CASH IS KING

The Digital Revolution: The Future of Cash

Alfred Rolington

The Cambridge Security Initiative

CSi

CASH IS KING

The Digital Revolution: The Future of Cash

Prepared by
Sir Richard Dearlove OBE, KCMG
Professor Christopher Andrew
Professor Stefan Halper
Dr Peter Martland
Dr Alan Dawson
Dr Alfred Rolington
Jamie Collier (Cyber Security Intelligence Limited)

The Cambridge Security Initiative

email: info@thecsi.org.uk
www.thecsi.org.uk

The Cambridge Security Initiative is a Limited Liability Partnership, registration number OC399111

Briefing Notes

1. For more than 50 years analysts have claimed that electronic money would replace printed and minted money. Yet today central banks are issuing printed money faster than ever.

2. Cash still accounts for at least eight out of ten transactions worldwide.

3. Criminal cyber theft, attacks on ATM machines and on electronic bank accounts have increased dramatically, thus disproving the widely held belief that a cashless society would reduce crime rates.

4. Currency is an important national asset and forms part of critical national infrastructure and national identity. In order to retain stability it has to be controlled and monitored both from a physical and an electronic perspective.

5. The underpinning of currencies by linking them to gold created strong monetary systems, which continued to enjoy considerable public trust even after President Nixon took the U.S. dollar off the gold standard in 1971.

6. Government control of their currency has to include the use of cutting edge anti-counterfeiting technology including increasingly complex design systems. This has to be paralleled with increasingly sophisticated and effective controls of electronic currency.

CONTENTS

1. Executive Summary

1.i. Over recent decades several leading financial analysts have predicted the disappearance of physical cash, notes and coins, arguing for their replacement by an electronic payment system using debit/credit cards, Bitcoin, or other crypto-currencies and electronic wallets. This, they believed, would create an increasingly cashless global society.

1.ii. In 2014, Sweden announced its aim of going cashless and more recently Denmark followed suit. Yet even as the Swedish government pronounced the death of cash, it also announced the introduction of a new series of bank notes which began circulating in October 2015.

1.iii. In August 2015 the frequency and severity of cyber-attacks on financial institutions prompted the US Federal Financial Institutions Examination Council (FFIEC) to instruct banks to enhance their information security programs. This move was designed to better defend customers against attacks that might compromise user credentials and deploy destructive software. [1] Furthermore, recent reports [2] suggest bank information systems have indeed been compromised, resulting in the theft of large volumes of user credentials, including passwords, usernames, and other forms of authentication information. In the UK during 2015 Royal Bank of Scotland (RBS) faced regulatory scrutiny after a technology failure resulted in the disappearance of thousands of customer payments. [3]

"...even as the Swedish government pronounced the death of cash, it also announced the introduction of a new series of bank notes "

The Cambridge Security Initiative

The FFEIC has acknowledged that many information systems have been rendered inoperable because the data they hold has been compromised by malware.[4]

1.iv. Some cyber analysts believe that a cashless society would require the elimination of not just cash but also credit cards. They argue that this would reduce the number of bank robberies and attacks on ATM machines and therefore reduce crime rates. Although these assertions make for good headlines, they do not take into account recent improvements in cash protection systems, and the severe cyber-attacks taking place.

1.v. In fact, cyber hacking of ATM machines and electronic bank accounts remains a growing but largely silent problem. It often goes unrecorded by police and crime agencies and bank customers are usually left unaware of the crime. Banks choose not to advertise the number of electronic attacks taking place on their systems but instead prefer to pay back the lost amount and then raise the general service charges.

1.vi. Furthermore, the police in almost all jurisdictions find they are losing many of their most experienced IT people to commercial employment because of the greater need in the sector and higher salaries.

1.vii. This environment seems a long way from the old ways of money being backed by gold. And so we have reached a point where existing technology allows us to make electronic money, removing it from the physical world altogether. Nevertheless, many central banks continue to print money faster than ever and to protect it they employ sophisticated anti-counterfeiting printing security making it far more difficult to replicate or corrupt than electronic currency. This turbulent environment highlights the strength of bank notes and suggests that they will not disappear anytime soon. In fact a recent Euromonitor International report found that $14.4 trillion in consumer payments were made with cash worldwide, compared to a consumer payment card transaction value of $9.6 trillion.[5] This in turn tells us that, despite the rise of plastic cards and electronic money transfers, globally, cash remains the principal means of payment.

"The stark warning that what many think is tomorrow's problem is already with us in the world of the hacker and the cyber-criminal."

Rt. Hon. Lord McNally, Minister for Data Protection 2010-2013 and Treasurer of the All Party Parliamentary Group on Internet, Communications & Technology.

"Cash is now used in 52% of UK transactions."

Ms Victoria Cleland
Bank of England, Chief Cashier

1.viii. In 2015 the French government announced limits on the amount of payable cash, in order to help track transactions used to finance and equip terrorist attacks such as *Charlie Hebdo*.[6] However our research suggests that the government's promotion of web-based electronic transactions has had the reverse effect, creating more significant terrorist targets.

1.ix. Also in 2015, eight of every ten transactions used cash as the payment method of choice, even fifty years after the invention of plastic cards. Certainly, within the recent digital revolution cash is still a required and necessary commodity, as was witnessed during the recent financial crisis in Greece, where cash remained one of the few ways of successfully completing transactions.

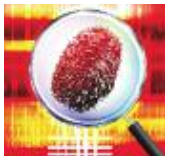
Global Percentage of Turnover of Transactions 2014

"It is our view that paper and coin currency still has a very long-term future, and will not, and certainly should not, be made to disappear."

The Cambridge Security Initiative







1.x. It is our view that paper and coin currency still has a very long-term future, and will not, and certainly should not, be made to disappear. Cash and coins should not be wholly replaced by electronic currency; although electronic money and digital currency has some benefits in macro-economic and security matters, cash still remains an active and purposeful commodity.

1.xi. From a broader perspective these cyber issues suggest governments will need to continue maintaining oversight of the different types of currency in use ensuring a balanced trajectory between printed and minted money through to a variety of electronic cyber currencies. Currency remains a critical element in national infrastructure and requires special protection.

1.xii. Government should continue to develop effective systems of control over electronic, printed and minted cash currency. They must ensure the right mix of the means of exchange within national economic and financial systems so that stability, control and sovereignty can be maintained. [7]

1.xiii. Our research suggests that the use of cash is fixed into the transaction processes of much of the world and is embedded into our societal culture.

"Complex economies need robust and mixed systems."

Sir Richard Dearlove KCMG OBE
Cambridge Security Initiative, Joint Chair, former Chief of Secret Intelligence Service, former Master of Pembroke College, Cambridge

"Government should continue to develop effective systems of control over electronic, printed and minted cash currency."

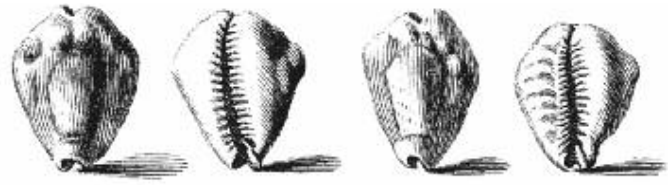
2. Introduction and Background

2.i. Cyberspace technology, its innovations, opportunities and the parallel threats to its security are becoming more and more apparent. So much so that they affect every aspect of geo-political and macro-economic analysis. For example, during the last decade international engagement with and discussion of cyber-attacks and digital changes have regularly hit the headlines.

2.ii. The influence of cyber on the world we inhabit represents one of the most important transformations to the global economy since the British Agricultural and Industrial Revolutions of the 18th and 19th centuries. Many have characterised cyber as the Third Industrial Revolution. Certainly this process of transformation represents a significant break from the old mechanical and analogue processes into the current interrelated global data information systems. However, the process might be better defined as the First Digital Revolution, marking as it does the start of the Cyber Information Age. Cyber has created and opened many areas of research, together with untold commercial and technical opportunities, which allow governments, corporates, businesses and individuals to inter-connect, research, analyse, alter and recreate their market understanding and client and personal connections.

2.iii. This revolution has already opened the possibilities of new technologies such as "The Internet of Things", [8] which has the potential to connect and radically change the way we live be it through improved controls at distance, driverless cars, or wide scale replacement of humans by robots in manual tasks.

"the process might be better defined as the First Digital Revolution, marking as it does the start of the Cyber Information Age."



Cypraea-moneta the money cowry, by Niccolò Gualtieri. Cowry shell money was important at one time or another in the trade networks of Africa, South Asia, and East Asia.

2.iv. From a government's perspective this Digital Revolution also offers new ways to monitor friend and foe, including criminals, as well as ways to understand and connect with their populations' broader thoughts, needs, risks and fears. This is clearly the beginning of a significant cultural change and when dramatic change has happened in the past they have impacted on and transformed other aspects of societal interactions, beliefs and processes; as for example with the impact of the printing press.

2.v. Despite an on-going revolution, many senior politicians and managers fail to fully understand the effects and implications of the Digital Revolution for their governments, for corporate structures, individuals and commercial and social processes. In order to help them better understand some of the changes this revolution is bringing we have reviewed and analysed areas that are already changing, such as the media industry, some on the cusp of change and others where change is happening but not in the way that has been reported and often predicted.

2.vi. One significant area where dramatic change is being predicted is in currency and in particular the effects the Digital Revolution is having on the printing and minting of cash. Some analysts think that these items could very rapidly disappear and be replaced by electronic transactions. Others have suggested that everything from debit/credit cards to Bitcoin and mobile money transactions would replace paper and minted cash. Yet this is not what our research has shown. Understanding the implications and future of this process is the central theme discussed in this Report.

2.vii. Cash is just one aspect of the currency and trading infrastructure affected by the cyber revolution. It has consequently broadened discussions about traditional cash and its future. Some consumers have already begun using electronic technology crypto currency, like Bitcoins, for transactions; crypto currencies, it is worth noting, are not backed by governments and often have a fluctuating value. Bitcoin is also untraceable and therefore unlike cash and credit/debit cards cannot be recovered if lost or destroyed.

"One significant area where dramatic change is being predicted is in currency and in particular the effects the Digital Revolution is having on the printing and minting of cash."

The six redesigned denominations of Swedish banknotes feature portraits of 20th century cultural icons of Sweden. Diplomat Dag Hammarskjold featured on the face of the new 1,000-krona notes.

"Many governments and organisations have neither researched nor understood the implications of developments in cyber space for their future strategy and current tactical planning."

2.viii. Over the past couple of decades the effect of cyber technology on currency and financial exchange has been significant. In 2015 Denmark debated whether retailers could ban cash transactions altogether. Sweden, which is considered one of the most cash free societies in the world, claims it has proved more efficient and reduced crime. However there are concerns about the impact on large proportions of the population, and certainly tourists, if these kinds of change are also made in other countries. Ironically, in October 2014, the Swedish government announced the issue of a new paper currency designed by Göran Österlun. Launched in late 2015, there are now over 300 million of these new bank notes and two billion coins in circulation. In launching the new issues Stefan Ingves, the Governor of Sveriges Riksbank, the central bank of Sweden, said:

"Many years of preparatory work is now reaching its conclusion. Today, we are pleased to be able to present the new banknotes and coins, which will provide Sweden with safe and efficient cash for many years to come. These banknotes will take us on an exciting cultural journey from Birgit Nilsson and the Öresund Bridge in the south to Dag Hammarskjöld and the Three-Country Cairn in the north". [9]

And so, even in Sweden with its cashless aspirations, printed money is not disappearing as quickly as had previously been thought.

2.ix. Research shows that although the exchange and currency markets are changing there is still a requirement, and there remains a significant need, for secure government printed notes and minted coins. A broader perspective of this issue suggests many governments and organisations have neither researched nor understood the implications of developments in cyber space for their future strategy and current tactical planning. It is crucial that they do so in order to alter the regulatory tools available to the government as economies undergo the rapid changes and repositioning of the Digital Revolution.

Figure to show the amount of cash assets people keep. In Japan, for example, cash represents over 50 percent of the assets people hold.

2.x. Money has proved to be one of the most influential innovations humans have ever created, and its success lies in its continued use for thousands of years. Money arose to improve the process of barter and, in the early days, included everything from cowrie shells, stone-disks to shiny gold stones, all of which were used for trading.

2.xi. Recently, the biggest near-term threat to cash appears to be from electronic payments, including systems based on cell phones and mobile wallets. We now have Google Wallets, Verizon and AT & T, T-Mobile and others. This move to digital, electronic and cyber is self-evidently based on strong commercial influences, market monitoring, functionality and global interconnectedness. However, the process does not adequately take account of potential weaknesses, security issues and unintended consequences produced by this digital revolution.

2.xii. Recently, in the UK, the Payment Council announced the phasing out of cheques in 2019. This 350 year-old payment system, the use of which has significantly declined in the last couple of decades, has been replaced in part by credit and debit cards and other types of electronic transfer and currency. David Birch from the Digital Money Forum, [10] using Bank of England statistics, suggests that cash payments represent 4% of all payments in Britain by value, although significantly they still represent over half the number of transactions because of the huge number of smaller payments made using printed and minted cash.

"Cash is classless, it is depended on by the 40 percent of the world that is unbanked"

Mr Martin Sutherland
De La Rue plc, CEO and CFO

"Money has proved to be one of the most influential innovations humans have ever created, and its success lies in its continued use for thousands of years."

"Our research and other studies, such as that by the Aite Group, [11] suggests that transactions using cash remains on a rising trajectory."

"Cash is an indispensable budgeting tools for many UK citizens."

Ms Victoria Cleland
Bank of England, Chief Cashier

2.xiii. Our research and other studies, such as that by the Aite Group, [11] suggests that transactions using cash remain on a rising trajectory. For example, cash transactions in the US totalled $1.2 trillion in 2010, and at least 20 percent of US citizens remain exclusively tied to cash. Looking at the wider world these numbers increase substantially. In the UK, for instance, ever since the financial crisis of 2008, demand for the £50 note has greatly increased. And so, despite the invention of electronic currency, cash in circulation has still been growing at exceptional rates in markets covered by this research; Australia, Canada, the Euro-Zone, Japan, and the United States. In some countries this process has been driven primarily by transactional cash, which is fuelled by sustained growth of GDP and consumer expenditure. The amount of people still using cash as an asset is large and increasing.

The next chapter will explore the broader historical context of traditional and electronic currency.

"Despite the invention of electronic currency, cash in circulation has still been growing at exceptional rates in markets covered by this research; Australia, Canada, the Euro-Zone, Japan, and the United States."

Denarius featuring emperor Marcus Aurelius (facing page).

3. The History of Money: From Coral Shells to Cyber Banking

3.i. Aristotle believed every object had two aspects to its being, first the practical purpose for which it was created and the second a value for which it could be bartered or sold.

3.ii. Money cannot be defined in such a precise way, as it has taken many different forms at different times. Today, money is mostly perceived of as a metal coin, or a piece of paper with a historic image on it, but in some regions of the world it remains natural objects such as shells.

3.iii. Importantly, the value people have placed on the trading item has nothing to do with the physical value of the money. Money derives its value by its role as a medium of exchange, a unit of measurement and a storehouse for wealth. Money allows people to trade goods and services indirectly. It also allows them to independently understand the price of goods. In the modern world economists have typically defined money by the three roles it plays in an economy:

First – It is a store of value, meaning that money allows you to defer consumption until a later date.

Second – It is a unit of account, meaning that it allows you to assign a value to different goods without having to compare them. So instead of saying that a diamond ring is worth six cows, you can just say either half a dozen particular cows or a specific diamond ring costs £2,500.

Third – Money is a medium of exchange. It is an easy and efficient way for people to trade goods and services with one another.

Mina of Antiochus IV Epiphanes (175 – 164 BC). From earliest Sumerian times, a mina was a unit of weight later becoming a unit of currency worth 60 shekels and one sixtieth of a talent.

An electrum Carthaginian shekel, c. 310–290 BC, bearing the image of Tanit, consort of Ba ʿal Hammon.

Merchants in Chengdu, China, distributed one of the earliest known forms of paper money, the Jiaozi, a printed-paper certificate (right), which dates back to the Northern Song Dynasty (960-1127). The local government established the earliest administrative and savings bank known as the Office of Jiaozi.

Money derives its value by its role as a medium of exchange, a unit of measurement and a storehouse for wealth.

All of these roles relate to buying and selling, which is how the modern world uses money, so much so that to us it seems peculiar to conceive of money in any other way.

3.iv. Yet in tribal and other less industrialised economies, money served a very different purpose, less a store of value or medium of exchange, much more a social lubricant. As anthropologist David Graeber put it in his book *Debt: The First 5,000 Years* [12] money, in those societies, was a way "to arrange marriages, establish the paternity of children, head off feuds, console mourners at funerals, seek forgiveness in the case of crimes, negotiate treaties, acquire followers."

3.v. Current forms of money date back at least 3,000 years to the Sumerians who created the first types of coin metal. This new form of exchange gradually took the place of bartering with barley and other items like shells. These coins gradually became the wider method of commercially trading within markets and between suppliers.

3.vi. The first mention of paper as money can be found in historic Chinese texts, highlighting the development of locally issue

The first paper money in Europe, issued by the Stockholms Banco in 1666.

The sealing of the Bank of England Charter (1694).

banknotes during the Tang Dynasty (618–690 and 705-907). Its roots lay in the use of receipts of deposit, when merchants and wholesalers sought to avoid the heavy bulk of carrying copper coinage to and from large commercial transactions. By 960 the Song Dynasty in China experienced a shortage of copper for striking coins. It responded by issuing the first generally circulating notes.

3.vii. Emperor Chen Tsung (998-1022) awarded rights to issue universal bills of exchange to 16 merchants. When, however, several of these merchants failed to redeem notes, the credibility of the money was undermined and the public refused to accept it. In 1023, the Emperor rescinded the merchants' issue rights and established a Bureau of Exchange within the government charged with issuing circulating paper notes. These are now considered the first true government-issued banknotes.

3.viii. In Europe, in the late 1650s, a Swedish banker called Johann Palmstruck created paper bank notes for Stockholm's Banco, the State Bank of Sweden, and this innovation began the use of paper currency in the West. In 1694 the Bank of England was established to raise money for King William III's war against France. Almost immediately the Bank started to issue notes in return for deposits. Like the goldsmiths notes, the crucial feature making Bank of England notes a means of exchange was the promise to pay the bearer the sum of the note on demand. This meant that the note could be redeemed at the Bank for gold or coinage by anyone presenting it for payment. These

"Cash provides a legitimate measure of privacy for law abiding citizens that we cannot simply dismiss."

Senior UK economist

Banknote of Bank of England, 1699.

The front of a 1779 fifty-five dollar bill of Continental currency. On the other side of the bill is a nature print that was developed by Benjamin Franklin for use on Pennsylvania currency in the decades before the American Revolution.

notes were initially handwritten on Bank paper and signed by one of the Bank's cashiers. But they tended to be for such significant sums relative to average income that most people went through life without ever coming into contact with them.

"In the USA the Bank of England model of paper money was used throughout the 19th Century, with at one time more than 5,000 different types of bank notes issued by American commercial banks."

3.ix. In the USA the Bank of England model of paper money was used throughout the 19th Century, with at one time more than 5,000 different types of bank notes issued by American commercial banks. However, only those issued by the banks with good credit ratings were widely accepted. Progressively, through the 20th century, most countries moved to limit note issue with greater government control and with that came the rise of the central bank. However there does remain some variation. For example, in the UK, Scottish notes circulate in parallel to those issued by the Bank of England, whilst the UK pound remains a single currency. Central banks and their contract security printers offered note users a high level of confidence and, as the century wore on and technology evolved, added multiple security features which we take for granted today.

3.x. The idea of using a card for transactions was first described by Edward Bellamy in his 1888 novel *Looking Backward.* [13] In it, Bellamy used the term credit card eleven times, although this referred to a card for spending a citizen's dividend from the government, a type of social credit, rather than borrowing.

3.xi. Charge coins and similar items were used in many Western countries from the late 1800s to the 1930s. They came in various

The Charga-Plate was an early predecessor to the credit card and used in the U.S. from the 1930s to the late 1950s.

shapes and sizes; with materials made out of celluloid (an early type of plastic), copper, aluminium, steel, and other type of whitish metals. Charge coins usually had a little hole, enabling it to be put in a key ring like a regular key. They were usually given to customers who had charge accounts in department stores, hotels, and so on. Such coins usually had the charge account number along with the merchant's name and logo. Due to the absence of the customer's name on the charge coin, almost any person could use it.

3.xii. Beginning in the 1930s, merchants began moving from charge coins to the newer Charga-Plate, developed in 1928, an early predecessor to the credit card and used in the US from the 1930s to the late 1950s. In 1934, American Airlines and the Air Transport Association simplified the process even more with the advent of the Air Travel Card. They created a numbering scheme that identified the issuer of the card as well as the customer account.

3.xiii. The concept of customers paying different merchants, using the same card, was expanded, in 1950 by Ralph Schneider and Frank McNamara, founders of Diners Club, to consolidate multiple cards. The Diners Club, which was created partially through a merger with Dine and Sign, produced the first "general purpose" charge card and required the entire bill to be paid with each statement. That was followed by Carte Blanche and in 1958 by American Express, which created a worldwide credit card network (although these were initially charge cards that later acquired credit card features).

3.xiv. The debit card has been around since 1966. As a result banks started to use the data collected on the use of cards. They were

"The Diners Club, which was created partially through a merger with Dine and Sign, produced the first "general purpose" charge card and required the entire bill to be paid with each statement."

The concept of customers paying different merchants, using the same card, was expanded, in 1950 by Ralph Schneider and Frank McNamara, founders of Diners Club.

pioneered by the Bank of Delaware and, by the 1970s, other banks were trying out similar ideas. Robert Manning, author of *Credit Card Nation* [14], said debit card usage picked up in the US during the 1980s and 1990s as more and more ATMs appeared. In 1990, debit cards were used in about 300 million transactions. In 2009, prepaid and debit cards were used in 37.6 billion transactions in the United States.

3.xv. Without most people understanding the implications, an electronic payment system has recently been created called Bitcoin. It is based not on trust but on cryptographic proof. Uniquely Bitcoin has neither the security features nor the government backing most people have come to expect from currency.

"Bitcoin has neither the security features nor the government backing most people have come to expect from currency."

The Cambridge Security Initiative

4. The Current Position of Electronic Currency

4.i. Bitcoin, the first electronic decentralised cryptocurrency, was invented by Satoshi Nakamoto and described in his 2008 research paper "Bitcoin: a peer-to-peer electronic cash system". [15] **It was launched in January 2009 as open source code.**

4.ii. Ben Lawsky, until recently New York State's Superintendent of New York's Department of Financial Services and thus a key figure in the financial world, granted 'itBit' a charter on May 7th 2015. This allowed the company's Bitcoin exchange to begin trading in New York State. On the same day itBit opened the exchange to people throughout the United States. However, permission to use itBit has been denied in several States though its charter provided a legal framework to operate in all fifty states. As *The New York Times* [16] put it, itBit appeared to be "the winner in a race among Bitcoin exchanges to become the first to be fully regulated in the United States."

4.iii. Bitcoin can be described thus: you purchase some Bitcoin via the Internet and install them in your Bitcoin wallet on your computer or mobile phone. This action will generate your first Bitcoin address and you can create another whenever you need one. You can disclose your addresses to a client so that they can pay you or vice versa. In fact this is very similar to how email works, though in order to keep transactions separate and secure Bitcoin addresses should only be used once.

"Digital money has weaknesses. Computer records are vulnerable to hacking and flaws in Near Field Communication, which is the set of protocols enabling electronic devices to communicate."

"Usage of digital currencies is presently very low and they do not currently pose a material risk to monetary or financial stability."

Senior UK economist

4.iv. The Block Chain is the public ledger that records bitcoin transactions. It is used by the Bitcoin network to record transactions in a database. All confirmed transactions are included in the Block Chain and it operates in the way a bank would record transactions. In this way, Bitcoin wallets calculate spendable balances and verify fresh transactions. The integrity and the chronological order of the block chain are enforced with cryptography. A transaction is a transfer of value between Bitcoin wallets that is recorded in the Block Chain database. The system is peer-to-peer and trading takes place without an intermediary who might charge a fee.

Bitcoin wallets keep hidden data called a private key or seed, which is used to sign transactions, providing a mathematical proof that they have come from the owner of the wallet. The signature is also an anti-fraud device designed to prevent the alteration of a transaction once it has been issued. Details of individual transactions are sent to users and are usually network confirmed within minutes of the transaction through a process called mining.

4.v. Like all forms of payment, digital money has weaknesses. Computer records are vulnerable to hacking and flaws in Near Field Communication, which is the set of protocols enabling electronic devices to communicate. According to a study by Ernst Haselsteiner and Klemens Breitfuss of Philips "*Near Field Communications*" (NFC) [17] this process has a number of glaring holes. Digital wallets, cell phones, wearable technology, and biometrics, may get lost or stolen,

just as wallets and purses are today. In this event, remote locking technology is available to protect accounts. Furthermore, it is possible to enhance security at the point of purchase by using graduated systems of verification. Small purchases might require just a finger tap, while larger ones might, for example, require retinal scan, PIN identification or text message verification.

4vi. It has been argued that the broader use of Bitcoin is evidence of an increasing acceptance of digital, non-traditional money, but it has also developed in other ways and has proved to be an effective enabler of illicit transactions and speculation. Innovative ways have been adopted by criminals to counter the enhanced scrutiny of these cloud-based payments. More worryingly, the cryptocurrency Bitcoin has thus far avoided government tracking and regulation. Combined with anonymous networks like Tor, Bitcoin's secrecy has facilitated online gambling and the now defunct Silk Road, which was a black market for drug purchases; but this has been replaced by new versions.

4.vii. But not everyone has smart technology. Ten percent of Americans and 50 percent of the world do not even have bank accounts. Homeless people depending on the "spare change" of strangers will struggle to tap into digital donations. The same goes for the charities, which ask for shoppers' pocket change.

4.viii. Present trends suggest the evolution to large digital payments will be fast, but interestingly this does not appear to herald the death of cash. Cash retains it societal value and promotes inclusion. Some will be slow to adopt exchanges conducted in the Cloud, just as there are people reluctant to adopt Cloud Computing in general.

"Not everyone has smart technology. Ten percent of Americans and 50 percent of the world do not even have bank accounts."

"Although the idea of electronic money replacing printed money still seems a futuristic fantasy, the increasing use of electronic payments and the rapid increases in the technologies to carry out such transfers mean that how individuals, companies and countries manage and safeguard their financial assets requires new skills, new awareness and new technical understanding of the digital revolution through which we are living."

Rt. Hon. Lord McNally, Minister for Data Protection 2010-2013 and Treasurer of the All Party Parliamentary Group on Internet, Communications & Technology.

5. The Importance and Security of Money

"We are starting to see something of a retaliation against the loss of individual privacy and security that necessarily follows from an increasingly cyber-based society. This is a basic human instinct that will always tend towards cash."

Senior UK banker

5.i. Money is a symbol of success. It represents the fruits of our aspirations, work and productivity and is part of our social standing. The identity money gives us cannot be digitised. The tangibility of cash is important not just as a symbol of the reality of money but as part of its role as a household budgeting tool.

5.ii. The 2012 fourth edition of the Agis, *Future of Cash* [20] study shows that the Great Recession, which began in 2008, increased global cash demand and use, as consumers attempted to shore up their savings and regain control over their budgets. With this in mind, it is essential for governments to maintain control of printed cash and continue to improve its quality and security. This is a key aspect of the government toolbox and is needed to control the national economy and security. It is also worth recalling the role which circulating cash played in the recent Greek economic crisis; in this case cash was one of the few means of commercial functionality when others are not working properly.

5.iii. Another factor propelling the continued use of cash has been the extension in the life of banknotes. This has been achieved by the use of new materials such as polymer; in 1988 Australia introduced the first polymer notes. Subsequently, spinoff advantages were found, for example in preventing counterfeiting. Polymer banknotes, which can survive a hot 90-degree washing-machine cycle are, according to the Bank of England, scheduled to replace the cotton paper £5 and £10 notes within the next few years. It is anticipated that these will last more than twice as long as existing notes, stay cleaner (they are resistant to dirt and moisture) and are almost impossible to tear. Today a typical £5 note lasts for two years. Polymer notes could last for around six years.

The Cambridge Security Initiative

Australia was the first country to have an entire note currency made of plastic which is extremely difficult to counterfeit.

The United States Federal Reserve recently released a new design for the $100 bill using a colour palette.

Clydesdale Bank decided in 2013 to make £5 and £10 banknotes from polymer. The current polymer notes are around 15% smaller than the current paper notes.

Quantum Money Illustrative.

5.iv. Ever since the invention of paper money, counterfeiters have attempted to create fake notes. Some of their modern handiwork, created with high-tech inks, papers and printing presses, make them difficult, in the first instance, to distinguish from the real thing. National banks combat counterfeiters with difficult-to-copy watermarks, holograms, forensic features and other sophisticated measures, which are being constantly improved by the banknote industry including security printers such as Crane & Co, Giesecke & Devrient, De La Rue, SICPA and Orell Fussli.

5.v. In their continuing efforts to stop counterfeiting the United States Federal Reserve recently released a new design for the $100 bill using a colour palette. This new bill has behind it a decade of security advances, anti-counterfeiting measures such as holograms, raised printing and ink-based artefacts that appear to move and change colour depending on the viewing angle. Despite these sophisticated security features, currency forgers have a big financial incentive to manufacture convincing fakes. In these circumstances the banknote industry is constantly looking at new ways to keep ahead. Some of these ideas are coming from the computing world, where experts have long looked to quantum mechanics to make unbreakable encryption.

"Currency forgers have a big financial incentive to manufacture convincing fakes. In these circumstances the banknote industry is constantly looking at new ways to keep ahead."

5.vi. At the moment, a number of concepts such as "quantum money" are being researched. The physicist Stephen Wiesner created the concept of quantum money around 1969. He suggested that banks insert a hundred or so photons, the quantum particles of light, into each banknote. [21] To validate the note later, the bank would simply check one attribute of each photon, for example, its vertical or horizontal polarization, leaving all other attributes unmeasured. The bank could then verify the note's authenticity by checking its records. There remain practicality and accessibility issues to be resolved before this idea becomes practicable, but in a world of cyber uncertainty the concept is attractive in as far as it exploits the most advanced ideas in material based security.

"The security of money in all its different guises has become a challenging financial control issue for banks everywhere; as exemplified by the two recent RBS IT failures which left 6.5 million RBS, Ulster Bank and NatWest customers unable to access their accounts."

5.vii. The security of money in all its different guises has become a challenging financial control issue for banks everywhere; as exemplified by the two recent RBS IT failures mentioned earlier in this report, which left 6.5 million RBS, Ulster Bank and NatWest customers unable to access their accounts. This is not a new technology crisis but a reoccurring one. For instance, Estonia experienced two banking crises related to digital technology in 1992-1994 (just after its breakaway from the USSR) and again in 1998-1999. Latvia too had a serious financial crisis in 2008-2009. On an almost daily basis it seems major companies with whom citizens share their precious financial data and identities have been hit by external and internal attackers. Many have simply not had adequate basic protection measures in place; others have been caught short by the ever-changing inventiveness of hackers with which they cannot keep pace.

5.viii. The Director General for Cyber Security at GCHQ [22] made pertinent comments on this subject at a 2014 conference for financial institutions. He spoke about the multiple motivations of perpetrators of attacks, be they state-led, terrorist, criminal, and gave illustrative examples of some of the many recent attacks:

- In March 2013, at a time of heightened tension on the Korean peninsula, 32,000 computers and servers serving three South Korean banks were wiped clean in a devastating cyber-attack.
- In 2012 and 2013 Iranian operators mounted a concerted series of "Denial of Service" campaigns against American financial institutions, not to make money but to seek

publicity in response to sanctions against Iran.

• In September 2013, UK police foiled two criminal plots to ransack British high street banks from the inside. Both involved installing new KVM (keyboard, video, mouse) switches directly on a system in a local branch. This shows cyber-attacks can have a physical dimension. Unlocked premises, a loose air vent, or whatever, can be a key vulnerability. [23]

5.ix. The Director General also described the development of a UK Government Cyber strategy within the financial sector. From this it is clear that the UK is among those attempting to install a workable framework both nationally and internationally. The difficulty in getting ahead of inventive minds has been recognised by experts globally; though the approach is necessarily and depressingly all too often reactive. The critical point here is that control of the economy by government is the key to global stability and security and should be something national strategic plans take into account.

5.x. Banks often do not explain to customers the cause of IT faults with their computer systems and the growing problem of hacking at ATMs and customer accounts. This should become a legal IT audit requirement that might go some way to restoring the population's faith in their financial systems.

5.xi. Effectively operating national financial systems are crucial to commercial security. These in turn depend upon a sound understanding and control of currency in all its forms. These are keys to national economic security and to combating cyber attacks on banking systems and the customers they are designed to serve.

"Control of the economy by government is the key to global stability and security and should be something national strategic plans take into account."

6. The Future of Currency: Digital Payments or Cash?

"Cash is indispensable in situations such as concerts where the broadband and Wi-Fi infrastructure is strained and electronic readers malfunction."

Senior UK economist

6.i. Mobile electronic cash as an alternative to printed and minted cash is now an established fact. And just as the plastic card and the Web made it easy for us to pay merchants, the mobile phone will soon make it easy for us to pay each other. When Edward de Bono wrote a pamphlet entitled *The IBM Dollar* in 1994 [18] he looked to a time when "the successors to Bill Gates will have put the successors to Alan Greenspan out of business," arguing that it would be more efficient for companies to issue money than equity. "Even if all I've got is Microsoft Moola, and you want to get paid in Samsung Shekels, who cares? Our phones can sort it out for us."

6.ii. Other obvious money-issuing entities will be communities constituting a natural domain for a kind of money, communities defined by region, political jurisdiction, or participation in some activity. In the UK's South London they have the Brixton Pound, a merchant-managed paper and e-currency that's exchangeable for regular pounds. Proponents say it fosters local business; detractors say it puts up an informal barrier to trade. In either case, it demonstrates a degree of local control over money.

6.iii. The Brixton Pound is a community project that launched Transition Town Brixton in 2009 with, initially, eighty local businesses accepting the alternative paper currency. In 2011 an electronic version of the currency was launched. Other towns in the UK using their own parallel currency include Bristol, Totnes, Stroud and Lewes. This

The Cambridge Security Initiative

In the UK's South London they have the Brixton Pound, a merchant-managed paper and e-currency that's exchangeable for regular pounds.

form of currency is known as "fiat" money. It is an agreed-upon medium of exchange with the value of money determined by the supply and demand of market forces. By the time computers and the Internet came along, money had in some areas partially become more of an abstract symbol of exchange.

6.iv. Virtual money is essentially a digital currency for any registered Internet-based community. Bitcoin sets up its network of registered users and issues encrypted credits to online wallets, which can be accessed anywhere, anytime by users from an Internet-enabled device. Digital wallets, such as the Google wallet, can store payment options and transaction history as well as virtual vouchers and loyalty cards.

6.v. But it is not just virtual currency that is changing the face of money. There is also e-commerce, or online payments for real goods and services. In this space, PayPal is the world leader. It has more than 100 million active users in 190 markets and operates in 24 currencies. One difference between e-commerce and virtual currencies such as Bitcoin and Facebook credits is that the former is an online payment mostly using financial instruments, for example credit cards, provided independently by financial institutions. Also, real goods and services are exchanged in e-commerce, linking this system more directly to the world economy.

6.vi. We must also expect an increase in the ways e-commerce and mobile phones are integrated. These technologies are forming a self-reinforcing virtuous cycle and the info-communication revolution in progress is likely to produce other examples of profitable convergence. At the moment, the marriage of the Internet and mobile telephony is dynamic, a game-changing convergence with potential to transform the way we live and work. It is thought that by 2018 more people will access the Internet via mobile devices than by PCs. It must be remembered, though, that 91 percent of mobile Internet use today is to socialise and not to buy online.

"Most people feel uncomfortable about the fact that credit and debit card systems are controlled by enterprises. In Brazil they have installed in access of 33,000 ATM's that use fingerprint validation only to vend cash without the need for a card. This direction of travel might bring cash back to the fore."

Dr Selva Selvaratnam
De La Rue plc, Chief Technology Officer

"The value of Bank of England notes in circulation is growing by around 5% per annum, and there is now about £1000 in banknotes per person in the UK. The annual banknote growth figures for the euro zone and Australia are both around 8%."

Ms Victoria Cleland
Bank of England, Chief Cashier

6.vii. In the payments industries there has been a surge of online payments through mobile devices, mostly using a PIN or password for authentication. PayPal recently noted a month-on-month increase of 25 percent in mobile payments. Traditionally, its online transactions have been from PCs. Now PayPal is piloting innovations such as mobile ticket purchase.

6.viii. Yet in the midst of this mobile-digital age, physical cash is categorically not being side-lined by plastic cards, electronic money and virtual money. This highlights the amazing resilience and competitiveness of cash as a technology. Just as plastic failed to replace cash following the invention of the credit card in New York in the mid-1950s, so electronic money has not overtaken cash as the preferred payment method across the globe. As previously noted, in the contemporary economy cash accounts for at least eight of every ten transactions. Furthermore, in 2011, the London-based market intelligence firm Euromonitor International found that $14.4 trillion in consumer payments was made with cash worldwide in 2010, compared to a consumer payment card transaction value of $9.6 trillion. Despite the rise of plastic cards and electronic money transfers, cash remains the most important kind of money in the world. [5]

6.ix. The secret of cash's longevity is that it is a simple, trusted, human-friendly technology, otherwise it would not have survived 27 centuries. This lifespan alone places cash as one of the top social technologies of all time. At the back of cash's popularity lies what physicist and futurist Michio Kaku calls the "Caveman Principle". [19] He suggests that our wants, dreams, personalities and desires have not changed much in 100,000 years and argues that whenever modern technology clashes with this primitive human self we carry around inside us, the primitive desires often win despite technological changes. There is a constant competition, Kaku argues, between high

"In the midst of this mobile-digital age, physical cash is categorically not being side-lined by plastic cards, electronic money and virtual money."

tech (e.g., watching a sporting event on television) and high touch (e.g., attending the live event in person). All other factors being equal, Kaka believes we will always choose high tech and cash; he considers digital money high tech. Moreover, he thinks most people will not change their beliefs for a long time to come.

6.x. Bitcoin founder Satoshi Nakamoto also highlighted what he saw as the strength of cash, explaining the costs and payment uncertainties of ensuring trust in electronic payments are largely avoided in person by using currency. What Nakamoto means is a cash transaction does not require the mediation of a whole system provided by a trusted third-party. It occurs directly and instantly between buyer and seller. Traditionally, the central bank has remained in the background guaranteeing the worth of the cash, and this is all part of the broad social contract existing between the citizen and government. By contrast, all forms of non-cash transactions, including plastic cards, electronic money or virtual money, are based on the mediation of an invisible and unaccountable system with all of the costs and risks this entails.

6.xi. Interestingly trust in cash is driving up demand at a rate faster than general economic growth rates. For example, between 2002 and 2011, the value of banknotes in circulation grew in the Eurozone, the US, Brazil and South Africa at the following compound annual growth rates, respectively: 10.6 percent, 5.5 percent, 14 percent and 9.5 percent. Humankind seems resistant to the idea of letting all of our money be digitised. In electronic and virtual forms of payment, no physical money passes from sender to recipient during transactions. And herein lies an important point about the meaning of money: money is not just information.

"High denomination notes are very valuable to elderly people, who tend to hold them as a store of value because they do not want the uncertainty that comes with entrusting a third party to manage their money."

Ms Victoria Cleland
Bank of England, Chief Cashier

7. The Death of Cash

"Technology is actually supporting cash in many instances, for example the iris recognition systems designed to improve security and efficiency at cash machines."

Senior UK economist

7.i. The death of cash has been exaggerated.

7.ii. The electronic money industry has been predicting the death of cash for more than fifty years. The profitable charges on all electronic transactions which the industry make, and the increasingly commonplace use of credit and debit cards has led to these predictions becoming more intense and self-serving. Furthermore, the development of new electronic money products appeared to lend weight to their arguments.

7.iii. The introduction of Bitcoin gave further impetus to the notion that printed cash and minted coins would soon become redundant. However, as we show, evidence for the death of cash is itself fatally flawed as it does not correspond to the experience of everyday life. In contrast to electronic currency, cash has a very long and successful history; it is easy to carry, it is a very acceptable exchange instrument and, unlike electronic currency, does not go out 'when the lights goes off', as ATMs and the electronic banking system did in the recent Greek financial crisis.

7.iv. Cash remains reliable, convenient and safe to use. Although electronic payments using credit and debit cards are now widely accepted, such transactions allow the trader, the electronic banking medium and potentially the state and criminals to monitor and intervene in the transactions of consumers.

7.v. Far from disappearing cash continues to circulate widely. During the financial crisis 2007 to 2012 cash circulation in the US grew by a staggering 42 percent and, according to bank note manufacturer Crane Currency, the average global growth of cash in circulation remains about seven percent a year. In 2013 in the UK fifty percent of consumer transactions were cash based.

7.vii. We feel safer and more secure holding and exchanging cash, particularly when there is a financial crisis or an electronic shutdown however brief. It is clear there and will be times and circumstances when people would rather have their money in their hand. As the American writer Mark Twain famously said 'reports of my death have been greatly exaggerated'. So in our view has the demise of cash.

"Since negative interest rates were introduced in Switzerland in 2014, Swiss Francs have increased in circulation by 20% and now represent more than 60% of notes in circulation. Fortunately many Swiss houses have mandatory nuclear bunkers in which to store the money."

Sir Richard Dearlove KCMG OBE
Cambridge Security Initiative, Joint Chair, former Chief of Secret Intelligence Service, former Master of Pembroke College, Cambridge.

8. Conclusions

8.i. Since money as the means of exchange is a major instrument of both sovereignty and economic management, the current control mechanisms should be regularly reviewed by nations and states. The on-going threats from crypto currencies, such as the Bitcoin and other electronic currencies and alternatives to cash, are growing and governments have the potential to lose control of their currencies and thereby the means to control other aspects of their national economy and finances.

8.ii. Interesting trends are developing in the way money is evolving and consequently in the tactical methods used by criminals, notably cybercriminals. They are developing simple but effective methods allowing them to use cyber tools and tactics to more easily steal money. And these methods can also be used in state-led attacks. In these uncertain circumstances, money must be seen as part of the critical national infrastructure.

8.iii. Electronic payment may appear to be more efficient and cost-effective than using cash, however its future is still only a part of the transactional process as 82 percent of all retail payment transactions worldwide are still done with cash, equivalent to about 54 percent of retail transaction value. Of total consumer spending, 34 percent by value is still done using cash. One of the more interesting questions for government to ponder is whether mobile money (such as Bitcoin) can be controlled by central banks and therefore nationally regulated? Central banks have at last woken up to the fact that their

"It's actually easier to move large quantities of money electronically than via cash – which suits criminals."

Mr Martin Sutherland
De La Rue plc, CEO and CFO

"Central banks have at last woken up to the fact that their wholesale interbank clearing and settlement systems can be bypassed by mobile-to-mobile payments."

The Cambridge Security Initiative

Retail Transactions 2014

wholesale interbank clearing and settlement systems can be bypassed by mobile-to-mobile payments. In which case, Bitcoin and the electronic platforms effecting the payments will have the capacity to create money.

8.iv. In the past central banks could only print money when it was backed by gold or promises to pay by the government. Today the parameters for controlling the money supply have changed. And notwithstanding public declarations of intent to the contrary, central banks in advanced economies are printing notes faster than ever. Cash is not likely to disappear in the near future, although as in recent decades different systems will coexist, with governments and central banks using both printed currency and different versions of electronic money to carry out their economic policies. In these circumstance we feel that the requirements for sophisticated currency security both in print and electronic formats will continue if government control of national currencies is to be maintained.

8.v. One way bank notes might develop would be to incorporate sophisticated security cryptography, giving them a unique identity that would be extremely difficult to forge. This and other aspects of the security of money will be dealt with in the next CSI report to be published later in 2016.

"Cash is not likely to disappear in the near future, although as in recent decades different systems will coexist, with governments and central banks using both printed currency and different versions of electronic money to carry out their economic policies."

9. REFERENCES, NOTES AND LINKS

(1) An FFIEC disclosure statement on the reported 2014 CRA data, in electronic form, is available for each reporting commercial bank and savings association. The FFIEC also has prepared aggregate disclosure statements of small business and small farm lending for all of the metropolitan statistical areas and non-metropolitan counties in the United States and its territories. These statements are available for public inspection on the FFIEC web site: https://www.ffiec.gov/cra/default.htm

(2) There was a 50 percent increase in the number of declared data breaches in 2014, with seven of the ten worst breaches of all time, as measured by the Breach Level Index.
http://www.intelligentenvironments.com/info-centre/blog/will-progressive-security-in-digital-financial-services-improve-customer-engagement?gclid=CLDH5rzv7McCFaPnwgodIE8Bxg

(3) *Financial Times* news report 17th June 2015 "Royal Bank of Scotland faces fresh regulatory scrutiny after a technology glitch caused the disappearance of thousands of customer payments only months after the bank was hit with a record fine for IT failures."
http://www.ft.com/cms/s/0/41c4579c-14d8-11e5-a51f-00144feabdc0.html#axzz3lLyvAjvZ

(4) Cyber Attacks on Financial Institutions Increasing in Frequency and Severity
http://www.privsecblog.com/2015/04/articles/financial-services/cyber-attacks-on-financial-institutions-increasing-in-frequency-and-severity/

(5) Euromonitor International global cash report
http://www.euromonitor.com/global-cash-and-carry-channel-wholesale-format-with-a-future-/report

(6) "France steps up monitoring of cash payments to fight 'low-cost terrorism'". Reuters, 18th March 2015.
http://www.reuters.com/article/2015/03/18/us-france-security-financing-idUSKBN0ME14720150318

(7) 3D printing or Additive Manufacturing, AM, is one of a variety of processes used to manufacture 3-dimensional objects. In 3D printing, additive processes are used, in which successive layers of material are laid down under computer control. These objects can be of almost any shape or geometry, and are produced from a 3-dimentional model or other electronic data source. A 3D printer is a type of manufacturing often using industrial robotics.

(8) "The Internet of Things" (IoT) is a network of physical objects or "things" embedded with electronics, software, sensors, and connectivity to enable objects to exchange data with the production, operator and/or other connected devices based on the infrastructure of International Telecommunication Union's Global Standards Initiative. "The Internet of Things" allows objects to be sensed and controlled remotely across existing network infrastructure, creating opportunities for more direct integration between the physical world and computer-based systems, and resulting in improved efficiency, accuracy and economic benefit. Each thing is uniquely identifiable through its embedded computing system but is able to interoperate within the existing Internet infrastructure. Experts estimate that the IoT will consist of almost 50 billion objects by 2020.
The term "Internet of Things" was coined by British entrepreneur Kevin Ashton in 1999. Typically, IoT is expected to offer advanced connectivity of devices, systems, and services that goes beyond machine-to-machine communications (M2M) and covers a variety of protocols, domains, and applications.
The interconnection of these embedded devices (including smart objects), is expected to usher in automation in nearly all fields, while also enabling advanced applications like a Smart Grid, and expanding to the areas such as Smart city.
https://en.m.wikipedia.org/wiki/Internet_of_Things#

(9) Swedish bank notes
http://www.riksbank.se/en/Press-and-published/Press-Releases/2015/Here-are-Swedens-new-banknotes-and-coins/

(10) David GW Birch is a Director of Consult Hyperion, an electronic identity and transactions consultant. He is the Chairman of the annual Digital Money Forum and Digital Identity Forum in London and he has written for several publications including more than a hundred 'Second Sight' columns for *The Guardian* newspaper. In 2007, he published *Digital Identity Management: Technological, Business and Social Implications* (Gower Publishing Ltd). He hosts the Consult Hyperion podcast, which are conversations with identity and digital transaction experts.

(11) Leading US Cash Management Vendors
http://aitegroup.com/report/leading-us-cash-management-vendors-winning-strategies-new-environment

(12) *Debt: The First 5,000 Years* by anthropologist David Graeber (2011). It explores the historical relationship of debt with social institutions such as money, cash, barter, friendship and slavery et al; in short, much of the fabric of human life in society has a direct connection to debt. The major arguments of the book are that when the imprecise, informal, community-building indebtedness of human economics is replaced by enforced debt impoverishment and violence often take place. And that debt is the historic means of trade with barter, cash and currency being developed later.

(13) *Looking Backward: 2000–1887* is a utopian science fiction novel by Edward Bellamy, a journalist and writer from Chicopee Falls, Massachusetts; it was first published in 1888.
https://en.m.wikipedia.org/wiki/Looking_Backward

(14) Robert Manning: "Credit Card Nation: The Consequences of America's Addiction to Credit."
After founding a company with credit cards and demonstrating their business acumen, most inexperienced entrepreneurs are shocked to learn that business growth and longevity do not necessarily attract greater interest from commercial lenders. This is due to the banking industry's discrimination, or "red-lining," policy against small businesses.
http://www.bloomberg.com/bw/stories/2001-04-29/credit-card-nation-the-consequences-of-americas-addiction-to-credit-part-2
http://m.democracynow.org/stories/10791

(15) "Bitcoin: A peer-to-peer Electronic Cash System"
Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double spending.
We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work.
The longest chain not only serves as proof of the sequence of events witnessed, and proof that it came from the largest pool of CPU power. As long as the majority of CPU power is controlled by nodes and these are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.
https://bitcoin.org/bitcoin.pdf

(16) *The New York Times* news report 7th May 2015, "New York State's top financial regulator has granted the first license to a Bitcoin exchange, allowing it to open legally to customers across the country.
The exchange, itBit, said Thursday morning that it was beginning to take on customers in the United States immediately after receiving a banking trust charter from New York State's Department of Financial Services and its superintendent, Benjamin M. Lawsky, who has been trying for some time to bring new rules to the fledgling virtual currency industry.
In addition to the new license, itBit, which has offices in New York and Singapore, also announced on Thursday that it had won $25 million in new financing and had appointed three prominent board members: Sheila C. Bair, the former chairwoman of the Federal Deposit Insurance Corporation; Bill Bradley, the former New Jersey senator; and Robert H. Herz, a Morgan Stanley director.
The trust company charter gives itBit a bank-like status and appears to make it the winner in a race among Bitcoin exchanges to become the first to be fully regulated in the United States."
http://www.nytimes.com/2015/05/08/business/dealbook/bitcoin-exchange-receives-first-license-in-new-york-state.html?_r=0
NYDFS Grants First Charter To A New York Virtual Currency Company
http://www.dfs.ny.gov/about/press/pr1505071.htm

(17) NFC (Near Field Communications)
http://events.iaik.tugraz.at/RFIDSec06/Program/papers/002 - Security in NFC.pdf
https://en.wikipedia.org/wiki/Near_field_communication

(18) "The IBM Dollar: The invention and the rise of bitcoin creates a dangerous precedent for business". Some experts now think that companies such as Starbucks or Amazon are well placed in order to issue their own currency and run their own "shadow economies" with goods, benefits, services and savings, which can be obtained with this money. These brands can very easily convince people that their currency has some solid intrinsic value (e.g. some coffee). This makes me think that Bitcoin is essentially just a well-known brand now, as the technological advancement of bitcoin is in fact very poor. As a brand, bitcoin will now have now to compete with other strong brands such as Amazon, Tesco or Orange. The main route to get there is that quite possibly the boring business of loyalty points is likely to evolve into a real payment ecosystem.
The Harvard Business Review had a paper about branded money in July 2013. Similarly Apple or mobile phone operators could easily convince young people to use their private currency: everybody understands that they can use it to get phone credit or with App store purchases.
http://blog.bettercrypto.com/?p=675

(19) "The Caveman Principle"
http://www.scienceforums.net/topic/84285-caveman-principle/ *Cave Man Principle* Michio Kaku
Why did these predictions fail to materialize? I conjecture that people largely rejected these advances because of what I call the Cave Man (or Cave Woman) Principle. Genetic and fossil evidence indicates that modern humans, who looked just like us, emerged from Africa more than 100,000 years ago, but we see no evidence that our brains and personalities have changed much since then. If you took someone from that period, he would be anatomically identical to us: if you gave him a bath and a shave, put him in a three—piece suit, and then placed him on Wall Street, he would be physically indistinguishable from everyone else. So our wants, dreams, personalities, and desires have probably not changed much in 100,000 years. We probably still think like our caveman ancestors.
The point is: whenever there is a conflict between modern technology and the desires of our primitive ancestors, these primitive desires win each time. That's the Cave Man Principle. For example, the caveman always demanded "proof of the kill." It was never enough to boast about the big one that got away. Having the fresh animal in our hands was always preferable to tales of the one that got away. Similarly, we want hard copy whenever we deal with files. We instinctively don't trust the electrons floating in our computer screen, so we print our e—mails and reports, even when it's not necessary. That's why the paperless office never came to be.
https://www.facebook.com/notes/michael-davis/cave-man-principle-written-by-michio-kaku/213732898648359

(20) Report on "The Future of Cash" by AGIS Consulting
http://www.agis-consulting.com/publications.html).

(21) The idea for "quantum money" can be traced to physicist Stephen Wiesner, a graduate student at Columbia University, who worked on quantum information theory in the 1960s and 70s. Although the principles are sound, the idea has been called impractical owing to the fact that the necessary technology does not yet exist.
http://www.hpcwire.com/2014/01/07/promise-quantum-money/

(22) Full text available at:
http://www.gchq.gov.uk/press_and_media/speeches/Pages/UK-financial-services-cyber-security-summit.aspx

(23) *Daily Telegraph* news report 13th September 2013, "Computer hackers arrested over plot to steal millions from Santander"
http://www.telegraph.co.uk/news/uknews/crime/10306466/Computer-hackers-arrested-over-plot-to-steal-millions-from-Santander.html

CREDITS, PHOTOGRAPHS AND LINKS

Design/Art Direction and Production
Tim Rawle Associates, Cambridge

Designer
Chris Jones Design4science Ltd

Specific Illustrations
Craig Dallas

Print
Pureprint Group,
Uckfield, Sussex

Cover Photo
Andrey Priyatkin/Shutterstock

Photographs
p3, p5, p7, p9, p31
Images courtesy of the Riksbank.
http://www.coinworld.com/news/paper-money/2015/01/New-Swedish-note-designs-celebrate-nations-culture.html

p3, p12, p31
© Rasiel Suarez - Tantalus Coins/Creative Commons
http://www.tantaluscoins.com/coins/39337.php

p8
© Public Domain/Creative Commons
https://commons.wikimedia.org/wiki/File:Cypraea-moneta-001.jpg#/media/File:Cypraea-moneta-001.jpg

p9
Courtesy of the Riksbank.

p13
Public Domain (E. Babelon, art. Mina, in C. Daremberg - E. Saglio (edd.), Le Dictionnaire des Antiquités Grecques et Romaines, III.2, Paris, 1904, p. 1910.)
https://en.wikipedia.org/wiki/Antiochus_IV_Epiphanes

p13
© Classical Numismatic Group, Inc. http://www.cngcoins.com Licensed under CC BY-SA 2.5 via Commons

p14
Public Domain
https://commons.wikimedia.org/wiki/File:Jiao_zi.jpg

p14
© Sweden-Crediyf-Zedels. Public Domain
https://commons.wikimedia.org/wiki/File:Sweden-Crediyf-Zedels.jpg#/media/

p14
© Lady Jane Lindsay - Alice Archer Houblon, The Houblon Family, vol. 1, 1907/Public Domain.

p15
Banknote © http://pfin.com.ua/istoriya-deneg-1682-1776/

p15
© "Benjamin Franklin nature printed 55 dollar back 1779" by Beyond My Ken - Own work. Licensed under CC BY-SA 3.0 via Wikimedia Commons - https://commons.wikimedia.org/wiki/File:Benjamin_Franklin_nature_printed_55_dollar_back_1779.jpg#/media/File:Benjamin_Franklin_nature_printed_55_dollar_back_1779.jpg

p16
© Marilyn Acosta/Creative Commons
Mahttps://www.flickr.com/photos/maya83/4892473137/in/photostream/

p22
© lovleah/Bigstock

p22
© Bureau of Engraving and Printing/ work of the United States government/Public Domain
https://commons.wikimedia.org/wiki/File:New100front.jpg

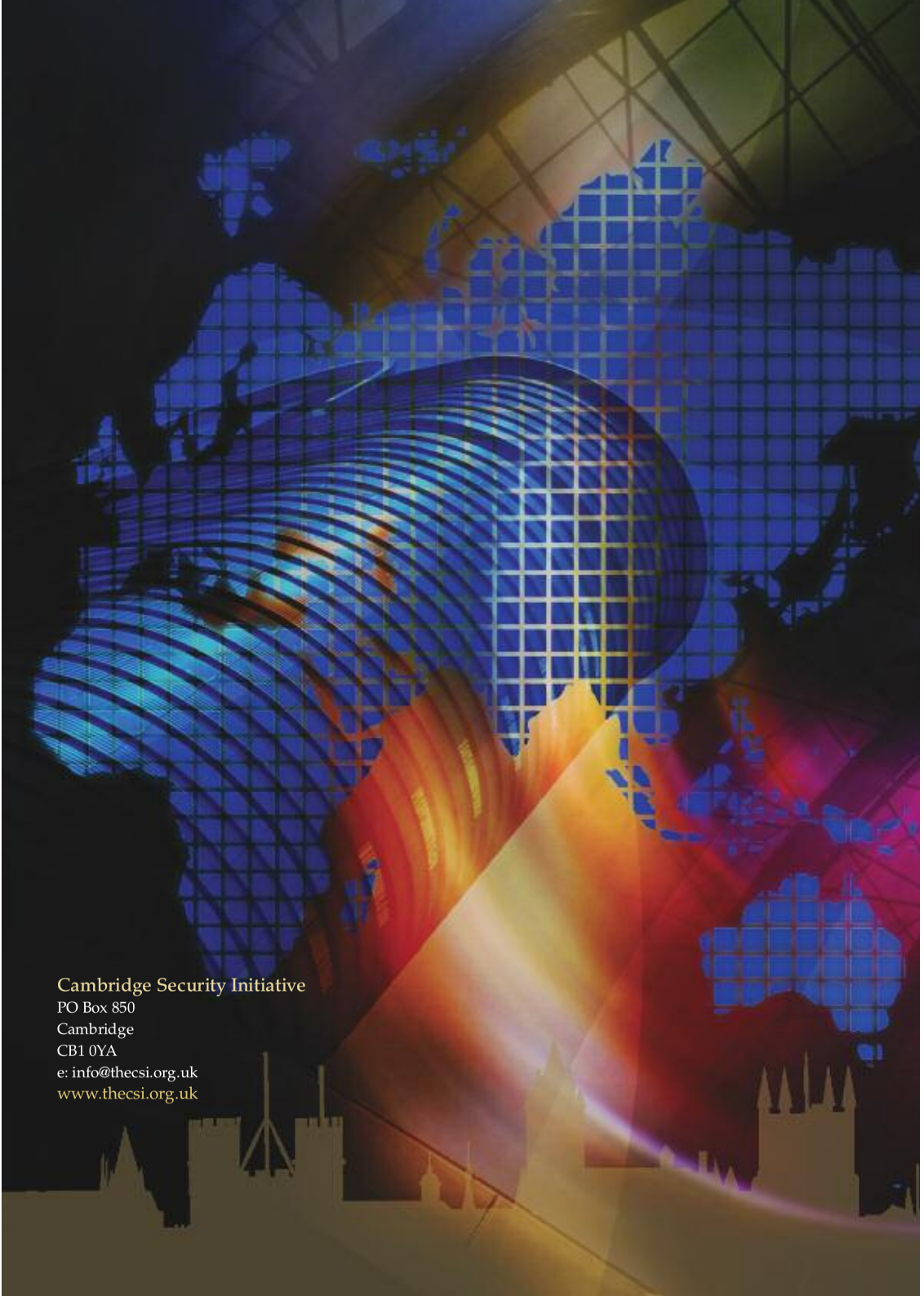
p23
Clydesdale Bank £5 note
http://blog.novationindustries.com/polymer-bank-notes
© Novation Industries
http://www.cbonline.co.uk/we-care-about-here/strong-foundations/the-cleaner-and-stronger-five-pound/features-of-our-new-polymer-note/

p26
Quantum Money
Source: NASA Quantum Future Technologies Document
http://quantum.nasa.gov/materials/2012-01-19-B1-Shor.pdf

p26
Brixton Pound
https://brixtonpound.org/showmemoney

p28
Google Wallet

Other images from Bigstock.com



Cambridge Security Initiative
PO Box 850
Cambridge
CB1 0YA
e: info@thecsi.org.uk
www.thecsi.org.uk