WORLD GOLD COUNCIL

RESEARCH STUDY 24

Digital Money & Its Impact On Gold:

Technical, legal & economic issues

Richard W. Rahn
Bruce R. MacQueen
Margaret L. Rogers
(Novecon Financial Ltd)

WORLD GOLD COUNCIL

RESEARCH STUDY 24

Digital Money & Its Impact on Gold:

Technical, legal and economic issues

Richard W. Rahn
Bruce R. MacQueen
Margaret L. Rogers
(Novecon Financial Ltd.)

The views expressed in this study are those of the authors and not necessarily the views of the World Gold Council. While every care has been taken, neither the World Gold Council nor the authors can guarantee the accuracy of any statement or representations made.

November 2000

Published by Centre for Public Policy Studies,
World Gold Council, 45 Pall Mall, London SW1Y 5JG, UK.
Tel +44(0)20.7930.5171 Fax +44(0)20.7839.6561
E-mail: cpps@wgclon.gold.org Website: www.gold.org

CONTENTS

INTRODUCTION

One of the consequences of the internet is the possibility it offers for the development of digital – or electronic – money. By offering a means to exchange value for goods and services while eliminating the need to use physical tokens this development could have a significant effect on the way individuals, institutions and companies do business.

The internet also makes one further development possible. Once again, entities other than governments or central banks could issue currency. Some of these currencies could be backed by gold or by other precious metals. One gold-based system – e-gold – has been in operation for several years while the launch of a second – GoldMoney – is scheduled to occur shortly after this report goes to press.

While the outlook for these possibilities remains uncertain, they have potentially profound consequences for the financial system and for gold. They raise a number of issues and concerns - but they also offer opportunities.

Richard Rahn, and his colleagues in Novecon Financial Ltd, are leading experts on the development of electronic money. The World Gold Council is therefore pleased to publish this report by them which examines first the potential for digital currencies in general and second the potential for gold.

Robert Pringle
Corporate Director, Public Policy and Research
World Gold Council

CHAPTER 1: OVERVIEW OF DIGITAL MONEY SYSTEMS

This report reviews the current status of and outlook for digital money and related products. It looks at the technical, legal, political, and economic issues that are likely to foster or retard the development of digital money-like products. In particular, it focuses on the risks and opportunities to develop gold-backed or gold-denominated financial instruments.

The age of digital money is upon us. The new technologies of the internet, digital electronics, public key encryption, and the rapid price declines of computing power and telecommunications bandwidth are having a dramatic effect on the financial world. These new technologies are enabling the development of financial markets, procedures, and instruments that economists in the past could only theorise about. Financial transactions can be settled in real time even though the contracting parties may be thousands of miles apart. Money and other assets can be moved at almost the speed of light to any point on the globe for a minuscule cost. Easy to use encryption programs enable almost anyone to move data or money around the globe with complete security.

Digital money is the monetary value of government- or privately-issued currency units stored in electronic form in an electronic device. It is one type of a digital financial instrument that fulfils most or all of the functions of money. The monetary value stored in the electronic device can be transferred to other such devices, allowing the users to engage in payment transactions. This is different from traditional electronic payment systems, such as credit and debit cards and wire transfers, which usually require online authorisation and may involve debiting and crediting bank accounts for each transaction.

Digital money systems provide a means to exchange value for goods and services, while eliminating the need to use physical tokens. The growth of electronic commerce in recent years has heightened the interest in the development of digital money. Currently, most of the transactions taking place over the internet rely upon the use of credit cards as the means of payment. Yet, credit cards are relatively costly for a merchant to accept, and force a customer to exchange sensitive financial information with a merchant. They are not suitable for small-value payments because of the high transactions cost. Neither can they be used for transactions between individuals. Consumers are wary of the possibility of theft, and are concerned about the security of their information, both in transit and in storage at a merchant's site. Infamous cases of unauthorised intruders accessing

merchant databases and stealing customer credit card numbers have added to consumers' fears. To fulfil the promise of electronic commerce, lower cost, more efficient and more secure payments systems are necessary. Digital money systems offer these advantages.

The rapidity of adoption of digital money systems by consumers depends on how their cost, convenience, and anonymity is perceived in relation to paper currency and coin. Unlike paper currency and coin, the various forms of digital money do require the receipient to have a device – smart card reader/writer, computer, or wireless device– that can receive and/or authenticate the monetary transfer. Early adoption of these ssytems tends to be slow, as the number of other consumers and merchants using these devices is directly related to their usefulness for any individual. (This problem is similar to the problem faced by the first sellers of fax machines. The machine had little value until many people owned them, at which point they almost became a necessity, particularly for business.) The technology has already moved to the point where the devices are as small or even smaller than the typical personal wallet used to contain paper currency and coin. The cost of such devices should continue to fall until, eventually, it will no longer be an impediment.

The advent of digital money also opens the possibility that money could be issued by entities other than governments and central banks. The state's monopoly over the issue of legal-tender currency is a relatively new development in the history of finance. The case for competing currencies has been argued in a number of fora, perhaps most famously by the great Nobel prize-winning economist F. A. Hayek who noted:

> There is no justification in history for the existing position of the government monopoly of issuing money. It has never been proposed on the ground that government will give us better money than anybody else could. It has always, since the privilege of issuing money was first explicitly represented as a Royal prerogative, been advocated because the power to issue money was essential for the finance of government – not in order to give us good money, but in order to give to government access to the tap where it can draw the money it needs by manufacturing it.[1]

[1] F. A. Hayek, "Toward a Free Market Monetary System," Journal of Libertarian Studies, vol. 3, no. 1 (1979), p. 7.

Hayek had also argued for competitive currencies. The new digital and encryption technologies allow the experiment to be conducted on a worldwide basis at low cost. The possibility that central banks could lose their monopoly over the issue of currency in the age of digital money has also been noted recently. For example, Mervyn King, deputy governor of the Bank of England, speculated on this possibility in a speech at the Jackson Hole Symposium in August 1999[2] .

Digital money systems can be divided into two general categories, accountable and non-accountable. In an accountable system, every transaction between a payee and payor is accountable by a third party, although this accounting may not happen at the exact moment of the transaction, and the payee and payor may not be personally identifiable. Non-accountable systems allow for the free movement of value, synonymous to the movement of physical cash. There are numerous variations of implementations for these systems. Some implementations are online, meaning that transactions require a connection with a third party, such as an issuer, for verification, while others are offline and require no contemporaneous connection to a third party. Additionally, systems may use ledger balances to hold value, or may choose "token-based" implementations.

"Token-based" systems exchange value through a denominated electronic token. This token, also called a "note" or "coin," is essentially a packet of information, typically consisting of a serial number and a denomination of value, which is digitally signed by an issuing institution to verify the validity of the token. Systems using this token-based model may also choose to have additional information attached to the token, such as an expiration date and transactional history. Depending upon the specifications of the system, an online verification with the issuer of the digital money may also occur at the time of the transaction.

Ledger-based systems are those in which value is recorded as a balance ledger, which can be increased and decreased as transactions are made. Ledger-based systems rely on transferring value from one account to another account based upon an exchange of instructions. Typically, a ledger is maintained by an account managing entity, and communications are established with the account manager to make a transaction. An instruction to the account manager would direct that a payment be made from the payor's account to the payee's account.

[2] Mervyn King, "Challenges for Monetary Policy: New and Old". Paper prepared for the symposium on "New Challenges for Monetary Policy", Jackson Hole, August 1999.

Specialised hardware, such as a smart card, may be incorporated into the implementation of a digital money system. Alternatively, some systems depend upon software that can be used from a consumer's own personal computer and which relies upon widely available communications channels such as the internet to transfer data and carry out transactions. Each of these alternatives has its advantages and disadvantages, and also requires different types of security measures to protect from fraud and theft. The choice of the type of system that would be best for any given payments system is dependent upon the features that the developer would like to implement to best suit the needs of the target users of the system.

To facilitate electronic commerce, a merchant may implement shopping cart software, which some digital money issuers provide to their users, to allow for a smooth interface between the merchant website and the payments system. This is highly desirable, as many potential customers choose not to engage in complicated processes to make purchases.

Although there are many alternatives available for digital money systems, there are a few points that should guide the design process. A good digital money product must be efficient, secure, easy-to-use, and widely accepted. Customers should feel confident that their money is safe within the system, and therefore the system should be solidly backed. To be able to accommodate many users and many merchants, the system must be designed with the potential for growth in mind. The potential to have anonymous transactions, with the same ease of use as cash, is also highly desirable from a user's perspective. Although anonymous systems require more sophisticated technical security solutions, the benefits to the consumer are likely to move systems in this direction. A highly successful product will be one that can be used in a variety of circumstances. For example, a digital money product that could be used to make purchases over the internet, at the local coffee shop, and at an unattended vending machine would be very appealing. Such a product might use a hardware-based implementation, which would have an inexpensive interface to be used with a personal computer.

Security and risk management for digital money systems

The security of a digital money system is one of the most vital aspects in system design. Payment systems are vulnerable to a number of types of risk, from counterfeit replications and malfunction of devices, to theft and unlawful use of

genuine devices or value. Some of the risks that digital money systems face are the same as for any other payments system. There are some unique risks that digital money systems face, which must be addressed in any implementation. Prevention of fraudulent use of the digital money system through cryptography and design protocols will be the first defence against attacks.

Cryptography, the art of writing in code, is probably the most basic security measure for any digital money system. For digital money systems, the importance of cryptography is in the ability to use mathematical algorithms and data strings, called keys, to manipulate message data in such a way as to make it unreadable to anyone who does not possess the key necessary to decrypt it. Through this process, it is possible to establish secure communications across otherwise insecure channels. Digital money systems use both symmetric key cryptography, in which a single key encrypts and decrypts a message, and asymmetric, or public-key cryptography, in which a key pair is used, one for encryption and the second for decryption. Strong cryptography depends upon the robustness of the cryptographic algorithms, as well as on the cryptographic keys. In general, the longer the key, the more secure it is.

In addition to the ability to secure message data from disclosure, cryptography can also be used to authenticate the source of a message and verify that the contents of the message have not been changed. Message authentication is achieved through the use of a key pair, in which message data is "signed" using an entity's secret key. Since only the entity has access to its secret key, a message that has been encrypted using that key could only come from the corresponding entity. The message is verified by using the public key of the key pair to decrypt the message and thus verify the signature. For example, in a token-based system, tokens are signed by the secret key of a key pair held by the issuing institution, allowing anyone to verify the validity of the token. Transactions communications are encrypted so that no outside party can "see" the information that is being transferred, and therefore cannot usurp the message or copy the information containing the value.[3]

[3]For a further discussion of cryptography as it relates to digital money, see the report produced by the Committee on Payment and Settlement Systems and the Group of Computer Experts of the central banks of the Group of Ten countries, "Security of Electronic Money," Bank for International Settlements, Basle August 1996. The report is available at: http://www.bis.org/publ/cpss18.htm.

Measures to detect and, if necessary, end any improper use of the system will also be important to manage risk. The design and choice of features of a digital money system will have an impact upon how easily detection of fraudulent activity can occur. For example, a system that requires more interaction with a central entity, such as the issuer, will have more opportunity to detect fraud or suspicious usage activity than a system that allows person-to-person transactions. Maximum values that may be held at any one time, and expiration dates for value could lower the potential financial gain and thus the incentive that criminals have to breach the security protocols. Systems can also implement means to block certain devices that have been used fraudulently, or serial numbers on tokens that have been compromised, in order to stop any further financial gain.

Myriad security protocols to protect digital payments systems are currently in use, and more have been envisaged for the future. As technology advances, new and stronger security measures will be needed to stay ahead of the methods devised to break through the protections in use. Good digital payments systems will continually adapt their overall security and risk management procedures to ensure their continued effectiveness. The types of security protocols that are required will of course depend on the specific type of digital money system that is being employed.

Model systems

A few basic models of digital money systems are token-based systems, smart card systems, and fully-accountable online systems. Most systems currently on the market are based on these models.

Token-based payments systems

One basic model for an electronic payments system is a software-based, "token" system. Token-based systems typically use a software "wallet," which stores "tokens," or packets of information that denote a certain value.

There are various implementations that token-based systems may use. Some are bearer-based, analogous to a dollar bill, in that the issuer is obligated to the holder of the token to redeem it at face value. In other implementations, tokens may also include information that directs the value of the token to be paid into a certain account.

A token-based system has the advantage that it can easily be adapted to provide anonymity to its users with respect to both the issuer and the other users in the system. Tokens need only have a valid serial number, a denomination, and a means of verifying that a token is valid, for instance through the digital signature of its issuer. Transaction history is optional, and may be desired for certain uses. Transaction history can be used as a method to prevent or detect fraud or double-spending of a token, but it is not the only means to do so. For example, eCash Technologies uses a challenge-response protocol that can detect double-spending and reveal the identity of the user who attempts to spend a token twice. If the token is only spent once, the spender remains anonymous.

Smart card systems

Smart card digital money systems typically offer an offline system, implementing a stored-value purse on an integrated circuit contained on a plastic card similar in appearance to a credit card.

The issuer generates digital cash from an issuer's computer. Each "note" has a serial number and an expiration date, and is signed by the private key of the issuer. Signed notes are transferred to a user's smart card when money is transferred into the system. Depending upon the specific system, money can be transferred from a user's account at the bank, or can be added to a card from a designated kiosk with cash or a credit card.

In some implementations, transactions may be made from card to card using a specialised device. When notes are transferred from one card to another, the sending card can add its signature to the note, so that an audit trail is formed. As notes return to the issuer, these signatures show where the note has been in order to control fraud and double spending. Although double spending is not caught at the moment of transaction, cards that engage in illegal activity can be shut out of the system.

It is also possible to split notes in order to make change. These split notes are collected, then compared with the original note to confirm that the exact value of the note is spent, and not more or less.

Smart card systems may also use a balance system, in which value is deducted from or added to a total balance on the card, based upon the type of transaction made.

Smart card systems can be designed to accommodate multiple currencies to allow for maximum flexibility. An exchange transaction would need to be made while connected to an outside device that could peg the exchange rate between currencies.

Fully accountable online systems

A third basic model for digital money is the fully accountable, online system. In this model, a user establishes an account with the issuer of the digital money, and sends a payment to fund the account. (This initial funding can be made via traditional means, such as wire transfer, cheque, or credit card, or by receiving a digital payment from another user within the system.) After the initial funds are credited, a user may make payments and spend the digital money in the account.

Users access their accounts online, viewing account records and making transactions. Access to accounts is generally made via secure connection, such as through a Secure Socket Layer (SSL) connection over the Internet. Accounts are passphrase-protected to guard against unauthorised access. For this reason, it is very important that users select a good passphrase that is not likely to be guessed or easily figured out.

This type of system generally does not allow for anonymity. A user must have an account, and personal information is requested in order to open an account. This information is held by the system's administrators, and every transaction passes through this third party. System administrators usually keep a log of transactions. Although it would not be impossible to allow for some degree of privacy within the system, this is not how most current systems have been designed.

The potential development of financial bearer instruments

Financial cryptographers have developed methods whereby people will be able to hold securely bearer digital cash, bonds, stock, and even financial derivatives, and make very low cost and anonymous transactions with them. A US dollar in paper form is a bearer instrument. That is, the person who holds it is normally considered to be its lawful owner. There is no list of owners of paper currency (a registration record); ownership is conveyed by physical possession. Gold coins are also bearer instruments.

The advantage of bearer instrument transactions is that settlement is in real time, and therefore there is no risk of non-payment, as there is in book entry transactions such as cheques and credit cards. There are no charge backs to the merchant,

and the risk of fraud (in the absence of counterfeiting) is greatly reduced. Bearer instruments are also anonymous, which can protect the owner from corrupt governments or criminal types. However, because of this anonymity, many governments do not like or have prohibited certain types of bearer instruments because they make it hard for tax officials to collect revenue.

The issuance of digital bearer financial instruments requires an underwriter who issues the digital bearer certificates, verifies every transaction to make sure that a given bearer certificate has not been copied and spent more than once, and markets its certificates. A trustee is also required to hold the reserves backing the digital financial instrument. The reserves could be cash, gold, bonds, stock, or other assets, or the full faith and credit of the issuing institution.

Earlier experiments in digital bearer instruments made the mistake of having the underwriter also serve as the trustee, which provided a less secure system. It is likely that a number of competitive underwriters and trustees will emerge for the various types of digital bearer instruments that will be created. Existing participants in the gold industry would be logical underwriters and trustees of gold-backed digital financial instruments.

CHAPTER 2: CONCERNS AND ISSUES

Digital monetary and financial products are "disruptive" technology, in that their creation upsets the existing legal and public policy order as to how money and financial products and institutions are regulated and organized. National borders are ceasing to have the relevance they once did. Both businesses and governments need to build the appropriate legal order for the digital age and understand how it should be managed. This will require changes in laws and regulations, leaving businesses in a thicket of uncertainty during the transition period. Central bankers, treasury officials, law enforcement authorities, and intellectual property administrators (patent officials, etc.) will by necessity have to adjust to a different world. Their challenge will be to create a new set of rules and procedures that bring the necessary order without impinging on the rights of privacy of individuals and institutions, or destroying the economic efficiencies that the new technology is bringing.

Legal implications of electronic payments systems

Many legal issues will arise as digital money becomes more prevalent. Given that most digital money will be global in the sense that the internet will facilitate its movement or use outside its issuing jurisdiction, the lack of legal uniformity between countries raises many policy issues. For instance, who has the liability if a failure does occur in a particular digital money system because of fraud or for some other reason? When digital money payments are made across national borders, who has jurisdiction? Does digital money violate the monopoly rights of central banks to issue money? May a central bank issue digital money? Do non-bank issuers of digital money need to be regulated, and if so, who should the regulator be? Who is going to determine if the clearing organisations have sufficiently robust and fraud proof systems?[4] Given that various digital money systems are now being developed and offered, the answers to the above questions will probably slowly evolve over the next few years as real problems emerge. Already, multilateral financial institutions like the Bank for International Settlements and the International Monetary Fund have established working groups to try to develop recommendations for their members in dealing with the above-mentioned issues. These BIS and IMF recommendations will be of particular interest to the world's central bankers who are facing the front line of change.

[4] See, for example: Bank for International Settlements, "Implications for Central Banks of the Development of Electronic Money," Basle, October 1996, p.9.

To the extent people use privately-issued digital money for transactions, the demand for government money is reduced. If people are willing to hold liquid balances in the form of digital money, the quantity of demand deposits (checking accounts) that people need or desire is smaller, hence reducing the central bank's supply of money. The same principle holds true for other money substitutes, from very limited money substitutes (e.g. balances held on telephone cards, or frequent flyer miles) to broad money-like products (eg digital gold). As these broad and narrow-use money substitutes grow in popularity because of their ease of use in the digital age, the amount of money supplied by central banks will decline. Until some non-government money reaches a critical mass whereby most users and businesses find they can do a substantial portion of their business in the "new money," virtually all digital money and money substitute products will be reconverted to central-bank-issued money at some point. However, even during this period of partial and temporary substitution of digital money for central bank money, the demand for central bank money will decline.

One effect of the decrease in demand for central bank money will be the disappearance of central bank seigniorage revenue. At present, the world's central bankers make a considerable income from issuing paper banknotes, which are non-interest bearing central bank liabilities. Among the G-10 countries, seigniorage as a percent of GDP ranged from a low of 0.28% in the UK to a high of 0.65% in Italy in 1996.[5] This seigniorage not only provides for all of the central bank operations, but also provides their treasuries with significant revenue. However, it is also apparent that the efficiency gains for the economy from digital money swamp any negative effect on government revenue of the loss of seigniorage revenue, which has been in effect a tax on the banking system. Finland is the furthest along in moving to various forms of digital money (see page 25), and it is clearly a net plus for the Finnish economy because it reduces the need to hold non-remunerative balances in paper currency.

It can be expected that the growth of digital money will have a direct and significant impact on the common measures of the money supply, particularly currency and demand deposits. Given that many central bankers target these monetary aggregates in the conduct of their monetary policy, the focus of monetary policy may need to change.

[5] Bank for International Settlements, "Implications for Central Banks of the Development of Electronic Money," Basle, October 1996, p.8.

The growth of digital money could ultimately cause a substantial drop in banks' demand for settlement balances. In the major economies, cash is the largest component of central bank liabilities. Extensive use of digital money is likely to shrink the balance sheets of central banks significantly. At some point the shrinkage might restrict central banks' ability to conduct open market operations or foreign exchange sterilisation operations. However, to the extent that the new digital monies are fully backed by assets such as gold or high-quality financial instruments, the need to conduct open market operations will diminish, because the supply of money for transactions should automatically adjust to demand.

As more and more transactions are settled on a real time basis, the risk of non-payment and fraud declines, and hence the need for regulation and monitoring also declines because large intraday liabilities within the banking system are greatly diminished. The role of the central bank may ultimately shrink to doing little more than defining the numeraire for the national money. This could be a modern version of the gold standard. This definition could apply to just the domestic currency, or a number of countries might well agree on a common definition, which would result in a true international currency. Specifically, a currency in the future may well be defined as a monetary unit that is equal to a basket of specified commodities, such as gold, and even some services. Any good or service having a one world price that is set in organised auction markets could be a candidate for a currency basket that would be used to define the value of the monetary unit. Some central banks might also continue to serve as a lender of last resort to large financial institutions, by using off balance sheet transactions. The need for such a lender of last resort might diminish in a world of instant information on almost all activities and institutions, and real time settlements.

The rapidity of adoption of digital money systems by consumers depends on how their cost, convenience, and anonymity is perceived in relation to paper currency and coin. Eventually, electronic transfer and digital money systems could replace paper and coin, as they would not incur heavy storage and security costs and may ultimately become more convenient. At the current level of technological advance, it appears that within relatively few years almost all monetary transactions , whether they involve a few cents or millions of dollars, could move over the internet, by wireless device, or by chip card for small transactions. The question of anonymity will remain an impediment until policy makers accept that the fundamental desire and right to personal privacy must be accommodated with the new technologies, to an extent no less than people now have with cash.

The role of central banks will change, and will possibly shrink, as a result of the new technologies. One danger to the world economy is that central banks will try to hold on to their traditional roles by restricting the new technologies or regulating them in such a way as to make them non-economic. Regulators should keep a hands-off approach until a problem has been clearly demonstrated, and at that time devise corrective actions to do the least damage to innovation and financial freedom.

Money laundering, crime and digital money

Law enforcement officials around the world have been concerned about the potential abuse of digital money systems for the purpose of money laundering, and hence are trying to restrict or ban them. One demand that has been made by officials in various governments is that they have the right and ability to have records of and monitor all transactions. It is true that digital money systems, particularly anonymous ones, may indeed make the job of money laundering easier. On the other hand, privacy advocates have been quick to point out that many government law enforcement agencies throughout the world have infringed against some basic rights to financial privacy. They note that the benefits of digital money greatly outweigh the potential criminal abuses, and hence argue that measures to restrict the use of digital money should be resisted. Without the availability of anonymous systems there will be strong resistance on the part of many individuals to move fully to e-payments systems and digital money.

When considering potential action against money laundering vis digital systems, it needs to be remembered that existing efforts against money laundering, primarily by the US and major European governments, have not proven very cost effective. For instance, in the US in 1998, only 932 people were convicted of money laundering, yet the cost to the private and public sectors of the anti-money laundering efforts were more than 10 billion dollars, which comes out to more than 10 million dollars per conviction. The distinguished British law professor, Barry Rider, has calculated that "the British state has been able to take out 0.004 per cent of the criminal money that has flowed through London."[6] Money launderers do not have a statistically significant chance of being caught and losing the profits from their misdeeds, and hence the deterrent effect of such laws is negligible.

[6]Barry Rider. "The Crusade Against Money Laundering - Time to Think!" European Journal of Law Review, vol. 1, no.4 (1999), p.515.

Privacy advocates have also documented that the money laundering laws are very arbitrarily enforced in many countries, including the United States. Money laundering is a crime of motive, rather than one of specific activity, hence its enforcement, by the very nature of the crime, is highly subjective. Because of the constant threat of the vagueness of the money laundering laws and regulations, constructive financial innovation has been retarded, particularly in the development of digital monies.

An additional argument is that stealing digital money is a much more complex undertaking than stealing paper currency, and will be beyond the capabilities of most common criminals. If there is no physical money, the incentive for criminals to steal will be greatly reduced. Thus it can be argued that abolishing anti-money laundering laws is likely to speed up the use of digital money, resulting in less total crime, and less wasted money by governments, even though it will make life slightly easier for money launderers.

As noted, public policy makers have primarily focused on the role of central banks, bank regulatory issues, and issues involving criminal use, of the new digital monies and related products. However, another important public policy issue is that of intellectual property protection for the new digital money and financial instruments that are being developed. Proper protection can spur innovation, but either no protection or too extensive protection can be a barrier to innovation. Lawmakers, regulators, and other interested parties are now involved in an intense global debate about how legally to treat development of new international financial instruments. This debate will probably go on for many years, leaving those in the business of developing such financial instruments in a limbo of uncertainty, while they try to navigate through conflicting and ever changing laws in various jurisdictions.

US Patents Related to Digital Money

One of the many consequences of the information age, at least in the United States, is the broadening of the definition of what can be patented. The *Street Bank & Trust Co. v. Signature Financial Group, Inc.* decision of 1998, confirmed that mathematical algorithms and business methods are indeed patentable. Consequently, many of the inventions related to digital money have been patented. Some of the more important ones are summarised below.[7]

[7]For a more detailed introduction to some of these and to other potentially important patents in the field, see "Altered States: Electronic Commerce and Owning the Means of Value Exchange," Robert D. Fram, Margaret Jane Radin, Thomas P. Brown, Stanford Technology Law Review 2 (1999). (http://stlr.stanford.edu/STLR/Articles/99_STLR_2).

David Chaum, the founder of DigiCash[8], has various patents covering "blind" signature systems and the confirmation of digital signatures.[9] Blind signature systems enable an issuer of digital cash to "sign" digital coins (tokens) without being able to trace where they are spent.

Citibank holds a number of patents, some broad in scope, relating to a non-accountable, smart card based electronic money system.[10] Mondex holds patents relating to a non-accountable, stored value card system that permits transfers of cash between cards by means of a hand-held special purpose device.[11] Electronic Payment Services, Inc. holds five patents concerning electronic funds transfer networks, only one of which requires stored value cards.[12]

Of particular relevance to digital gold and other digital commodities is James J. Turk's patent, "Method and system for commodity-based currency for payment of accounts and elimination of payment risk."[13] Turk proposes a system "for permitting gold or other commodities to circulate as currency... The gold is kept in secure storage at a deposit site for the benefit of the users. The payments in gold are effected through a computer system having data storage and transaction processing programs that credit or debit the units of account of gold held for the account of each system user." The Turk system does not depend upon smart cards.

While the enforceability of such patents will remain uncertain until they are tested in the courts, developers and potential licensees of digital cash systems should nevertheless be aware of possible conflicts with the many existing patents in digital payments and electronic commerce.

[8]Although DigiCash, Inc. is no longer in operation, Chaum's blind signature technology is in use in the eCash Technologies system.
[9]For example, U.S. Pat. No. 4,759,063, "Blind Signature Systems," and U.S. Pat. No. 4,759,064, "Blind Unanticipated Signature Systems."
[10]For example, U.S. Pat. No. 5,453,601 and U.S. Pat. No. 5,455,407, both entitled, "Electronic-Monetary System."
[11]U.S. Pat. No. 5,440,634 and U.S. Pat. No. 5,623,547, both entitled "Value Transfer System."
[12]For example, U.S. Pat. No. 5,577,121,"Transaction System for Integrated Circuit Cards."
[13]U.S. Pat. No. 5,671,364.

CHAPTER 3: THE MONETARY POTENTIAL OF GOLD IN THE AGE OF DIGITAL MONEY

The argument as to what the appropriate monetary role for gold is might actually be settled in the digital age. Experiments in creating digital gold systems have already begun. Will people find digital gold superior to government-issued currencies or to other forms of private currency? And if yes, what type of digital gold? Initially a gold standard required that the issuer have 100% gold reserves. A gold exchange standard allowed countries to economise on gold by allowing central banks to hold some of their reserves in the currency of countries tied more closely to gold, while the fractional reserve system required only a portion of the reserves to be held in gold. The open question is which variant of private digital gold systems will prove to be most successful. The answer to this question depends partly on the ability of the gold and financial industries to develop sufficient markets for gold-backed financial products that can be used by issuers of gold-backed currencies and other financial instruments to offset or hedge their gold liabilities.

An impediment to developing privately-issued, gold-backed digital money is the way that some countries choose to tax commodity transactions. It will be difficult to have a pure test because the US and some other governments currently apply capital gains taxes to changes in commodity prices. Thus for US citizens there will be the complication of calculating capital gains and losses via the US dollar when moving back and forth between the gold system and the dollar system.

The potential demand for digital gold products

Gold is only one of many forms that digital money may assume. Whether gold achieves wide circulation as a digital money or holds only a small, exotic niche in the market for currencies depends upon a number of factors. Some of these factors are almost entirely within the control of promoters of gold money systems, while others are almost entirely outside their control.

Gold has two key advantages. First many people instinctively trust it. It is tangible, free of government control and the idea that gold is intrinsically valuable is ingrained in folk history, in literature and common sayings throughout the world. Thus a digital currency perceived to be adequately backed by gold would have an automatic advantage in competing for people's trust over many other currencies.

The second important advantage of gold as a digital currency is the substantial demand that already exists for holding gold assets for purposes other than as a medium of exchange. The reasons for this have been thoroughly discussed and debated for many years. For present purposes, it is the fact that gold assets are commonly held for non-monetary purposes, not the motivation of such holdings, that is of interest. Individual holders of gold assets constitute a substantial and obvious target market that must be given priority in any effort to market a digital gold currency, or other digital gold financial products.

Similarly, some banks and other major custodians serving this market would increase the appeal of their services if the balances held in their gold custody accounts were made liquid. This pre-existing demand for gold assets gives gold an important head start over all competitors, except of course major national currencies. Through a custodial arrangement with an issuer of gold currency, a bank could, upon instruction of its client, transfer gold from the client's account to that of the digital money supplier.

Gold held for private investment purposes is clearly a significant but also uncertain quantity. In addition, there are 33,000 tonnes of gold held in official reserves.[14] While institutional demand for gold in developed countries is currently limited other investment demand for gold has been running at about 400 tonnes per year.[15] Certainly, a significant amount of gold is held by people who have no access to the internet and who cannot be expected to convert their gold holdings to electronic form in the foreseeable future. Nevertheless, certain current private gold investment holdings represent a natural base for any digital gold currency system.

At least as important, gold investment will become far more attractive as gold is more readily and conveniently spendable in electronic form. As a digital gold currency attracts new users, the demand for gold will increase because the currency (at least initially) should be 100% backed by physical gold or by gold-determined financial instruments if it is to achieve and maintain credibility.

[14]International Monetary Fund; International Financial Statistics.
[15]World Gold Council; Gold Demand Trends database. The WGC is aware of purchases by US institutional investors of around 50 to 55 tonnes per year.

While gold enters the digital currency competition with two important strengths, it must surmount some important barriers before achieving broad acceptability.

Very few e-commerce or physical world businesses accept gold in exchange for goods and services. While gold investors are a pre-existing base of digital gold account holders, they will have little incentive to participate in a digital system that offers few opportunities to spend. Marketing to e-commerce merchants must therefore be a top priority for any promoter of a digital gold currency seeking to achieve critical mass.

Widespread confidence in the financial integrity of a gold currency system must be established. Promoters without well-known and respected brand names will have to invest in advertising and promotional activities to establish their names. More fundamentally, any successful gold currency system is likely, at least initially, to be 100% backed by gold assets of undoubted quality, with frequent audits to ensure that gold liabilities (currency) are not over issued with respect to the amount of reserve-quality assets. A gold currency that is not fully gold-backed is unlikely to attract and retain the confidence of users, except in the special case that it is underwritten by an established financial institution of unquestioned strength and with gold liabilities that are a small part of its total balance sheet. In all other cases, a digital gold "central bank" should match its liabilities, consisting of gold currency issued, with gold assets. To the extent that the issuing "bank" runs a mismatch between the denominations of its assets and liabilities, or to the extent that it invests in less than reserve-quality gold assets, the integrity of the system will be at risk. For example, if a gold currency is 50% backed by gold and 50% by US dollars, a sharp rise in the price of gold in dollar terms renders the system insolvent — assets in gold terms are less than liabilities.

A digital gold currency that is not fully gold-backed would be prone to a "run on the currency" and therefore subject to failure. In a sharply rising gold market, gold currency holders would note that they hold a gold asset that is worth substantially more than the assets that back it. They would have a strong incentive to claim their gold for full value ahead of other gold currency holders. As in a bank run, the last in line would find themselves empty-handed.[16]

[16]Mutual funds are also immune to runs because they do not undertake to redeem liabilities at par. Conceivably a mutual fund investing in any portfolio of assets could choose to "denominate" its share prices in gold, but of course the price of its shares would not be "determined" by gold except to the extent the portfolio consisted of gold assets. Throughout this paper gold assets are considered to be gold-determined.

Transaction costs must be competitive by comparison with competing payment methods (e.g. credit cards and bank transfers) and competing digital currencies. A gold currency faces a disadvantage in that physical gold holdings can yield a negative return in gold terms — they do not earn interest (even if invested in the gold leasing market returns are currently small), yet incur storage costs. Transaction fees must be charged to finance the operation of the gold currency system, whether in the form of "exchange commissions" on the purchase or sale of gold, time-based fees on balances maintained, or fees on payments.

Note that non-accountable *digital cash,* which would circulate from user to user much as banknotes denominated in a national currency, faces a more formidable problem than an accountable digital gold payments system: a circulating digital cash system has no means of charging transaction fees. It must rely entirely on returns on its reserves. Similarly, it has no means of identifying and paying interest to holders of digital cash. To cover its costs, a non-accountable digital gold system must either invest in sufficiently remunerative gold assets, rely upon high fees on the issuance and redemption of digital gold cash, or debase its currency by holding gold assets significantly less than its gold liabilities.

There are today virtually no liquid gold debt instruments in which to invest. (France issued a gold-linked bond in the 1970s, but such examples are rare.) Because of the dual requirements to ensure the integrity of the system with gold-denominated reserves and to minimise transaction costs, *a substantial part of reserves would ideally be invested in interest-bearing, gold-denominated financial instruments of undoubted quality and marketability*. This would ensure that the reserves would earn a positive return (in gold terms, of course) and reduce the need for transaction fees.

It is probably no exaggeration to say that the rarity of top quality, interest-bearing gold-denominated financial instruments is the single most important impediment to the development of a competitive gold currency. Short-term leases of gold to gold-lending banks, typically under 2% per year, offer a partial solution, but this market is already well-served by central bank leasing programs. A wider range of gold financial instruments, such as notes and bonds traded in liquid markets, is needed. Significantly, the advent of digital gold currencies represents a major step toward the solution to this problem. Markets evolve, with sellers encouraged by the growing presence of buyers and *vice versa.* Digital gold currencies represent a new, potentially significant, demand for gold-denominated assets, and that demand should itself encourage potential borrowers to consider issuing gold financial instruments.

Potential gold borrowers include gold mining companies, central banks (eg of gold-producing emerging market countries) and commercial banks active in gold lending. Some of these borrowers, do not represent the sort of undoubted credit quality that a digital gold "central bank" would require for its reserves. By contrast, financial instruments issued by strong commercial banks (to fund their gold loans to less creditworth borrowers) will often be of sufficient quality to serve as backing for a gold currency.

If gold instruments become more widespread, financial institutions may develop a market for securitised packages of formerly illiquid gold loans. Securitisation would free the balance sheets of institutional lenders to extend more gold loans, and some higher quality packages of securitised gold assets may prove suitable to be included among the reserves backing a gold currency.

A digital gold currency must be technically secure, and users must be convinced that their digital gold holdings are not at risk because of flaws in system design. This is not an impediment peculiar to digital gold systems, so there is no need to dwell on the subject here. Suffice it to say that the technical problems are surmountable with existing technologies and that the challenge lies in convincing the public of the technical integrity of the system.

Well-known and respected brand names fulfil an important economic function in minimising the burden of information costs imposed on potential users seeking to assess the technical strength of a system. Therefore, established financial corporations have a distinct, although not necessarily unassailable, advantage in achieving the establishment of a major, widely recognised digital gold currency. Smaller players will have to rely heavily upon associations with respected, well-known names for their technical and financial audits; they will also have to invest in advertising these associations and the technical strengths of their systems.

A digital gold currency must be easily explained and used. The same can be said of any digital currency system, but a digital gold system faces the same tasks to a different degree. First, most on-line transactions are denominated in national currencies, particularly US dollars, and will continue to be for the foreseeable future. A digital gold system must offer real time conversion rates in order to ascertain the amount of gold to be paid in settlement at the time of the transaction. It is quite conceivable that digital gold could achieve prominence as a medium of exchange without achieving significant use as a unit of account.

Second, a digital gold system faces far more "foreign exchange" transactions than a digital US dollar system in relation to its volume of transactions in gold. That is, digital gold will normally be purchased and redeemed, at least initially, against national currencies. In this respect, gold is still an "exotic" currency — those holding their balances in other currencies will tend to buy or sell the exotic currency to reflect immediate transaction needs. As a digital gold currency matures, the ratio of exchange transactions to purely gold transactions can be expected to decline. In the meantime, it is important for a digital gold system to offer a fast and inexpensive exchange service, particularly the facility for online exchanges.

Ideally, a digital gold currency would be usable in the physical world as well as in cyberspace. Again, the same can be said for digital national currencies, but digital gold faces a more imposing task in establishing its acceptability in the physical world. In particular, the problems of conversion rates and exchange rates must be addressed. While some merchants may accept digital gold in payment, they will be rare in the early stages of development of a digital gold currency. Therefore, a digital gold user should have the capacity to exchange gold for national currency in real time so as to be able to render, say, US dollars at the physical point of sale in exchange for a basket of groceries. This barrier is not as daunting as it may first appear — technology is rapidly supplying a solution in the form of internet-enabled mobile telephones. Such phones are now common in Finland and Japan and are growing in importance elsewhere. In Finland, mobile phones are now used to "beam" payments for groceries or other items at the point of sale. If a real time currency exchange system is incorporated into an electronic gold system, the merchant desiring to receive Finnish marks need not know whether the payer's balances were held in gold, US dollars, or another currency.

Ideally, a digital gold currency could be purchased at physical points of sale, as well as online. Physical distribution of digital gold permits participation in the system of those without credit or bank accounts. For example, in Peru a high percentage of internet use takes place in publicly accessible internet kiosks or cafés. Users of these systems can purchase, in exchange for national currency, prepaid cards (comparable to prepaid telephone cards now widely available around the world) that can be used to make payments online. The availability of a digital gold system to users without access to credit or bank accounts will help a digital gold currency to reach critical mass in terms of transaction volumes and — given the potential of prepaid versions in even poor countries — geographic breadth.

High transaction fees currently make uneconomic the online purchase of digital gold by credit card. However, the growing importance of internet banking will make increasingly common the purchase of digital gold through efficient online transfer instructions.

Digital gold in the settlement of international payments

Digital currencies will realize their greatest potential when they are used routinely to settle cross-border transactions including those of the smallest amount. Very low transaction costs and immediate settlement give digital currencies a solid advantage over the alternatives. Credit cards entail high transaction costs, barriers to cross-border usage, and the risk of charge backs to merchants; neither can they be used to settle transactions by individuals. Inter-bank transfers are prohibitively expensive for small transactions and entail time delays of up to two weeks before a beneficiary receives payment.[17]

Like the US dollar, gold is recognised worldwide as a store of value, however mixed the reputations of each may be. This certainly makes gold a candidate as an international digital medium of exchange, particularly for relatively small, online transactions. Conversely, with one significant exception, there appears to be no reason for digital gold to make significant inroads into the current dominance of digital dollars in large international settlements. The exception lies in the prospect that more large, marketable debt obligations will be denominated or determined in gold. Digital gold "central banks" in particular can be expected to prefer to pay or receive gold in settlement.

The more internationally widespread the use of digital gold, the more likely will there be competing issuers. Of course it is also quite likely, particularly in large countries like the US, that issuers will compete in domestic markets as well. In any case, multiple issuers suggest the need for a clearinghouse for payments among the various digital gold "central banks."

[17]The time delays are within the control of banks, and the presence of excessive delays in some jurisdictions generally indicates collusion among local banks seeking to maximise the float from delayed payments. Competition from non-bank international settlement alternatives would do wonders for the "efficiency" of bank payment processing in these places.

The settlement function could in principle be fulfilled through reciprocal account relationships covering all of the possible two-way combinations of issuers. If the number of issuers is small, this is likely to be how settlement between issuers will be conducted. But as the number of digital gold issuers grows larger, it becomes more practical for each issuer to maintain an account at one entity (which might be one of the issuers rather than an independent entity) for settlement purposes. In any case, settlements between issuers should be real time, as for all digital gold payments, so as to eliminate systemic risk.

A number of desirable characteristics of digital monies, as well as some peculiar challenges faced by promoters of digital gold, have been identified above. The following key attributes of a successful digital gold currency derive from these characteristics and challenges:

Recommended attributes of a successful digital gold currency

1. The currency should be 100% backed by gold-denominated and gold-determined assets of undoubted quality.

2. Reserves should be frequently audited by a firm of top international reputation.

3. The system should be designed for ease of use on the internet and for account accessibility by internet-equipped mobile phones.

4. The system should be accountable so that transaction fees can be charged. A non-accountable, circulating cash system must wait until marketable, interest bearing, gold-denominated financial instruments of undoubted creditworthiness are more commonly available.

5. The system must be fully secure and subjected to an operational audit by an information systems and internet security firm of undoubted reputation.

6. Marketing should initially be targeted to those who already maintain investments in gold. Financial institutions that serve as gold custodians should also be given priority in marketing.

7. Marketing should then focus on inducing major online merchants and service providers to accept digital gold. Internet service providers should be prime targets.

8. Next, marketing should focus on international users seeking an inexpensive and reliable means of settling online cross-border transactions. Finally, marketing should be extended to the physical world — point-of-sale distribution of digital gold and recruitment of merchants.

9. For settlement purposes, reciprocal accounts should be established with other digital gold providers. Isolation only increases the likelihood that no system will achieve critical mass. A clearinghouse may eventually evolve as the number of issuers grows.

SUMMARY AND CONCLUSIONS

The question is no longer whether we will have digital money, but how soon it will be before most paper currency and coin is eliminated, what portion of digital money will be issued by private institutions, and how much of that will be gold. Digital money can either be privately- or government-issued money whose value is stored in electronic form in such devices as "smart cards," computer disks, and personal digital assistants, including some types of cell phones. Digital money should eventually become the dominant form of money because it is less costly to handle than cash, cheques, or credit cards, and is more secure and efficient.

Digital money does require specialised, but inexpensive, hardware to make transactions using the money on computer chips. It can be securely transferred over the internet, or by infrared beams at almost zero cost. Digital money can be in the form of digital coins or "tokens," or merely reside in accounts. Very secure system designs and high levels of cryptography are required to make sure that digital money is not subject to theft or counterfeiting. Digital money systems may be "online," requiring an independent confirmation of every transaction, or offline, in which the money is passed from device to device. The systems can either be designed to be fully accountable or completely anonymous.

As digital money becomes more and more important and the use of traditional government monies declines, central banks will become less important, and their ability to influence national economies by traditional routes may decline. New rules and legal procedures will need to be developed for the world of digital money, and technologically obsolete regulations, like many of those designed to control money laundering, will need to be eliminated.

Developers of new digital money systems will need to be aware of the many patents which now exist. The digital world will allow the development of bearer financial instruments, including money, bonds, stock, and financial derivatives. Institutions that currently own or produce gold are logical developers and marketers of digital gold products. There are no longer technological reasons why private companies cannot create international gold-backed monies to compete with government monies.

The first company offering digital gold (e-gold) is now in existence. Others are planning to enter the market, notably GoldMoney. Success will depend on the ability to design and market digital gold products that meet the needs of consumers, businesses, and investors better than the existing methods of holding gold, such as coins, bullion, and gold futures contracts, or have advantages over existing non-gold-backed financial instruments, including government-issued money. Issuers of digital gold money need the development of many liquid gold debt instruments in which to invest, in order to offset the liability of the digital gold money they have issued.

The gold industry is now faced with an historic opportunity, as well as a danger, as a result of the new digital technologies. The debate as to whether gold will have any future monetary role, or be relegated to becoming just another commodity, is more likely to be settled by financial innovators than the world's politicians. If financial innovators, including members of the gold mining and processing industry, successfully develop and market digital gold products, gold's continued monetary role will be assured. In addition to developing a digital gold currency product, the industry should actively seek to get one or more governments to recognize it as a legal parallel currency. However, if such innovation in digital gold does not take place, while other digital money and financial instruments are developed, the pressures to remove gold from any remaining monetary role could increase.

APPENDIX: SELECTED DIGITAL MONEY SYSTEMS

Non-gold-based systems

PayPal

PayPal[18] payments system operated by X.com. PayPal allows a person to send money to anyone else with an e-mail address. PayPal can be used through e-mail, or an internet-enabled mobile telephone. Money can be put into the PayPal system by credit card, bank account debit, or by sending a cheque to PayPal. A person may also fund a PayPal account by receiving funds from another PayPal user.

To open an account, a user must submit his name, address, telephone number and e-mail address. A credit card number or bank account information may be required in order to access such features as funding an account or receiving payment for a withdrawal of money from the PayPal system.

To withdraw money from a PayPal account, a user may request a direct deposit into a bank account (which credits within three to five business days), or may request a personal check from PayPal (which may take one to two weeks for delivery).

There are no fees involved in using a personal PayPal account. For a business PayPal account, a small transaction fee of 1.9% per transaction is charged for receiving money.

The PayPal system is currently available for US residents only. The company expects to expand access to international users in the near future. As of October 2000, PayPal had over 4 million users and was processing over $2 billion per year.

[18]More information about PayPal can be found at its website (http://www.PayPal.com).

MilliCent

MilliCent[19] provides a means of making micropayments (from one-tenth of a cent to ten dollars) to pay for online content. The MilliCent system envisions three sets of entities involved in the total transaction process: users, brokers, and vendors. Users are those who wish to purchase online content. Vendors are the operators of websites that deliver content for a small fee, on a "pay-per-click" basis. Brokers buy and sell vendor scrip. This scrip is what is used to pay for a certain amount of online content. A user has a relationship with one broker, and is able to receive vendor-specific scrip from the broker, who will have (or have access to) a variety of different vendors' scrip. A vendor has a relationship with at least one broker, who purchases bulk amounts of the vendor's scrip, or perhaps purchases a license to generate certain amounts of vendor scrip. In this way, a cost saving from the bulk purchase of scrip is allowed, while giving users access to very small amounts of any individual vendor's scrip. A user may return an unused portion of a vendor's scrip for his broker's scrip, and then may purchase another vendor's scrip when he needs it.

A user who wishes to access a pay-per-click page of a website that uses MilliCent's system must open a MilliCent account, then fund the account either through an online credit or debit transaction, or by selecting direct billing through his internet service provider or on his telephone bill. Prepaid cards are also available for purchase anonymously at convenience stores.

A vendor that would like to make use of the MilliCent system also opens a MilliCent account, then either can integrate the MilliCent software directly with his website, or may leave the details to MilliCent and simply assign prices for the pages that the vendor wishes to charge users to access.

MilliCent takes care of receiving payments from users, making payments to vendors, and currency conversion, if necessary. MilliCent operates in Japan, and expects to be available in North America and Europe in the near future.

[19] Additional information about MilliCent can be found at its website (http://www.MilliCent.com).

Mondex

Mondex[20] is a smart-card based electronic cash system. The microchip on the smart card contains a "purse" which contains value electronically. The Mondex card can carry up to five currencies - sterling, euro, dollar and yen are among those supported. As value is held directly on the card, transactions can take place offline and from card to card. Value is transferred immediately. The Mondex card stores information on recent transactions, in addition to the value information.

Mondex offers several devices for use with the card, such as card-enabled telephones, wallets, balance readers, and point-of-sale (POS) devices. Card-enabled telephones and PCs allow users to transfer money to others with a Mondex card and card-enabled telephone/PC, or to transfer money to or from a bank. Mondex wallets can be used to transfer money from one card to another, or to check card balances, transaction history, etc. Point-of-sale devices are used by merchant sites. The Mondex card goes into the POS terminal, and the amount of a purchase is transferred from the card to the merchant's card residing in the terminal.

Security for the Mondex system is managed both in hardware design and by the software operating on the card. The microchip is designed to resist tampering, to protect data from unauthorised modification or from disclosure. There are also security measures resident on the microchip, which check for unusual activity and can close down the card if necessary. Further, cards that have been reported stolen, or are being used in a fraudulent manner, can be shut out of the system.

Mondex cards are also protected by the ability to switch between two separate and complete security protocols. As stated on its website, "when cards are issued, each contains two different and separate security schemes, A and B — each comprising one or more 'keys' or more cryptographic algorithms — or other security features. Initially the cards will be set to operate on scheme A but will have the potential to switch over to scheme B when instructed." This protection should ensure that security can continually be changed and upgraded as necessary.

[20]Additional information about the Mondex system can be found on its website (http://www.mondex.com).

Digital gold systems

e-gold

e-gold[21] is a product of e-gold Ltd, a Nevis Corporation. e-gold Ltd is a family of electronic currencies 100 percent backed by gold, silver, platinum and palladium. As such, a quantity of e-gold constitutes title to a precise weight of precious metal. e-gold provides an online system for customers to spend fractional amounts of metal to settle accounts with other customers in the system (a payment can be made for as little as 0.000010 troy oz, with precision in accounting to 0.000001 troy oz). The e-gold system is a fully accountable, online system based upon users holding accounts, with payments taking place by means of instructions to transfer amounts of metal from one account to another. (Users' accounts are held in the metal of their choice.)

Gold & Silver Reserve (G&SR), the Delaware company (with headquarters in Florida) that originally developed and administered the e-gold system, serves as primary distributor. G&SR makes an exchange market enabling customers to obtain e-gold with USD, CAD, DEM, JPY, GBP, F Franc, S Franc, and AUD and other currencies. G&SR accepts national currencies only by wire transfer and imposes a minimum transaction size for exchanges. There are a number of third parties that provide additional means of funding accounts. These are businesses that are unrelated to e-gold and its management, which are offering to exchange government currency for e-gold. These businesses accept cheques, money orders, PayPal payments, and credit card payments, even for small amounts of currency for exchange to e-gold.

At present,G&SR updates their bid and ask rates for the various e-metals every couple of hours throughout the business day in North America, and 2-3 times during the night.

To use the e-gold system, a user must go to the e-gold website and open an account. Using the Account Creation Form page, the user must supply the information necessary to open the account, which includes an account name, a user name, a point of contact, and a passphrase. An account number is assigned and appears on the screen within a few minutes, along with instructions about how to use the account.

[21]Additional information about e-gold can be found at its website (http://www.e-gold.com).

To fund an account, the user may wire funds to the G&SR/OmniPay bank account, or use a third party service to fund an account by credit card, PayPal, or cheque. Depending upon the method of account funding, it may take one to seven days (plus mailing delay) for the e-gold to be credited to the account.

After an account has been funded, a user may begin to make payments to other e-gold account holders. These payments are made by: a) going to the e-gold website and clicking on the "spend" icon; b) the e-gold Shopping Cart Interface, an automated interface designed for integration into merchant websites; or c)web-enabled mobile phone[22]. Both browser-based interfaces take the user to a secure page with the e-metal payment order form. For User-to-User spending, the user fills in the recipient's account number, the amount of the transaction, denominated in USD, CAD, DEM, JPY, GBP, F Franc, S Franc, AUD, ounces of metal (gold, silver, platinum, or palladium), or grams of metal. These fields are already filled in with Shopping Cart implementations. The user then authenticates the payment order by entering his account number, and his passphrase, and clicks the "Preview" button to submit the page. The user will then see a preview of the order, with the account name and number of the recipient, and the amount of the transaction, in both the chosen denomination and in ounces and grams of metal. The preview also indicates the conversion factors applicable to the transaction, including the current gold exchange rate, the currency ratio, and the number of grams to the troy ounce of metal. If the information is correct, the user clicks the "Confirm" button and the transaction is complete. The sender will receive a confirmation, and a payment reference number.

All transactions are recorded and can be viewed by clicking on the Account History icon. This history page displays the dates of transactions, batch numbers (the payment reference number), a description of the transaction, the metal used, the exchange rate at the time of the transaction, and the credit or debit in troy ounces. This information is updated immediately after a transaction is confirmed.

G&SR and multiple independent companies also provide exchange from e-gold to national currencies on a competitive base. G&SR's OmniPay facility (http://www.omnipay.net) enables users to use their e-gold to order and fund payments in national currency (cheque or wire) to third parties, such as to pay mortgage, credit card or utility bills. Omnipay affords a user experience similar to an online chequing account but is actually inline exchange functioning as a hybrid payment system.

[22]See mobile e-gold.com

e-gold is not electronic cash, per se, as it is not a bearer instrument. e-gold's payments system is essentially an accounts-based transactions clearing mechanism, in which title to physical gold is transferred from account to account.

There is a minimal transaction fee for payments within the e-gold system. If the payment is $50.00 (USD-equiv.) or less, the transaction fee is 1%, deducted in e-metal from the recipient. For payments over $50.00, a flat $0.50 (worth of e-gold) is charged. A 1% per annum storage fee is also assessed in monthly installments based on the average daily account balance over the preceding month.

DigiGold[23]

DigiGold Ltd. issues gold denominated digital cash designed to serve as a financial currency. DigiGold requires a software "wallet", a client program that performs crytographic functions including secure and authenticated communication with the settlement server. DigiGold supports User-to-User payments, either directly or in bearer form but does not offer automated interfaces for retail payments. The intended applications for DigiGold are: a) reserve asset and medium of settlement for financial institutions, and b) medium of payment/settlement for securities trading on the Systemics Market Server, a specialised market that enables immediate (digital bearer) settlement.

Currently, DigiGold can be obtained by: a) exchanging e-gold for DigiGold; or b) exchanging other instruments that trade on the Systemics Market Server. Exchanges can be made through OmniPay, and cost a flat 0.1 grams of gold per transaction, no matter how much gold is exchanged. Unlike e-gold, DigiGold is a fiduciary instrument, ie not 100% backed with gold. Rather, it is 25-40% backed with e-gold, and 60-75% backed with gold-denominated securities. There are no storage fees and no transaction fees.

DigiGold grams of gold are payable to bearer gram for gram in e-gold, on demand. E-metal reserve accounts held to back DigiGold are open to public inspection.

DigiGold currently works only with the Java-based WebFunds wallet. The WebFunds wallet software runs on the user's computer. The user's account information is stored on the user's computer. The digital information that entitles the user to a specified amount of e-gold held by DigiGold is contained in a "contract." These contracts are held in the user's account on the user's computer. The user can make and receive payments with other persons who have a WebFunds

[23]Additional information about DigiGold can be found on its website, (http://www.digigold.net).

wallet. Payments can be made as direct payments, or as bearer payments. Direct payments can be made if the name or the hash of the account of the recipient is known. Direct payments are deposited directly into the recipient's account. Bearer payments are sent to the recipient, who then deposits the payment in his wallet. DigiGold transactions can be entirely anonymous.

GoldMoney[24]

GoldMoney is an e-commerce payment system, being developed by James Turk and colleagues. The developers claim it will enable buyers and sellers of goods and services to transact and make nearly instantaneous payments in weights of gold. GoldMoney will allow payments in weights of gold called GoldGrams. Each GoldGram will be further divisible into thousandths of a gram.

As stated on its website, the proposed GoldMoney system emphasizes three advantages: peace of mind (due to the elimination of payment risk, state-of-the-art hardware and software, and high strength encryption), ease of payments (processed in real time, 24 hour access and availability of funds, and global access), and control of costs (low transaction fees, and payments made immediately, eliminating "float" and time needed to clear payments).

GoldMoney expects to have transaction fees of less than one US dollar per transaction.

The development company for GoldMoney, G.M. Network Ltd, is located in the Isle of Man, British Isles. The operating company is expected to be a subsidiary of G.M. Network Ltd; the country in which the subsidiary will be established has not yet been announced. The GoldMoney system is backed by several patents. The company expects the system to be in operation in December 2000, with further enhancements becoming available in 2001.

[24]More information about GoldMoney is available on its website, (http://www.goldmoney.com).

Authors

Richard W. Rahn is Chairman of Novecon Financial, Ltd, and is a Senior Fellow at the Discovery Institute, and an Adjunct Scholar with the Cato Institute. He was the former VP and Chief Economist of the US Chamber of Commerce, and has served as an economic advisor to senior government officials in the US and other countries. Dr. Rahn is a frequent commentator on economic issues in the news media and has testified before the US Congress on tax and economic policy issues more than seventy-five times. He has written hundreds of articles on economic issues for newspapers, magazines, and professional journals. He holds a Ph.D. from Columbia University and is the author of *The End of Money and the Struggle for Financial Privacy*.

Bruce R. MacQueen is President of Novecon Financial, Ltd, and has nearly 25 years of experience in international banking and corporate finance. He was the Managing Director of the French and Belgian subsidiaries of Manufacturers Hanover Trust, earlier serving as its Chief Representative in Australia and chief marketing officer in Korea. In the 1990s, his activities covered a broad range of international financial advisory assignments, including mergers and acquisitions, project finance, insurance and banking, valuation and privatisation, economic policy, and new digital forms of money and settlement. He is fluent in French and has a knowledge of Russian and Spanish. His undergraduate degree is from Washington and Lee University and his MBA is from Duke University.

Margaret L. Rogers is Vice President of Novecon Financial, Ltd. She has managed a number of projects for Novecon Financial, including a successful multimillion-dollar venture capital acquisition project for Sterling Semiconductor. Ms. Rogers has also researched and edited numerous articles that have appeared in leading newspapers and magazines, authored reports, and edited a book on digital money and financial privacy. Ms. Rogers received her B.A and B.S. from The Evergreen State College, specialising in mathematics.

WGC CENTRE FOR PUBLIC POLICY STUDIES

No. 1 *Derivative Markets and the Demand for Gold* by Terence F Martell and Adam F Gehr, Jr, April 1993

No. 2 *The Changing Monetary Role of Gold* by Robert Pringle, June 1993

No. 3 *Utilizing Gold Backed Monetary and Financial Instruments to Assist Economic Reform in the Former Soviet Union* by Richard W Rahn, July 1993

No. 4 *The Changing Relationship Between Gold and the Money Supply* by Michael D Bordo and Anna J Schwartz, January 1994

No. 5 *The Gold Borrowing Market - A Decade of Growth* by Ian Cox, March 1994

No. 6 *Advantages of Liberalizing a Nation's Gold Market* by Professor Jeffrey A Frankel, May 1994

No.7 *The Liberalization of Turkey's Gold Market*by Professor Ozer Ertuna, June 1994

No. 8 *Prospects for the International Monetary System* by Robert Mundell, October 1994

No. 9 *The Management of Reserve Assets* Selected papers given at two conferences,1993

No. 10 *Central Banking in the 1990s - Asset Management and the Role of Gold*Selected papers given at a conference on November 1994

No. 11 *Gold As a Commitment Mechanism: Past, Present and Future*by Michael D Bordo, January 1996

No. 12 *Globalisation and Risk Management* Selected papers from the Fourth City of London Central Banking Conference, November 1995

No. 13. *Trends in Reserve Asset Management*by Diederik Goedhuys and Robert Pringle, September 1996

No. 14. *The Gold Borrowing Market: Recent Developments* by Ian Cox, November 1996.

No. 15 *Central Banking and The World's Financial System,* Collected papers from the Fifth City of London Central Banking Conference, November 1996

No. 16 *Capital Adequacy Rules for Commodities and Gold: New Market Constraint?*by Helen B. Junz and Terrence F Martell, September 1997

No. 17 *An Overview of Regulatory Barriers to The World Gold Trade* by Graham Bannock, Alan Doran and David Turnbull, November 1997

No. 18 *Utilisation of Borrowed Gold by the Mining Industry; Development and Future Prospects,* by Ian Cox and Ian Emsley, May 1998

No. 19 *Trends in Gold Banking* by Alan Doran, June 1998

No. 20 *The IMF and Gold* by Dick Ware, July 1998

No. 21 *The Swiss National Bank and Proposed Gold Sales,* October 1998

No. 22 *Gold As A Store of Value* by Stephen Harmston, November 1998

No. 23 *Central Bank Gold Reserves: An historical perspective since 1845* by Timothy S Green, November 1999

No. 24 *Digital Money & Its Impact on Gold: Technical, Legal and Economic Issues* by Richard W Rahn, Bruce R MacQueen, Margaret L Rogers

Switzerland's Gold, April 1999

A Glittering Future? Gold mining's importance to sub-Saharan Africa and Heavily Indebted Poor Countries, June 1999

Proceedings of the Paris Conference "Gold and the International Monetary System in a New Era", May 2000

20 Questions About Switzerland's Gold, June 2000

Gold Derivatives: The Market View by Jessica Cross, September 2000

Available from Centre for Public Policy Studies, World Gold Council, 45 Pall Mall, London SW1Y 5JG, UK. Tel + 44.(0)20.7930.5171, Fax + 44.(0)20.7839.6561. E-mail: cpps@wgclon.gold.org Website: www.gold.org

World Gold Council Offices

Headquarters: UK

45 Pall Mall
London SW1Y 5JG, UK
Tel. +44.(0)20.7930.5171
Fax.+44.(0)20.7839.6561

Website:
www.gold.org

Americas/Europe
Regional Office & USA

444 Madison Avenue
New York, NY 10022
Tel. +1 212.317.3800
Fax. +1 212.688.0410

Brazil

Avenida Paulista 1499
Conj. 706
01311-928 Sao Paulo
Tel. +55.11.285.5628
Fax. +55.11.285.0108

Mexico

Consejo Mundial del Oro
Av. Reforma No. 382,
Despacho 701,Col. Juarez
Delagacion Cuauhtemoc
06500 Mexico D.F.
Tel/Fax +52.5.514.5757/2172

East Asia
Regional Office & Singapore

6 Battery Road No. 24-02A
Singapore 049909
Tel. +65.227.2802
Fax. +65.227.2798

China (Beijing Office)

Room 1706, Scitech Tower
22 Jian Guo Men Wai Da Jie
Beijing 100 004
Tel. +861.0.6515.8811
Fax. +861.0.6522.7587

China (Hong Kong)

13th Floor, Printing House
6 Duddell Street, Central
Hong Kong
Tel. +852.2521.0241
Fax. +852.2810.6038

China (Shanghai Office)

Room 203B, Central Place
No. 16 He Nan Road (S)
Shanghai, PRC 200 002
Tel. +86.21.6355.10078/9
Fax. +86.21.6355.1011

Indonesia

Tamara Center Level 6, No 602
Jl. Jenderal Sudirman Kav 24
Jakarta 12920
Tel. +62.21.520.3693/94/95
Fax. +62.21.520.3699

Malaysia

Menara Dion No. 12-05
27 Jalan Sultan Ismail
50250 Kuala Lumpur
Tel. +60.3.381.2881
Fax. +60.3.381.2880

Thailand

14th Floor, Thaniya Plaza,
52 Silom Road, Bangrak
Bangkok 10500
Tel. +662.231.2486/7
Fax. +662.231.2489

Taiwan

Room 808,
205 Tun Hwa N. Road, Taipei
Tel. +886.2251.47.400
Fax +886.2251.47.466

Vietnam

No 6 Phung Khac Khoan St,
Room G7
District 1, Ho Chi Minh City
Tel. + 848 8256 653/654
Fax + 848 8221 314

Japan/Korea
Regional Office & Japan

Shin Aoyama Building / W21F,
1-1-1 Minami-Aoyama
Minato-ku, Tokyo 107 0062
Tel. +81.3.3402.4811
Fax. +81.3.3403.2477

South Korea

19th Floor, Young Poong Bldg.
33, Seorin-dong, Jongro-ku
Seoul 110 752
Tel. +82.2.399.5377
Fax. +82.2.399.5372

Middle East
Regional Office & UAE

Dubai World Trade Centre
P.O. Box 9209 – Level 28
Dubai, UAE
Tel. +971.4.3314.500
Fax. +971.4.3315.514
gold@wgcdubai.org.ae

Turkey

Mim Kemal Öke Caddesi
Dost Apt. 8/4
Nisantasi, 80200 Istanbul
Tel. +90.212.225.1960/22
Fax.+90.212.225.1913

India
Regional Office & Mumbai

101, Maker Chamber VI
10th fl., 220 Nariman Point
Mumbai 400 021
Tel. +91.22.230.1323
Fax. +91.22.230.1324

India (Chennai Office)

B-2 Alexander Square
34/35 Sardar Patel Road
Guindy
Chennai 600 032
Tel. +91.44.230.0083/0084
Fax. +91.44.230.0086

India (New Delhi Office)

47, Basant Lok
Vasant Vihar
New Delhi 110 057
Tel. +91.11.614.9394/95
Fax. +91.11.614.8281

India (Calcutta Office)

World Trade Center Calcutta
Somnath Building, 4th Floor
8/1A, Sir William Jones Sarani
Calcutta 700 016
Tel. +91.33.249.4318
Fax. +91.33.292.793