THE LEGAL STATUS OF ONLINE CURRENCIES: ARE BITCOINS THE FUTURE?

Introduction[1]

> "Small tribes have often used unique forms of money. Until recently, west Africa's Ashanti had perhaps the oddest. Eschewing the convenience of metal discs, stones or shells, they used metal painstakingly moulded into the shape of small chairs, representing the tribal chief's throne. But the latest cult currency—Bitcoin—is stranger still. Invented in 2009, this computerised money exists only as strings of digital code."[2]

Bitcoin has been described as a decentralised virtual currency. A currency is a means to store value, measure value and facilitate transactions. Currencies tend to have the following features: scarcity, divisibility, portablity and easy storage. Currency has a legal meaning in some countries, relating to seignorage and legal tender. For example currency has a technical legal meaning under the Reserve Bank Act and Currency Act in Australia.

Money, payment and currency are simply social constructs. What people are willing to treat as payment are payments, same as money.[3] Historically many different things have been used as money or currency: conch shells, pieces of gold or silver, servings of rum and so on.[4] Any artefact, physical or virtual, can potentially be used. Match sticks or jelly beans can be effective, presuming of course that payers and payees are happy to treat them as valid and effective payment! Many tokens or commodities are used as limited currencies today, such as cigarettes in prisons.[5] As such, we should not be too surprised to see electronic or virtual currencies arise from time to time.

Previous attempts have been made to commercialise purely software-based stored value facilities (sometimes known as electronic cash or digital cash).[6] Instead of using a plastic card with an

---

[1] Dr Rhys Bollen, PhD RMIT, MBA Melb Bus School, LLM (Cambridge), M Bus Law (Sydney), BBus LLB (UTS); Senior Fellow, Monash University Faculty of Law. Thanks to David Greenaway for insightful comments on a draft of the article. The views in this article, including any errors or omissions, are the author's only. This article is based on the law as at 1 May 2013.

[2] The Economist, "Digital currencies: A new specie" 13 April 2013, (www.economist.com/news/leaders/21576104-regulators-should-keep-their-hands-new-forms-digital-money-such-bitcoin-new-specie, accessed 24 April 2013)

[3] Rhys Bollen, 'What a Payment is (and how it continues to confuse lawyers)' (2005) *MqJBL* 189

[4] SJ Butlin, 'Foundations of the Australian Monetary System 1788-1851', Sydney University Press, 2002, (http://hdl.handle.net/2123/7702, accessed 1 May 2013)

[5] RA Radford, 'The Economic Organisation of a P.O.W. Camp' (1945) 12 *Economica* New Series, 189 (http://www.jstor.org/stable/2550133, accessed 5 May 2013)

[6] Weerasooria WS, *Banking Law and the Financial System in Australia* (5th ed, Butterworths, 2000) at [8.16]; Kreltszheim, Kreltszheim D "The Legal Nature of 'Electronic Money': Part 1" (2003) 14 JBFLP 161 at at 170; R Bollen, Bollen R, "The Regulation of Internet Banking" (2001) 12 JBFLP 5 at 7; Tyree Dr A, "Digital Cash in Australia" (1998)

embedded magnetic strip or computer chip, the customer's balance is recorded on the customer's PC, phone or other device.[7] Reducing the customer's balance and increasing the merchant's balance vis-à-vis the scheme operator is how the payments are made. In theory, an electronic cash system could operate at very low cost, allowing for commercially viable payments of small amounts.[8] This would support business models such as online magazines where the operator charges a consumer (say) 50 cents to read an article.

Early digital cash schemes could be likened to the Electronic Funds Transfer Point of Sale **(EFTPOS)** system without the physical infrastructure and cards.[9] Digital cash is a completely intangible, software-based payment system. Traditionally the participants transfer a unique digital message or file that can be redeemed at a bank for cash or the equivalent credit to an account.[10] The message or digital 'coin' contained certain information including a serial number, an expiration date,[11] the name of the issuing institution and the value represented.[12]

Consumers could request that their institution[13] issue a digital 'coin' which would be authenticated by the issuer and encrypted[14] so that the coin could not be intercepted whilst in transit.[15] When the person receiving the coin desires to use it, they would further encrypt the coin and send it to the merchant from whom goods or services were to be bought. The business would check with the issuer to ensure that the coin was legitimate and that it had not been spent previously.[16] Assuming that these enquires were satisfactorily answered, the merchant can attribute value to the coin received

---

9 JBFLP 5 at 5; Beatty A, Aubrey M and Bollen R, "E-payments and Australian regulation" (1998) 21 UNSLJ 489 at 490.

[7] For example, a smart phone or Personal Digital Assistant

[8] Blay S and Clark E, Australian Law of Financial Institutions (2nd ed, Harcourt Brace, 1996) at [9.20].

[9]Legally, it is also similar to the use of cheques as a payment mechanism. Frank Quin "'Electronic money' - a legal misnomer?" [1996] NZLR 223 at 224

[10]In some situations the digital cash may be transferred between various parties prior to redemption at a bank. That is, the digital "coin" would be in circulation. See Alan Tyree "Virtual Cash - Payments on the Internet: Part I" at 35

[11]if applicable

[12]Financial institutions are not the only organisations capable of offering such "coins".

[13]At present St.George Bank is one of the few Australian financial institutions offering digital cash services (www.stgeorge.com.au/ecash)

[14] For a discussion of encryption and the public key authentication system see the discussion of digital signatures under the heading "Possible solutions" below.

[15]Alan Tyree "Virtual Cash - Part II" (1996) 7 JBFLP 139 at 139

[16]Alan Tyree "Virtual Cash - Part II" at 139; M Sneddon , Cyberbanking and Payment Products: Legal and Regulatory Issues, a paper presented at the 14th Annual Banking Law and Practice Conference, Sydney, 22 May 1997, at 11

and provide the goods or services requested. The merchant's bank account would be credited for the value of the coin.[17]

As we will see in the next section, virtual currencies such as Bitcoins are a form of money and a payment system. However, being a decentralised system, there is no central issuer, authority or register-keeper. No party or authority, no matter how well motivated, can confiscate Bitcoins from a user, nor prevent two users from transacting. Nor is the endorsement of any particular party or authority needed to open an account or make a transaction. At this stage, it is not clear that these virtual currencies are currencies as such as we will see later.

> *"Bitcoin is not the only digital currency, nor the only successful one. Gamers on Second Life, a virtual world, pay with Linden Dollars; customers of Tencent, a Chinese internet giant, deal in QQ Coins; and Facebook sells "Credits". What makes Bitcoin different is that, unlike other online (and offline) currencies, it is neither created nor administered by a single authority such as a central bank."*[18]

In the next section, we give an overview of how virtual currencies like Bitcoin work.

What are virtual currencies and how do they work?

Bitcoin is a decentralised and loosely managed payment system. It is described as a 'currency' in part to refer to the fact that it is denominated in its own units of account, rather than in say Euros or US dollars.

> "Unlike traditional currencies, which are issued by central banks, Bitcoin has no central monetary authority. Instead it is underpinned by a peer-to-peer computer network made up of its users' machines, akin to the networks that underpin BitTorrent, a file-sharing system, and Skype, an audio, video and chat service. Bitcoins are mathematically generated as the computers in this network execute difficult number-crunching tasks, a procedure known as Bitcoin "mining". The mathematics of the Bitcoin system were set up so that it becomes progressively more difficult to "mine" Bitcoins

[17] This may occur via an interbank clearing system, depending upon the whether the merchant and consumer used the same institution for their banking. It is uncertain to what extent coins issued by one bank will be honoured or accepted by another. Frank Quin "'Electronic money' - a legal misnomer?" at 224; Alan Tyree "Virtual Cash - Part II" at 140

[18] The Economist, "Virtual Currencies: Mining digital gold", Apr 13th 2013 (http://www.economist.com/news/finance-and-economics/21576149-even-if-it-crashes-bitcoin-may-make-dent-financial-world-mining-digital, accessed 15 April 2013)

> over time, and the total number that can ever be mined is limited to around 21m. There is therefore no way for a central bank to issue a flood of new Bitcoins and devalue those already in circulation."[19]

Unlike some previous digital currencies, Bitcoins are not denominated in an existing currency. Bitcoins are denominated in their own numerations: each Bitcoin (BTC) is subdivided into 100 million smaller units called satoshis, defined by eight decimal places.[20]

There is no fixed exchange rate between Bitcoins and regular currencies. Indeed, much of the recent media interest in Bitcoins has been because of the great volatility in these exchange rates. While the 'proper' exchange rate is beyond the scope of this paper (if indeed there is an objective proper value), suffice to say the volatility of Bitcoin's exchange rate in recent times has been of great interest to consumers and regulators. This is so much so that Bitcoins have attracted investors and speculators, interested in holding Bitcoins not for their transactional capacity but for their potential to appreciate in value.

The currency grew in usage and popularity through 2010. It first received broad media attention in June and July 2011. This resulted in a boom and bust in Bitcoin prices. This was a precursor to the 2013 boom.

> *"The scale of the recent boom-and-bust has been staggering indeed. At the start of the year, a Bitcoin was worth $13.51. Earlier this week, it traded as high as $266. And on Thursday, it plummeted to less than $100, as one of the exchanges where Bitcoins are traded closed temporarily. This would be comparable to the exchange rate for the British pound soaring from $1.62 (where it was on Jan. 1) to $31.90 and then falling back to $12."21*

Bitcoin has been described by its community as "one of the first implementations of a concept called crypto-currency, which was first described in 1998 by Wei Dai on the cypherpunks mailing list".[22] Acknowledging the historical development of currencies and money, they appreciate that money is a social construct. Any object, artefact or record,

[19] TS, "The Economist explains: How does Bitcoin work?" 11 April 2013, The Economist (http://www.economist.com/blogs/economist-explains/2013/04/economist-explains-how-does-bitcoin-work, accessed 14 April 2013)
[20] Bitcoin Foundation, "About Bitcoin", (www.bitcoin.org/en/about, accessed 15 April 2013)
[21] Michael Sivy, "The Real Significance of the Bitcoin Boom (and Bust)", Time Magazine, 12 April 2013 (business.time.com/2013/04/12/the-real-significance-of-the-bitcoin-boom-and-bust/print/, accessed 24 April 2013)
[22] Bitcoin Foundation, "About Bitcoin"

> *"accepted as payment for goods and services and repayment of debts in a given country or socio-economic context, Bitcoin is designed around the idea of a new form of money that uses cryptography to control its creation and transactions, rather than relying on central authorities."*[23]

"In 2009, the first Bitcoin specification and proof of concept was published in a Cryptography mailing list by a member under the pseudonym of Satoshi Nakamoto."[24] He or she appears to have since left the project. Their identity remains unknown.

The Bitcoin system is an open source project. The Bitcoin Foundation was created on 27 September 2012. It "standardizes, protects and promotes the use of Bitcoin cryptographic money for the benefit of users worldwide".[25]

> *"As a non-political online money, Bitcoin is backed exclusively by code. This means that—ultimately—it is only as good as its software design. By funding the Bitcoin infrastructure, including a core development team, we can make Bitcoin more respected, trusted and useful to people worldwide. ... Cryptography is the key to Bitcoin's success. It's the reason that no one can double spend, counterfeit or steal Bitcoins. If Bitcoin is to be a viable money for both current users and future adopters, we need to maintain, improve and legally protect the integrity of the protocol."*[26]

The decentralised nature of Bitcoin, and its independence from central banks and monetary authorities, is one of its core attractions to many of its followers. Through the ongoing global financial crisis, central banks have pursued aggressive expansionary monetary policies and significantly increased the money supply. Known as 'printing money', this unconventional approach has a number of detractors who fear it will undermine confidence in money and encourage general inflation and an asset price bubble.[27] One consequence of this has been an increased demand for gold and other 'safe havens'. It has also led to an increased debate about the need for a return to the 'gold standard' or other similar restrictions on the money supply.[28]

Linking the supply of currency, such as the US dollar, to the supply of gold under the control of the government was a traditional way of enhancing confidence in an otherwise artificial or fiat currency whose notes and coins are really only of token value. The other effect of a gold standard was to limit

[23] Bitcoin Foundation, "About Bitcoin"
[24] Bitcoin Foundation, "About Bitcoin"
[25] Bitcoin Foundation, "About Bitcoin"
[26] Bitcoin Foundation, "About Bitcoin"
[27] Ambrose Evans-Pritchard, "Warren Buffett sees 'brutal' damage for savers from central bank money printing" The Telegraph Online, 5 May 2013 (http://www.telegraph.co.uk/finance/financialcrisis/10038882/Warren-Buffett-sees-brutal-damage-for-savers-from-central-bank-money-printing.html, accessed 6 May 2013)
[28] Richard N. Cooper, Rudiger Dornbusch and Robert E. Hall, "The Gold Standard: Historical Facts and Future Prospects", (1982) Brookings Papers on Economic Activity 1 (http://www.jstor.org/stable/2534316, accessed 5 May 2013)

the government's ability to print additional currency (at least unless they acquire additional gold to back such currency).[29]

One of the core design features of Bitcoin reflects this rationale. Indeed, it is one of the attractions of Bitcoin to many users, especially those using it as an investment (ie as a medium-long term store of value, rather than short-term transactors). There are a finite number of Bitcoins in the system. The system is designed so that there is a slow release of additional coins into the system, through a process known as 'mining'. There is also a hard limit on the number of coins that can ever be created in the system. This has some adverse economic impacts, as covered elsewhere by prominent economists such as Paul Krugman.[30]

All Bitcoin users have an electronic wallet, which gives them an electronic address and identity. Payments can be made to them and by them to others (by directing payments to a specific wallet's electronic address). A public/private key pair is allocated to eachdigital wallet. This wallet, and access to the public/private key incorporated in that wallet, gives the user the ability to give payment instructions.

Each party involved in a public/private key scheme has two keys associated with them (their public key (A) and private key (B)). Using a mathematical relationship (eg the RSA algorithm) these two keys can be used to cipher and decipher[31] messages. The algorithm ensures that a message ciphered (scrambled) with A can only be deciphered (unscrambled) with B. It is not possible to cipher and decipher a message with the same key. Further, the nature of one key cannot be discovered from the other key in the pair. Hence anybody can send a confidential message ciphered using A (this key, being the public key, is freely available) without fear of interception because only by using B can the message be deciphered and understood. The person associated with A is the only one with access to B.

The corollary is also true. If the sender of a message wanted the recipient to be sure that the message had come from the sender and nobody else, the sender would cipher some or all of the message with key B. With the ciphered message there would be a "plain-text" instruction that key A should be

[29] above
[30] Paul Krugman, "Golden Cyberfetters", New York Times, " 7 September 2011 (krugman.blogs.ny times.com/2011/09/07/golden-cyberfetters, accessed 21 April 2013)
[31] ie encrypt and decrypt

used to decipher the main message. The recipient would attempt to decipher the main message using A and, if successful, would know for certain that the message originated from the sender. That is because no other person has the ability to encode a message such that A could decode it (only by using B can this be done). Finally, the recipient can be sure that the message had not been altered after the original sender sent it. If the communication had been tampered with, deciphering would only produce nonsense characters and symbols.

Each is Bitcoin 'owned' by a user. That is, each has been recorded as being under the control of a particular wallet and key pair. The person who controls that key pair (via the associated wallet) controls and therefore owns that coin. Unlike previous digital coin systems, each Bitcoin is not actually a packet of data (ie a series of binary digits) kept by the owner on their computer and itself transferred to the new owner in the course of the payment. Instead the payment involves reallocating a coin in the various registers from the payer to payee as set out below.

The user can be anonymous. The holder of the wallet and key pair do not need to identify themselves to any national regulator or financial institution before obtaining the wallet. For this reason, Bitcoins have some attraction to those preferring anonymity, both for political reasons (eg supporters of non-approved political and other movements such as Wikileaks[32]) and those carrying out criminal enterprises.

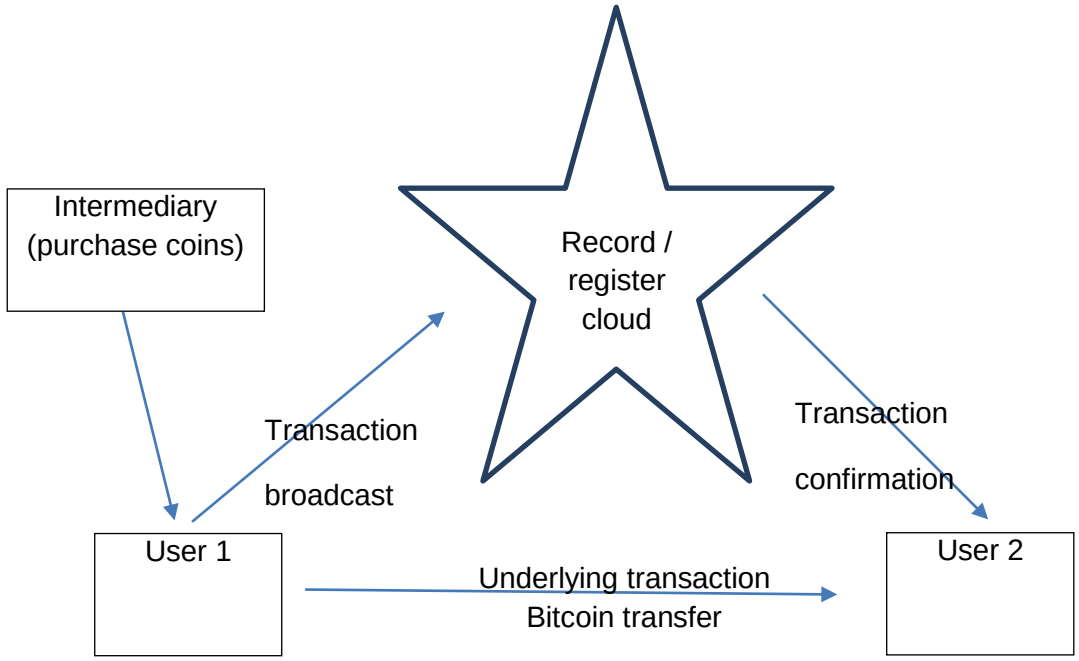
The person controlling the key pair is the *only* one who is able to transfer the associated Bitcoins to another person, whether as consideration for a purchase, payment of a debt or as a gift. They can use their private key as their digital signature, both to show their agreement to the transfer and to authenticate it (ie show that it is a genuine and voluntary transaction).

The wallet and key pair is the only method of accessing the Bitcoins. If the key pair is lost (eg because the PC on which it is stored crashes without a working backup), the coins are inaccessible and are lost (ie will become dormant).

A sample transaction is set out it the diagram below. The payer and payee agree on an underlying transaction (eg sale of online music), and agree that it will be paid for by a set number of Bitcoins. The payer either already has a balance of Bitcoins, or purchases some from an intermediary for this

[32] http://shop.wikileaks.org/donate

purpose. The transfer of coins is made and broadcast into the network. In the Bitcoin system, transfers are irrevocable. They are received by the cloud of record-keeping computers ('nodes'), and if a critical mass of nodes accept the transaction it becomes part of the accepted record and is confirmed. The payee accepts the Bitcoins which are recorded against their wallet, and either holds them for later use or can sell them via an intermediary to obtain regular currency.



With Bitcoin transactions are cheap, and often mostly free. The actual transfer is free – the individuals agree to transfer the coins and the register is updated. No fees attach to these steps. Of course, users pay to acquire Bitcoins, usually from an intermediary or through a market. Users may pay a commission or fee as part of this transaction, either express or implied (ie built into the mark up between the price the intermediary pays to acquire the coins and what it on-sells them for). Those who acquire them as miners also expend time and resources to acquire their coins.

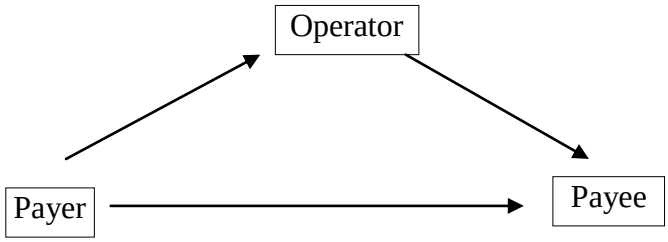
Being a decentralised payment system, and like most open source projects, the more committed users also maintain and manage the system (on a voluntary basis).

> *"The entire network is used to monitor and verify both the creation of new Bitcoins through mining, and the transfer of Bitcoins between users. A log is collectively maintained of all transactions, with*

> *every new transaction broadcast across the Bitcoin network. Participating machines communicate to create and agree on updates to the official log. This process, which is computationally intensive, is in fact the process used to mine Bitcoins: roughly every 10 minutes, a user whose updates to the log have been approved by the network is awarded a fixed number (currently 25) of new Bitcoins. This has prompted Bitcoin fans to build powerful computers, or even to hijack other people's computers, for use in Bitcoin mining."*[33]

The payee needs a way to check that the payer does actually own the Bitcoin being offered as payment. They need to be confident that the payer can and will transfer a valid coin to them. They also need to ensure that the coin hasn't been stolen, and that it also hasn't already been spent or transferred to someone else.

With digital currency, the traditional approach to addressing this issue was to maintain a central register of digital coins. A trusted party records who owns each coin, and transfers (payments) are effected by payers instructing the central register-keeper to reallocate the coin from the payer's to the payee's account.



Unlike previous electronic currencies (eg digital cash, digicash, ecoin), with Bitcoin there is no central register. Instead there are a series of records of the entire history of Bitcoin transactions (the 'registers'). These can be checked to see to which wallet (and key pair) a given coin was last transferred. A coin cannot be on-transferred without a digital signature from that wallet holder, whoever it was last transferred to can be assumed to still be the correct owner and the only party entitled to and capable of transferring it.

While there are multiple transaction records or registers kept in the Bitcoin system, the system protocols check the best record available and rely on it. The various registers are synchronised

[33] TS, "The Economist explains: How does Bitcoin work?" Apr 11th 2013, (http://www.economist.com/blogs/economist-explains/2013/04/economist-explains-how-does-bitcoin-work, accessed 14 April 2013)

across a peer-to-peer network. The best and longest record is the one that prevails. As there are a large number of transaction records and keepers of those records, the system can ensure with a reasonable degree of confidence that there is a neutral, complete and accurate transaction record available at all times. As there are a large number of copies of the register being kept across the network, there is little incentive or gain for any particular register-keeper to falsify the record (eg in an attempt to enrich themselves). Creating a false competing record of equal or longer detail (which would be necessary in any attempt to fool the system) than the others is mathematically very difficult, which also acts as a deterrent. Where there are competing transaction histories, the system allows them to coexist until one of them becomes accepted as authoritative (based on how many nodes adopt it and build on it). Quickly one becomes accepted as the authoritative record and the system proceeds from there. This process of resolving competing records is generally accomplished in a few minutes, such that within about one hour (and often as little as ten minutes) a transaction can be confirmed.

> *"Bitcoin is a solution to the double-spending problem of using a peer-to-peer network to manage transactions. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record or chain that cannot be changed without redoing the proof-of-work. The longest chain of records (called blocks) serves not only as proof of the sequence of events witnessed but also as proof that it came from the largest pool of computing power. As long as a majority of computing power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain of records and outpace attackers."*[34]

The payment system's register and transaction record is essentially kept in the 'cloud'. Each transaction is broadcast immediately across the network. All active 'nodes' add this transaction to their record. There are a large but varying number of nodes keeping records. Transactions are broadcast within seconds and verified within 10 to 60 minutes. This confirmation occurs once the transaction has been included in the new system record by a sufficient number of active nodes, and becomes an accepted part of the total record of Bitcoin transactions (known as the 'block chain').

This delayed confirmation is not ideal for large value real time transactions. However, delayed clearance is familiar in many payment systems, from cheques to direct debits and credits. For small value real time transactions (eg online delivery of digital content) the vendor may be willing to take the risk of insufficient payment and supply the goods before the payment is cleared. And for non-real time transactions (eg online book sales) the payment can still be confirmed in plenty of time to ensure prompt delivery of the goods.

[34] http://en.wikipedia.org/wiki/Bitcoin

The process of keeping and checking the translation history is also part of the process for mining new Bitcoins. This creates some incentive for record keepers (known as nodes or miners in the system) to expend the computational power and energy needed to actively run their record-keeping node. However, one risk inherent in the system is that the number or quality of record keeping nodes will diminish over time, as voluntary register-keepers tire of the effort involved and for-profit nodes become uneconomic as the mining of coins becomes harder and new coins are released more slowly (as provided under the protocols).

The decentralised cloud register is the key innovation that sets Bitcoin apart from previous digital currencies.

> *"A block chain is a transaction database shared by all nodes participating in a system based on the Bitcoin protocol. A full copy of a currency's block chain contains every transaction ever executed in the currency. With this information, one can find out how much value belonged to each address at any point in history.*
>
> *Every block contains a hash of the previous block. This has the effect of creating a chain of blocks from the genesis block to the current block. Each block is guaranteed to come after the previous block chronologically because the previous block's hash would otherwise not be known. Each block is also computationally impractical to modify once it has been in the chain for a while because every block after it would also have to be regenerated. These properties are what make double-spending of bitcoins very difficult. The block chain is the main innovation of Bitcoin."*[35]

Decentralised record keeping in payment systems is not entirely unique. Smart cards, transit cards and traditional passbook accounts work on this basis. Indeed, any product which does not involve real time confirmation of balances and transactions with a central register involves decentralised record keeping to some extent.

As an open source project, the protocols and rules underlying the system are public domain. Security is not based on secret codes and protocols in use, nor private networks and hardware, (unlike many existing services),[36] but a distributed system that makes fraud or attack very difficult and generally uneconomic. There is the risk that a flaw in the protocols may be discovered at some future time, allowing (for example) additional coins to be created or the transaction record to be

[35] https://en.bitcoin.it/wiki/Block_chain

[36] Ben Grubb, "Free ride: students crack ticket algorithm", 12 November 2012, (http://www.smh.com.au/digital-life/consumer-security/free-ride-students-crack-ticket--algorithm-20121112-2984x.html#ixzz2SVxtIuAt, accessed 24 April 2013)

surreptitiously altered. However, to date, no such flaws have been discovered and its supporters believe such a risk to be highly unlikely.[37]

The process is not entirely failsafe, but is an ingenious attempt to create a viable currency without the need for a central register and trusted register-keeper. There have only been occasional reports of significant discrepancies in the register that took more than a few minutes to resolve. One, on 12 March 2013, resulted in competing versions of the transaction log that lasted for a few hours.

> *"This split resulted in two separate transaction logs being formed without clear consensus, which allows for the same funds on both chains to be double-spent. In response, the Mt.Gox bitcoin exchange temporarily halted bitcoin deposits. The price of a bitcoin fell 23% to $37 on the Mt.Gox bitcoin exchange as this event occurred but subsequently rose most of the way back to its prior level of approximately $48. … User funds largely remained unaffected and were available when network consensus was reached. The network reached consensus and continued to operate as normal a few hours after the split."*[38]

Other than miners of coins (ie active members of the system who mine coins by participating in the transaction record keeping and checking process), coins are obtained by either (a) accepting them as payment from another user or (b) purchasing them from a user or intermediary in exchange for some other payment mechanism (eg a credit card or cash).

Money and payment operate by mutual consent and trust. What the parties agree is payment is by definition payment.[39] That is, what constitutes valid payment is largely a matter of contract law. So if a payer and payee agree that transfer of a digital currency such as Bitcoin constitutes payment, it *is valid* payment as between them. This is the underlying transaction in the diagram above.

Any means by which the payer can enrich or transfer value to the payee is a valid payment in an economic sense. And it is likely to be viable if it is sufficiently cheap, convenient, safe and reliable by comparison to other payment options, including cash, credit cards and paper instruments. Virtual electronic currencies like Bitcoin are likely to be an attractive payment method for many consumers and businesses.

[37] https://en.bitcoin.it/wiki/Block_chain
[38] en.wikipedia.org/wiki/Bitcoin
[39] Rhys Bollen, 'What a Payment is (and how it continues to confuse lawyers)' (2005) *MqJBL* 189

Legal status and characterisation

Circulating property rights

Bitcoins are a form of intangible private property, a valuable digital artefact. They are not a contractual promise by or debt owed by one party to another. They are an asset and are the valuable property of their current owner, who can transfer them as and when she pleases.

Bitcoins are analogous with other forms of intangible private property, such as digital music, shares, licenses, trademarks, copyright, goodwill, domain names, frequent flier points and brands. Unlike copyright or trademarks, they are not recognised or protected by international treaty or domestic legislation. This does undermine their legal status, however, as a valuable and transferable form of private property.

Further, unlike a digital music file, frequent flier points or trademarks, Bitcoins have no alternate use – they are purely of token value. They are valueless other than as a currency. However, they have some of the unique properties of a currency missing from (say) a digital music file – Bitcoins are scarce, finite in number, divisible, easily stored and so on.

There is not a clear *issuer* or party responsible for creating, distributing and honouring Bitcoins. A loose collection of individuals cooperate to operate the Bitcoin system. They mine new coins, refine the underlying protocols, and maintain the transaction record and verification system. And this is overseen by the Bitcoin Foundation discussed earlier.

Bitcoin does constitute a payment scheme or system in the general sense. It is clearly a system: "an assemblage or combination of things or parts forming a complex or unitary whole".[40] It is also clearly a scheme, being "any system of correlated things, parts, etc., or the manner of its arrangement".[41]

While it is based on a group of loosely coordinated actors together implementing a common scheme or system, unlike most payment systems the participants are not bound by a set of express contracts committing them to central rules. There *are* central rules and protocols, however, which are hard-wired into the system. It is arguable that participants consent to abide by the central rules and

[40] Macquarie Dictionary online, 26/4/2013
[41] Macquarie Dictionary online, 26/4/2013

protocols, and indicate this by their initial and continued participation. Indeed, many contractual arrangements in the financial services industry involve acceptance by this type of conduct rather than express words, whether oral or in writing.

Participants who are intermediaries (ie buying Bitcoins from and selling Bitcoins to users in exchange for regular currency) in the system generally do so on a commercial basis and will be bound by the general commercial and contractual laws that apply to financial intermediaries. The same is true for those organisations that conduct a market where users can themselves buy and sell Bitcoins. The best known such market is MtGox.[42] As will be seen in the next section, the regulatory arrangements applying to these two special groups of participants (intermediaries and market operators) should be similar to those for other financial services firms conducting such activities.

At their core, most payment facilities rely on contracts to set out the rights and responsibilities of each party.[43] Legislation, common law and industry codes also have some impact. That is, the contracts do not set out exhaustively the rights and responsibilities of each party.[44] For example, the *Australian Securities and Investments Commission Act 2001* (Cth) (ASIC Act) prohibits providers of financial services engaging in unfair terms, unconscionable, harassing or misleading conduct.[45]

Almost all payment facilities operate through the creation, transfer and cancellation of rights; usually in the form of debt obligations.[46] However, the rights may also take other forms, such as bailment. The number of steps and their order varies, but the broad concept remains the same. As a general rule, in "modern society, all payments have one or two basic foundations, namely cash, or an instruction to transfer a claim to cash."[47] Virtual currencies may not fit this traditional analysis, however. They do operate via the creation and circulation of rights. However, these rights are not a claim to cash. They are simply a valuable tradable right. [Negotiable instrument / bill of exchange analogy?]

[42] www.mtgox.com
[43] D Kreltszheim "The legal nature of 'electronic money': Part 1" (2003) 14 JBFLP 161, at 163; Tyree Dr A, "The Legal Nature of Electronic Money" (1999) 10 JBLFP 273 at 273; Beatty A, Aubrey M and Bollen R, "E-payments and Australian regulation" (1998) 21 UNSLJ 489, at 494.
[44] Tyree Dr A, "The Legal Nature of Electronic Money" at 273-274; cf Galvin A, "The Legal Nature of Stored Value Transactions" (1999) 10 JBFLP 54, at 56.
[45] Sections 12CA, 12CB and 12DJ of the *Australian Securities and Investments Commission Act 2001* (Cth).
[46] Blay S and Clark E, *Australian Law of Financial Institutions* at [9.02]; Tyree Dr A, "Digital Cash in Australia" (1998) 9 JBFLP 5.
[47] Weerasooria WS, Banking Law and the Financial System in Australia (5th ed, Butterworths, 2000) at [7.2].

Compare, for example, the simple goldsmith's scenario. The goldsmith is bailee of the payer's gold, following the payer's earlier deposit of gold with the goldsmith. The payer is obliged to pay the payee some money – for example, to cover the purchase of some timber. If the payee is agreeable, the payer pays for the timber not in cash but by giving the payee rights against the goldsmith of a value equal to the purchase price.

Rights to goods other than by way of bailment can also be circulated as a payment scheme. For example, some gift vouchers are designed as rights to acquire or receive goods in the future. Depending on the circumstances, these rights could themselves be circulated between parties as the basis for a payment scheme (for example, gift vouchers are often given as rewards to employees).

Rights to services can also be circulated to form the basis of a payment scheme. It can work in much the same way as the circulation of rights to gold or other goods. For example, the value transferred could be the right to use a transport or telecommunications service in the future.[48] Depending on the circumstances, these rights could be circulated between parties as the basis for a payment scheme. Again, the core of the system is the presence of rights that are valuable, transferable and contractually based.

A debt-based payment scheme can be illustrated by a simple historical banker's scenario. The banker is indebted to the payer, who earlier deposited money with her. The payer is obliged to pay the payee some money – for example, to cover the purchase of some clothes. If the payee is agreeable, the payer pays for the clothes not in cash but by giving the payee monetary rights against the banker of an amount equal to the purchase price.

Account-based facilities?

[48] A prepaid transport or telephone card could be used as the core of a payment system. If multiple parties were willing to accept as payment the tender of a prepaid transport card, then the card could be used as the basis for the payment system. Each payer would tender one or more cards when making a payment, which they would transfer to the payee (presumably by delivery). This is the logic behind many mobile phone payment systems in the developing world, eg mPesa in Kenya.

Many commentators have distinguished between account-based facilities on the one hand and stored value facilities on the other.[49] They also imply that it is only those facilities where an account is present that are based on the circulation of liabilities via one or more financial intermediaries and that non-account based facilities transfer funds by some other method.[50] Stored value facilities are sometimes alternatively described as token, electronic money or embedded rights facilities. As will be seen below, with respect this author believes the above is an unfortunate and often unhelpful dichotomy. But because it is a distinction established in the literature and some legislation (and quasi-legislation),[51] it is considered below. Since there is little case law on these relatively new products, there is yet to be consensus reached on the appropriate legal characterisation of these products.[52]

Bank style products like cheque accounts are clearly account-based.[53] At the fundamental core of the system is the account maintained by the intermediary for each payee and payer and, at a lower level in the system, between each intermediary with a final settlement authority such as a central bank. Each transaction in this system involves the debiting and crediting of two or more accounts, with the active participation of the keepers of those account records (the financial intermediaries).[54] Indeed, with these facilities the payment transaction cannot be effected *but for* the cooperation of the account-keepers. Further, the balance of each account is at all times known by the account-keeper. For example, if a person attempts to spend more than the account balance (or credit limit), the account-keeper will refuse the transaction and the payment won't proceed. In fact, almost all current non-cash payment schemes are account-based, at least those of an electronic nature.[55]

This has led some people to conclude that a scheme *must* involve the active co-operation of an account keeper (eg an issuer), in each transaction, in order to be account-based (ie based on debiting and crediting of intermediary accounts). Taken further, it has been suggested that, in order to be

[49] For example, Kreltszheim D "The Legal Nature of 'Electronic Money': Part 1" at 174; D Kreltszheim "The Legal Nature of 'Electronic Money': Part 2" (2003) 14 JBFLP 261 at 267; cf Tyree, Tyree Dr A, "The Legal Nature of Electronic Money", at 274.
[50] Taken to the extreme, the argument is that if the scheme is not "account-based" it is not based on the circulation of institutional liabilities.
[51] Financial Services Authority, Handbook of rules and guidance, "Electronic Money"; *Payment Systems (Regulation) Act* 1998, EFT Code (ASIC).
[52] Kreltszheim, D "The Legal Nature of 'Electronic Money': Part 1" at 172.
[53] Kreltszheim, D "The Legal Nature of 'Electronic Money': Part 1" at 168.
[54] Blay and Clark, *Australian Law of Financial Institutions* at [9.02].
[55] Kreltszheim, "The Legal Nature of 'Electronic Money': Part 1" at 167. There are some paper-based systems relying on a negotiable instrument model, although many of these are account based as well in its broadest sense (ie they do also rely on the circulation of institutional liabilities for their fundamental effectiveness).

account-based, the account-keeper must positively know (or at least have the means to ascertain) each customer's balance at all times.[56] However, this is an unnecessary, and in the author's view undesirable, general deduction from the specific case. While it is true that many account-based facilities involve the active participation of account-keepers for every transaction, it is not therefore true that all account-based facilities must by definition have this feature.

Traditional passbook-based banking products predate the electronic banking revolution. In some cases the passbooks were effectively mirror records of the balance and transaction data held at the bank's ledger. But in other cases the passbook contained the *only* record of that customer's balance and transactions. However, few if any would say this product was other than an account-based one. It was a debt product, and based on traditional analysis the client's rights were a debt measured using a decentralised account-based recording system. Tyree has by analogy shown that an electronic 'stored value' system is no different in substance to a passbook-based system. They are both account-based systems with distributed or decentralised account keeping.[57]

Some payment facilities are less clearly account-based. With some facilities, the issuer does not know at all times the balance of each client, nor is the issuer consulted at the time of each transaction to check that the payer has adequate funds. The issuer will of course have measures in place to protect its interests and ensure that it is not materially out-of-pocket, as will the merchant. So issuers usually provide merchants (payees) with an alternate means of checking the payer's ability to pay before accepting a payment.

With newer microchip-based facilities, each smart card can maintain its own balance record.[58] Modern chip-based debit and credit cards can accept certain transaction offline, with the amount thresholds set by the issuer, and store balance and transaction information until next online.[59] Assuming the technology is reasonably secure, payers and payees can have some confidence that only valid payments will be able to proceed. Take for example an anonymous smart card able to process payments offline. Let us assume the card can be used to effect payments at vending machines and other merchants not continuously linked to the issuer (eg buses and trains). The vending machine does not need to contact the issuer before accepting each payment. Instead, the

[56] Kreltszheim, "The Legal Nature of 'Electronic Money': Part 2" at 267.
[57] Tyree, "The Legal Nature of Electronic Money", at 275.
[58] Smart Card Alliance, EMV FAQs (http://www.smartcardalliance.org/pages/publications-emv-faq, accessed 1 May 2013)
[59] Smart Card Alliance, EMV FAQs

vending machine keeps track of transactions made with it and each card keeps a record of transactions which its holder has made. These records are reconciled with the issuer's records periodically when the card is presented for recharging or when the vending machine operator periodically settles with the issuer (eg monthly). It is in many ways a decentralised form of ledger or account keeping.[60]

Does the fact that the issuer doesn't know the balance of each holder at all times, and that the merchant need not confirm a payment with the issuer before accepting it, mean that the transaction is inherently different to a conventional account transaction? No. In the smart card example, the system still relies on the maintenance of customer accounts.[61] The intermediary will almost certainly reconcile records from each card with records from each merchant intermittently and will have processes in place, including on the card itself, to ensure that the card accurately keeps track of the holder's balance. This is to ensure that the intermediary is not obliged to settle payment transactions in excess of value deposited[62] by customers. [63]

With the exception of cash, almost all current payment facilities operate on the basis of accounts kept by trusted intermediaries.[64] A card or token-based system requires that merchants are willing to accept something less than cash as payment. They will do this only if they are confident of receiving later reimbursement from a trusted third party (the issuer). They effectively keep a record of what the issuer owes them and settle that "account" with the issuer periodically. It is therefore still an account-based system, even if the issuer does not directly maintain the account.

The preceding arguments are not to deny there are substantial differences in character between more centralised payment facilities like cheque accounts and less centralised facilities like anonymous "smart" cards able to process payments offline, nor is it to deny that different regulatory and policy issues may arise, or may apply differently, to different payment facilities. For example, unauthorised transactions necessitate a different response for anonymous and offline products compared with identified and online products. Similarly, the risk allocation for lost and stolen cards. However, they

[60] Kreltszheim, "The Legal Nature of 'Electronic Money': Part 2", at 268.
[61] Tyree Dr A, Banking Law in Australia (4th ed, Butterworths, 2002) at [37.3].
[62] Or prepaid or credit.
[63] Tyree Dr A, "The Legal Nature of Electronic Money" at 276.
[64] Tyree Dr A, Banking Law in Australia (4th ed, Butterworths, 2002), at [37.3].

are each in essence account-based facilities in the sense that they depend at some level on an account record maintained by the issuer or on its behalf and for its benefit.[65]

Bitcoin appears to be a decentralized account based payment system without an issuer or central counterparty. It involves the circulation of valuable rights but not rights to cash as such. The valuable rights are a form of intangible property, transferred irrevocably and immediately (albeit with delayed confirmation) by electronic order.

However, Bitcoin is still an account-based payment system. Coins themselves are not stored on a user's device. While the register is kept by multiple collaborating nodes, the block chain keeps a full record of transactions and by a process of deduction a balance for each user. This is effectively the transaction history and account record for the parties. All transactions are recorded on and confirmed by the block chain system. Transactions can only occur and be confirmed via the central transaction record. No offline transactions are possible. Therefore, in this author's view, the Bitcoin system is an account based payment system, albeit with decentralized account keeping by a cloud of autonomous but cooperating account record keepers.

Regulatory status

There are a number of elements to a discussion about the regulatory status of Bitcoin. In most countries, the following groups of issues arise:

- general financial services regulation,
- specific banking regulation, and
- currency regulation and legal tender.

This article will consider each in turn, and illustrate them by reference to the prevailing regulatory regimes in the US, EU, UK and Australia.

[65] Tyree, Banking Law in Australia at [37.3].

Financial services regulation

Most developed jurisdictions have a regime for dealing with broad consumer protection and market integrity issues in the financial services industry. Each jurisdiction defines the products and services to be covered by such a regime in different ways. In the more modern regimes (eg UK, EU, Australia), payment products and electronic money are included. For example, in Australia Bitcoins would appear to be a financial product. The analysis is as follows.

Australia

ASIC regulates *financial services* that relate to *financial products* (both widely defined) under the *Corporations Act 2001*. Services include advice and issuing, and products include non-cash payment facilities, investment facilities and deposit products.

As discussed above, Bitcoins are valuable rights and intangible property. A facility includes "intangible property", "an arrangement or a term of an arrangement (including a term that is implied by law or that is required by law to be included)" or "a combination of intangible property and an arrangement or term of an arrangement".[66] Bitcoin is therefore a facility.

Bitcoins are clearly used to make non-cash payments. Under the Corporations Act, "a person makes non-cash payments if they make payments, or cause payments to be made, otherwise than by the physical delivery of Australian or foreign currency in the form of notes and/or coins".[67] Bitcoins are not a physically deliverable currency and therefore the Bitcoin system is means of making non-cash payments. They are, include or are part of a facility for making non-cash payments.

Combining these two concepts, Bitcoin is a facility through which, or through the acquisition (and transfer) of which, people make non-cash payments. As such, they appear to be an example of a financial product under Australian law.

The next part is more complex. Clearly, Bitcoins are made available to users. In this sense, the author would argue that they are *issued:* "a financial product is issued to a person when it is first

[66] Corporations Act, s762C
[67] s763D

issued, granted or otherwise made available to a person".[68] Bitcoins are probably issued when they are first mined and brought into existence within the system according to the system protocols.

However it is unclear whether there is a person or group of persons (eg a partnership or association) who in a legal sense *issues* the product. Generally under Australian law the issuer is the person or persons responsible for honouring or performing any obligations under the facility. Specifically:

> *"(4) Subject to this section, the issuer, in relation to a financial product issued to a person (the client), is the person responsible for the obligations owed, under the terms of the facility that is the product:*
>
> *(a) to, or to a person nominated by, the client; or*
>
> *(b) if the product has been transferred from the client to another person and is now held by that person or another person to whom it has subsequently been transferred—to, or to a person nominated by, that person or that other person.*
>
> *Note: For example, the issuer of a direct debit facility is the financial institution with which the account to be debited is held, rather than the persons to whom payments can be made using the facility." (s761D)*

Bitcoins do not appear to have an *issuer* in this sense. They do not have someone who is the counterparty to coins, who is obliged to honour them or perform obligations owed under them (eg to execute transactions).

A court may perhaps interpret the above section as inclusive in its meaning of issuer. If so, they may be willing to consider that the informal consortium of Bitcoin miners and record keepers *are* the issuers of the currency. They are certainly the parties creating and making the currency available to users in a broad sense. The law already accepts the concept of joint issuers, whether acting under a formal or informal arrangement.

The Bitcoin system is an organised arrangement governed by a set of rules and protocols. It is decentralised, without an operator or governor. It has a governing body of sorts in the Bitcoin Foundation discussed earlier.

[68] s761D(2)

On balance, it appears that Bitcoins probably do not have an issuer in the legal sense under the Act. This is not a fatal flaw in the regulatory regime however, as we will see shortly. Indeed, it may well be an inspired piece of drafting, albeit probably unintended.

The next question is whether any financial services are being provided *in relation to* those financial products (the Bitcoins). If so, the providers of these services, if doing so as part of a business, may need to hold an AFS licence.[69]

People do acquire and dispose of Bitcoins, so do deal in them.[70] Many do so for their own consumer purposes (ie exempt self-dealing).[71] Some people act as intermediaries, in that they sell Bitcoins to or purchase Bitcoins from users for regular money. This may be a financial service of dealing, making or operating a market. Others operate markets in Bitcoins (eg MtGox as referred to earlier).[72] Some parties provide users with advice about such coins. These are examples of a regulated financial service under the Act.

Intermediaries who are carrying on a business (ie system, repetition, regularity, not necessarily profit) of buying and selling Bitcoins (either on their own balance sheet or as agents for users) will be carrying on a financial services business. They will therefore require a licence unless one of the various exemptions apply.[73]

As there is no issuer in a technical legal sense, there will be no mandatory consumer friendly product disclosure statement. Unlike regular retail banking and payment services (eg cheque accounts, online payment services like PayPal), no there will be no Product Disclosure Statement setting out the features, risks, fees and charges.

US

The legal framework governing payment services as well as the regulatory structure for financial institutions that provide payment services in the United States is complex and somewhat fragmented.

[69] Part 7.6, Corporations Act 2001
[70] s766C
[71] S766C
[72] www.mtgox.com
[73] Part 7.6, Corporations Act 2001

Financial institutions are chartered at either the state or federal level, and are supervised by one or more agencies at the state or federal level, or both.

The United States' model law on funds transfers, Article 4A of the Uniform Commercial Code, may be relevant here. Most US states have adopted Article 4A. This deals with various issues surrounding non-cash payments, including the passing of risk from payer to payee, the revocability of payments, and the rights and obligations of each party to a funds transfer.[74]

For the purposes of Article 4A, a payment order is defined as 'an instruction of a sender to a receiving bank, transmitted orally, electronically, or in writing, to pay, or to cause another bank to pay, a fixed or determinable amount of money to a beneficiary' where:

- the instruction is unconditional, 'the receiving bank is to be reimbursed by debiting an account of, or otherwise receiving payment from, the sender', and

- the instruction is transmitted by the payer to their bank or to an agent, funds transfer or communication system for transmission to the payer bank.[75]

Article 4A is deliberately limited to funds transfers through the banking system, and excludes payments via remittance dealers and other arrangements.[76] The Article defines a bank as 'a person engaged in the business of banking and includes a savings bank, savings and loan association, credit union, and trust company'. The requirement for a transfer through the banking system means that the Article will not apply to virtual currencies like Bitcoin at this time.

Most states have broadly defined money transmission regimes. They apply to services to move money from one person to another by any means. Most money services business regimes have been amended in recent years to cover stored value also. Most have updated their money transmission regime from a remittance dealer type regime to cover stored value products broadly defined also.

[74] B Geva, *Bank Collections and Payment Transactions*, Oxford University Press, 2001, at 213, 290.
[75] § 4A-103(a)(1).
[76] ALI & NCCUSL, *Official Commentary on Article 4A*, Commentary to § 4A-104.

The Financial Crimes Enforcement Network of the Department of the Treasury (**FinCEN**) has defined money services businesses to include five distinct types of financial services providers, being:

- currency dealers or exchangers;
- cheque cashers;
- issuers of traveller's cheques, money orders, or stored value;
- sellers or redeemers of traveller's cheques, money orders, or stored value; and
- money transmitters.

For the first four categories, a firm is only regulated if it "engages in such transactions … in an amount greater that $1,000 for any person on any day in one or more transactions".[77] Some money services business principals are required to register with FinCEN. Additionally, many states require money services businesses to obtain a license

FinCEN appears to be taking a similar approach to that discussed above in relation to the general purpose financial services regime in Australia.

> *"The Financial Crimes Enforcement Network ("FinCEN") is issuing this interpretive guidance to clarify the applicability of the regulations implementing the Bank Secrecy Act ("BSA") to persons creating, obtaining, distributing, exchanging, accepting, or transmitting virtual currencies.1 Such persons are referred to in this guidance as "users," "administrators," and "exchangers," all as defined below.2 A user of virtual currency is not an MSB under FinCEN's regulations and therefore is not subject to MSB registration, reporting, and recordkeeping regulations. However, an administrator or exchanger is an MSB under FinCEN's regulations, specifically, a money transmitter, unless a limitation to or exemption from the definition applies to the person. An administrator or exchanger is not a provider or seller of prepaid access, or a dealer in foreign exchange, under FinCEN's regulations."*[78]

[77] FinCEN Advisory, 'Guidance to money services businesses on obtaining and maintaining banking services', 26 Apr. 2005.
[78] US Treasury Financial Crimes Enforcement Unit, FIN-2013-G001,: March 18, 2013, "Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies"

That is, persons carrying on a business of broking Bitcoins (ie buying and selling them in exchange for regulator currency) or running an organised exchange will be regulated as financial services firms, but not a user. This author suggests that this is the appropriate approach here.

EU and UK

The recent EU Payment Services Directive probably does not extend to virtual currencies. As such, these products will probably not require licensing under this regime in the EU, including the UK.

The Directive covers e-money issuers, credit institutions, 'post office giro institutions',[79] and payment institutions authorised under the Directive.[80] Payment services are defined as "the execution of payment transactions on behalf of a natural or legal person" carried on as a 'business'.[81] The latter proviso is presumably intended to incorporate the common law concept of carrying on a business and to exclude services carried on without system, repetition and regularity.[82] Payment is defined broadly, as "the act, initiated by the payer or by the payee, of depositing, withdrawing or transferring funds from a payer to a payee, irrespective of any underlying obligations between the payment service users".[83]

The payments services covered by the Directive include:

- cash deposits to a payment account,
- cash withdrawals from a payment account,
- execution of "payment transactions, including transfer of funds, where the funds are held on deposit in a payment account", including direct debits, payment card transactions and credit transfers,[84]
- payments from a line of credit, including direct debits, payment card transactions and credit transfers,

[79] See Directive 2000/12/EC
[80] Article 6
[81] Article 2(1)
[82] *Hungier v Grace* (1972) 127 CLR 210; *Ferguson v FCT* (1979) 9 ATR 876
[83] Article 2(1)
[84] Annex to the Directive

- issuing and/or acquiring payment cards that allow funds transfers,
- electronic funds transfers involving e-money,
- "money remittance" services,[85] and
- execution of payment transactions "where the consent of the payer to a payment transaction is transmitted by means of any telecommunication, digital or IT device" and the payment is made to the service provider who is acting solely on behalf of the payment service user.[86]

There are a number of activities excluded from the Directive, including cash payments and refunds, currency exchange, cheque payments, vouchers and cards for closed networks,[87] and payments within a securities clearing and settlement system.[88]

> *"Another European law that might have some relevance to virtual currency schemes like Bitcoin is the Payment Services Directive (2007/64/EC). This Directive lays down rules on the execution of payment transactions where the funds are electronic money, yet it does not regulate the issuance of electronic money, nor does it amend the prudential regulation of electronic money institutions as provided for in the Electronic Money Directive. Therefore, the new category of payment service provider it introduces – payment institutions – should not be allowed to issue electronic money. As a consequence, Bitcoin clearly falls outside the scope of the Payment Services Directive."*[89]

Again, the lack of an issuer or party responsible to fulfil obligations under the facility means the Bitcoin system is unlike to be a payment service under the Directive.

In contrast to the Australian and United States approaches, the European Community has limited the issuing of "electronic money" to banking or similarly regulated institutions.[90] This is "due in large

[85] Annex
[86] Annex
[87] "services that can be used to acquire goods or services only within a limited network of affiliated service providers and are based on instruments like vouchers and cards in so far as such instruments are not redeemable". This appears to cater for small scale schemes like University campus and shopping centre cards.
[88] Article 3
[89] ECB, Virtual currency schemes, October 2012, 43
[90] European Parliament, *Directive 2000/46/EC on the Taking Up, Pursuit of and Prudential Supervision of the Business of Electronic Money Institutions* (2000) http://europa.eu.int viewed 26 February 2005.

part to the general agreement among European policy analysts that issuing electronic currency is equivalent to taking bank deposits".[91] E-money is defined as

> *"monetary value as represented by a claim on the issuer which is:*
>
> *(i) stored on an electronic device;*
>
> *(ii) issued on receipt of funds of an amount not less in value than the monetary value issued;*
>
> *(iii) accepted as means of payment by undertakings other than the issuer."*[92]

There are essentially three criteria for determining whether a product is e-money. There needs to be an electronic device, on which value is recorded that was originally issued in return for funds equal to (or exceeding) the stored value, and merchants other than the issuer must accept the e-money.[93]

In the United Kingdom, issuers of electronic money need to hold an authorisation from the Financial Conduct Authority (**FCA**).[94] The FCA regime imposes conduct and disclosure obligations on issuers, as well as requiring minimum capital, product disclosure and dispute resolution processes.[95]

> *"Can Bitcoin be considered an electronic money institution? Bitcoin probably complies with the first and the third criteria, but not with the second. Moreover, it is important to consider the conversion into another currency, which was clearly not envisaged in the Directive. In fact, Art. 11 explicitly says that "Member States shall ensure that, upon request by the electronic money holder, electronic money issuers redeem, at any moment and at par value, the monetary value of the electronic money held". This cannot be ensured in a virtual currency scheme like Bitcoin (or in any other Type 3 scheme). A last key aspect that should be taken into account is the "mining" activity, which leads to money creation without the receipt of funds.1 It is difficult to assess how this could be interpreted within the scope of the Directive."*[96]

Virtual currencies are probably not e-money as defined in the EU directive as they are not issued in return for money.[97]

---

[91] B Smith and R Wilson, "The Electronic Future of Cash: How Best to Guide the Evolution of Electronic Currency Law", at 1,113.
[92] Article 1
[93] European Commission, *Commission Staff Working Document on the Review of the E-Money Directive (2000/46/EC)*, Brussels, 19 July 2006, SEC(2006) 1049, at 11
[94] FSA Handbook (http://www.fsa.gov.uk/Pages/handbook/ viewed 26 February 2005)
[95] FSA Handbook (http://www.fsa.gov.uk/Pages/handbook/ viewed 26 February 2005)
[96] ECB, Virtual currency schemes, October 2012, 43
[97] Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 On the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC

Hence Bitcoin participants will probably not require licensing or disclosure under the EU (and in member states like the UK). Intermediaries and market operators will not require a licence to deal in this product either. That is, unlike the US and Australian approach, the EU and UK approaches are not designed in a way to easily cater for payment facilities without a clear issuer.

Banking regulation

Banking regulation centres on deposit-taking institutions. While the definitions vary, the scope generally focusses on organisations that accept deposits, make payments on behalf of clients and make loans to third parties. The Bitcoin system by itself does not meet this definition.

> *"The case for regulation will get stronger as the infrastructure supporting Bitcoin (or its successors) becomes more sophisticated. There are already Bitcoin banks, for instance. If digital banks start to mimic conventional lenders and make loans that exceed the amount of deposits they keep on hand, the system will become prone to runs. Banking regulators will need to step in (after hi ring some computer whizzes)."*[98]

In most countries, deposit taking services are regulated more intrusively than other financial services. There are a range of definitions of 'banking', but most include taking money on deposit from customers and lending that out again and/or providing payment services linked to that deposit.[99]

Australia

In Australia, prudential supervision is divided between the Reserve Bank of Australia (RBA) and the Australian Prudential Regulation Authority (APRA). The payments system as a whole is supervised by the RBA at a systemic stability and efficiency level. The RBA is also a prudential regulator for "purchased payment facilities".[100]

Deposit-taking institutions are supervised by APRA, including operators of those purchased payment facilities available for use on a wide basis and where the outstanding value can be redeemed for

[98] The Economist, "Digital currencies: A new specie" 13 April 2013
[99] Commissioners of the State Savings Bank of Victoria v Permewan Wright & Co Ltd (1915) 19 CLR 457; United Dominions Trust Ltd v Kirkwood [1966] 2 QB 431
[100] Tyree and Beatty, *The Law of Payment Systems*, p 25.

cash.[101] The precise overlap between the RBA and APRA's prudential supervision of payment facilities is unclear and a regime having two prudential regulators is unnecessarily complicated, not to mention contrary to the initial Wallis Committee recommendations to bring financial sector prudential regulation under one agency, the new APRA.[102] Which regulator has supervisory responsibility for a given facility depends on the extent to which the purchased payment facility is available for use on a wide basis and whether the outstanding value can be redeemed for cash.[103]

For historical reasons, in Australia only those institutions that both take deposits and make loans were required to be licensed as banks. United States courts have also taken a similar approach.[104] The United States approach focuses regulatory attention on "the potential abuses associated control over commercial credit when combined with the bank's role as a depository of funds".[105] The rationale is that "the safety of customer deposits" is less at risk where the deposit-taker is not also in the business of commercial credit.[106]

Following the Wallis report,[107] a new concept of an authorized deposit-taking institution was inserted into the *Banking Act*.[108] An ADI is a company that has received an authority to conduct "banking business" from APRA.[109] Banking business is defined as:

> *"(a) a business that consists of banking within the meaning of paragraph 51(xiii) of the Constitution; or*
>
> *(b) a business that is carried on by a corporation to which paragraph 51(xx) of the Constitution applies and that consists, to any extent, of:*
>
> *(i) both taking money on deposit (otherwise than as part-payment for identified goods or services) and making advances of money; or*
>
> *(ii) other financial activities prescribed by the regulations for the purposes of this definition."*[110]

[101] *Banking Regulations 1966* (Cth).
[102] Wallis Report, 1997
[103] *Banking Regulations 1966* (Cth); Tyree, n 134.
[104] Conjura C, "Comment: Independent Bankers Association v Conover: Nonbank banks are not in the business of banking" (1986) 35 *American University Law Review* 429 at 430; Symons, n 25 at 678.
[105] Conjura, "Comment: Independent Bankers Association v Conover: Nonbank banks are not in the business of banking", at 448.
[106] Conjura, "Comment: Independent Bankers Association v Conover: Nonbank banks are not in the business of banking", at 449.
[107] Wallis Report.
[108] ss 5, 9(3)
[109] s 9

The combination of the concepts of deposit-taking and advance encompasses a wide range of financial services. This is much broader than the traditional notion of a bank and includes building societies, credit unions, friendly societies and the like.[111] It may also extend to the operators of some other payment systems, such as some credit and charge cards.

A fairly recent addition to financial sector regulation in Australia is the *Payment Systems (Regulation) Act 1998* (Cth) (PSR Act). It establishes a separate scheme for the regulation of purchased payment facilities, being those (s 9):

> *"purchased by a person from another person ... able to be used as a means of making payments up to the amount that, from time to time, is available for use under the conditions applying to the facility ... [and where] those payments are made by the provider of the facility or by a person acting under an arrangement with the provider of the facility (other than the user of the facility)."*

The holder of the stored value of such a facility, being the provider of the facility or another person who makes the payments referred to above, is regulated under the PSR Act. This is to ensure the stability of the facility itself and payment systems generally.[112] To lawfully be the holder of stored value, a corporation must either have an authority from APRA to carry on banking business, or an authority or exemption granted by the RBA under the PSR Act.[113]

Issuing or distributing Bitcoins alone is not banking business. The relevant person must be taking deposits and making loans. One or both limbs could be denominated in Bitcoins. Accepting deposits denominated in Bitcoins and making loans, should this business model arise, would probably be covered.

Nor are Bitcoins purchased payment facilities. There is no issuer or operator who makes payments as directed by the customer. The decentralised nature of Bitcoin means that there is no provider of the facility who is committed to making payments as and when directed by customers. The definition does not cater for decentralised systems without a coordinating issuer and operator.

---

[110] s5, Banking Act

[111] For example, there is no longer any differentiation based on whether the funds are only lent to members.

[112] House of Representatives Explanatory Memorandum, Ch 5 (discussing *Payment Systems (Regulation) Act 1998* (Cth), Pt 4); Beatty et al, "E-payments and Australian Regulation", at 502.

[113] Payment Systems (Regulation) Act 1998 (Cth), ss 9(3), 23, 25; Beatty et al, "E-payments and Australian Regulation", at 502-504.

Bitcoin participants will probably not require licensing or disclosure under the Australian banking regimes. However, taking deposits and making loans denominated in Bitcoin currency would probably attract the attention of Australian regulators. The author submits that this is probably the most desirable public policy response, being technologically and functionally neutral.[114]

United States

Bank regulation in the United States is more fragmented than other G20 countries, where most countries have only one bank regulator. In the US, banking is regulated at both the federal and state level. Depending on a banking organisation's charter-type and organisational structure, it may be subject to numerous federal and state banking regulators. Unlike Singapore, Australia and the United Kingdom, where prudential regulatory authority over the banking and insurance industries is combined into one single agency, the US maintains separate prudential regulators for banking and insurance firms, and at both the federal and state levels.

There is no one definition of banking or deposit-taking applying across the US financial regulatory system. However, by way of illustration, the *Wall Street Reform and Consumer Protection Act* defines it as:

> *(a) the acceptance of deposits, maintenance of deposit accounts, or the provision of services related to the acceptance of deposits or the maintenance of deposit accounts;*
>
> *(b) the acceptance of funds, the provision of other services related to the acceptance of funds, or the maintenance of member share accounts by a credit union; or*
>
> *(c) the receipt of funds or the equivalent thereof, as the Bureau may determine by rule or order, received or held by a covered person (or an agent for a covered person) for the purpose of facilitating a payment or transferring funds or value of funds between a consumer and a third party.*[115]

'Policy makers at the state level also have demonstrated reluctance to unduly restrict issuance rights of financial institutions.'[116] As such, few have demanded that electronic payment facility issuers obtain a banking licence. The Federal Reserve Board and the Federal Deposit Insurance Commission have taken much interest in new payment facilities (e.g. smart cards and electronic cash), but in

[114] R Bollen, "Best practice in the regulation of non-cash payment services" (2011) 22 JBFLP 147
[115] Title 12. Banks and Banking; Chapter 53.
[116] B Smith and R Wilson, "The Electronic Future Of Cash: Article: How Best To Guide The Evolution Of Electronic Currency Law" (1997) 46 American University Law Review 1105 at 1112.

general have not required the issuers to hold a banking authorisation. 'Addressing each of the three prerequisites for a deposit, the FDIC concluded that generally stored value cards do not qualify as deposits because the money is not held on behalf of a customer nor for a special purpose.'[117]

Consistent with the Australian analysis, Bitcoin participants will probably not require licensing under the US banking regimes. However, taking deposits and making loans denominated in Bitcoin currency would probably attract the attention of US regulators. The author submits again that this is probably the preferable public policy response.

EU and UK

Banking services are regulated under a number of pieces of EU legislation. The EU regulates the carrying on of banking business by credit institutions broadly in accordance with the Basel Accords.[118] There have been a number of European banking directives, the most recent major one being the Directive 2006/48/EC of the European Parliament and of the Council of 14 June 2006 relating to the taking up and pursuit of the business of credit institutions (2006 Directive).

The 2006 Directive applies to credit institutions broadly defined, not just banks in the conventional sense. Credit institutions are defined as an undertaking whose business is to receive deposits or other repayable funds from the public and grant credit from its own account.[119] As above, virtual currencies are unlikely to meet this definition.

> *"In the meantime, some initial attempts to define the legal status of Bitcoin are already happening in Europe. The French law courts are looking into the issue after local banks shut down the currency exchange facility for accounts handling the currency, on the presumption that Bitcoin should conform to electronic money regulations."*[120]

Currency and legal tender

[117] Catherine Wilson 'Banking On The Net: Extending Bank Regulation To Electronic Money And Beyond' (1997) 30 Creighton Law Review 671 at 695.
[118] See http://www.bis.org/bcbs/index.htm
[119] Article 4
[120] ECB, Virtual currency schemes, October 2012, 43

A currency is money in any form in actual use or circulation, as a medium of exchange, especially circulating paper money and coins. The simplest and strongest example is banknotes and coins, being the physical tokens used for money by a government.[121] Currency is its broader meaning is synonymous with money, being anything that is used as a medium of exchange.

When used in legal contexts, currency is a system of money in common use, especially in a nation. This would include British pounds, US dollars, and European euros in their various contexts. Currencies in this sense are not necessarily physical commodities. They are stores of value that may be traded electronically and cross-border (eg through foreign exchange markets). However, they usually have a primary area of usage and acceptance (in their national geographical boundaries). Some currencies are widely used outside the country of issue, such as US dollars.

It is also possible for currencies to be internet-based and purely digital (ie with no associated notes or coins). Examples include Bitcoin, Ripple Pay or MintChip. These need not be tied to any specific country.[122]

Currency use is based on the concept of *lex monetae*; that a sovereign state decides which currency it shall use.[123] In most countries, the national government or its agent is the only party authorized to produce and distribute physical currency (fiat money) in its geographical area of control. It also regulates the production of non-physical currency (money) by banks (credit) through its monetary policy, usually implemented via the central bank. In some countries, alternate currencies are permissible, but only the nationally sponsored currency has the status of legal tender. And in still other countries (the third group) a foreign produced currency is both acceptable currency and legal tender.

Legal tender is a special status the government can give to certain forms of money in its jurisdiction. It means that this money (generally paper notes and coins) is recognized by law as valid for meeting a financial obligation. Legal tender is variously defined in different jurisdictions. It is anything which when offered in payment extinguishes the debt. Thus, personal cheques and credit cards are

[121] Peter Bernstein, "Chapters 4–5". A Primer on Money, Banking and Gold (3rd ed.). 2008 Hoboken, NJ: Wiley
[122] Vitalik Buterin "The MintChip: The Canadian Government's Answer to Bitcoin" Bitcoin magazine, 05 Apr 2012 (http://bitcoinmagazine.com/the-mintchip-the-canadian-governments-answer-to-bitcoin/, accessed 1 May 2013)
[123] Gianviti, François. "Current Legal Aspects of Monetary Sovereignty." Seminar on Current Developments in Monetary and Financial Law, IMF, Washington, DC, May. 2004.

not usually legal tender. For payments other than via legal tender, the payer and payee have to *agree* to use this payment method.

In some jurisdictions legal tender can be refused as payment if no debt exists prior to the time of payment. This applies where the obligation to pay arises at the same time as the offer of payment, such as taking goods on display in a store the counter and offering to purchase them. For example, traders may reject large banknotes: as shopkeepers displaying the goods is simply an invitation to treat, that shoppers may respond to by offering to purchase and offering a payment in return. As a result, vending machines and transport staff do not have to accept the largest denomination of banknotes. By contrast, restaurants that do not collect payment until after a meal is served must accept that legal tender for the debt incurred in purchasing the meal.

Bitcoins are not legal tender and are unlikely to be so in the short-medium term. Legal tender simply refers to the default means of payment in a country or economy. This is the means of payment authorised and supported by the state, and the means that parties are effectively entitled to use as of right, regardless of whether they subjectively agree that it is the preferred method.

In Australia, the creation of legal tender, in the form of notes and conventional metal coins, is a matter solely for the Federal Government.[124] Only pure gold and silver coins can be minted by states, which still do so from time to time (usually for largely commemorative purposes).[125]

The *Currency Act* 1965 regulates those who issue anything that is to be used as a "token for money or as purporting that the holder is entitled to demand any value denoted on it".[126] In a similar line, the *Reserve Bank Act* 1959 prohibits, without authority, the issue of bills or notes that are intended for circulation as means of payment.[127]

Australian notes are legal tender for all amounts.[128] Australian coins for general circulation are also legal tender up to a certain amount (generally up to $20).[129] Legal tender has a slightly different meaning in Australia. While a person is not legally required to accept legal tender, even for an

[124] Commonwealth Constitution, s115.
[125] See for example the Perth Mint, owned by the Western Australian Government.
[126] section 22
[127] section 44
[128] Reserve Bank Act 1959, s??
[129] Currency Act 1959,

existing debt, failure to do so may be prejudicial in future legal proceedings (the other party would have a full defence in any debt action where they had offered legal tender).

A virtual electronic currency would not appear to meet the legal definition of currency in Australia and would also not be legal tender.

Euro coins and banknotes became legal tender in most countries of the Eurozone on January 1, 2002. Note are tender for an unlimited amount, coins are only legal tender for payments using up to fifty coins.[130]

A similar approach is taken in the UK. Bank of England notes are legal tender in England and Wales to an unlimited amount. Coins are legal tender up to ten pounds, depending on the coins being used.[131] Slightly different rules apply in Northern Ireland and Scotland, where some notes issued by private banks are also in use.

The US Coinage Act of 1965 states (in part): "United States coins and currency (including Federal reserve notes and circulating notes of Federal reserve banks and national banks) are legal tender for all debts, public charges, taxes and dues. Foreign gold or silver coins are not legal tender for debts."[132] However, unless there is a pre-existing debt, a person is not obliged to accept legal tender. So a trader need not accept notes or coins as for payment for goods or services – they can agree another method of payment or (subject to anti-discrimination legislation) decline to serve the customer. Some privately issued notes do circulate in the US, but have no formal legal status and are clearly not legal tender.

Virtual currencies are not a legal currency under the above definitions. Nor are they legal tender and nor are they likely to be so any time soon.

[130] European Regulation EC 974/98
[131] British Royal Mint, "Legal Tender Guidelines" (http://www.royalmint.com/corporate/policies/legal_tender_guidelines.aspx, accessed 28 April 2013).
[132] 31 U.S.C. § 5103

Conclusion and recommendations

Bitcoin is unique not because it is a virtual currency, but because it is proof of concept of a decentralized *non-issued* electronic currency. Bitcoin has a number of weaknesses and may have long-term viability issues for the economic reasons referred to earlier.[133] But it shows that virtual currencies can and probably will succeed in time, as innovators build on the lessons from the Bitcoin experience.

Participants who buy Bitcoins from and sell Bitcoins to users in exchange for regular currency generally do so on a commercial basis and will be bound by the general commercial and contractual law that applies to financial intermediaries. The same is true for those organizations who conduct a market where users can themselves buy and sell Bitcoins (eg MtGox).[134] The regulatory arrangements applying to these two special groups of participants (intermediaries and market operators) should be similar to other financial services firms conducting such activities.

Regulation of virtual currencies is at a very early stage. Most regulatory regimes are not well designed to cater for this type of payment system.

> *"Usually regulation lags behind technological developments by some years. This is also the case in virtual currency schemes (at least in their current form), which were already being established as early as the late 1990s. It was only in 2006 that a number of US government agencies started considering these schemes. The following year, some of these companies were charged with operating unlicensed money transmitting businesses. Since then, a number of other legal actions have been taken and many of these schemes operating in the United States have been closed. Subsequently, China has also taken a stance against the use of virtual currency schemes for the purchase of real goods and services. Recently, in the context of a survey on innovation in payment systems carried out by the Reserve Bank of Australia (RBA), Microsoft asked the Australian central bank to consider adjustments to the domestic payments market to help consumers conduct transactions in virtual currencies."*[135]

This author has set out best practice design principles for payment services regulation in detail elsewhere.[136] One such principle is that the scope of the regime should be broad, outcomes focussed, technology neutral and future proof to the extent possible.

---

[133] Paul Krugman, "Golden Cyberfetters", New York Times, " 7 September 2011 (krugman.blogs.ny times.com/2011/09/07/golden-cyberfetters, accessed 21 April 2013)
[134] www.mtgox.com
[135] ECB, Virtual currency schemes, October 2012, 44
[136] R Bollen, "Best practice in the regulation of non-cash payment services" (2011) 22 JBFLP 147

The Australian general financial services regime is better designed than most to deal with decentralised virtual currencies. This is because it does not presuppose nor depend on the existence of a distinct *issuer*. The way it is designed, it applies to a certain type of product and then to anyone who carries on a business (not limited to being an issuer) in relation to that product. As is appropriate, it will not regulate private users of the currency, but will regulate promoters, distributors and market operators.

> *"Authorities need to consider whether they intend to formalise or acknowledge and regulate these schemes. In this regard, a likely suggestion could sooner or later involve virtual currency scheme owners registering as financial institutions with their local regulating authorities. This is a similar trajectory to the one PayPal has undergone, as it was granted a banking licence in Luxembourg in 2007 after its service became popular. This is not an easy step, but it looks like the only possible way to strike a proper balance between money and payment innovations on the one hand, and consumer protection and financial stability, on the other."* [137]

While it may be that Bitcoins do not have an issuer in the legal sense, this is not a fatal flaw in setting up an appropriate regulatory response however. Indeed, the Australian general financial services regime approach may well be an inspired piece of drafting and one that others may be able to adapt. As has been discussed elsewhere, a well designed and proportionate legal and regulatory regime will support user confidence in, and therefore growth of, innovative payment systems such as virtual currencies.[138] Because "the chances are that some form of digital money will make a lasting impression on the financial landscape".[139]

A recurring issue is how to engender sufficient consumer trust and confidence in a new form of payment service. Payment and money are inherently intangible and abstract constructs.[140] Payment and money are sociological and economic phenomena – certain things are accepted as money or payment by social consensus – and while this can change over time, trust in new forms of money takes time to develop. Singh explains: 'There is nothing inherent in a piece of paper, a plastic card or electronic information that converts it into money. Money is money only when it is trusted that it

[137] ECB, Virtual currency schemes, October 2012, 44
[138] R Bollen, "Best practice in the regulation of non-cash payment services" (2011) 22 JBFLP 147
[139] The Economnist, "Virtual currencies: Mining digital gold", 13 April 2013 (http://www.economist.com/news/finance-and-economics/21576149-even-if-it-crashes-bitcoin-may-make-dent-financial-world-mining-digital, Accessed 1 may 2013)
[140] V Zelizer, "Pasts and Futures of Economic Sociology" (2007) 50 *American Behavioral Scientist* 1056, [http://abs.sagepub.com/cgi/content/abstract/50/8/1056, accessed 1 October 2009], at 1063

will be honoured in your networks of use and exchange.'[141] Creating and protecting trust therefore becomes a crucial issue in the regulation of payment services.[142] The national financial regulatory system will affect the development of new payment services.[143] It is generally accepted that adequate regulation is a key pre-cursor to consumer acceptance of new payment methods, including mobile banking and payments.[144]

[141] S Singh, "Designing for Money Across Borders" 15 Feb 2005, RMIT University/Smart Internet Technology Cooperative Research Centre, [www.ucd.smartinternet.com.au/Documents/Designing_Money.pdf, accessed 1 October 2009] at 1

[142] S Singh "Electronic Commerce and the Sociology of Money" (2000) Sociological Research Online , vol. 4, no. 4, http://www.socresonline.org.uk/4/4/singh.html, at 3.4.

[143] Choi, Collins, Urs and Lovelock, 'Mobile payments: Asia Pacific report' (2008) 2 *E-Finance and Payments Law and Policy* 10.

[144] M Budnitz 'Stored value cards and the consumer: the need for regulation' Mark Budnitz "Stored value cards and the consumer: the need for regulation" (1997) 46 American University Law Review 102 ; SJ Hughes, 'Regulation Of Electronic Commerce: A Case For Regulating Cyberpayments' (1999) 51 Administrative Law Review 809 at 811-12