# The History of Banks, the U.S. Government & Payment System Improvements:

## The past's implications for future payment systems including digital cash.

by Kawika Daguio



Columbia Institute for Tele-Information
Graduate School of Business
809 Uris Hall
New York, New York 10027
(212) 854 4222

THE PURPOSE OF THIS PAPER IS TO PROVIDE A STARTING POINT FOR BANKS AND THE GOVERNMENT TO BEGIN DISCUSSING "DIGITAL CASH" AND OTHER POTENTIAL ELECTRONIC PAYMENT MECHANISMS. (6/14/94)

# The History of Banks, the U.S. Government & Payment System Improvements:

## The past's implications for future payment systems including digital cash.

**Kawika Daguio**
**Federal Representative**
**Operations and Retail Banking**
**American Bankers Association**
**(202) 663-5434**
**kdaguio@aba.com**

## The History of Banks, the U.S. Government & Payment System Improvements

In addition to their central purpose of facilitating commerce, banks have historically been the primary watchdogs of the United States payment system against attacks by counterfeiters & fraud artists. Banks have also recently been made responsible for detecting money-laundering and other related financial crimes. Banks make it easier for individuals and firms to engage in trade, while minimizing the risks to all parties involved, including the government.

Banks manage both the daily operation and long-term evolution of the payment system. More than $2 trillion currently moves electronically each day between U.S. institutions. Banks facilitate commerce between parties with no prior relationship by providing letters of introduction or credit and bank guarantees. Banks have created numerous payment credit risk reduction mechanisms to reduce the likelihood that the failure of major credit counter-parties (i.e. financial institutions [FIs] w/ each other, FIs w/ large companies, FIs w/ governments) would cause the failure of the entire payment system through a domino effect. Banks have cooperatively developed these mechanisms to minimize risk, increase efficiency and convenience.

Prior to the establishment of our current dual banking system under the National Currency Act of 1863, banks issued private banknotes or private-label currency backed by U.S. Government minted gold and silver coins to fund their activities. Widespread counterfeiting and lack of familiarity with a particular bank and its notes caused severe problems with acceptance of these instruments outside of a bank's immediate environs. This method of funding has been replaced with deposit liability funding. The Governments issuance of Gold & Silver Certificates eased the problems with paper currency acceptability. Later Federal Reserve Notes replaced these instruments.

Under "par checking," prior to the establishment of our current checking system, checks and other draft instruments were not widely accepted or widely used by consumers and many firms because of credit risk and extremely high processing costs. The changes which increased the use of these instruments by individuals and firms included the American Bankers Association's issuance of ABA Routing Numbers, establishing bank clearing house associations, the creation of Federal Reserve check clearing operations and crafting of federal regulations.

**Payment instruments must be widely accepted, convenient, cost effective, safe and confidential to assure wide usage. The legitimate public policy interests of the government must also be recognized. Cooperative efforts between banks as an industry, and between banks and the government have made current payment instruments successful & widely used, and can make future payment mechanisms similarly successful.**

**Payment certification, netting, and settlement must be performed only by banking industry regulator supervised institutions in order to assure that the interests of the US taxpayer and government in the soundness of the currency, and the safety of financial institutions, is sufficiently secured.**

**NII-Future Payment Mechanisms**

After entertainment and education related services, home banking is the most common feature/service mentioned in discussions regarding the "National Information Infrastructure" (NII) or "information superhighway". Home banking by itself, and as part of electronic commerce (e.g. home shopping) will require extensive security resources and payment system innovation in order to be both safe and useful.

Most of the foreseeable types of activities or transactions on the NII will require the user to pay the information provider and the network carrier for the services provided. Government services and education related services are the only promised (by Clinton/Gore & telephony/cable companies) free services as of today. It is expected that businesses and non-profit organizations will offer the NII equivalent of 1-800 services. All other activities will require the user to have an open account with the provider or another means of paying for the transaction on-line.

One approach to NII payments is the "network accounting server" model. Under this approach, the user would have a single account with a network carrier which would credit the accounting server of the information or other service provider from whom the user is purchasing information or other services. The user would pay only one firm for all or most of the services used, rather than paying each individual provider either once or several times a period.

A second approach is on-line or off-line debit or credit account transactions with the payment message travelling either along with the purchase instructions or separately through a secure mechanism. An example of an on-line debit system would be an ATM network compatible message containing a payment instruction. One example of an off-line debit transaction could be a message containing a credit card account number with the expiration date and other information required to initiate a credit card payment.

A third approach is digital cash. The following discussion is designed to elicit answers to a number of important questions from the perspectives of law enforcement agencies, central banks, and commercial banks.

## Digital Cash

An increasing number of banks and non-banks are in the process of designing or will soon be pilot testing "digital cash" payment mechanisms. "Digital Cash" is electronically stored value that is transferable in real time between individuals, between individuals and firms, or between firms. Digital cash is alternatively named electronic currency, or electronic cash, but distinct from other electronic payment mechanisms (ACH, Electronic Checks, etc.). This stored value can reside in "smart cards," and portable or other computers and/or devices.

Digital cash is intended (according to the technologies pioneers) to be used first in the "virtual world" (i.e. on-line on the information superhighway), in a parallel fashion to the way paper cash (coin and currency) is used in the "real world." Later implementations may establish credit risk free payment mechanisms for corporate or bank value transfers. No one has fully explored the possibilities of this type of payment mechanism from business and public policy perspectives.

The industry and public policy implications of these formerly "science fiction" payment system mechanisms are numerous, and few of these issues have been addressed. The following are a few of the questions which must be answered:

## Questions

What should a system look like?
- Commercial/Retail
- Small dollar/Large dollar
- Traceable/Untraceable-Anonymous

Who creates the monetary value (Govt., Banks, Non-Banks)?

What security features will be included?
- Digital Signatures
- Serial Numbers
- Severability-Changemaking capacity
- PINS
- Lockable
- Traceability

**What risk management (credit & operational risk) efforts are required?**

**Regulatory compliance**

- **What regulations will apply? (Wire Transfer, Reg E or new regs.)**
- **Who will regulate the service providers?**

**What limits will be imposed on maximum value per instrument?**

**What reporting requirements will be imposed? On whom?**

## Affected Parties

**Law Enforcement Interests**

- **Counterfeiting**
- **Theft**
- **Money laundering**
- **Other law enforcement crime reduction efforts**
- **Bank Security**
- **Bank Secrecy**

**Central Bank Interests**

- **Money supply**
- **Payment system risk**

**Commercial Bank Interests**

- **Operational**
- **Business**

# DIGITAL CASH TALKING POINTS 4/21/95

## Background

Digital Cash is a payment mechanism built on a cryptographic technology. It is designed to securely transfer financial value electronically in a manner approximating the transfer of physical currency. Some digital cash systems are relatively secure, others are easily compromised. Cryptography is controlled as an matter of national security by the State Department, Department of Commerce, and the National Security Agency. "Money" and other financial instruments are regulated by the Treasury, Federal Reserve, and Securities and Exchange Commission. It is unlikely that a technology combining these two highly regulated businesses will escape close government scrutiny and control.

The high-tech nature of the future payment systems under development requires early answers to a number of questions which, at present, are unanswered. Some types of "electronic money" (emoney) have already become widely used. The volume of money ($2.4 trillion a day) moved by current consumer and commercial emoney systems dwarfs that moved by the paper currency and check based payment systems.

A number of individuals and firms are developing digital cash payment systems, designed to provide anonymity for the parties involved in electronic and traditional commerce. These systems are unintentionally or, in some cases, intentionally, designed so that their systems will not accommodate law enforcement agencies or financial regulators interests and requirements. Other systems have gaping security weaknesses which will result in significant fraud and counterfeiting losses. Very few of these developers have had any discussions with government officials.

Among the issues which concern regulators and law enforcement agencies are "old issues," including counterfeiting and fraud, as well as new issues, including the repercussions of anonymity for money laundering and other traditional crimes. In addition there are a variety of unique cryptographic export control and sovereignty questions which derive from the global nature of the emerging information infrastructure.

Last year, ABA sponsored a meeting between a number of operations level employees of Treasury (including FinCEN), Federal Reserve, the National Labs (Sandia) and ABA staff to discuss the implications of digital cash for financial institutions and their regulators. The ABA's goal is to ensure that policy-makers make informed decisions early and give pioneering companies guidance prior to their making investments of millions of dollars and thousands of man years into algorithm specific enterprises.

## Issues

### Crime

Counterfeiting and other financial instrument frauds are extremely costly in terms of their direct impact on the economy and on the morale of consumers. The technological obsolescence of the anti-counterfeiting mechanisms in U.S. paper currency has lead to a rapid growth rate in casual and organized crime, as well as state sponsored terrorist counterfeiting. Check fraud by itself costs the banking industry alone over $18 billion a year, the remaining losses are borne by the companies accepting fraudulent checks. Credit card and debit card fraud losses also are growing at a geometric rate. Because consumers and commercial firms rely on sound money and secure payment systems

in order to prosper, the payment system must be secured against fraud to the greatest degree possible. Part of this security can be gained through the appropriate use of technology, the remainder must be obtained by regulatory and law enforcement activities. There are many issues which must be settled before digital cash will gain general acceptance.

Anonymity vs Traceability

It is uncertain how much demand there is by the average business or person for unlimited amounts of fully anonymous emoney (i.e. digital cash). What often underlies the call for anonymity can be identified as the desire for security and privacy. Although there will be more anonymous emoney in our future, the number of applications and users will be severely limited. The applications will be limited primarily by a lack of general demand, and also limited by the natural conservatism of banks and regulatory agencies. It is more likely that, in the long run, the security of sensitive financial information and payments against theft and misappropriation will increase, and demands for anonymity will abate. Any payment system that provided no accountability or traceability mechanisms would either be merely incapable of day-to-day business use, or would be specifically designed for covert use to facilitate money laundering and other illicit transactions.

Bankers' and law enforcement agencies' ability to address fraud and theft also depend on the capacity to trace transactions. Another reason to limit anonymity is the desire not to facilitate the commission of untraceable crimes. Anonymity in itself raises significant questions. If anonymous money is stolen from your computer, how do you catch the criminal? A banker's worst nightmare would be to have his bank robbed tracelessly by computer hackers.

In addition, business people, such as bankers, can be kidnapping targets. If a kidnapper requests that the bank e-mail him fully anonymous funds, how do you catch him? Today most kidnappers and other criminals are captured when the police stake out the briefcase containing the money.

Traceability can indeed be critically important to law enforcement. Fully anonymous payment mechanisms could be used to launder the proceeds of drug ring operations. The accountability systems banks have in place provided the means for law enforcement agencies to trace the money used in the World Trade Center bombings, and bankers' warnings alerted law enforcement to the activities of CIA traitor Aldridge Ames.

Privacy

The ABA recognizes the privacy interests of individuals and businesses in financial information and transactions. Banks have a history of providing security and privacy protection for customers' financial and other personal information. In addition, the Right to Financial Privacy Act, the Fair Credit Reporting Act, and other laws and regulations imposed on banks already govern the disclosure and use of sensitive information.

We are confident that our customers will be satisfied with the ongoing improvements in security and privacy measures taken by banks to enhance traditional payment system applications. While anonymity may have its place in some activities, the nature of commerce and banking leave little room for anonymous emoney as a means of exchange for legitimate commercial transactions.

**The Actual Characteristics of "Real Money" Transactions**
**Money Laundering and Bank Secrecy Act Issues**

Q: Is Physical Currency an Anonymous Media?
A: - NO!, Not in large amounts.

Physical Cash is presumed by many people to be anonymous. Those who believe that people engaged in large dollar transactions using paper currency retain their anonymity today are mistaken.

The transfer of physical cash in large amounts is an observable activity in that cash in large amounts occupies large volumes of space. It's location can be monitored by intent observers and the person transporting it followed. In addition, serial numbers and marking technologies allow certain transfers to be traced and recorded. Exploding dye bags and radio transmitters are often included in the bags of money that bank robbers take with them.

Today, laws govern the reportability of large cash transactions. Evading the reporting requirements is itself a crime. A great deal of law enforcement agency resources are dedicated to addressing the issue of money laundering. Changing the nature of payments from paper to electronic will not reduce the interest or the authority of regulators and law enforcement agencies to address this type of crime.

The transfer of physical cash when performed anonymously creates significant risk to the value transferred. The primary risks are that knowing or unknowing couriers might steal or lose the money transferred. The supervised transfer of physical (illicit) cash (i.e. drug proceeds, kidnap ransoms) creates significant risk of exposure to observation to the persons transferring the money.

In the "real world" one can transfer value anonymously if you are willing to risk losing money, or one can securely transfer the money and allow limited exposure of personally identifiable information.

Digital cash technology might soon make secure and anonymous transfers possible. Fully anonymous digital cash could be a immense boon to those wishing to avoid supervision and accountability.