of goods and services. Economists regard transactions costs as a form of economic friction: if economic friction is reduced, more productive potential will be released. The Mengerian view asserts that money has evolved over the centuries to minimise the friction of transactions costs that are involved in mediating exchange.

The process can be seen from the development of the very first monetary products. Conducting economic transactions in barter economies was uneconomical: a double coincidence of wants between buyers and sellers was the necessary pre-condition for exchange. Transactions costs were considerable because a lot of time and effort was involved in finding a suitable barter partner. At first glance it may appear that e-cash is the opposite – having the potential to lead the monetary system to an even higher evolutionary point. To a non-technician, the transactions costs involved in e-cash may seem to be almost zero whilst the benefits are much the same as conventional cash. But the picture is in fact more complex.

Another element in the evolution of money was the need for divisibility and fungibility. Limits on the divisibility of goods and services created problems: if a loaf of bread is worth a tenth of a goat, what's the solution? The advent of commodity money made the process of transacting more economical by allowing people to specialise in production according to their strengths and by enabling monetary authorities to mint coins in convenient denominations, creating divisibility and fungibility: when people withdrew coins from a bank they did not have to withdraw the same coins that they deposited because all coins of a particular denomination were homogenous and standardised. This reduced the complexity of exchange.

As for the role of government, within a commodity money system a monetary authority is not essential. As long as people believe that their commodities or coins represent purchasing power then the commodity is its own

[2] For analyses of the nature and evolution of money, including electronic money, see Davies, 2002 and Solomon, 1997; Baddeley and Fontana, 2004.

guarantor. But government usually has a key role in legitimising coinage by affixing a stamp to guarantee that a coin contained a given amount of precious metal. Nonetheless, risks of counterfeiting and debasement remained. Also, using commodity money whether based upon gold, other metals, or cigarettes, meant either that extra resources were devoted to producing more of the commodity; or that limitations had to be imposed on the use of the commodity for non-monetary purposes. Also, costs were incurred in storing, holding and carrying commodity monies. An early solution came via token money: with trusted goldsmiths issuing transferable certificates to register gold reserves, commodity money could survive without the need to carry around the commodity itself.

Gradually, the issuing of notes by private banks was supplanted by central bank control of cash in the economy. Initially, central banks issued convertible paper currencies e.g. the gold standard or dollarisation. The development of convertible paper currencies allowed a decrease in the costs involved in the production, storage and use of money. The average cost of printing and storing a bank note or coin are far less than the value of that note or coin. It is likely that electronic money will have the capacity further to reduce these production and holding costs, though the role of government is likely to be constrained.

Another distinctive characteristic of conventional money over electronic money is the importance of fiat money: money that is declared by government fiat to be legal tender with people being obliged to accept it as such. It seems unlikely that governments will be willing or able to declare similar fiats with respect to electronic money. This is the essence of the problem with any form of non-commodity money: why would a person hold something inherently worthless as a store of value or medium of exchange? They hold it because they believe in it; using fiat money as a medium of exchange is vitally dependent upon a social convention. This is the essence of the Chartalist view, popularised by Knapp (1924), of money as a social relation. Whilst there are still risks of forgery and fraud associated with fiat money, the most important advantage that fiat monies have is that they are cheap. They are cheap because they are based upon a social convention supported by trusted institutions and a legal system. Credibility is crux of the system; fiat money cannot work if people are not prepared to use their tokens as a medium of exchange. And for people to be prepared to use tokens in exchange, the tokens must be legal tender or at least almost universally acceptable. This is one of the key problems for e-cash: encouraging people to adopt the convention. For conventional money, reliable monetary institutions support the fiat; modern central bankers focus on the interactions between monetary policy, inflation and purchasing power. It follows that the private production of money must be illegal: if anyone can produce monetary tokens, central banks would not be prepared to guarantee the value of money and the social convention would collapse. But for electronic cash, the private producers are the innovators and monetary authorities have had little direct impact on the various e-cash alternatives available.

So history shows that all money has evolved to meet a set of essential requirements including wide acceptability; low production/carrying/storage costs; fungibility, divisibility; and resistance to forgery.[3] For future developments in electronic money, there is no doubt that technology has evolved to a stage at which e-cash systems will be able to supplant conventional cash systems in terms of some of these characteristics. Conventional token or fiat monies do incur production, storage, carrying and handling costs which, whilst less substantial than those involved in commodity money systems, are still likely to be greater than the costs of effective e-cash systems. In addition, if systems can be devised to limit on-line processing costs, e-cash systems have the potential to be more secure than conventional cash systems. However, many barriers remain if e-cash systems are to replicate the liquidity, ubiquity and anonymity of conventional cash, particularly as ease of access to conventional cash has increased with the proliferation of ATMs (The Economist, 2000*a*, p. 21).

3.2 Constraints on the evolution of e-cash

Some of the constraints on the effect evolution of e-cash systems emerge in designing instruments that are able easily to mimic some of the essential characteristics of conventional cash, e.g. in terms of efficiency, wide acceptability, security, anonymity**,** easy transferability (including an ability to support multiple payments).

Efficiency: The costs involved in producing and storing electronic cash are likely to be lower than those involved with printing, storing and carrying conventional cash. These cost savings will create some gains in terms of economic efficiency if the use of e-cash becomes more widespread. However, the costs involved in exchanging e-cash are relatively high in comparison with the costs involved in exchanging conventional cash. The current technology used in security protocols involves relatively high transactions costs and is not economical for 'micro-payment' systems' (Foo, 1997). Innovations such as NetCard can support micro-payments by incorporating a digital signature into a whole stick of coins that can then be spent individually (with a given merchant). This system allows a reduction in computational complexity for series of low value payments to given merchants but is not particularly helpful for customers who want to spend their coins at a number of different sites (Anderson, 2000).

[3] For a more exhaustive summary of the desirable properties of e-cash, see Neumann and Medvinsky, 1998; Choi, Stahl and Whinston, 1997.

Another way of reducing the transactions costs involved in digital payment systems is via de-coupling the various tasks that characterise the exchange of goods and money thereby making the system more suitable for low value transactions (Kravitz, 1998). Voucher schemes, lottery ticket and coin-flipping protocols all have the potential to minimise the number of messages involved in each transaction (Rivest, 1997; Foo, 1997; Lipton and Ostrovsky, 1998). Foo's method also transfers the processing burden onto banks, which may be appropriate if banks have the specialist skills and technology to be able efficiently to mediate financial transactions. In addition, electronic vouchers can be transferable but the problem remains that they cannot mimic conventional cash because direct exchange between buyers and sellers is not possible - financial intermediaries are still involved and this will increase the transactions costs of exchange. In addition, coin-flipping and lottery ticket protocols are based upon the assumption that economic agents are risk-neutral and will be satisfied with fair bets. It does not address the issue of risk-averse economic agents who prefer guaranteed sums of money to fair bets.

Acceptability: No existing e-cash is universally acceptable; most are not even widely acceptable. Existing e-cash systems are forms of 'inside' money (available to a select group of insiders) and this is particularly true for vendor-specific schemes. If an e-cash system is to be successfully adopted, it will have to attract a wide constituency, i.e. to become 'outside' money. It is because current e-cash schemes are not widely accepted that they must piggyback on the non-cash money supply i.e. bank deposits and credit accounts. This implies that e-cash is just a means of re-distributing 'IOU money' (i.e. based on deposit and credit accounts) and financial intermediaries must necessarily be involved in its exchange. This contributes to the overall transactions costs involved in the exchange of deposit-based electronic cash systems.

In conventional cash systems, there is a simple bilateral interaction between buyers and sellers; the fact that no middle-people are involved means that the transactions costs are lower. This bilateral exchange works because it is based upon a trusted social convention: cheap bits of paper/metal represent value. The backing of powerful institutions is required to support this sort of fragile social convention. What are the implications for effective virtual cash systems? Some observers may believe that we will come to live in a world of 'Disney dollars and Virgin pounds' (Birch and McEvoy, 1997). However, most people are too risk-averse to trust their fortunes to the fate of a single private enterprise; history has shown that even the most successful multi-national companies do not necessarily prosper forever. If an e-cash is to survive as a true cash system, then it requires the backing of trustworthy, stable institutions such as central banks – these could implement common protocols and act as unifying institutions. The development of e-cash as a form of outside money seems unlikely if e-cash systems do not receive this sort of government backing.

Security and Anonymity: Hypothetically, the potential security of virtual money is greater than that of conventional money given the sophisticated printing and counterfeiting methods used for conventional cash. For e-money however, adoption of widely available technologies that are tamper-resistant is limited by the US government's regulation of 'strong' cryptography, including export limits on 'long' (i.e. complex) keys. It is only in practice and because of governmental constraints that the security and privacy of e-cash systems is limited (Swire, 1997). Many existing e-cash systems, particularly those that can be used with a number of different merchants, are not completely anonymous because the monitoring of their use is actually essential to the proper operation of these systems in order to prevent the double spending of virtual coins. This monitoring may be very costly requiring collusion between institutions. The use of a conventional cash system allows direct interaction between buyer and seller and so it is not possible to monitor transactions taking place mediated using conventional cash. Anonymity is ensured. Conventional cash will be preferred by those involved with criminal activities as long as criminals and tax evaders believe that electronic transactions will always leave some trace (Goodhart, 2000). It can be argued that complete anonymity is not desirable from a social welfare point-of-view (de Solages and Traore, 1998). In theory, a system of anonymity that is only revoked by some trusted authority when criminal activities take place would mean that criminal activity could be more effectively monitored and punished in a world of e-cash. But, in practice, the whole point is that criminals would not use a system that they believe allows effective monitoring and punishment. Even with such a system, until complete anonymity can be assured electronic cash cannot substitute completely for conventional cash for illicit transactions and there will always be a demand for conventional cash, whether or not agents admit their real reasons for holding it.

Partial / complete transferability and multiple payment systems: Within any system of e-cash, there are difficult trade-offs to manage between anonymity/privacy and security/reliability. These trade-offs surface in assessing the desirability of easy transferability of e-cash. Sander and Ta-Shma argue that non-transferability is an important feature for e-cash systems as it imposes limits on criminal abuses (Sander and Ta-Shma, 1997). However, whilst limiting transferability will reduce the potential for fraud, non-transferable e-cash systems will be less flexible and more costly. Assuming that double spending of electronic cash can be prevented, an e-cash system that allows multiple-payments is likely to lower the monetary costs of transactions. However, for many e-cash systems devised

so far (e.g. lottery ticket and voucher systems) each unit of e-cash can only be spent once, even if the tickets/tokens/vouchers are transferable before use (Rivest, 1997; Foo, 1997). So each unit of currency is only partially transferable, i.e. it is transferable only until it is spent. In contrast, conventional cash is spent many times by many different people; it is completely transferable. In response to this problem, some multiple-payment schemes have been suggested (Pagnia and Jansen, 1997). In multiple payment systems, the costs of issuing electronic cash will be greatly reduced as long as there is an effective mechanism to allow a given unit of currency to be transferred easily between many buyers and sellers. If this transferability is possible and a token can be spent many times, then the average cost per transaction of issuing a given unit of currency will tend towards zero.

The use of methods such as Chaum's blind signature scheme (BSS) have some potential to promote transferability if a central-bank can issue signed coins and release its public signature key to all traders and consumers so that they can authenticate e-cash received (Chaum, 1992). Concerns about crime and fraud can also be addressed within such schemes, i.e. by using fair BSS in which trusted authorities have the power to monitor suspect transactions (de Solages and Traore, 1998). However, the problem remains that large databases of past transactions must be maintained in BSSs in order to prevent double spending. This requirement adds to the costs and limits the scalability of such systems. Transactions costs are reduced in systems such as NetCash because only outstanding tokens are monitored (Neumann and Medvinsky, 1998). However, these tokens are still not perfectly transferable because the holders of digital tokens/coins do not have to relinquish ownership of the digital coin when they spend it and the prevention of double-spending requires processing time even if this is reduced in comparison with other BSSs. In contrast, for conventional notes and coins, holders relinquish ownership of a physical entity when they spend a conventional note or coin and so the monitoring of double spending is not necessary.

3.3 Constraints on e-cash: some real world examples

Whilst e-cash systems may in theory have the potential to provide advantages not provided by conventional cash systems, as outlined above, designers of effective e-cash systems have the task of exploiting the efficiency gains of electronic transfer whilst mimicking desirable characteristics of conventional cash in terms of widespread acceptability, security, anonymity and easy transferability. But many early electronic cash innovative e-cash products have not stood the test of time, for example schemes such as DigiCash and CyberCash (The Economist, 2000*b*, p.77-9). Can this failure to develop e-cash systems in the real world be explained in terms of the characteristics outlined above? What underlies the success (or lack of success) of real-world e-cash systems?

Paypal is generally held to be the most successful example of an electronic cash system. The essence of its success lies in the fact that it is relatively widely accepted, being the preferred payment system for the widely popular e-Bay auction site (and it was bought-up by e-Bay in 2003). In addition, the verification systems and buyer insurance instruments used by PayPal reassure customers about the relative security of the system. Anonymity is not a characteristic of PayPal, however, and easy transferability only applies to people who want to re-spend their money within the system; it is more difficult to extract money out of the system than to set up an account in the first place. Nonetheless, PayPal does seem to have captured some first-mover advantages in the implementation of an effective micropayments system and its customer base has grown rapidly from about 185,000 in 2000 to over 45 million by 2004 (Sources: The Economist 2000*b*, http://www.paypal.com/). It also has relatively low transactions costs (http://www.wired.com/news/ebiz). The links between PayPal and e-bay has been an ingredient for success as it has helped to ensure relatively wide acceptability. And it is generally true that barter exchange payment systems designed complement some sort of virtual marketplace (e.g. Barter Trust, BigVine, LassoBucks) have been relatively successful (Economist 2000*b*, p. 78).

Other real-world micropayment systems have been less successful. DigiCash was designed to mimic the anonymity of conventional cash but ran into problems of limited acceptability, a problem that was exacerbated not only by the multiplicity of alternative, incompatible systems but also by the limited capital financing available for the project. In addition, the process of transferring money into an electronic 'mint' then to be spent in purchasing digital coins was relatively complicated (http://news.com.com/). CyberCash's CyberCoins system ran into similar problems.

PayDirect offers systems with low costs of entry, which are secure from a merchant's point of view but do not address the problem of merchant fraud. The initial accounts based system is relatively widely accepted but its interface with user accounts means that, in principle, spending is not anonymous and can be monitored. In 2003 PayDirect introduced its World Card – a stored value card that can be used to access local currency via ATMs. To an extent this may promote easy transferability but users of the World Card have to be identified when the cards are purchased.

Ultimately the real constraint is an economic or institutional constraint rather than a technological constraint and lies in generating widespread acceptability and this is the problem that has been overcome most effectively by PayPal. Given the increasing dominance of PayPal within the electronic marketplace, its first-mover advantage will

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.