Curbing economic crime with RFID enabled currency

Lorne D. Booker* and Nick Bontis

DeGroote School of Business,
McMaster University,
Hamilton, Ontario L8S 4M4, Canada
E-mail: bookerld@mcmaster.ca
E-mail: nbontis@mcmaster.ca
*Corresponding author

Abstract: Information and Communication Technologies (ICTs) enable us to conduct business efficiently and effectively on a global scale. At the same time ICTs provide criminals with new capabilities with which to circumvent law enforcement efforts. Consequently, law enforcement agencies need new tools and new capabilities. RFID enabled money (r-money) is one such tool. R-money would make money visible to information systems. In this paper the potential benefits of r-money are presented and some of the societal, technical and governmental issues associated with r-money are discussed.

Keywords: RFID; r-money; currency; electronic money; traceability; economic crime.

Reference to this paper should be made as follows: Booker, L.D. and Bontis, N. (2010) 'Curbing economic crime with RFID enabled currency', *Int. J. Business Governance and Ethics*, Vol. 5, Nos. 1/2, pp.26–37.

Biographical notes: Lorne D. Booker is a PhD student majoring in management information systems. His research interests include knowledge management, academic relevance, technology adoption, e-commerce and 3D immersive environments. His previous research has been published in *Management Decision* and in *Knowledge and Process Management*.

Nick Bontis is an Associate Professor of Strategic Management at the DeGroote School of Business, McMaster University. He received his doctoral education at the Ivey Business School, University of Western Ontario. His research expertise covers intellectual capital, knowledge management and organisational learning.

1 Introduction

In the high technology world of the 21st century, traditional currencies seem out of place. We live in a world that is connected globally; we buy high technology gadgets that are designed in California, manufactured in China and we get our customer support from India. We work in a digital economy that is weightless, borderless, virtual and efficient (Sharma, 2005). Many of us work, shop and socialise in the virtual world of the internet. Yet, we still live in a world driven by cold hard cash. Therein lies the problem.

Cash is inefficient and insufficient for the modern world (Gemmell, 1997). In a world where so many business processes have been reengineered, automated and streamlined our handling of cash is still largely a manual endeavour. Handing cash takes time and costs money. Businesses have to count cash then they have to make entries into their computer system. Then their cash is deposited in the bank where the bank has to go through the same process. Machines can be used to count money but in many places counting is still done by hand. All of this counting and accounting is inefficient. Then there is the matter of security. Businesses spend a lot of time and effort instituting internal controls over cash. Cash still gets stolen. Similarly, retail outlets like convenience stores are prone to robbery despite the best efforts that they make. Once money is in the hands of a thief it usually is not possible to determine that it was acquired through illegal means. Then there is the problem of economic crime. Vast sums of funds are misappropriated every year. Once the money is gone it vanishes without a trace. In each case, lack of traceability is a problem.

Every problem is an opportunity awaiting a solution. This paper explores some benefits that could be obtained by embedding RFIDs into money – r-money. RFID technology is introduced and the functionality that RFID technology provides is discussed. After that the history and evolution of money will be described. Then the role of government regulation in the evolution of money is explored. Several possible phases in the roll out of RFID technology in money are discussed. In each phase, the capabilities provided are described. Also, the possible expansion of government regulation is evaluated. Then, economic crime is described and the value of r-money in curbing economic crime is evaluated.

2 RFIDs

RFID is an acronym that means Radio Frequency Identification technology. When people talk about RFID technology they usually refer to the small RFID tags – tiny electronic devices that contain microchip and a tiny transmitter. However, the tag is only one component of a larger system which consists of the RFID tag (or transponder) placed on objects or embedded in them, RFID readers which can read the information on RFID tags, RFID writers that can record information on tags and information and communication technologies including software and networked computers that make use of the information provided by the RFIDs. The microchip in the tag can be programmed with information about the object that the tag is placed on and the transmitter can broadcast information stored on the chip. Essentially, RFID technologies give computer networks the ability to see. This enables them to adapt to suit our needs instead of requiring us to adapt to them (Want, 2004).

Traditionally RFID tags have been placed on shipping containers to allow computer systems to track their location as they move from railcar to truck to ship. However, as the tags get smaller and the technology gets cheaper it becomes feasible to track smaller items. At the moment their role in supply chain and logistics management is expanding. Early adopters such as Walmart and the United Stated Military embed RFID tags on packages and on skids of merchandise in order to keep track of the location of their inventory. Today RFID technology is utilised in enhanced photo identification cards like the Enhanced Driver's Licences (EDL) and passports. Soon they may be embedded in all products or packages to automate the check out process at places like the grocery

store (Zipkin, 2006). When the technology is perfected consumers ought to be able to walk their grocery cart through a check out without having to unload their cart. Their purchases would automatically be identified and recorded.

The weak link in this vision of the future shopping process is the payment process. People will still have to count out bills and tellers would still have to count out change. RFID enabled money (r-money) could speed payment processes and reduce opportunities for human error. Other benefits can be obtained as well. These will be discussed later.

3 Proposed functionality of r-money

It is not easy to describe the functionality that can be achieved by embedding RFIDs in currency is not a straightforward task. RFIDs can be designed with an assortment of features providing them with a variety of functionality. They can have their own battery or they can be powered by the signal from the RFID readers; they can be made to have read only capability or they can rewritable memory as well; they can have data processing capabilities and eventually they will even have sensors. It becomes a question of deciding what new forms of value r-money can provide for society. The matter is further complicated by the fact that RFID tags need to be deployed in conjunction with a system of RFID readers, computers and communication networks which can also be designed and integrated with existing systems in a variety of ways. A large degree of vision and foresight will be needed to decide what r-money will be required to do before a lot of time and resources are invested into an information infrastructure. Similarly, a degree of vision is needed to envision the capabilities that RFIDs will provide as their costs drop, their sizes shrink and their capabilities improve.

In the late 1990s an effort was made to reinvent money. That effort can be used as a starting point for the effort presented here. The earlier effort was based on an effort to facilitate electronic commerce by devising a form of money that would be entirely electronic. Their effort was not based on expanding the capabilities of money. Instead, they sought to capture all of the current features of money. In addition to the intended roles of money – a store of value, unit of measure, unit of exchange etc. – they sought to capture all of the features of money; even the unintended ones.

Money is difficult to trace, not mediated and non-revokable. As a result of those attributes, money is private. The visionaries have ardently asserted that e-money should have the same attributes as traditional money; e-money must be anonymous, untraceable (Hanácek, 1998) and individual currency units must be indistinguishable from each other (Chaum and Bands, 1997).

The features they wish to emulate are characteristics of money by accident not by design. They do not serve any particular societal role or provide essential value. This is particularly true of the traceability attribute. In fact, in Europe there has been a trend towards treating banks as an arm of the state (Levi, 1991). In the United States the Bank Secrecy Act (which requires banks to maintain a minimum level of information about clients to facilitate law enforcement) has been repeatedly amended to provide law enforcement with more information and more power. The US Patriot Act provided further measures to combat money laundering by requiring banks to maintain a minimum level of identifiably of clients (Section 326), to cooperate more closely with law enforcement and to report suspicious activities and to establish a highly secure network to improve communications with the Financial Crimes Security Network (Section 362)

(107th Congress of the United States, 2001). In Canada, Proceeds of Crime (Money Laundering) and Terrorist Act has similar provisions. Traceability of cash is valued by government bodies.

Nontraceability does not seem to be valued by consumers either. The few e-money instruments that have been untraceable have not found widespread use. Mondex's smart cards did not achieved widespread acceptance despite having the support of a network of banks. Digital purses and m-money dispensed by cell phones have had only limited application. However, debit card and credit cards transactions are being used more frequently by consumers and they are both traceable and mediated by the bank. Credit card transactions are revocable under limited conditions. These attributes enable credit card companies to provide a limited form of consumer protection. Interestingly, debit cards and credit cards are being enhanced with chip-based technologies.

Consumers instinctively distinguish between confidentiality and privacy. If you think about it, none of us truly keep all of our information private. Our physicians keep extensive information about our health conditions and generally know more about our health than we do. We do not prevent them from having our health information. Instead, we trust that they will keep that information confidential by refraining from allowing others to access it. We have a similar arrangement with our banks and credit card companies. They are a third party to our transactions but they know the aggregate details; time, value, who was paid. They keep this information in confidence. If consumers valued complete privacy over protection then they would not use credit cards or debit cards. Consumers seem to value a compromise position in which information about their transactions are kept for their protection, but kept in confidence.

This paper takes the position that a greater degree of traceability is needed for currency. Since the word most commonly associated with RFID technology is 'visibility' this paper takes the position that RFID technology should be used to extend the traceability of currency. The question becomes one of the extent of traceability that is provided. Some issues that related to this question are described in the sections that follow.

4 The evolution of money

In the section that follows the history of money will be discussed and the role of governments in regulating currencies will be examined. The implications of the future evolution on government regulation are projected. A timeline of the evolution of money is presented in Figure 1.

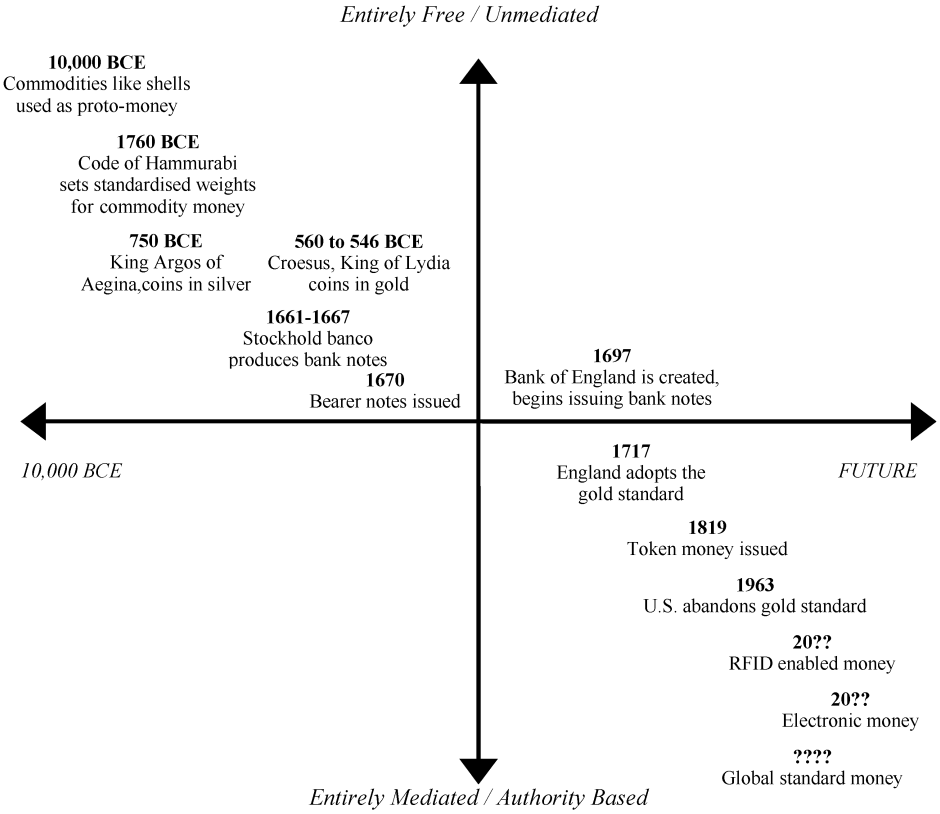
The earliest forms of currency required little authority. Commodities like barley, cocoa or conch were used as a unit of exchange. The first involvement by authorities is seen with the Mesopotamians who established the first systems of weights and measures. The economic significance of that practice can be seen in the earliest codes of law. The Code of Ur-Nammu and the Code of Hammurabi set standard weights and in doing so they standardised the weight of commodities to be use in trade. This of course enabled government to impose taxes and prescribe standard fines for specific crimes. It also enabled trade to flourish.

In time, precious metals became the generally accepted commodity of choice. Their rarity, durability and portability made them popular units of exchange. Anatolian traders are credited with creating the first coins. In order to free themselves from the task of

having to weigh precious metal with every transaction they inscribed the weight of each piece. The acceptability of the inscribed bits of precious metal required In time, governments became trusted third parties who regulated the quality of the metal being used for exchange. The first official currency was created in 750 BCE by King Argos on the Greek island of Aegina. According to Aristotle, Argos minted coins of silver. A later Greek, Croesus, King of Lydia is believed to be the first monarch to coin in gold.

The Chinese are credited with being the first to use paper money. They are believed to have begun using at around 1024 A.D. The first European use of paper money was envisioned by Johan Palmstruch. He founded the Stockholm Banco with the intention of producing paper money. In 1661 he succeeded but by 1667 his bank had issued too many notes and had collapsed.

Figure 1 The evolution of money



A more successful and gradual transition to paper money occurred in England. People there used to entrust their excess gold with goldsmiths. The goldsmith would provide a deposit note thus fulfilling the first role of accounting – to provide a record of ownership (Wright and Sayed, 2003). In 1670 goldsmiths began taking gold on deposit and issued bearer notes payable to whoever had possession of them. These instruments became popular. Then in 1697, the Bank of England was created. Almost immediately, it set about issuing bank notes. Twenty years later their bank notes were secured against specific quantities of gold.

By 1819 confidence in the authority of governments was such that governments could issue token currency – coins whose face value was in excess of the value of the metal used to make the coin. In 1963, the USA abandoned the gold standard and the transition to fiat money was complete.

Each stage of the evolution of money, from the early proto-money based on commodities to the fiat money we use today, was characterised by an increased involvement on the part of government. The earliest codes of laws regulated the weights and measures used in trade. Later governments minted standard coins and set laws which prescribed the legal tender acceptable within their jurisdictions. Later still, governments issued bearer notes as currency. Eventually, the level of confidence and trust in government was such that they were able to issue token currency and fiat money. In each stage of the evolution of money greater reliance was placed upon the authority of government and the rule of law. It is likely that this trend will continue into the future.

The issue that has been eluded to is that money is a technology that has immense societal impact. As our technology has evolved society has had the opportunity to enhance money even further. The forms that money will take in the future will not be assessed on its technical feasibility alone. The social feasibility must be assessed as well. In the section below some possible future phases in the evolution of the traceability of money will be explored. The phases range from partial traceability of limited utility to completely traceable. The technical feasibility and social acceptability of these futures are discussed.

5 The future of money

When the future of money is discussed in the context of a digitalised society the discussion is not about money alone, it is about creating a supporting digital financial infrastructure. Enabling money with RFID technology is not as simple as embedding RFID tags into bank notes. RFID technology has to be supported by a network of technologies that include readers, networks, computers, servers, software and standards.

In all likelihood the information systems that support r-money will be rolled out in phases. Initially, the financial costs and social responses will restrict the use of r-money reading systems but as prices drop, capabilities improve and social acceptability increases more information systems will be implemented to take advantage of the technology. In other words, the visibility provided by r-money technology will expand as the systems that support them get phased in. This paper envisions several possible phases in the roll out of the information systems that support r-money. Bear in mind that this discussion is not prescriptive: it is speculative. There are too many permutations of possibilities. Instead, several possible phases are discussed ranging from the feasible to the improbable.

The first phase of r-money implementation would likely see RFID readers for money (r-money readers) installed in banks and in banking machines. Automated teller machines would record who withdrew which bills and at what time. Similarly banks would record the bills as they get deposited and it would identify which business or individual deposited them. It is likely that the law would only require banks to record who withdrew specific bills and who deposited them. Police would need a court order to access that information. This initial stage would provide law enforcement agencies with the ability to flag specific bills as they enter back into the financial institutions. This stage would leave

many grey areas in which law enforcement agencies would have no idea where money had gone between the time money left one financial institution and returned to another. Law enforcement agencies would have visibility over a select set of bills in limited situations.

The second likely stage of r-money implementation would likely see businesses utilise r-money information systems to improve their internal controls over cash. Money counting systems, safes and even doorways would likely be equipped with r-money readers. Money counting machines would not just count money mechanically; they would also be assisted by r-money readers. This would enable businesses to record which bills they had on hand. Ideally, safes could be enhanced with r-money readers in order to keep a record of which bills had been placed in the safe and which bills had been removed. R-money readers could also be installed at key points such as doorways to detect when currency is being moved without authorisation. Each institution would keep its own record of the specific bills that had been in its possession. That information would only be revealed to law enforcement agencies in the event of a crime.

The system supporting the r-money reader could provide an audit trail for auditors, forensic accountants and law enforcement officials. When cash is stolen the organisation will have a record of that last time and place it was seen. If money had been removed businesses would be able to notify authorities of which specific bills had been stolen. These bills could then be flagged for action when they re-enter the sphere of visibility provided by r-money information systems. At the same time security over money could be enhanced. If money that is recorded in the system as belonging to the organisation is flagged as leaving its prescribed area then alarms could be sounded and an appropriate response could be triggered. Also, if r-money is utilised in conjunction with RFIDs in employee identification devices then it would be possible to track who had been in the proximity of money.

In the third possible stage, r-moneys reader would be installed on cash registers. They could assist in the automatic counting of money. Initially, the quality of r-money technology may not be good enough to place complete reliance on automatic counting of money but as the technology improves this practice should become technically feasible. Cash registers would record the receipt and issuance of individual bills. That would provide an audit trail that is even more extensive than in the previous phase. If a record was kept of every bill that was kept of every bill placed in a register's float (supply of money) then the system could track every bill through a business from receipt to deposit or payment.

Another feature is possible if r-money readers are installed in cash registers. Just as computer virus definitions are downloaded to personal computers on a regular basis, it would be possible for authorities to download lists of flagged bills to businesses and cash registers. If bills that had been associated with crimes are used to pay for items then the teller could be notified of actions that should be taken. While this arrangement could be technically feasible it might not be legal. It all depends on the laws that are created and enforced and the level of interaction allowed between the information systems used by businesses and law enforcement. Will society allow such interoperability? Will government impose standards of interoperability?

At this point, it is useful to consider what will happen if information from r-money information systems is used in conjunction with information from other sources. For example, what happens if information regarding specific bills is used in conjunction with customer loyalty programs? In this case it becomes possible to link individual bills

with specific customers. This raises issue of privacy and confidentiality. Each society will have to decide how to address this possibility. Society will either have to accept the fact that it might be possible to piece together that information or laws would have to be enacted to protect the privacy of consumers.

This leads to a fourth possible phase. This phase has little to do with the expansion of the supporting information system. It has to do with the expansion of regulatory powers granted by society. What happens if a shift is made from opportunistically combining information from r-money information systems with information from customer loyalty programs to requiring people to present RFID enhanced photo identification with every purchase? That requirement would provide a definite record of who had paid with specific bills. In effect, that would expand the visibility over the money supply into the wallets of consumers.

It is difficult to imagine future phases of r-money systems implementation beyond what has already been discussed. There is another possibility to be considered though. If information systems that support r-money ever becomes so pervasive as to allow complete visibility over the money supply then another possibility arises. It is possible to imagine a world where all money becomes electronic. Earlier theorists have imagined electronic money in the form of virtual purses and smart cards. What is theorised here is the possibility of having a central record of every transaction. It is also possible to see a government body like the central bank maintaining an official record of accounts. This arrangement has possibilities that are both wonderful and terrible.

If all money is electronic and the government kept an official record of accounts then the government has the capability to prevent economic crime. If you did not carry money on your person it would be difficult for people to steal it. If criminals did manage to steal money then it would be possible for government to declare the transaction to be illegal and have the transaction reversed out. It would also be possible to detect unusual transactions in real time using intelligent agents (Gao et al., 2009). At the moment, credit card companies flag unusual purchases and contact their card holders to inform them about unusual events. The same technology can be applied to money.

The exact form that r-money information systems will take will be the result of a delicate balance between capability and privacy. It is a question of which features will society value and which it will balk at. A hint about how some of these issues could play out has been provided recently in Britain. There the government had hoped to maintain a central record of all internet activities including e-mail and website visits. The British government has dropped the plan. Instead, they are pursuing a more moderate plan in which internet service providers to maintain their own records of a more limited set of information. Home Secretary Jacqui Smith noted that it is necessary to find a balance between security and privacy (The Associated Press, 2009). The same will be true of r-money. Historically, each enhancement to currency has been maintained by the expansion of regulatory powers. The question becomes how much visibility over money do we need?

6 Economic crime

Economic crime is a significant problem for businesses, consumers and society. According to PriceWaterhouseCoopers, 43% of companies sampled across 40 nations experienced at least one significant economic crime resulting in reported total losses

greater than US$ 4.2 billion (PWC Investigations and Forensic Service, 2007). They conclude that no industry is immune to economic crime. In Canada, it has been estimated that 1 million Canadians have been victim of investment fraud – a single category of economic crime (Alberro, 2007). Economic crime affects everyone.

There is no single authoritative definition of economic crime. In fact, reports and conferences differ in their selection of crimes to discuss. Most reports agree that business or consumer fraud, corruption, intellectual property infringement and money laundering are economic crimes. Price Waterhouse Coopers considers asset misappropriation to be an independent category of economic crime (PWC Investigations and Forensic Service, 2007) and the Royal Canadian Mounted Police discuss currency counterfeiting and securities fraud (RCMP, 2006). Some view human trafficking and terrorist financing as an economic crime.

If economic crime is becoming a larger problem due in part upon the new capabilities of the digital economy then new solutions are needed. Law enforcement will need new capabilities to combat economic crime in the digital economy. Perversely, criminals are able to enjoy the benefits of their crimes because governments provide a secure infrastructure for them. The economic systems that allow trade to flourish allow crime elements to flourish as well. Part of the solution to the growth of economic crime resides in the evolution of money. If properly designed, r-money could serve to curb a variety of economic crimes. It could also serve as an aid to investigators and auditors. Criminals are taking advantage of ICT to perpetuate crime. Law enforcement has to have the tools that will enable them to quickly identify and respond to threats. They need new tools to enable a coordinated response to a threat that is increasingly. Traditional currency does not provide law enforcement with the tools that they need to fight economic crime.

7 R-money and economic crime

In the foreseeable future r-money will not be a panacea for economic crime. As the technology improves and the capabilities expand r-money would, if implemented, provide law enforcement with increased capacity to curb economic crime. Of the economic crimes discussed earlier in this paper only a few would be addressed directly by r-money.

The area of economic crime where r-money would have its most direct impact is counterfeiting. When people speak of counterfeiting they are talking about the creation of a replica of a valued item usually for the purpose of trading the item for something of greater value. Although the term counterfeiting can be used to describe the production of ‘knock off’ brand named consumer goods it is the counterfeiting of bank notes that is of greatest concern. Our currency is feit money. It is not redeemable for gold or anything else of value. As a result, our financial system is based on trust. The integrity of our money supply is essential to the smooth functioning of our economy.

At the moment, technology has allowed government bodies to stay ahead of the predatory prey problem. In the USA, the value of counterfeit notes was estimated to be less than $70 million, with $56.2 million worth of counterfeit currency was detected and seized in 2005 (Secretary of the Treasury, 2006). In Canada, only $4 million was seized – down from $13 million in 2004 (RCMP Criminal Intelligence, 2007). In Europe, 565,000 bills were seized with the € 20 note being the most popular bill (European Central Bank, 2007). These amounts are not vast; less than one bill in 10,000 is fake

(Secretary of the Treasury, 2006). When it comes to economic crime there is a predator prey problem. At the moment, authorities are ahead of the predators. If history serves as a lesson then it should be expected that eventually criminals will find a way to circumvent the security features on money.

Even simple RFIDs embedded in money accompanied by the right supporting infrastructure could reduce the threat of currency counterfeiting further. In most cases, people do not inspect small bills to ensure that they are genuine. R-money would enable that process to be automated. In fact, counterfeiting may be the easiest economic crime to prevent using RFIDs. It would be prohibitively expensive for most entities to reverse engineer proprietary RFIDs – especially if they utilise technology that is a generation or two ahead of that available for common applications.

The second area of economic crime where r-money could play a role is in money laundering. The illegal nature of crime and the anonymous nature of currency makes cash transactions the favoured method of payment among criminals. Consequently, successful criminals accumulate large sums of cash. The downside of cash is that it is bulky and difficult to move in large quantities. Criminals prefer to get their funds into the mainstream financial system. The other problem that criminals face is that law enforcement agencies are suspicious of large incomes that materialise without a legitimate source. After all, even Al Capone was taken down by the tax man. Successful criminals disguise the true origin of their income. The process by which they hide the origin of their income is called money laundering. It is the activity of processing money through the financial system to disguise its illicit origin and make its origins appear to be legitimate.

The most vulnerable stage of the money laundering process is the first stage the proceeds of illegal activities and depositing them into the mainstream financial system (Buchanan, 2004). The first step is often achieved through cash rich businesses like cheque cashing businesses and liquor stores. In businesses such as these reasonably large sums of money (less than the $10,000 amount that banks are required to report) can be regularly deposited without raising suspicions. These deposits are then layered through the financial system. They are moved around across national borders in order to create a confusing audit trail.

R-money could be used to assist in tracking money laundering at the first vulnerable stage. Narcotics officers could purchase drugs or other illicit goods using r-money that has been registered. If the first stage of the architecture proposed above was employed then the bills could be flagged when they are deposited into a bank. Authorities would then have information regarding which businesses are involved in money laundering. Criminals would have to resort to the riskier method of physically smuggling the bills out of the country.

8 RFID challenges

There are technical issues that will have to be resolved before r-money can be utilised. One of the biggest problems concerns cross tag reading. When passive tags are employed the RFID reader emits a signal which then turns the tag on causing it to broadcast its signal. The RFID reader can cause several tags to broadcast at once. For some applications that may be desirable but for most it presents a real problem. Technical solutions will have to be designed that prevent that problem from occurring.

Technical standards are another challenge that should be addressed in advance of implementing r-money solutions. Since economic crime is increasingly a transnational phenomenon, the solution has to be a multinational effort. For that reason, international agreement for the technical standards of the RFIDs embedded in money is desirable.

It is likely that bank notes will contain more than one RFID, each serving a different purpose or representing a different technical standard. As new technical standards evolve the new standards may be represented in separate tags. For example, the national standards of the UK may be presented on one tag and the standards and requirements of the European Union on another. Also, each tag would likely employ different encryption protocols.

It would be beneficial to have different tags for different purposes. For example, it may be useful to have a tag that broadcasts at longer range to identify the type of currency, denomination and current record of owner and a separate tag that broadcasts at extremely short range to broadcast the information identifying the bill and verifying its identity. Long range tags serve to enhance security and internal controls over cash and the extremely short range tags for transaction processing. Longer range RFIDs – up to a few feet – may be problematic because without encryption or shielded purses and wallets otherwise r-money could allow criminals to determine how much cash a person is carrying. Extremely short range tags are necessary to prevent the reader system from triggering a response from a tag on another bill. Again, each tag for each purpose would likely need its own encryption protocol. Undoubtedly, there are technical issues that will have to be worked out.

RFIDs are vulnerable to physical abuse. At the moment there is nothing to prevent people from breaking the RFIDs. Such acts would make it necessary to replace bank notes – an expensive undertaking. Even if laws were created that made the destruction of RFIDs in money illegal they would have little impact on a crime that is carried out in private.

9 Conclusion

In the modern era, businesses have utilised information and communications technologies to achieve a greater level of efficiency and coordination than we have achieved in the past. At the same time, criminal interests are utilising ICT to bypass national jurisdictional boundaries and to circumvent law enforcement efforts. A new tool is needed to enable law enforcement agencies to trace the flow of money and to allow businesses to achieve greater levels of efficiency and effectiveness in their control over cash. RFID tags embedded in bank notes have the potential to provide law enforcement agencies with another tool to detect, prevent and solve crimes. RFID tags embedded in bank notes would provide a greater degree of traceability of money. At the same time, r-money would provide businesses with improved internal controls over cash. Eventually, they may provide a greater degree of efficiency in their handling of money.

This paper has addressed some issues surrounding r-money from the perspective of the information systems discipline. The real issues surrounding r-money are not associated with having RFID tags embedded in bank notes. The tags just allow computer information systems to be able to sense objects. The real issues are associated with the information systems that support r-money. Societies will have to balance security against privacy in determining the degree to which the supporting information systems will be

allowed to interoperate and the circumstances under which authorities will be allowed to access the information that they contain.

References

107th Congress of the United States (2001) *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism*, Public Law 107-56-26 October, USA.

Alberro, F. (2007) *CSA Study Shows One in 20 Canadians a Victim of Investment Fraud*, Canadian Securities Administrators, Updated 2 October, 2007, http://www.securities-administrators.ca/aboutcsa.aspx?id=213&terms=fraud

Buchanan, B. (2004) 'Money laundering – a global obstacle', *Research in International Business and Finance*, Vol. 18, pp.115–127.

Chaum, D. and Bands, S. (1997) 'Minting' electronic cash: electronic equivalets of tradtional cash payment systems are being launched worldwide', *IEEE Spectrum*, Vol. 34, pp.30–34.

European central bank (2007) *Biannual Information on Euro Banknote Counterfeiting*, 12 January, Viewed 5 January, 2009, http://www.ecb.int/press/pr/date/2007/html/pr070112.en.html

Gao, S., Xu, D., Wang, H. and Green, P. (2009) 'Knowledge-based anti-money laundering: a software agent bank application', *Journal of Knowledge Management*, Vol. 13, pp.63–75.

Gemmell, P.S. (1997) 'Traceable e-cash', *Ieee Spectrum*, Vol. 34, pp.35–37.

Hanácek, P. (1998) *Security of Electronic Money*, in Rovan, B. (Ed.), Springer-Verlag, Berlin.

Levi, M. (1991) 'Pecunia non olet: Cleansing the money-launderers from the Temple', *Crime, Law and Social Change*, Vol. 16, pp.217–302.

PWC Investigations and Forensic Service (2007) *Economic Crime: People, Culture and Controls: The 4th Biennial Global Economic Crime Survey*, Price Waterhouse Coopers, Halle-Wittenberg, Germany.

RCMP (2006) '2005 Economic crime', *RCMP Feature Focus*, Royal Canadian Mounted Police, Viewed 7 January, 2009, http://www.rcmp-grc.gc.ca/ec-ce/index-eng.htm

RCMP Criminal Intelligence (2007) *Counterfeit Currency in Canada*, Royal Canadian Mounted Police, December, Ottawa.

Secretary of the Treasury (2006) *The Use and Counterfeiting of United States Currency Abroad, Part 3*, United States Treasury Department, Washington, DC.

Sharma, S.K. (2005) 'Socio-economic impacts and influences of e-commerce in a digital economy', in Kehal, H.S. and Singh, V.P. (Eds.): *Digital Economy: Impacts, Influences and Challenges*, Idea Group Publishing, Melbourne.

The Associated Press (2009) *British Government Backs Down Over Database Plan*, http://www.ctv.ca/servlet/ArticleNews/story/CTVNews/20090427/britain_database_090427/20090427?hub=SciTech

Want, R. (2004) 'Enabling ubiquitous sensing with RFID', *Computer*, Vol. 37, pp.84–86.

Wright, C.S. and Sayed, N. (2003) 'Accounting practice and theory: a social institute account', *Journal of Accounting and Finance Research*, Vol. 11, pp.119–129.

Zipkin, P. (2006) 'The best things in life were free: on the technology of transactions', *Manufacturing and Service Operations Management*, Vol. 8, pp.321–329.