DIGITAL CASH AND MONETARY FREEDOM

JON W. MATONIS

ABSTRACT

Much has been published recently about the awesome promises of electronic commerce and trade on the Internet if only a reliable, secure mechanism for value exchange could be developed. This paper describes the differences between mere encrypted credit card schemes and true digital cash, which presents a revolutionary opportunity to transform payments. The nine key elements of an electronic, digital cash are outlined and a tenth element is proposed which would embody digital cash with a non- political unit of value.

It is this final element of true digital cash which represents monetary freedom — the freedom to establish and trade negotiable instruments. For the first time ever, each individual has the power to create a new value standard with an immediate worldwide audience.

If all that digital cash permits is the ability to trade and store dollars, francs, and other governmental units of account, then we have not come very far. Even the major card associations, such as Visa and MasterCard, are limited to clearing and settling governmental units of account. For in an age of inflation and government ineptness, the value of what is being transacted and saved can be seriously devalued. Who wants a hard drive full of worthless "cash"? True, this can happen in a privately-managed digital cash system, but at least then it is determined by the market and individuals have choices between multiple providers.

The section on key elements of a private digital cash system compares and contrasts true digital cash with paper cash as we know it today. Each of the following key elements will be defined and explored within the bounds of electronic commerce:

- ***Secure (unable to alter or reproduce)***
- ***Anonymous (untraceable)***
- ***Portable (physical independence)***
- ***Infinite duration (until destroyed)***
- ***Two-way (unrestricted)***
- ***Off-line capable (availability)***
- ***Divisible (fungible)***
- ***Wide acceptability (trust)***
- ***User-friendly (simple)***
- ***Unit-of-value freedom (non-political)***

The transition to a privately-operated digital cash system will require a period of brand-name recognition and long-term trust. Some firms may at first have an advantage over lesser-known name-brands, but that will soon be overcome if the early leaders fall victim to monetary instability. It may be that the smaller firms can devise a unit of value that will enjoy wide acceptance and stability (or appreciation).

True digital cash as an enabling mechanism for electronic commerce depends upon the marriage of economics and cryptography. Independent academic advancement in either discipline alone will not facilitate what is needed for electronic commerce to flourish. There must be a synergy between the field of economics which emphasizes that the market will dictate the best monetary unit of value and cryptography which enhances individual privacy and security to the point of choosing between several monetary providers. It is money, the lifeblood of an economy, that ultimately symbolizes what commercial structure we operate within.

Economic Notes No. 63

ISSN 0267-7164 ISBN 1 85637 293 6

An occasional publication of the Libertarian Alliance, 25 Chapter Chambers, Esterbrooke Street, London SW1P 4NN
www.libertarian.co.uk email: admin@libertarian.co.uk

Printed with permission from the Internet Society. This paper was presented at INET '95, the annual conference of the Society.

Jon Matonis is the founding director of Private Payment Systems, a research organization for private currencies on the Internet based in Moss Beach, California. He has held positions of Foreign Exchange Manager for Deak International's World Bank office, Director of Futures Trading for Sumitomo Bank Ltd., and Foreign Exchange Manager for a major credit card association,

In 1982, Mr Matonis founded the not-for-profit Institute for Monetary Freedom which has published several academic articles on monetary economics and free banking. In 1988, he developed the proprietary Freedom I Trading System which has been used by institutional money management funds and hedge funds in the United States. He is a former member of the National Futures Association and holds a B.A. in Economics from George Washington University.

DIGITAL CASH AND MONETARY FREEDOM

JON W. MATONIS

"Money does not have to be created legal tender by governments like law, language and morals it can emerge spontaneously. Such private money has often been preferred to government money, but government has usually soon suppressed it." — F. A. Hayek[1]

1. Prologue

The year is 2005. I buy lunch at a deli and I pay in wireless digital cash from my Electronic wallet. Currently, all promised visions of the future — with one notable exception. The cashier gives me a choice of monetary units which are both displayed on the flat-panel screen for me to view. My turkey and cheese sandwich will cost me US $50 or 5 pvu. The monetary symbol "pvu" is an abbreviation for "private value units", which now compete in most commercial settings with the US Dollar and have stayed remarkably stable since their initial issuance in mid-1996.

The future belongs to superior private currencies and the linchpin for successful digital cash ventures will undoubtedly be freedom in the unit of value. We are witnessing nothing less than the birth of a new industry — the development, issuance, and management of private currencies. Once seeded, digital cash as the representation of binary value will pave the way to a further off-network revolution in money.[2]

Much has been published recently about the awesome promises of electronic commerce and trade on the Internet and World Wide Web if only a reliable, secure mechanism for value exchange could be developed. This paper highlights the differences between mere encrypted credit card schemes, as Visa, Mastercard, and others are currently developing, and "true" digital cash, which presents a revolutionary opportunity to transform payments. The nine key elements of an electronic, digital cash are outlined and a tenth element is proposed which would embody digital cash with a non-political unit of value.

It is this final element of true digital cash which represents monetary freedom — the freedom to establish, circulate, and trade negotiable monetary instruments. The opportunity to launch an alternative monetary system on a grand scale simply has not been available until recently. Granted, small local experiments, such as LETS and constants, with limited real-world penetration have always seemed to exist in one form or another. But, only lately with a global, inter-networked society can we truly say that the established monetary order is susceptible to challenge.

Specifically, the Internet provides (1) ease of mass issuance and circulation, (2) accessible encryption technology, (3) affordable currency transfer infrastructure, and (4) real-time conversion between competing units. Essentially, for the first time ever, each individual has the power to create a new value standard with an immediate worldwide audience. This should serve as a friendly warning to the clearing associations, banks, and financial service providers of the current paradigm.

2. Why Monetary Freedom is Important

Monetary freedom is essential to the preservation of a free-market economy. As the current trend on the Internet demonstrates, robust economic commerce depends on a flexible, responsive monetary system which can best be provided by unbridled market competition.[3] This implies not only market competition among issuers but strong competition among the units or representative units that are being issued. Ultimately, the competition for the standard of value should be no different than the competitive market of multiple providers that we see for toothpaste or shoes.[4]

When a single currency issuer, such as the "Fed", controls the supply of money and the specific units being transacted, the potential exists for monetary manipulation and an overbearing control of the economy. With the unprecedented growth of the Internet, the standards for electronic commerce are still evolving. Neither the US Dollar, nor any other governmental unit, has gained a foothold into this new economy. The monetary landscape is ripe and wide open and private currencies should infiltrate now.

If all that digital cash permits is the ability to trade and store dollars, francs, marks, yen, and other goverranental units of account, then we have not come very far. Even the major card associations, such as Visa and MasterCard, are limited to clearing and settling governmental units of account. For in an age of inflation and government ineptness, the value of what is being transacted and saved can be seriously devalued. Who wants a hard drive full of worthless digital "cash"? True, this can happen in a privately-managed digital cash system, but at least then it is determined by the market and individuals have choices between multiple providers.

3. Key Elements of a Private Digital Cash System

As would-be currency providers should note, there are ten key elements to a successful, private digital cash system. This section compares and contrasts true digital cash to paper cash as we know it today. Each of the following key elements of a digital cash "token" will be defined and explored within the bounds of electronic commerce. I have yet to discover a working digital cash system which meets all ten criteria although several are reportedly close. In 1991, Tatsuaki Okamoto and Kazuo Ohta proposed six properties of an ideal digital cash,[5] which are incorporated into elements one through six below:

3.1 **Secure**. The transaction protocol must ensure that a high-level security is maintained through sophisticated encryption techniques.[6] For instance, Alice should be able to pass digital cash to Bob without either of them, or others, able to alter or reproduce the electronic token.

3.2 **Anonymous**. Anonymity assures the privacy of a transaction on multiple levels. Beyond encryption, this optional untraceability feature of digital cash promises to be one of the major points of competition as well as controversy between the various providers.[7] Transactional privacy will also be at the heart of the government's attack on digital cash because it is that feature which will most likely render current legal tender irrelevant.[8] Both Alice and Bob should have the option to remain anonymous in relation to the payment. Furthermore, at the second level, they should have the option to remain completely invisible to the mere existence of a payment on their behalf.

3.8 **Portable**. The security and use of the digital cash is not dependent on any physical location. The cash can be transferred through computer networks and off the computer network into other storage devices, Alice and Bob should be able to walk away with their digital cash and transport it for use within alternative delivery systems, including non-computer-network delivery channels. Digital wealth should not be restricted to a unique, proprietary computer network.

3.4 **Two-way**. The digital cash can be transferred to other users. Essentially, peer-to-peer payments are possible without either party required to attain registered merchant status as with today's card-based systems, Alice, Bob, Carol, and David share an elaborate dinner together at a trendy restaurant and Alice pays the bill in full. Bob, Carol, and David each should then be able to transfer one-fourth of the total amount in digital cash to Alice.

3.5 **Off-line capable**. The protocol between the two exchanging parties is executed off-line, meaning that neither is required to be host-connected in order to process. Availability must be unrestricted. Alice can freely pass value to Bob at any time of day without requiring third-party authentication.

3.6 **Divisible**. A digital cash token in a given amount can be subdivided into smaller pieces of cash in smaller amounts. The cash must be fungible so that reasonable portions of change can be made. Alice and Bob should be able to approach a provider or exchange house and request digital cash breakdowns into the smallest possible units. The smaller the better to enable high quantities of small-value transactions.[9]

3.7 **Infinite duration**. The digital cash does not expire. It maintains value until lost or destroyed provided that the issuer has not debased the unit to nothing or gone out of business. Alice should be able to store a token somewhere safe for ten or twenty years and then retrieve it for use.

3.8 **Wide acceptability**. The digital cash is well-known and accepted in a large commercial zone. Primarily a brand issue, this feature implies recognition of and trust in the issuer. With several digital cash providers displaying wide acceptability, Alice should be able to use her preferred unit in more than just a restricted local setting.

3.9 **User-friendly**. The digital cash should be simple to use from both the spending perspective and the receiving perspective. Simplicity leads to mass use and mass use leads to wide acceptability. Alice and Bob should not require an advanced degree in cryptography, as the protocol machinations should be transparent to the immediate user.

3.10 **Unit-of-value freedom**. The theme of this paper: the digital cash is denominated in market-determined, non-political monetary units. Alice and Bob should be able to issue non-political digital cash denominated in any defined unit which competes with governmental-unit digital cash.

4. Implementing a Non-political Unit of Value

The transition to a privately-operated digital cash system will require a period of brand-name recognition and long-term trust. Some firms may at first have an advantage over lesser-known name-brands, but that will soon be overcome if the early leaders fall victim to monetary instability. It may be that the smaller firms can devise a unit of value that will enjoy wide acceptance and stability (or even appreciation).

4.1 Potential Unit Providers

Who will be the new monetary unit providers? Opportunities abound for almost anyone but in reality the greatest advantage currently goes to the on-line shopping malls and the large merchant sites on the Internet, such as Open Market, Internet Shopping Network, and Net Market. For it is this group that will directly influence the payment channel between consumer and merchant through their extensive contact with both. And, this influence can be utilized to their advantage to build preference for their "site" through money issuance in much the same way that various forms of scrip and coupons build customer loyalty and guarantee repeat visits.[10] As will be explained later, the true business gain is realized when the units are negotiable in their own right and not merely accepted at the mall only.

Other potential unit providers include internet service providers (ISPs), bulletin board system operators (BBSs), content publishers, card-based payment networks, and well-known manufacturer or service companies. They all share in common the existence of an extensive base of on-line customers. As the new digital cash providers, international brand names, such as Coca-Cola, Microsoft, and IBM, find themselves in an enviable position to capitalize immediately on their global name recognition.

4.2 Distribution and Circulation

What will the providers be issuing and how will they circulate it?

Probably the least exploited system in the world of money is the metric system. To cite an example, I propose a decimal unit-of-value measurement system that is based on the 1864 metric system, It possesses built-in ease of calculation and is universally recognized. Hypothetically, it would have the following monetary unit prefix designations:

kilo- (1,000)
hecto- (100)
deka- (10)
base unit name (1)
deci- (0.1)
centi- (0.01)
milli- (0.001)

The base unit name becomes the unit which is being distributed, such as a pvu in the 2005 example. Initial distribution techniques for the new private money include elimination of discount fees for merchants,[11] free coupons or promotions to consumers, and royalty schemes for content providers that accept payment in the new digital cash. This area affords unique opportunities for innovative advertisers and marketers to involve themselves in electronic commerce. Once digital cash has hit the market, circulation will then be a factor of merchant acceptance and the rewards of ultimate redemption.

4.3 Redemption and Convertibility

What will back the new monetary units and how will they be redeemed?

Suggestions for monetary backing include equity mutual funds, commodity funds, precious metals, real estate, universal merchandise and/or services, and even other units of digital cash. Anything and everything can be monetized. This will undoubtedly develop into a main basis for competition among digital cash providers as each one promotes their underlying currency backing as the strongest and most reliable. Unlike today's national monetary systems, the benefits of a strong currency will be immediately noticeable within a country's borders. With multiple monetary unit providers, domestic prices will adjust rapidly to reflect relative values of monetary units and the holders of stronger currencies will benefit. This is a vastly different world than we have now and consumers will analyze currencies as the investments that they really are.

Focusing on the option of equity mutual funds, this does not imply that a prospective digital cash provider learn to become adept at managing an entire portfolio. Mutual funds of mutual funds exist today and contracts can be executed with the specialist managers of those funds. Outsourcing the portfolio function takes advantage of the experts in the field today who compete already on reliability and overall performance — prime benchmarks for a private monetary unit. The issuer's skills should concentrate on distribution, monitoring geographic circulation of the unit, and managing the rate of redemption.

5. Managing a Non-political Unit of Value

After initial issuance and circulation, the digital cash providers must turn their attention to the management of the monetary unit if it is to survive in an ultra-competitive environment. This can prove the most difficult area due to the perennial temptation of over-issuance.

5.1 Digital Cashflow Administration

Since electronic monetary units on a client/server network can return to the issuer almost instantaneously, extreme diligence is required in accounting for digital cash and tracking redemption patterns. This need not be solely the function of the issuer and probably will not be as newsheets and databases evolve to manage the discounting and exchange function. As multiple currencies infiltrate the market, their relative values will dictate that they trade at a discount or premium to some other benchmark.

These free-market clearinghouses act as a central bank forcing each issuer to maintain an adequate balance between digital cash outstanding and the chosen reserve backing. Systems of clearing and

redemption are a necessity for the smooth operation of free banking as they provide a check on over-issuance and the general deterioration in sound credit.[12]

Therefore, the manager of a private monetary unit can rely on these clearinghouse parties to communicate to the public the unit's standing in the economy. Moreover, if the discount of a particular unit begins to deteriorate, it can alert management to the fact that some market forces are affecting the demand for that unit.

5.2 Issuer Benefits

Taking the proposal one step further, let us assume that, after witnessing the on-line successes with monetary freedom, a point-of-sale brand such as American Express wanted to capitalize on its global infrastructure and issue proprietary monetary units, in both digital cash and non-digital cash form. Just as with our on-line provider, the benefits to American Express are substantial if an American Express monetary unit can gain worldwide acceptance. Primarily, American Express will benefit from:

(a) Increased acceptance of American Express card products at merchant locations. This will be possible because of the lower fees and discount rates derived from managing a private unit of account.

(b) Increased demand for American Express card products in countries without established currencies and in countries with severe monetary instability of the established currency. This applies to several new democracies in Eastern Europe and the volatile third world nations of Africa and South America. Devaluations and revaluations of a currency have always plagued American Express from a financial management perspective. However, a new American Express monetary unit will provide these countries with a stable alternative to their own currency without the political ramifications of adopting the "imperialist" US Dollar.

(c) Natural marketing benefits associated with a private currency or unit of account. It is easiest to displace cash and cheques by becoming cash and cheques. American Express will gain clout from the name association and brand identification that accompanies a pricing system. Since American Express's private monetary unit will be the first non-governmental unit of account. it is difficult to compare with other products, but it is fair to say that from a trade perspective American Express will benefit in much the same way that the United States benefits when products globally are priced in US Dollars.

(d) Transaction volume that remains within the American Express system by providing a unit of account with ultimate redemption only at an American Express location. A sharp, sustained increase in transaction volume can be expected because the majority of cardholder transactions made in the American Express monetary unit will be duplicated by the acceptor of the Axnerican Express monetary unit. This will occur because of the incentive to avoid costly conversion out of the American Express monetary unit. The user incentive is maintained by providing a stable unit of value with strong merchant acceptance. The great irony occurs when Visa and Mastercard begin accepting and processing transactions denominated in the American Express monetary unit through their authorization and clearing systems.

(e) Open market operations conducted by American Express that expand or contract the available supply of American Express currency. The gains in this case are derived from the fact that American Express can determine its own monetary unit's short-term interest rate, and hence lending revenue, by manipulating its own unit's supply. The capital for these operations is generated from the difference between the digital cash face value and the cost to produce and ultimately back the electronic token. Issuers may lend capital or spend capital that is generated in this fashion.

Since the treasury division of American Express would resemble, in some respects, the dealing room of the Federal Reserve Bank, American Express could artificially expand the supply of its own monetary unit to generate direct corporate revenue with the obvious constraint being the long-term preservation of the unit's market value. This may prove to be a tricky endeavor and it is the tightrope that a monetary issuer walks.

(f) Increased corporate borrowing capacity resulting from an almost immediate increase in overall capitalization of the company. Over time, the balance sheet of the issuing entity will largely be a function of the American Express monetary units in circulation. A stronger balance sheet can only enhance the strategic position of the corporation in financial markets.

(g) Potential unrealized profits from a managed portfolio comprised of a reserve-backed currency at a time when government fiat currencies are sufferng from international market instability. The profits of currency held are a direct result of the appreciation of the new monetary unit relative to other monetary units.

6. Epilogue

True digital cash as an enabling mechanism for electronic commerce depends upon the marriage of economics and cryptography. Independent academic advancement in either discipline alone will not facilitate what is needed for electronic commerce to flourish. There must be a synergy between the field of economics which emphasizes that the market will dictate the best monetary unit of value and cryptography which enhances individual privacy and security to the point of choosing between several monetary providers. I refer to this new sub-discipline as cryptonomics. The Internet is a new world and a new world demands a new currency — a new standard of value.

As an enabling mechanism for social change, digital cash has vast implications for macro-economics in the area of a government's money monopoly and taxing authority, just to name a few.[13] In light of the growing attacks on individual privacy both in the United States and abroad, there has never been a more important time to emphasize the concepts behind the vigilant protection of total financial and monetary privacy. It is money, the lifeblood of any economy, that ultimately symbolizes what commercial structure, and hence what political structure, humans operate within.

REFERENCES

1. F. A. Hayek, *Denationalisation of Money — The Argument Refined*, Institute of Economic Affairs, London, 1978.
2. J. Matonis, *The Political Appropriation of the Monetary Unit*, Institute for Monetary Freedom, Moss Beach. California, November 1984.
3. K. Dowd, *Private Money: The Path to Monetary Stability*, Institute of Economic Affairs, London, 1988.
4. E. C. Riegel, *Private Enterprise Money: A Non-Political Money System*, Harbinger House, New York, 1944.
5. T. Okamoto and K. Ohta, "Electronic Digital Cash" in *Advances in Cryptology CRYPTO'91*, J. Feigenbaum (ed.), Springer-Verlag, Berlin, pp. 324-350, 1991.
6. S. Garfinkel, *PGP: Pretty Good Privacy*, O'Reilly & Associates, Inc., San Luis Obizbo, 1995.
7. B. Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C, John Wiley & Sons, Inc., London, 1994, pp. 117-125.
8. D. Chaum, "Security Without Identification: Transaction Systems to Make Big Brother Obsolete" in *Communications of the Association of Computer Mathematics*, Vol, 28 no. 10, October 1985.
9. K. Kelly, *Out of Control: The Rise of Neo-Biological Civilization*, Addison-Wesley Publishing Co., Wokingham, Berkshire, pp. 208-229, 1994.
10. M. Eichenbaum and N. Wallace, "A Shred of Evidence on Public Acceptance of Privately Issued Currency" in Federal Reserve Bank of Minneapolis, *Quarterly Review*, Winter 1985,
11. W. Baxter, "Bank Interchange of Transactional Paper: Legal and Economic Perspectives" in *Journal of Law and Economics*, vol. 26, October 1985.
12. G. Trivoli, *The Suffolk Bank: A Study of a Free-Enterprise Clearing System*, Adam Smith Institute, London, 1979.
13. M. Rothbard, *What Has Government Done to Our Money*, Pine Tree Press, Colorado Springs, Colorado, 1964; Rampart College, Santa Ana, California, 1974.