Harvard Journal of Law & Technology
Volume 10, Number 2 Winter 1997

COINS, NOTES, AND BITS: THE CASE FOR LEGAL TENDER ON THE INTERNET

Joshua B. Konvisser[*]

"What is digital cash? . . . Is this, in fact, a replacement for currency, in which case you would want it produced and issued by the Treasury? Or is it the next generation of Discover card, in which case it should be regulated under banking laws?"[1]

I. INTRODUCTION

"Right behind sex, commerce on the Internet seems to excite people the most."[2] Electronic commerce is growing at a rapid pace. Yet the modes of exchange currently available on the Internet are inadequate to support the true promise of Internet commerce — a market of information purchases. This Note argues that, in order to realize that promise, the United States government should issue electronic cash ("e-cash") as legal tender currency.

Part II of the Note identifies a number of payment system technologies now implemented on the Internet, examines the proper role of e-cash in electronic commerce, and describes the proposed system. Part III then explains why government backing is essential. Part IV explores the security concerns implicated by e-cash and their technological solutions. Finally, Part V examines other concerns surrounding the widespread use of electronic cash, including crime, privacy, and taxation.

---

* J.D., Harvard Law School, Class of 1997; M.S. (Computer Science), 1994, University of Texas at Austin. This Note is based on a paper submitted to the Seminar on Law, Internet, and Society at Harvard Law School. The author wishes to thank Professor Charles Nesson for his invaluable assistance in forging and honing the ideas presented here.

1. Benjamin Wittes, *The Dark Side of Digital Cash*, LEGAL TIMES, Jan. 30, 1995, at 1, 25 (quoting cryptographer Ernest Brickell).

2. Don Clark, *Microsoft, Visa to Jointly Develop PC Electronic-Shopping Software*, WALL ST. J., Nov. 9, 1994, at B9 (quoting James Bidzos, President of RSA Data Security, Inc.).

II. THE ROLE OF E-CASH IN INTERNET COMMERCE

A. The Growth of a New Marketplace

The Internet market is experiencing explosive growth. In 1995, commerce on the Internet amounted to over $159 million in sales.[3] By the end of 1999, that number is expected to grow to over $400 billion.[4] Not only is the dollar volume of trade exchanged on the Internet burgeoning, but so too is the Internet itself. In January 1996, the Internet had approximately 9.5 million hosts (machines connected); this figure had increased 94% since January 1995 and nearly 700% since 1993.[5] Of these new hosts, by far the most rapidly expanding sector is the ".com" domain used by commercial enterprises. Last year there were approximately 2.4 million ".com" hosts representing just over one quarter of the Internet.[6]

Businesses currently employ four revenue models to capitalize on the Internet's increasing ability to reach customers.[7] These four models are as follows: (1) selling advertising space on web pages; (2) selling tangible goods over the Internet; (3) selling information; and (4) charging for on-line services.[8]

The first model — advertising — is one of the most prevalent.[9] One can scarcely access a service on the Internet without being bombarded by an advertisement. The advertising model, however, is not central to this Note; it is generally implemented through contracts requiring no

---

3. *See ABC News: Internet Fraud* (ABC television broadcast, Mar. 10, 1996).

4. *See id.*; *see also* Penny Lunt, *Payments on the 'Net: How many? How Safe?*, ABA BANKING J., Nov. 1, 1995, at 46, 46 (noting that $1.25 trillion in Internet sales are predicted by 2005 and that "[w]hile only 32% of Internet users said they currently shop on the Internet, 90.7% said they plan to in the future"). *But see* David C. Churbuck, *Where's the Money?*, FORBES, Jan. 30, 1995, at 100 (quoting a corporate executive who has "discovered that the Internet can potentially be the company's biggest productivity reducer").

5. *See* Daniel Akst, *Internet Hosts Doubling Yearly*, BOSTON GLOBE, Feb. 29, 1996, at 29.

6. *See id.* This presence is remarkable when one considers that the Internet first grew out of the Defense Department's ARPANet. Initially, the network was used only by the Defense Department and academic institutions. The arrival of commercial business on the Internet, and the genesis of the ".com" domain, are relatively recent. *See Electronic Money: So Much for the Cashless Society*, THE ECONOMIST, Nov. 26, 1994, at 21; *see also* DAVID BOLLIER, THE FUTURE OF ELECTRONIC COMMERCE 2 (1995) <http://www.aspeninst.org/dir/polpro/CSP/Abstracts/ElecComm.html>.

7. *See* Kate Maddox et al., *Making Money on the Web*, INFO. WK., Sept. 4, 1995, at 31.

8. *See id.*

9. *See generally* BOLLIER, *supra* note 6, at 18-21.

exchange or payment over the Internet (though the companies may negotiate via e-mail sent across the Internet).[10]

The second model employs the Internet to sell tangible goods. Many of today's Internet vendors are familiar companies that have traditionally marketed their wares over the telephone and through mail-order catalogs.[11] These companies have simply moved the same process to the Internet. Rather than sending a catalog through the mail, the seller provides one on-line. The customer selects from the on-line catalog, transmits her credit card number to the seller, and waits for the goods to arrive by parcel post.[12] Though these sellers are reaching their customers electronically, their ties to the physical delivery mechanism prevent them from utilizing the full power of the Internet.[13]

By contrast, the Internet is uniquely suited to the third business model — the sale of information — and some information-intensive companies are starting to capitalize on this fit. Many publishers now provide their materials on-line.[14] This mode of distribution has manifest advantages. Because the materials can be feasibly divided into small segments, users may pay only for the information they want, instead of an entire newspaper or magazine. On-line distribution divorces content from costly packaging that, according to one estimate, "comprise[s] between 50 and 80 percent of the cost of consumer products."[15] Moreover, Internet publishing transcends traditional print media such as newspapers, books, and magazines: pictures can be sold by the view, while music can be sold by the song.[16]

---

10. Note that many advertisements are actually links to the advertiser's own page, where an exchange may take place. In such a case the exchange will fall under one of the remaining three business models.

11. For example, both Timberland and Pizza Hut are among the multitude of familiar businesses now selling via the Internet. *See, e.g., Timberland from Higher Ground,* <http://www.ultramall.com/HIGHGRND/TMB/TMB.htm>; *Welcome to Pizza Hut!,* <http://www.pizzahut.com>.

12. This credit card system is explained more fully below. *See infra* Part II.B.

13. Indeed, according to one commentator:

> While a diverse group of companies has begun selling their products directly on the Web, its power as a sales vehicle has proved to be inversely proportional to the size of the seller — small companies are doing better than big ones. The reason: The Web's worldwide reach can instantly transform a small outfit into a global distributor. By contrast, large corporations that already have their distribution networks in place often find the Web to be a niche channel, with direct Web sales registering only a fraction of their total revenue.

Maddox et al., *supra* note 7, at 32.

14. *See generally,* BOLLIER, *supra* note 6, at 13-14 (discussing on-line magazines).

15. *Id.* at 5.

16. *See infra* note 31.

In particular, software is quintessentially amenable to Internet distribution. Most software distributors rely on a tangible goods model left over from the early days of mass software sales, when the Internet was not a viable means of exchange — they still sell software on a physical medium such as a diskette or CD-ROM. Sending the information over the Internet directly to the purchaser is significantly cheaper.[17]

The fourth business model — the Internet services market — is also potentially lucrative. Marketable services include on-line document searches, web searches to find relevant sites, links to other sites, and expedited e-mail delivery.[18]

The third and fourth business models can succeed only if there is a payment system tailored to purchases of information and related services over the Internet. We will see that e-cash is such a mechanism, and that in the absence of an e-cash regime these models have faltered. First, however, we must examine the non-cash payment systems now operating on the Internet so that we can understand their inadequacies.

B. Noncash Payment Systems

Throughout history, economic development has depended on the creation of new monetary abstractions.[19] Long ago currency supplanted barter in our society; more recently, paper checks and plastic cards have replaced currency in many contexts. Likewise, electronic payments may soon achieve primacy in the settlement of accounts.[20] Currently there are three principal payment systems in use on the Internet.[21] One, e-cash, is introduced in the next section and is the focus of this Note. The two non-cash systems are credit card-based systems and on-line checking.

The first non-cash system is based on the well-known credit card. A number of off-line credit card-based systems, or "electronic shopping malls,"[22] grew up in the early days of Internet commerce, when unsecured transmissions created a substantial risk of stolen card numbers. In

---

17. *See* Debora Spar & Jeffrey Bussgang, *Ruling the Net*, HARV. BUS. REV., May-June 1995, at 125, 125. The Internet Shopping Network, a division of television's Home Shopping Network, sells software over the Internet with overhead costs of between 20¢ and 50¢ per transaction. *See Internet Shopping Network* (1997) <http://www. Internet.net>. Software sold over the telephone through 1-800 mail order houses and through traditional stores incurs respective overhead costs closer to $5 and $15 per transaction. *See* BOLLIER, *supra* note 6, at 6. Thus, selling software over the Internet can lead to a reduction in overhead of up to 90% over 1-800 distributors and up to 98% over traditional stores.

18. *See Electronic Money: So Much for the Cashless Society*, *supra* note 6, at 22.

19. *See* BOLLIER, *supra* note 6, at 24.

20. *See* Gary H. Anthes, *Electronic Currency: A Cash Cow*, COMPUTERWORLD, Jan. 30, 1995, at 54.

21. *See generally* Lunt, *supra* note 4.

22. *Electronic Money: So Much for the Cashless Society*, *supra* note 6, at 22.

such a system the consumer opens an account with a "facilitator" (usually a bank) and provides her credit card number off-line. The consumer may then make purchases over the Internet from participating merchants (the members of the so-called "shopping mall"). The merchant transmits a record of the sale to the facilitator, which sends a confirmation e-mail to the purchaser. Once the purchaser confirms the transaction, the facilitator debits the purchaser's account off-line, transmits the funds to the merchant, and retains a small transaction fee.[23] More recently, as improved encryption techniques have become more prevalent, and security fears have diminished, on-line transmission of encrypted credit card numbers has become a useful payment system.[24]

The second non-cash system is digital checking. Under this paradigm, electronic checks are sent over the Internet and cleared off-line. As with traditional checks, the purchaser has an account with an on-line bank from which checks may be drawn.[25] The current proposals for this scheme involve a hardware checkbook coupled to the user's personal computer as well as additional hardware at the merchant's end. The consumer writes an electronic check, signs it with a digitally encrypted signature,[26] and sends it to the merchant. The merchant then forwards the check to an automated clearing house for processing and payment.[27]

---

23. *See First Virtual* (1997) <http://www.fv.com>; *see also* BOLLIER, *supra* note 6, at 18-19 (noting reasons, including the inappropriateness of current payment systems, for the lack of success of on-line shopping malls).

24. A number of companies have entered or are in the process of entering the market in encrypted credit card payment systems. For instance, Wells Fargo Bank has joined with Virtual Vineyards to allow purchases of wine over the Internet. *See Virtual Vineyards* (1997) <http://www.virtualvin.com/vvdata/112509210/welcome.html>; Russell Mitchell, *Safe Passage in Cyberspace: Theft-Proof Credit-Card Travel Means Cybertrade Can Take Off*, BUS. WK., Mar. 20, 1995, at 33. Additionally, MasterCard and Netscape have collaborated to create a secure credit card payment system, as have Visa and Microsoft. *See* Jared Sandberg, *MasterCard Aims to Link Internet with Credit Cards*, WALL ST. J., Jan. 10, 1995, at B7; Clark, *supra* note 2. Other startup companies working on such systems are First Virtual, Open Market, and CyberCash. *See First Virtual* (1997) <http://www.fv.com>; *Open Market* (1997) <http://www.openmarket.com>; *CyberCash* (1997) <http://www.cybercash.com>.

25. *See* Lunt, *supra* note 4, at 50-51.

26. For further discussion of digital signatures, see *infra* Part IV.A.

27. *See* Lunt, *supra* note 4, at 50-51.

C. Electronic Cash

Money was originally in coins. Then, as commerce grew, coins became impracticable for many purposes and notes were created. The culmination of this progression is electronic cash.[28] In an e-cash system, users store tokens, or electronically encoded sequences of bits, on their personal computers. These tokens are withdrawn from a bank over the Internet, just as one might withdraw hard cash from an ATM. The user spends e-cash by sending the tokens across the Internet to other users who may store them for later use or deposit them in their bank accounts.

1. The Virtues of E-Cash

To date, most companies employing the information-related Internet business models[29] have been forced to piggyback them on one of the other models. For instance, software is tied to the delivery of goods under the tangible goods model. Newspapers using the Internet either provide their information for free or make it available only through limited subscriber services. These services then charge for usage and pay royalties to the newspaper.[30] The same problem appears with music distribution.[31] And companies providing Internet services generally do so for free, passing their costs on to customers via the advertising business model.[32]

The reason for this failure of the information and Internet services models is clear: the means of payment they require does not exist. Because the Internet frees information distribution from medium and delivery costs, it makes possible sales the prices of which are on the

---

28. *See* David Bank, *Cash Comes to Net*, NEW ORLEANS TIMES-PICAYUNE, Feb. 4, 1995, at C1.

29. That is, models three and four. *See supra* Part II.A.

30. *See, e.g., The Boston Globe On-Line* (1997) <http://www.boston.com:80/globe/glosearch.html>.

31. For example, 1-800 Music Now (a telephone-based music seller) now allows Internet users to listen to song clips, but still makes its profits by taking credit card orders and delivering compact discs through the mail. *See 1-800 Music Now* (1997) <http://www.1800musicnow.mci.com>; *see also Firefly* (1997) <http://www.ffly.com> (an on-line music recommendation system that makes its profits via the advertising business model).

32. For instance, many of the web search programs are full of advertisements — at the time of initial search request, on the page displaying the search results, or both. *See, e.g., Net Search* (1997) <http://home.netscape.com>; *Magellan Internet Guide* (1997) <http://www.mckinley.com>. The proprietor of the web site charges a fee which the advertiser includes in the prices of the advertised goods. *See* Jane Hodges, *Words Hold the Key to Web Ad Packages: Sponsoring Search Terms Becomes a Popular Option*, ADVERTISING AGE, Jan. 15, 1996, at 38.

order of pennies or less.[33] Such transactions, which we may call "micropurchases,"[34] cannot be consummated under the non-cash paradigms. The cost of a credit transaction will generally exceed the price of a micropurchase. Thus, on-line credit systems have been limited to the second business model (the sale of tangible goods); they have not been applied to micropurchases. Similarly, on-line checking transactions take between twenty-four and thirty-six hours to clear.[35] While many consumers may appreciate this delay as an opportunity to ensure the availability of sufficient funds, it adds costs, making on-line checks prohibitively expensive for very small purchases.[36]

What is needed is a new payment system allowing for instantaneous exchanges over the Internet, the transaction costs of which are low enough to make micropurchases feasible. That system is e-cash. A number of different e-cash systems are being developed;[37] one of the most tested is DigiCash's.[38] In a test trial, DigiCash gave participants an allotment of e-cash and allowed them to engage in mock transactions. Following the success of that trial, the Mark Twain Bank in St. Louis, Missouri began issuing DigiCash's e-cash for actual purchases on the Internet.[39] More recently, DigiCash announced that the Merita Bank in

---

33. Note that there is no fundamental problem with creating new denominations of currency smaller than one cent. *See Electronic Money: So Much for the Cashless Society*, *supra* note 6 at 22 ("Electronic money of this type could be created in any denomination — even very tiny ones to pay for, say, expedited delivery of an e-mail message — and spent at the click of a mouse-button.").

34. *See* BOLLIER, *supra* note 6, at 30-31; *Cyberscrip: When a Penny is Too Much to Pay*, BUS. WK., Jan. 15, 1996, at 90. *Cf.* Spar & Bussgang, *supra* note 17, at 130 (referring to "microtransactions").

35. *See* Lunt, *supra* note 4, at 52.

36. It is likely that high transaction costs have hindered the overall growth of commerce on the Internet. *See* Churbuck, *supra* note 4, at 100 (discussing the general failure of attempts to sell tangible goods).

37. An example is Digital's Millicent, for which a patent application has been filed. *See Cyberscrip: When a Penny is Too Much to Pay*, *supra* note 34, at 90. VeriFone, a credit card-processing giant, is also developing a wallet-type system for Internet payments including e-cash, secure credit card payments, and electronic checks. *See* Sandberg, *supra* note 24.

38. *See DigiCash Home Page* (1997) <http://www.digicash.com>; *see generally* Jeffrey Kutler, *Money Creators: A Different Drummer on the Data Highway*, AM. BANKER, May 12, 1995, at 14; Steven Levy, *E-Money (That's What I Want)*, WIRED, Dec. 1994, at 174, <http://www.hotwired.com/wired/2.12/features/emoney.html> (discussing DigiCash, its e-cash algorithm, and David Chaum, the president of DigiCash and owner of many of the relevant patents).

39. *See First Bank to Launch Electronic Cash* (1996) <http://www.digicash.com/publish/ec_pres3.html>.

Finland will be issuing its e-cash for large-scale use on the Internet in that country.[40]

E-cash systems have proven successful because they provide for nearly instantaneous, inexpensive, on-line transactions of any size. Additionally, a number of e-cash systems (including DigiCash's) provide for anonymity, thereby making e-cash tokens even more similar to hard cash. By contrast, credit card and checking systems are based on contractual allocations of risk. Thus the user's identity remains critical until the transaction is cleared, often at a time remote from that of the exchange of goods or services.[41]

It is important to recognize that e-cash is unlikely to replace credit card and checking systems on the Internet. Rather, e-cash will coexist with these other payment mechanisms, just as cash, checks, credit cards, and wire transfers coexist today. There will remain classes of consumer transactions — e.g., those in which large values must be exchanged — better suited to credit cards and checks. This will not change on the Internet. E-cash will, however, fill the void that currently exists on the Internet by enabling micropurchases. Just as there are certain purposes to which either coins or notes are uniquely suited (e.g., pay telephones and ATM withdrawals respectively), the Internet presents an area of commerce for which electronic payments are uniquely suited.[42]

2. A Proposed System of E-Cash

The virtues of an e-cash system are thus apparent. But what should this e-cash system look like? The central thesis of this Note is that the existing schemes, under which private banks issue their own e-cash, are sub-optimal; the federal government must step in and issue a uniform electronic currency, granting it legal tender status and thus making it

---

40. *See First European Electronic Cash System Opens for Business on the Internet* (1996) <http://www.digicash.com/publish/ec_pres4.html>.

41. For a discussion of the issues surrounding anonymity, see *infra* Parts V.B & C.

42. No problem is presented by an electronic token with the same value as already exists in hard currency. While in the United States there is rarely an overlap in denominations between notes and coins (an exception is the Susan B. Anthony dollar), such overlap is common in other countries, such as Israel, where both a coin and a note with value NIS 10 are in common circulation.

Note that it is also possible to create electronic currency existing apart from the Internet. For instance, many companies (most notably Mondex in the United Kingdom and Canada) and governments are already considering or testing "smart cards," or wallet-sized cards with electronic chips holding e-cash. *See, e.g.*, GERALD STUBER, THE ELECTRONIC PURSE: AN OVERVIEW OF RECENT DEVELOPMENTS AND POLICY ISSUES 35-54 (Bank of Can. Tech. Rep. No. 74, 1996) (discussing the advent of smart cards in Canada and listing other smart card projects worldwide); <http://www.bank-banque-canada.ca/english/tr_abs.htm#74/> (providing an abstract of Gerald Stuber's report).

equivalent to the hard currency the government already issues. How this system would work is explored below; later sections will examine the virtues of the system and potential problems in its implementation.

In the proposed system, e-cash transactions involve three sets of entities: the Federal Reserve,[43] which mints the tokens and verifies their authenticity; the private banks with which users have accounts; and the buyers and sellers in the market. E-cash tokens enter the marketplace when the private banks purchase them from the Federal Reserve. Private individuals may withdraw e-cash from their bank accounts just as they currently use ATMs to withdraw hard cash. The e-cash tokens are sent over the Internet and stored on the user's personal computer. When the user wishes to make a purchase, she sends tokens to the seller; whereupon the seller's computer automatically forwards them to the Federal Reserve for verification.[44] If the tokens are indeed unused, the Federal Reserve destroys them, generates new ones, and sends the new tokens to the seller's computer.[45] This verification process is rapid and occurs before the transaction is consummated. Once the seller's software receives the bank confirmation and newly minted tokens, the transaction is complete. The buyer no longer has the tokens, and the seller has equivalent tokens. The currency has been exchanged. The seller may hold the tokens for later use or deposit them in her private bank. When such a deposit is made, the bank's computer will ask the Federal Reserve to verify the tokens just as the seller's computer did when it received the tokens from the buyer.[46]

If, during the transaction, the Federal Reserve discovers that tokens with the same serial numbers have already been spent, it will so inform the seller's computer, at which point the transaction will cease. The

---

43. This could just as easily be the Treasury, or any other institution capable of functioning as a central bank. For convenience, this Note will assume that the Federal Reserve is the central bank in the proposed model.

44. The parties could skip this automatic verification step, placing risks on sellers who do not bother to voluntarily verify the tokens received. While this may make sense for transactions involving a high degree of trust (e.g., between close friends or family members), copying is so easy that the level of risk will generally be quite high. Inevitably, e-cash users will become lazy about taking affirmative steps; thus automatic verification is preferable.

45. Each token is used only once to avoid counterfeiting. *See infra* Part IV.B.

46. If there is a fear of counterfeiting by banks, tokens may also be verified when withdrawn from the bank.

seller has not received any value but has also prevented the buyer from accessing the information or service sought. Furthermore, the Federal Reserve destroys the counterfeit tokens before they can be used.[47]

III. THE BENEFITS OF FEDERAL REGULATION AND BACKING

A. The Power to Grant Legal Tender Status

As early as the Constitutional Convention, it was clear that the federal government was to hold the power over the money supply.[48] The Constitution states: "The Congress shall have Power . . . [t]o coin Money [and] regulate the Value thereof, and of foreign Coin . . . ."[49] The Constitution also restricts the power of the states in this regard, forbidding them to coin money, emit bills of credit, or grant legal tender status to anything but gold and silver coins.[50] The implication of these clauses, read together, is that Congress holds the exclusive power to create legal tender.[51]

---

47. For a fuller explanation, see *infra* Part IV.B. Note that both the Mark Twain Bank in the United States and the Merita Bank in Finland are already embarking on ventures involving verification and deposit on every transaction. *See supra* notes 39-40 and accompanying text. Thus it should be quite feasible to create a system that simply includes a new token in the seller's verification message instead of depositing the token in the seller's account.

48. *See* JAMES WILLARD HURST, A LEGAL HISTORY OF MONEY IN THE UNITED STATES, 1774-1970, at ix (1973) (noting that "[t]he clearest policy set in the convention was distrust of allowing state legislatures to determine monetary policy").

49. U.S. CONST. art. I, § 8.

50. *See id.*, § 10, cl. 1. Under the law of contracts, legal tender discharges all debts for which the payment of money is specified when tendered in the appropriate amount and in the proper manner. *See, e.g.*, 5A ARTHUR CORBIN, CORBIN ON CONTRACTS § 1235 (1964); 70 C.J.S. *Payment* § 12. Sufficiency of tender turns on business custom as well as the terms of the contract; thus tender of payment by check, a customary method among most businessmen, generally discharges the debt as well. *See* CORBIN, *supra*, at 524. Federal law currently specifies legal tender as "United States coins and currency (including Federal reserve notes and circulating notes of Federal reserve banks and national banks)." 31 U.S.C. § 5101 (1994).

51. *See* THOMAS WILSON, THE POWER "TO COIN" MONEY: THE EXERCISE OF MONETARY POWERS BY THE CONGRESS 5 (1992) ("The states, therefore, were stripped of all monetary functions, except the power to charter (and regulate) banks."); *see also* Knox v. Lee, 79 U.S. (12 Wall.) 457, 545 (1871) (noting in dictum that "[s]o far from its containing a lurking prohibition, many have thought [the clause] was intended to confer upon Congress that general power over the currency which has always been an acknowledged attribute of sovereignty in every other civilized nation than our own, especially when considered in connection with the other clause which denies to the States the power to coin money, emit bills of credit, or make anything but gold and silver coin a tender in payment of debts").

In particular, Congress can make e-cash legal tender. In *Hepburn v. Griswold*,[52] the Supreme Court struck down the Legal Tender Act of 1862, which purported to create the "greenbacks," the first legal tender paper money issued under the Constitution.[53] The Court reversed itself, however, only one year later, in the Legal Tender Cases,[54] upholding the Legal Tender Act. And in *Julliard v. Greenman*,[55] according to one commentator:

> Finally . . . the Supreme Court ruled that the Congress had the authority to make the notes of the government a legal tender in payment of private debts when it chose to do so. The Court resolved the matter of congressional authority to issue legal tender paper money by placing it among the powers belonging to sovereignty and not expressly withheld from the Congress.[56]

More recently, one court has recognized that "Article I, section 8 of the United States Constitution clearly gives the United States Congress the power to make *anything it wishes legal tender*. Congress is not limited to gold or silver coins."[57]

Furthermore, under the celebrated case of *McCulloch v. Maryland*,[58] Congress has the power to cast the Federal Reserve in the role of central bank for e-cash and the Treasury in the role of mint. In *McCulloch*, the state of Maryland challenged the power of Congress to charter a national bank. The Supreme Court held:

> Although, among the enumerated powers of government, we do not find the word "bank," or "incorporation," we find the great powers to lay and collect taxes; to borrow money; *to regulate commerce*; to declare

---

52. 75 U.S. (8 Wall.) 603 (1870).

53. *See id.* at 614 ("It has not been maintained in argument, nor, indeed, would any one, however slightly conversant with constitutional law, think of maintaining that there is in the Constitution any express grant of legislative power to make any description of credit currency a legal tender in payment of debts."); *see also* WILSON, *supra* note 51, at 141.

54. *See* Knox v. Lee, 79 U.S. (12 Wall.) 457, 545 (1871) ("Whatever power there is over the currency is vested in Congress. If the power to declare what is money is not in Congress, it is annihilated.").

55. 110 U.S. 421 (1884).

56. WILSON, *supra* note 51, at 144; *see also* Guaranty Trust Co. v. Henwood, 307 U.S. 247, 259 (1939) (noting that "Congress was authorized to establish, regulate and control the national currency and to make that currency legal tender money for all purposes").

57. Lowry v. State, 655 P.2d 780, 782 (Alaska Ct. App. 1982) (emphasis added).

58. 17 U.S. (4 Wheat.) 316 (1819).

> and conduct a war; and to raise and support armies and navies. The sword and the purse, all the external relations, and no inconsiderable portion of the industry of the nation, are intrusted to its government. . . . [B]ut it may, with great reason be contended that a government . . . must also be intrusted with ample means for their execution.[59]

The *McCulloch* Court reasoned that the Necessary and Proper Clause[60] grants Congress the power to charter a national bank, a function "consistent with the letter and spirit of the Constitution" and indispensable to the exercise of Congress's enumerated powers relating to money.[61] This reasoning applies with equal force to the control and regulation of e-cash: e-cash is just another form of money, and the Internet, which comprises both interstate and international commerce, is well within the commerce power. Thus Congress has the power both to grant legal tender status to e-cash and to assign the corresponding banking functions to the Federal Reserve.

B. The Virtues of Legal Tender Status

1. A Single Regulatory Framework

Federal sponsorship will allow a single system of regulation to govern e-cash transactions. Such transactions are not currently subject to any specific set of regulations comparable to those governing checks and other common payment systems.[62] This lack of regulation, if not remedied, will lead to risks for parties involved in Internet commerce. One potential risk is the following:

> Issuers might invest the funds they receive in exchange for [e-cash] in risky assets in order to increase their earnings. But riskier investments can turn sour, possibly impairing the issuer's ability to redeem stored-value balances at par and imposing losses on consum-

---

59. *Id.* at 407-08 (emphasis added).

60. U.S. CONST. art. I, § 8, cl. 18 (empowering Congress "[t]o make all Laws which shall be necessary and proper for carrying into Execution the [enumerated] Powers, and all other Powers vested by this Constitution in the Government of the United States").

61. *McCulloch*, 17 U.S. (4 Wheat.) at 421 (1819).

62. *See The Future of Money — Part 2: Hearing Before the Subcomm. on Domestic and Int'l Monetary Policy of the Comm. of Banking and Fin. Servs.*, 104th Cong. 65 (1996) (prepared statement of Alan S. Blinder, Vice Chairman, Board of Governors of the Federal Reserve System) [hereinafter Blinder].

> ers and other holders (if the obligations are not insured).[63]

In a system of privately issued e-cash, the federal government or the individual state governments would have to embark on the difficult task of enacting new regulations to stabilize the e-cash market. At the very least, they would have to piggyback the law of e-cash on preexisting regulations that might not be properly suited to this new form of currency. In order to protect against poor investments on the part of e-cash issuers, the regulations must include such familiar elements as required disclosure,[64] restrictions on the types of permissible investments, and government insurance equivalent to the FDIC. By contrast, with legal tender status, the only entity issuing e-cash is the federal government, and no new regulatory framework is necessary. Because e-cash is fungible with hard cash in this system, the current framework of bank regulation will suffice.[65]

2. Fostering Public Trust

Declaring e-cash equivalent to hard cash will help engender the public trust required for the acceptance of any monetary system by the merchants and consumers who will use it.[66] In the days before the Federal Reserve System, state-chartered banks were permitted to mint bank notes for use by the public. These bank notes were frequently discounted at banks other than the one issuing the notes; the result was

---

63. *Id.* at 66.

64. Compare, e.g., the filings now required by the Securities and Exchange Commission.

65. At the very least, the Federal Reserve should regulate the use of e-cash to create money. Private banks create money by maintaining accounts for depositors in excess of the reserves they hold in vault cash or on account with the Federal Reserve. *See, e.g.*, Albert Gailord Hart, *How To Reform Banks — and How Not To*, CHALLENGE, Mar.-Apr. 1991, at 16-18. The Federal Reserve controls this bank-created money by regulating the "money multiplier," or the fraction of deposit-check money that the banks must hold on reserve. *See id.*; ROBERT J. BARRO, MACROECONOMICS 431-33 (3d ed. 1990). The Federal Reserve has hinted that it will not so regulate the issuance of e-cash — that is, non-bank entities may be able to issue e-cash unhindered by the reserve requirements imposed on demand deposit accounts. *See infra* note 117. The resulting potential for money creation beyond the control of the Federal Reserve could be problematic if e-cash becomes a prevalent form of currency.

Compare the issuance of credit card accounts, another form of money creation. The Federal Reserve currently regulates credit card transactions. *See* Truth in Lending (Regulation Z), 12 C.F.R. §§ 226.2, 226.12 (1996); 1 Consumer Cred. Guide (CCH) ¶ 670. Though unable to exert direct control over the amount of credit extant, the Federal Reserve can monitor this money creation, account for it, and fix other regulations accordingly.

66. *See* BOLLIER, *supra* note 6, at 24-26 (discussing the difficulty of encouraging public trust in a system where the parties never see a physical exchange).

an unstable monetary system.[67] "Some notes circulated at a discount, depending on distance and the reputation of the institution."[68] This turmoil prevailed until 1933, when "an Act was approved . . . which ma[de] all Reserve notes as well as all National Bank notes full legal tender for all debts, public and private."[69]

Of course much of this turmoil was the result of distance and lack of reputational knowledge, concerns which have been mitigated in our age of instantaneous communication and verification. Nevertheless, discounting and consumer distrust may plague the Internet cash marketplace until the government fixes an e-cash standard by granting legal tender status. Kawika Daguio of the American Bankers Association warns that:

> We may be in a situation analogous to the 1860s — in those days, before our current Federal Reserve system, bank checks backed by different institutions weren't as widely accepted — they circulated and were usually discounted. Chartered banks also printed private-bank notes. Now, we see that some institutions are interested in printing their own versions of electronic money and following their own rules.[70]

In addition, the electronic purse, which stores currency in a chip on a plastic card, illustrates consumers' possible distrust of new forms of currency. Gerald Stuber of Canada's central bank notes that:

> Consumers may be hesitant to use electronic purses unless the devices are widely acceptable by merchants, while retailers may hold back on their investment in equipment unless the purse becomes widely acceptable to consumers or until they know which kind of purse is

---

67. *See* WILSON, *supra* note 51, at 128.

68. *Id.*; *see also* Blinder, *supra* note 62, at 62 ("And in the nineteenth century the United States had considerable experience — not always happy — with private bank notes.").

69. WILLIS A. OVERHOLSER, A SHORT REVIEW AND ANALYSIS OF THE HISTORY OF MONEY IN THE UNITED STATES 55 (1936).

70. Levy, *supra* note 38; *see also* John. P. Caskey & Gordon. H. Sellon, Jr., *Is the Debit Card Revolution Finally Here?*, ECON. REV. (Fed. Reserve Bank of Kan. City), Fourth Quarter 1994, at 79, 82-87 (discussing the way in which network effects have slowed the acceptance and utility of ATM and debit-card systems).

> the most popular with consumers (the "VHS-Beta problem").[71]

Consider as well the experience with the greenbacks.[72] Each of these notes was legal tender subject to two exceptions printed on its face: "This note is a legal tender at its face value for all debts, public and private, *except duties on imports and interest on the public debt.*"[73] Because only gold could be used to satisfy these latter debts, banks discounted the greenbacks with respect to gold.[74] E-cash may suffer the same fate, at least before the establishment of the networks necessary to make it a widely-accepted mechanism for purchases.[75]

3. Efficient Operation of a Natural Monopoly

Allowing the market to operate with many parallel e-cash networks is costly. Consider the recent history of the ATM networks. As is now the case with e-cash, the Federal Reserve (as well as the Department of Justice) adopted a wait-and-see approach to the developing world of the ATM networks.[76] Having observed merger after merger of ATM networks, however, the Board of Governors of the Federal Reserve noted in *Banc One Corp.*[77] that "as a result of economic and market conditions, regions are likely to have one dominant network."[78] In reaching that conclusion, the Federal Reserve noted that "[n]etwork externalities . . . tend to promote consolidation of regional ATM networks. . . . One recent study indicates that the ten largest regional networks now account for 80

---

71. STUBER, *supra* note 42, at 30. On the VHS/Beta, or "network externality" problem, see *infra* note 79.

72. *See supra* text accompanying note 53.

73. OVERHOLSER, *supra* note 69, at 42 (emphasis added).

74. *See id.*

75. In this connection consider also the use of e-cash outside the United States:

> If you pay yen for electronic dollars in Tokyo and buy something from a merchant based in Paris who cashes them for francs, a currency conversion has taken place. That, however, is an activity towards which most governments feel highly defensive. . . . Probably, therefore, e-cash will, at least in its early forms, be denominated in single conventional currencies and exchanged at conventional market rates.

Electronic Money: So Much for the Cashless Society, *supra* note 6, at 23. Making e-cash legal tender will encourage foreigners to use e-cash as conventional United States currency subject to the same exchange rates.

76. *See* Donald I. Baker, *Shared ATM Networks — The Antitrust Dimension*, 41 ANTITRUST BULL. 399 (1996).

77. 81 Fed. Res. Bull. 492 (1995), *cited in id.*

78. *Id.* at 497.

percent of all regional ATM network transactions in the United States."[79] The Federal Reserve felt that the economies of scale and related efficiencies outweighed any anticompetitive effects, and allowed the merger in question.

The Federal Reserve is not the only entity to recognize the efficiencies of large ATM networks. One commentator has gone so far as to analogize these networks to the St. Louis Terminal Railroad case[80] — the classic example of natural monopoly, in which the Supreme Court recognized that, rather than breaking up a monopoly in the railroad bridges over the Mississippi River, it was more efficient simply to require that competitors be granted fair access.[81]

Of course, even if large ATM networks are most efficient, it may be that the free market should be left alone to reach that result. This approach, however, also creates significant costs. The most obvious cost is simply the time it takes for the market to converge on the efficient result — in the meantime, society must bear the costs of a suboptimal system. An example is the interchange fee regularly charged when ATM transactions are switched across different networks.[82] Another cost is the potential for antitrust violations and associated litigation.[83] Until recently, the ATM industry had seen little antitrust enforcement by the Department of Justice. Now, however, such suits are becoming so costly for private plaintiffs that many are seeking legislative instead of judicial

---

79. *Id.* Economists apply the label "network effect" where the actions of individuals depend on those of others. Familiar examples are the VHS and Beta VCR standards, the QWERTY keyboard, and the DOS and Macintosh operating systems. In each case, compatibility with the standards others adopt is vital; thus the individual decision whether to invest in a standard turns on the investments others make or are expected to make. The term "network externality" refers to the exploitation of a network effect to achieve market power. *See generally* S.J. Liebowitz & Stephen E. Margolis, *Network Externality: An Uncommon Tragedy*, J. ECON. PERSP., Spring 1994, at 133, 135.

Network externalities are the subject of an ongoing academic debate: some commentators hail them as a classic market failure requiring government intervention. *See, e.g.*, W.B. Arthur, *Competing Technologies, Increasing Returns, and Lock-in by Historical Events*, 99 ECON. J. 116 (1989). Others argue that these externalities will be rare in an otherwise well-functioning free market system. *See, e.g.*, S.J. Liebowitz & Stephen E. Margolis, *Should Technology Choice Be a Concern of Antitrust Policy?*, 9 HARV. J.L. & TECH. 283 (1996). Insofar as the proponents of the first view are correct, avoiding the network externality problem is another virtue of a centralized e-cash system.

80. *See* United States v. Terminal R.R. Ass'n, 224 U.S. 383 (1912).

81. *See* Baker, *supra* note 76, at 423-25.

82. *See id.* at 419-20; *see also* Karen L. Grimm & David A. Balto, *Consumer Pricing for ATM Services: Antitrust Constraints and Legislative Alternatives*, 9 GA. ST. U. L. REV. 839 (1993); Daniel I. Prywes, *ATM-Related Antitrust Developments*, 46 BUS. LAW. 1063 (1991).

83. *See* Baker, *supra* note 76, at 422; Grimm & Balto, *supra* note 82; *see also* Margaret E. Guerin-Calvert, *Current Merger Policy: Banking and ATM Network Mergers*, 41 ANTITRUST BULL. 289 (1996).

assistance. This trend towards legislative resolution has led to a heavily regulated industry dominated by a few large players.

Furthermore, the existing system of ATM networks tolerates unnecessarily high transaction costs. The trend toward larger networks may preserve regional boundaries within the United States, with transactions between regions still subject to the costs noted above. In addition, banks are now beginning to charge fees for transactions by non-customers and in circumstances such as point-of-sale and convenience transactions;[84] such costs would not disappear even if all banks were to use one network. Transaction costs of this nature would preclude a system of micropurchases, in which the amounts involved are a tiny fraction of the costs noted above.

By contrast, the checks of many banking institutions are currently cleared through a system with no such surcharges. This is because the Federal Reserve now runs a unified system for clearing checks.[85] Rather than waiting a number of years to reach a highly-regulated, monopolistic e-cash system with inflated transaction costs, the Federal Reserve should establish one nationwide e-cash system akin to the check clearing system it now manages.[86]

IV. THE PROBLEM OF SECURITY

The designers of any e-cash system face two security hurdles. First, no Internet payment scheme would be viable if unauthorized third parties could read or alter the contents of messages being sent. In addition, the recipient of a message must be certain of the sender's identity.[87] This pair of problems will be referred to as protecting the integrity of the

---

84. For example, casinos and hotels. *See* Grimm & Balto, *supra* note 82, at 857-59 (discussing Valley Bank v. Plus Sys., Inc., 749 F. Supp. 223 (D. Nev. 1989), *aff'd*, 914 F.2d 1186 (9th Cir. 1990)). An individual at a casino or hotel will likely submit to a significantly higher surcharge than an individual on a downtown corner with multiple banks from which to choose.

85. *See id.* at 839.

86. For a brief discussion of the economic arguments for no central bank activity at all in the advent of new systems of currency, see STUBER, *supra* note 42, at 22-24 (concluding that the mainstream view still regards central banking as necessary).

87. "On February 10, 1995, the [Information Infrastructure Task Force] proposed five security tenets for public comment, based on the general proposition that people who use the [National Information Infrastructure] want to know that their information goes where and when they want it to and nowhere else." INFORMATION INFRASTRUCTURE TASK FORCE, OFFICE OF MANAGEMENT & BUDGET, NATIONAL INFORMATION INFRASTRUCTURE SECURITY: THE FEDERAL ROLE 5-6 (1995) <http://www.uark.edu/~niiac/fedrole.html> [hereinafter IITF]. The National Information Infrastructure ("NII") is a system of interconnected telecommunications networks currently under construction which includes the Internet as well as cable and wireless communications. *See id.* at 1.

message. The second problem is counterfeiting. Just as physical bank notes include numerous features to defeat the usual ways of duplicating printed material (such as photocopying),[88] e-cash purveyors must take steps to counteract the ease with which strings of electronic bits can normally be reproduced.[89] Unless both security problems are solved satisfactorily, the regime of e-cash will not enjoy widespread use.

A. Integrity

1. RSA Encryption: Public and Private Keys

The long-accepted method of solving the integrity problem is encryption. All encryption systems rely on keys — algorithms for transforming a message into an unintelligible form and then back.[90] Traditional encryption requires both the sender and recipient to share a single key. The weaknesses of such a system are twofold. First, before sending an encrypted message, the user must transmit the key to the recipient, presenting an opportunity for the theft of the key. Second, as the persons with whom an individual transacts increase in number, so too do the copies of his key, and his lock becomes correspondingly less secure.[91] In view of these weaknesses, the solution of choice for securing the integrity of Internet messages is RSA encryption.[92] The genius of RSA encryption is its use of two keys: the user has a single public key that "is published for all to see"[93] and a second private key calculated "from certain arithmetic facts — facts [the user] keeps to himself — about the published encoding key. The mathematics of this system is such that the public key gives no clue as to how to construct the secret decoding key."[94]

By using these keys, a sender can (1) guarantee to the recipient that she is the sender, (2) guarantee that only the intended recipient can read the message, or (3) both. First, imagine that a sender wishes to guarantee

---

88. *Cf.* Peter Alan Harper, *The Buck Starts Here: New $100 Bills Puzzle, Excite Cashiers*, BOSTON GLOBE, Mar. 26, 1996, at 58 (discussing public reactions to the newly released $100 bill, modified to keep ahead of future counterfeiting technology).

89. *See* NII, *supra* note 87, at 11-12.

90. *See* Simson L. Garfinkel, *Patented Secrecy*, FORBES, Feb. 27, 1995, at 122.

91. *See id.*

92. *See* U.S. Pat. No. 4,405,829 (Sept. 20, 1983). Note that while RSA encryption can be used to protect information from being read by unwanted parties and to identify alterations to the message, it cannot repair such alterations. *See* NII, *supra* note 87, at 37-38.

93. *See* NII, *supra* note 87, at 37-38.

94. Garfinkel, *supra* note 90, at 123; *see also* Andrew Kantor, *Can you Keep a Secret? A Key to Using PGP*, INTERNET WORLD, Feb. 1995, at 20; Russell Mitchell, *The Key to Safe Business on the Net*, BUS. WK., Feb. 27, 1995, at 86.

to a recipient that a message is indeed from her (i.e., to "sign" the information). She uses her private key to encode the signature portion of the message. On receiving the message, the recipient decodes the signature using the sender's public key. If the public key works, the recipient knows that the signature has indeed been encoded with the sender's private key.[95] Second, suppose that a sender wants only the recipient to be able to understand the message. In this case, the sender encrypts the message with the recipient's public key, and the message can be decoded only by using the recipient's private key. For example, a purchaser from an Internet vendor could use the vendor's published key to encode and transmit her credit card number.[96] Third, it may be useful both to sign a document and to send private information. In this situation both types of encryption may be used on the same document — that is, a sender will encrypt with both her private key and the recipient's public key. The recipient will then use her private key and the sender's public key to decrypt the message. This ensures both that the message was from the sender and that only the recipient can read the message.[97]

2. Public Key Registries: The Telephone Book

If RSA encryption is to be useful for Internet commerce, public keys must be readily available to all users in a public key "telephone book." As recognized by the Office of Management and Budget's Information Infrastructure Task Force, public key encryption "require[s] a public key infrastructure to provide a trusted third party, which will allow verification that the signer of a given document is indeed who he or she claims to be."[98]

---

95. Of course if a third party manages to obtain the sender's private key, the sender's security will be compromised, just as with a conventional lock.

96. *See* Mitchell, *supra* note 94; *see also* NII, *supra* note 87, at 24.

97. Although there seems to be substantial agreement that RSA encryption is the means to successful commerce on the Internet, until recently there was little agreement over the specific protocol (the implementation of RSA encryption) to be used. *See* Clinton Wilder, *A Matter of Standards*, INFO. WK., Mar. 13, 1995, at 14. Netscape, the producer of the leading web browser, has developed and embraced its Secure Sockets Layer (SSL) protocol, which it delivers in all copies of its browser. Meanwhile, most other entities interested in secure commercial transactions on the Internet have endorsed Secure HTTP (Hypertext Transfer Protocol). *See id.* Recently both sides have recognized that "[t]he lack of security standards is the major obstacle to consumer and merchant confidence in commerce on the Internet." Clinton Wilder, *A New Safety Net: Top Internet Vendors Agree to Online Security Protocol*, INFO. WK., Apr. 24, 1995, at 14, 14 (quoting Emily Green, a senior analyst with Forrester Research, Inc.). In consequence, a number of major Internet players, including IBM, Netscape, America Online, CompuServe, Prodigy, and RSA Data Technology, have joined together to create a hybrid SSL/Secure HTTP standardized protocol for sending secure information over the Internet. *See id.*

98. IITF, *supra* note 87, at 23.

Furthermore, the law must recognize digital signatures as legally binding before RSA encrypted documents are commercially viable.[99] Utah has taken the lead by enacting legislation authorizing specific entities to maintain registries of digital signatures.[100] These registries fall within the regulatory sphere of the Utah Division of Corporations and Commercial Code, within the Utah Department of Commerce.[101] The statute requires that the state agency conduct regular audits of the registries.[102] A digital signature is legally binding once it has been entered in an authorized registry.[103] Congress should enact a similar law giving legal effect to digital signatures throughout the United States.[104]

3. Export Controls on Cryptography

The last obstacle to securely encrypted Internet transactions is the current governmental policy regarding encryption. While the government does not proscribe the importation or domestic use of cryptography,[105] it classifies cryptography as a munition that may not be exported.[106] The government has recently moderated this restriction: "In

---

99. *See* Henry H. Perritt, Jr., *Payment Infrastructures for Open Systems*, 3 DATA LAW REP. 1 (1995) <http://www.law.vill.edu/chron/articles/dlr.htm> (discussing both the technological and legal infrastructures needed for electronic payments involving secure transmissions); *see also* Richard Raysman & Peter Brown, *Electronic Signatures*, N.Y.L.J., Oct. 30, 1995, at 3 (arguing for the recognition of electronic signatures as legally binding).

100. *See* Utah Digital Signature Act, UTAH CODE ANN. § 46-3 (1995).

101. *See id.* § 46-3-103.11.

102. *See id.* § 46-3-202.

103. *See id.* § 46-3-401.

104. While such regulation may appear to be matter for state contract law, it is well within the commerce power. *See* U.S. CONST. art. I, § 8, cl. 3. Like the interstate highways, the Internet is an integral part of interstate commerce. The federal government has taken control of interstate truck regulation. *See* Surface Transportation Assistance Act of 1982, Pub. L. No. 97-424, 96 Stat. 2097 (codified in scattered sections of 23 & 26 U.S.C.). Congress is thus free to preempt the laws of Utah and the other states in favor of a uniform standard of digital signatures on the Internet.

105. *See* Sylvain André, *Data Encryption and the Law(s) — Results* (1994) <http://www.cnam.fr/Network/Crypto/survey.html>; *see also* Bert-Jaap Koops, *Crypto Law Survey* (1996) <http://cwis.kub.nl/~frw/people/koops/lawsurvy.htm>.

106. The Arms Export Control Act empowers the President to define "defense articles" and "defense services." 22 U.S.C. § 2778 (1994). Under regulations promulgated by the State Department, cryptography is a defense article and may not be exported without a license from the National Security Agency. *See* The United States Munitions List, 22 C.F.R. § 121.1 (XIII)(b)(1) (1996). This license is not easy to obtain. *See* Licenses for the Export of Defense Articles, 22 C.F.R. § 123 (1996).

A domestic Internet market could still flourish under these regulations. However, by limiting Internet commerce to the United States, the government fails to foster the global marketplace to which the Internet is so well suited. Consider in this regard the attempts of certain Asian countries, such as China, to surround themselves by a firewall in order to prevent certain Western ideas from entering the consciousness of their citizens.

1995, the Administration proposed a mitigation of the export controls. Cryptography using keys up to 64 bits (as opposed to the current maximum of 40 bits) would be exportable, provided it implements key escrow (Government Access to Keys)."[107] On February 16, 1996, the government "establish[ed] an exemption for the temporary export of cryptographic products for personal use."[108] Although this amendment does not lift all regulations on the use and export of cryptography, it is at least a step in the right direction.[109]

B. Copying

Preventing the unauthorized duplication of material by an individual authorized to read it is a more complex problem.[110] It is, moreover, quite serious in the e-cash context, where easy counterfeiting would destroy the system. DigiCash's solution is the single-use token. In DigiCash's system, both the purchaser and the seller have accounts at the central bank. The user withdraws cash from the bank and stores it on her personal computer. To make a purchase, she sends tokens to seller, who sends them directly to the bank. The bank verifies the tokens and credits the seller's account balance accordingly. If the seller wishes to make an e-cash purchase later, she must then withdraw her own coins.[111] In the proposal offered in this Note,[112] tokens are likewise single-use, and validated when spent. However, instead of depositing the tokens in the seller's account, the bank automatically generates new tokens, with new serial numbers, and sends them directly to the user along with the confirmation that the received tokens were valid.[113]

---

107. Koops, *supra* note 105. Under a key escrow system, the government holds a copy of the encryption key which it may access only under certain circumstances, such as a properly granted warrant. *See generally* A. Michael Froomkin, *The Metaphor is the Key: Cryptography, the Clipper Chip, and the Constitution*, 143 U. PA. L. REV. 709 (1995).

108. Amendment to the International Traffic in Arms Regulations, 61 Fed. Reg. 611 (1996) (to be codified at 22 C.F.R. §§ 123, 126).

109. For a more complete discussion of the laws governing cryptography, see Froomkin, *supra* note 107. *See also* Peter Swan, *A Road Map to Understanding Export Controls: National Security in a Changing Global Environment*, 30 AM. BUS. L.J. 607 (1992) (discussing the need to relax, or in some cases to abolish, export controls on high technology after the fall of Communism in the Eastern Bloc, given the short life span of most technology).

110. *See* NII, *supra* note 87, at 24.

111. *See Ecash Security and Privacy* (1997) <http://www.digicash.com/ecash/aboutsecurity.html>.

112. *See supra* Part II.C.2.

113. Note that because every token issued must be validated when spent, it makes sense to have a single entity perform the validation and retain the list of spent tokens. This is another reason why the system is best implemented through a central bank rather than a distributed network of private banks.

A possible concern here is the processing cost of real-time verification of all the e-cash transactions in the rapidly expanding Internet marketplace. However, while the initial fixed costs of machinery and software may be high, once they are incurred the marginal costs of transactions are negligible. Compare this with the costs of continually collecting and destroying physical notes, as the current scheme requires. The notes are made from special papers and inks incorporating elaborate and costly security measures. Thus, while the fixed costs of establishing an e-cash infrastructure may be significant, hard cash will cost more than e-cash over time.[114]

V. OTHER DIFFICULTIES

A. The Government

It is clear that the proposal offered here depends for its success on the endorsement of the federal government. Unfortunately, according to Stephen R. Malphrus, Director of Information Resources Management at the Board of Governors of the Federal Reserve System, the Federal Reserve is recommending a wait-and-see approach to electronic commerce.[115] The theory is that any position the government adopts this early in such a dynamic area will stifle potentially important research in other directions.[116] In order to prevent taking a wrong turn, the government has thus far chosen to take no turn at all.[117]

---

114. *Cf.* Harper, *supra* note 88 (discussing public reactions to the most recent modifications to the $100 bill, designed to outpace future counterfeiting technology).

115. Telephone Interview with Stephen R. Malphrus (Feb. 21, 1996) [hereinafter Malphrus].

116. *Id.*; *see also* Blinder, *supra* note 62, at 62-63.

117. This is in marked contrast to the European Union countries which allow, for the most part, only state regulated banks to distribute electronic currency. *See* Blinder, *supra* note 62, at 68. Such regulations would prevent companies like Microsoft and Intuit from using e-cash to conduct banking-like activities. The Federal Reserve is not yet prepared to embrace this position. Malphrus, *supra* note 115. Predictably, the United States banking industry has asserted that only regulated banks should be able to issue e-cash:

> [The American Bankers Association] is not happy with some of these e-cash models. "We have a problem with companies like DigiCash where they're opening up what looks like an account for a customer, where they hold funds and then transmit them to a merchant," says Phillip S. Corwin, director and counsel of operations and retail banking. Only banks should be allowed to create money through fractional reserving or to create demand deposit accounts, he says. "Otherwise you have people establishing banking account relationships without banking regulation or FDIC protection."

Lunt, *supra* note 4, at 54.

The Federal Reserve has also indicated a fear of seignorage losses resulting from the widespread use of electronic currency. Every note in circulation represents a sum of money held on account by the government. In effect, the government receives an interest-free loan in this amount from the holder of the note: the government holds the funds and can invest them, but pays no fee for their use. The money the government earns in this way is referred to as seignorage. According to Alan Blinder: "In effect, holders of the roughly $400 billion of U.S. currency are lending interest-free to the government. In 1994, for example, the Federal Reserve turned over about $20 billion of its earnings to the Treasury, most of which was derived from seignorage on Federal Reserve notes."[118]

If Federal Reserve note usage is displaced by private e-cash, the Federal Reserve will need to respond by constraining the money supply in order to fight inflationary pressures.[119] The government will lose seignorage gains to the extent of the reduction in total volume of circulated notes.[120] However, as even the Federal Reserve recognizes, government control and legal tender status would eliminate this problem: "Government-issued electronic currency would probably stem seignorage losses and provide a riskless electronic payment to consumers. In addition, should the industry turn out to be a 'natural monopoly' dominated by a single provider, either regulation or government provision of electronic money might be an appropriate response."[121]

As argued above,[122] control of money is a natural monopoly, and the federal government is the proper issuer and regulator. Yet the Federal Reserve believes that it is still "premature" to conclude that electronic currency is a natural monopoly.[123] Additionally, the Federal Reserve is hesitant to incur the costs of minting electronic cash in the absence of reliable evidence that the system will be a success. "[T]he government's

---

118. Blinder, *supra* note 62, at 63.

119. On the Federal Reserve's ability to regulate the money supply, see *supra* note 65.

120. The Federal Reserve is not alone in recognizing the importance of losses stemming from privately issued electronic currency. Canada's central bank, the Bank of Canada, is also concerned about such potential losses. *See* STUBER, *supra* note 42; *see also* Richard Blackwell, *Smart Cards Could Cost Ottawa Millions*, FIN. POST, Feb. 21, 1996, at 1. Blackwell discusses the Bank of Canada's practice of holding government securities as assets to back all bank notes in circulation. The securities generate interest while notes do not. In 1994, the notes amounted to $28.3 billion, and the resulting revenue totaled $1.7 billion. The government retains the balance of this revenue after paying bank expenses. *See id.*; *see also* Vanessa Houlder, *Delving into Standards for a Cashless Society*, FIN. POST, Feb. 21, 1996, at 6.

121. Blinder, *supra* note 62, at 64. On the natural monopoly problem, see *supra* notes 75-79 and accompanying text.

122. *See supra* Part III.B.3.

123. Blinder, *supra* note 62, at 64.

entry into this new and risky business might prove unsuccessful, costing the taxpayer money."[124] So far, the government appears to have adopted the approach advocated by the Federal Reserve. The government is actively watching the development of electronic commerce, but is taking no real action. The question remains, however, whether such a policy is prudent.

B. Privacy

Any e-cash system must balance the privacy of its users with the law-enforcement benefits of traceable transactions.[125] Law-enforcement agencies fear that "widespread use of truly anonymous transactions could greatly hamper [police] in money-laundering, drug-trafficking, and anti-terrorism investigations."[126] In particular, a former head of computer crimes investigation for the FBI notes that "[a] lot of crime gets detected by following the money trail around. Obviously, all that goes out the window under digital cash."[127] E-cash cannot be marked the way bills are; moreover, law enforcers would have no electronic equivalent to the proverbial briefcase stuffed full of notes.[128] Such problems are exacerbated by the Internet's global size and instantaneous speed, and the ease of concealing identities over the Internet through anonymous

---

124. *Id.* Although perhaps the loudest, the Federal Reserve is not the only voice in government to be heard on this issue. Robert Rasor, Deputy Assistant Director of Investigations for the United States Secret Service, has recognized that electronic currency is here to stay regardless of what the government does. Therefore, he feels, the government should regulate electronic currency. *See Hearings Before the Subcomm. on Domestic and Int'l Monetary Policy of the Comm. of Banking and Fin. Servs.*, 104th Cong. (1996) (statement of Robert Rasor, Deputy Assistant Director of Investigations for the United States Secret Service); *see also* Fred H. Cate, *Global Information Policymaking and Domestic Law*, 1 IND. J. GLOBAL LEGAL STUD. 467, 467 (1994) ("Both the economic importance of the rapidly growing information services sector and the central role of information in almost all political and economic activities, particularly multinational business, necessitate the creation of consistent, multinational legal and technical standards.").

125. *See* Wittes, *supra* note 1, at 24; NII, *supra* note 87, at 22 ("Strong cryptography can be used to thwart law enforcement's legitimate ability to understand the contents of lawful wiretaps. On the other hand, weak cryptography will not provide effective protection of confidentiality of citizens' sensitive communications.").

126. Wittes, *supra* note 1, at 24.

127. *Id.* (quoting James Settle).

128. *See id.* (quoting Georgetown University cryptographer Dorothy Denning: "With paper money, transactions are sort of anonymous, but not really anonymous. Bills have marks, and cash transactions are face to face . . . [o]nce you get on-line, everything is faceless."). For a more complete discussion of the relationship between e-cash and money laundering, see *infra* Part V.C.1.

remailers.[129] Law enforcement officials fear as well the ability of hackers to infiltrate e-cash "mints" and create counterfeit tokens.[130] Unmarkable cash will likely increase the difficulty of catching counterfeiters.

All the same, privacy is a fundamental value in our society. Even those opposed to anonymous e-cash recognize that "consumers would almost certainly be concerned if each purchase from a vending machine [were] recorded for possible reporting to marketers and others."[131] And, as one commentator has noted, guaranteeing a modicum of privacy is "essential to widespread use of electronic commerce applications over the information infrastructure."[132]

Three pieces of federal legislation now control the degree of privacy afforded to financial transactions over the Internet.[133] The first is the Privacy Act of 1974.[134] That Act, among other things, prevents federal agencies from disclosing information about individuals without their written consent, except in certain enumerated circumstances.[135] The second is the Right to Financial Privacy Act of 1978[136] ("RFPA"), pursuant to which the government may obtain an individual's records from a financial institution only where the information is relevant to a legitimate "law enforcement inquiry."[137] Finally, the Electronic Communications Privacy Act of 1986[138] ("ECPA") prohibits the intentional interception, disclosure, or use of electronic communications obtained in any way by any party.[139]

---

129. *See id.* (quoting Kawika Daguio of the American Bankers Association: "Military-grade cryptography plus anonymous re-mailers plus fully anonymous digital cash plus bad guys equals perfect crimes."). A remailer is a service that strips the identifying markings from an e-mail message before sending it on to its intended destination, thus rendering it nearly untraceable.

130. *See id.*

131. Blinder, *supra* note 62, at 70.

132. INFORMATION INFRASTRUCTURE TASK FORCE, OFFICE OF MANAGEMENT AND BUDGET, COMMON GROUND: FUNDAMENTAL PRINCIPLES FOR THE NATIONAL INFORMATION INFRASTRUCTURE (1995) <http://nii.nist.gov/pubs/common-ground.txt>.

133. For further discussion of this legislation, see generally Catherine M. Downey, *The High Price of a Cashless Society: Exchanging Privacy Rights for Digital Cash*, 14 J. MARSHALL J. COMPUTER & INFO. L. 303 (1996).

134. 5 U.S.C. § 552a (1994).

135. *See id.*

136. 12 U.S.C. §§ 3401-3422 (1994).

137. 12 U.S.C. §§ 3405(1), 3407(1) (1994). Note that this standard is not as demanding as probable cause; it requires merely a "lawful investigation or official proceeding inquiring into a violation of, or failure to comply with, any criminal or civil statute or any regulation, rule, or order issued pursuant thereto." 12 U.S.C. § 3401(8) (1994).

138. Pub. L. No. 99-508 (codified in scattered sections of 18 U.S.C., primarily 18 U.S.C. §§ 2510-2518 (1994)).

139. *See* 18 U.S.C. § 2511 (1994).

These three Acts combine to prevent an e-cash provider (or any other party) from divulging any information about e-cash transactions to the general public. Furthermore, assuming that e-cash providers are "financial institutions" under the RFPA, the government may not obtain such information from these providers except where there is a legitimate investigation underway. Finally, even where the government has access to such information, it cannot divulge such information to private parties (e.g., marketing research businesses) without express consent from the individual.

This legislative structure indicates a strong desire to protect the privacy of financial transactions over the Internet. However, the structure suffers from one severe defect. The standard for government access to financial information is actually quite low. Instead of requiring probable cause, as for physical searches,[140] the government must merely be involved in a "lawful investigation."[141] This standard may not adequately protect the financial information of e-cash users. Furthermore, the RFPA as applied generally does not provide for judicial review until the information has already been divulged,[142] whereas searches ordinarily require a judicially issued warrant absent exigent circumstances.[143]

There is also an argument based on a fundamental right to privacy guaranteed by the Constitution. Recognized in the celebrated article by Warren and Brandeis in 1890,[144] such a right has more recently been embraced by the Supreme Court in the case *Griswold v. Connecticut*.[145] Because this "penumbral" right is not mentioned in the constitutional text, but emanates from the specific guarantees of the Bill of Rights,[146] its scope is unclear. In fact, the Supreme Court has refused to recognize an unqualified right to financial privacy.[147] In *California Bankers Association v. Schultz*,[148] the Court upheld the constitutionality of the Bank Secrecy Act of 1970,[149] which requires banks to maintain records of certain financial transactions. And in *United States v. Miller*[150] the Court refused to recognize a Fourth Amendment privacy interest in the

---

140. *See* U.S. CONST. amend. IV.

141. 12 U.S.C. § 3401(8) (1994).

142. *See* Downey, *supra* note 133, at 319.

143. *See, e.g.*, Chambers v. Maroney, 399 U.S. 42, 51 (1970).

144. *See* Samuel Warren & Louis Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

145. 381 U.S. 479 (1965).

146. *See id.* at 484-85.

147. *See* Downey, *supra* note 133, at 314, 320-21.

148. 416 U.S. 21 (1974).

149. Pub. L. No. 91-508, 4 Stat. 1114 (codified in scattered sections of 12, 15, & 31 U.S.C.).

150. 425 U.S. 435 (1976).

bank records of a criminal defendant,[151] allowing disclosure the records maintained under the Bank Secrecy Act pursuant to a subpoena.[152]

Thus it may appear that the existing legal structure does not support the implementation of an anonymous e-cash system. This is not actually the case, however. The primary concern of the existing scheme is that financial institutions keep records of transactions, reporting them to the government when necessary. Yet it is not the transactions with financial institutions that must be anonymous if e-cash is to thrive. Rather, it is the individual cash transactions between non-financial institutions (e.g., micropurchases) — precisely the type of transactions protected by the ECPA. Hence the current statutory scheme can be harmonized with an e-cash system that protects transactional anonymity in practically all matters.[153]

C. Crime Enforcement

Still another concern is that a successful e-cash regime will facilitate crime.[154] It is important to recognize, however, that many of the crime enforcement issues posed by e-cash are identical to those implicated by hard cash. The e-cash token is just like a new denomination of note or coin in this regard. Furthermore, many of the government's present fears will disappear under a system granted legal tender status.

1. Money Laundering

Perhaps the highest hurdle facing an anonymous e-cash system is the potential to facilitate illegal money laundering.[155] One commentator has noted that:

---

151. *See id.* at 437-40.

152. *See id.* at 444; *see also* Downey, *supra* note 133, at 314.

153. In this regard one commentator suggests: "Maybe what we're looking at in the future is a system that has cash anonymity at the lower levels and then accommodates law enforcement by requiring reporting at the higher levels." Wittes, *supra* note 1, at 25 (quoting Mark Rotenberg, head of the Electronic Privacy Information Center, a Washington non-profit organization that advocates privacy in cyberspace). This would be similar to the large cash transaction reporting requirements with which banks are now familiar.

154. According to Stanley Morris, director of the Treasury Department's Financial Crimes Enforcement Network: "The changing technology could open up potential for money laundering, counterfeiting, credit card fraud, and other fraud." Lunt, *supra* note 4, at 54.

155. Money laundering means hindering attempts to trace illegally acquired cash by passing it through ostensibly legitimate commercial transactions. Eric Hughes, Address before the Seminar in Law, Internet, and Society at Harvard Law School (Apr. 1, 1996).

> While we would caution against establishing restrictive rules that could stifle innovation, the eventual opportunities for money laundering using electronic products may be serious. . . . Over the longer term, . . . it seems possible that electronic mechanisms that can hold large balances and make large untraceable transfers over communications networks could become attractive vehicles for money laundering and other illicit activities — especially if they are widely used and bypass the banking system. Existing anti-money-laundering regulations may then need modification.[156]

While money laundering has been around for as long as so-called consensual crimes have existed,[157] it has been criminalized in few countries, and only recently in the United States.[158] It became a federal crime with the passage of the Money Laundering Control Act of 1986.[159] That act provides, in pertinent part:

> (a)(1) Whoever, knowing that the property involved in a financial transaction represents the proceeds of some form of unlawful activity, conducts or attempts to conduct such a financial transaction . . . —
>
> . . . .
>
> (B) knowing that the transaction is designed in whole or in part —
>
> (I) to conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds of specified unlawful activity; or
>
> (ii) to avoid a transaction reporting requirement under State or Federal law,
>
> shall be [criminally] sentenced . . . .[160]

---

156. Blinder, *supra* note 62, at 70-71; *see also* STUBER, *supra* note 42, at 22 (discussing the increased risks of money laundering with the advent of the electronic purse).

157. Hughes, *supra* note 155. Consensual crimes are actions made unlawful despite the consent of all participants. Such crimes often involve a voluntary payment for goods or services; nevertheless, the money is the fruit of a crime. *Id.*

158. *Id.*

159. Pub. L. No. 99-570, 100 Stat. 3207-39 (codified at 18 U.S.C. §§ 1956, 1987 (1994) & 31 U.S.C. § 5324 (1994)).

160. 18 U.S.C. § 1956(a)(1) (1994).

E-cash money laundering transactions seem to fall squarely within the prohibition of the Act.[161]

The difficulty here is one of enforcement: a number of features of e-cash render it particularly well-suited to illegal money laundering activities. These include the rapidity of e-cash exchanges, the inability to mark bills in an anonymous transaction system, and the inability of law enforcement officials to witness the transfer of large amounts of cash.[162] Thus, despite the formal applicability of the law, many question its continuing effectiveness in a world which has accepted e-cash as a means of exchange.[163]

It may be possible to limit e-cash transactions to the small micro-purchases to which they are best suited. While such a limitation would not make e-cash money laundering activities more detectable, it would make them less practicable. For instance, it would take 10,000 transactions worth 0.1¢ just to launder ten dollars.[164] The problem is that this solution essentially declares that e-cash tokens are "legal tender for all debts public and private *except debts over one dollar.*" Such a limitation on the legal tender status of e-cash would likely produce the same problems that occurred with the greenbacks — e-cash would suffer devaluation with respect to hard currency.[165]

Another possible solution is to use only one-way anonymity in e-cash transactions: i.e., the purchaser remains anonymous but the seller does not. This is the method used by DigiCash and its issuing banks (Mark Twain Bank in the United States and Merita Bank in Finland).[166] This approach is viable in theory; note, however, that DigiCash's one-way anonymity has already been subverted by hackers, so that DigiCash users can transact with two-way anonymity.[167]

---

161. The Act prescribes a similar penalty, with a similar mens rea requirement, for anyone who "transports, transmits, or transfers" money along a path at least one endpoint of which is in the United States and some part of which is in a foreign country. 18 U.S.C. § 1956(a)(2) (1994). Courts have recognized that this subsection applies not only to physical movement but also to electronic communications such as wire transfers. *See* United States v. Piervinanzi, 23 F.3d 670 (2d Cir. 1994); United States v. Monroe, 943 F.2d 1007 (9th Cir. 1991). The Act, however, has no corresponding provision to cover purely domestic transportation.

162. *See supra* text accompanying notes 125-30.

163. *E.g.*, Hughes, *supra* note 155. It may appear that e-cash will be no worse in this regard than the electronic funds transfers criminals can already use. It must be understood, however, that electronic funds transfers do not guarantee anything like the anonymity of the e-cash transactions proposed here.

164. *Cf. Cyberscrip: When a Penny is Too Much to Pay*, *supra* note 34 (discussing the impracticability of many very small fraudulent transactions).

165. *See supra* notes 73-74 and accompanying text.

166. *See Ecash and crime* (1997) <http://www.digicash.com/ecash/about.html>.

167. Hughes, *supra* note 155.

Still another solution is to define a class of suspect transactions (such as those above a certain amount) and isolate this class for recording. In the proposed system, all e-cash tokens must go through the automatic clearance system upon receipt. Thus it is possible for the system to record the identity of the recipient, even though it normally would not do so in order to preserve anonymity. Of course money launderers could defeat this arrangement by simply dividing large transactions into many smaller ones; they would, however, run into the problems of practicability noted above.[168]

Though less satisfactory from a law-enforcement perspective, a more reasonable solution along these lines may be recording the receipts of only suspect *recipients* (rather than suspect transactions) and only under a court order.[169] Though it would not catch all criminal activity, this system seems the most appropriate inasmuch as recording would attach only if there were probable cause.[170] Moreover, under this method the criminal could not avoid detection by subdividing transactions. The solution is also easily administrable, fitting well within the established framework for issuing search warrants.

2. Embezzlement Within the Banking Industry

Some observers fear that e-cash systems will facilitate embezzlement by members of the banking industry.[171] While current regulated bank auditing schemes have time lags on the order of days,[172] e-cash transactions are almost instantaneous. Thus a thief stealing e-cash could easily disappear before the audit uncovered any evidence of foul play. If such activity could be detected immediately, however, the thief could be stopped from absconding with the e-cash. There are currently algorithms for instantaneous on-line auditing that would identify improper activity while maintaining the anonymity of individual accounts and transactions.[173] By modifying bank regulations to require such on-line

---

168. *See supra* text accompanying note 164.

169. This solution assumes that the technology can be designed in such a way that the government can reliably record e-cash transactions. This idea is called into question, however, by the DigiCash users' ability to circumvent that system's one-way anonymity. *See supra* text accompanying note 167.

170. *Cf.* Katz v. United States, 389 U.S. 347 (1967) (holding that the warrantless wiretapping of a public telephone booth unconstitutionally denied the defendant's reasonable expectation of privacy); Payton v. New York, 445 U.S. 573, 576 (1980) (holding that "the Fourth Amendment to the United States Constitution . . . prohibits the police from making a warrantless and nonconsensual entry into a suspect's home in order to make a routine felony arrest").

171. Hughes, *supra* note 155.

172. *Id.*

173. *Id.*

auditing — at least with respect to e-cash — the embezzlement problem could be largely avoided. In addition, if such auditing were applied to all cash, presumably the number of hard cash thefts by bank employees would also be reduced, as their activity would be caught almost instantly rather than within a few days.

The embezzlement problems may be more severe if unregulated non-bank entities such as Microsoft and Intuit are allowed to mint and issue e-cash.[174] With no regulatory framework to guide on-line auditing, insider theft could become nearly impervious to direct governmental control. In the proposed system, however, e-cash issuance is limited to the government and e-cash banking functions to regulated banks. Under this regime, the government would be able to take appropriate steps to prevent embezzlement.

D. Tax Considerations

Another concern is the feasibility of a mechanism for taxing e-cash transactions.[175] Where the buyer and seller reside in a single state, merchants would remain responsible for assessing any applicable sales tax at the time of purchase and forwarding it to the state treasury. What complicates matters is that most Internet transactions involve purchasers in one state, sellers in another state, and a network of hosts in still other states. The question here is whether a state sales tax would impermissibly burden interstate commerce in violation of the dormant Commerce Clause.[176] In *Quill Corp. v. North Dakota ex rel. Heitkamp*,[177] the Supreme Court held that the states may impose taxes on out-of-state vendors only if they have a "physical presence" within the state.[178] This requirement has been interpreted to include stores, factories, and other usual commercial facilities.[179] As online commerce becomes more prevalent, however, courts will face the question whether

174. *See supra* note 117.

175. *See* Lunt, *supra* note 4.

176. A state tax is permissible under the Interstate Commerce Clause when it "is applied to an activity with a substantial nexus with the taxing State, is fairly apportioned, does not discriminate against interstate commerce, and is fairly related to the services provided by the State." Complete Auto Transit, Inc. v. Brady, 430 U.S. 274, 279 (1977). *See also* Commonwealth Edison Co. v. Montana, 453 U.S. 609 (1981) (validating a tax on coal most of which was sold in interstate commerce).

177. 504 U.S. 298 (1992).

178. *Id.* at 317 (following National Bellas Hess, Inc. v. Department of Revenue, 386 U.S. 753 (1967)).

179. *See* BOLLIER, *supra* note 6, at 31.

a local server constitutes a "physical presence" satisfying *Quill*.[180] The federal government could obviate this problem by simply authorizing the states to tax e-cash purchases.[181] Or it could levy a tax on Internet sales under its power to regulate interstate commerce.[182] The government could either keep the proceeds of a federal sales tax or establish a scheme for distributing them among the states.

E-cash also presents a potential problem for income tax collection. The technology makes it quite easy for individuals to store vast sums of e-cash in off-shore accounts — that is, on computers located outside the United States.[183] Imagine that e-cash received in the United States is sent to an off-shore account. The e-cash has flowed through the United States; can it therefore be taxed? Again, this is not a new problem. People will still receive most of their taxable income from employers or from regulated investments in securities. In either case, under current law the payor either withholds or reports the appropriate amount. Furthermore, most such payments occur by check or direct deposit; the advent of e-cash will leave these transactions unchanged. Note also that "under the table" hard cash payments are at least as difficult to track today as e-cash payments will be tomorrow.

VI. CONCLUSION

E-cash is the best means for purchasing on-line information efficiently and conveniently. In order for e-cash to become a stable addition to the money supply, it should be issued by the government as legal tender. Government backing would lend e-cash credibility and render it fungible with hard cash. The government should involve itself now to institute a secure and effective means of electronic cash payments, properly tailored to micropurchases, that will safely direct and encourage commerce on the Internet.

---

180. *See generally The Supreme Court, 1991 Term — Leading Cases*, 106 HARV. L. REV. 163, 163-73 (1992) (favorably discussing *Quill*); Anna M. Hoti, Comment, *Finishing What* Quill *Started: The Transactional Nexus Test for State Use Tax Collection*, 59 ALB. L. REV. 1449 (1996).

181. *See Quill*, 504 U.S. at 305.

182. Indeed, the federal government already imposes a tax on long distance telephone service. *See* 26 U.S.C. § 4251 (1994).

183. "When global digital cash becomes a reality, taxmen will have their work cut out deciding how to assess assets that might be stored on a different computer in a different country every day, even assuming that they could ever find the assets or the computers." *Electronic Money: So Much for the Cashless Society*, *supra* note 6, at 22; *see also* Kelly Holland & Amy Cortese, *The Future of Money: E-Cash Could Transform the World's Financial Life*, BUS. WK., Jun. 12, 1995, at 66, 78.