Bitcoin: Bubble or Blockchain?

Philip Godsiff

University of Exeter Business School, Exeter, U.K.
p.godsiff@exeter.ac.uk

Abstract. This paper sets out a brief, deliberately non-technical, overview of Bitcoin, a new, but becoming more mainstream, crypto currency, generated and managed by a distributed multi–agent system. Bitcoin was developed in late 2008 by "Satoshi Nakamoto". The nature of Bitcoin as a disruptive currency, payments system and asset, is juxtaposed against the potential for its transactional ledger, the blockchain, to usher in a revolutionary way of recording "digital truth". The main contribution of this paper is to progress the debate around Bitcoin beyond the technical and towards legal and ethical issues and the nature of money and memory itself.

Keywords: Bitcoin · Cryptocurrency · Money · Regulation · Disruption · Community ·

1 Introduction

This paper sets out a conceptual overview of Bitcoin, the crypto-currency invented in 2008 and launched in January 2009 by an entity known as "Satsohi Nakamoto".

Bitcoin is a private crypto-currency and encrypted payment system, relying on a peer to peer network with no centralised authority and hence not intermediated by a trusted (or untrusted) third party. Bitcoins, whose eventual total supply has been deliberately fixed at 21m, are "mined" by "operator miners" solving increasingly complex problems, requiring increasing amounts of computing resources. This activity of mining also serves to validate transactions which are recorded in the "blockchain", a community validated secure virtual ledger in which transactions are irreversible, and which eliminates the "double-spend" issue associated with non-physical currencies.

The table below shows figures for volume, dollar price, and "market capitalisation" annually since inception, clearly demonstrating recent price fluctuations.

As at January	2009	2010	2011	2012	2013	2014	2015
Volume	50	1,629m	5,027m	8,008m	10,617m	12,204m	13,675m
Price (US$)	0	0	0.3	5.2	13.6	746.9	315.7
Capitalisation (US$)	0	0	1.5m	41.6m	144m	9,115m	4,317m

Bitcoins may also be purchased from other users through exchanges, and are now sold via some ATM's, are acceptable in many shops and internet mediated services in many cities. It is claimed that Bitcoin fulfils all the requirements of a currency: acting as a unit of account, a medium of exchange and a store of value. In the public conversation surrounding bitcoin, there has been emphasis on its speculative nature, the associated risks, and its alleged use in illegal activities.

Bitcoin is technologically innovative, truly virtual, and potentially disruptive not only to currencies and payment systems, but also to the centralised control, by the state or large corporations, of both. It is also redolent of pre-coinage currencies and means of transacting and recording, based more on collective group memory, and thus less reliant on state underwriting and less susceptible to state interference. The "blockchain", based on community verification and irreversible, offers a potential method of establishing an immutable "digital truth".

In the next section of this paper, aspects of how Bitcoin currently operates as a currency are discussed. Following that the (alleged) more speculative aspects of its ability to behave as or be considered to be an asset (or a liability), are considered, and whether it is a "bubble" or a "fad". Its treatment by various sections of different government authorities is explored. Following that is a discussion on the nature and uses of the blockchain, the nature and uses of money, and the potential for Bitcoin and the blockchain philosophy to support or shape the digital future.

2 Bitcoin: Currency (and Crime)?

2.1 Bitcoin as a currency

In response to its own rhetorical question: What is Bitcoin? a recent Bank of England report answered "Bitcoin was the first, and remains the largest, functioning digital currency. Several thousand businesses worldwide currently accept bitcoins in payment for anything from pizza to webhosting. Payments can be made at any time and between any two users worldwide" [1]. Bitcoin has been described as a "global phenomenon" with nearly 50,000 "members" in 68 countries and up to 1m. U.S. digital currency accounts [2]. The first bitcoin ATM opened in Vancouver in October 2013 [3]. Bitcoin fulfils all the requirements of a currency, acting as a unit of account, a medium of exchange and a store of value [3]. But in the public conversation surrounding Bitcoin, there has been emphasis on its speculative nature [4], the associated risk and its alleged use in illegal activities [5].

Bitcoin is truly virtual with each transaction (employing public cryptography, based on well-known standards such as SHA-256 [6]) treated as a "tuple" of buyer, seller and amount [7]. It is non-denominated, which enables splitting; it is infinitely divisible: down to one hundred millionth of a bitcoin, (known as a "satoshi" [8]), and in the absence of intermediaries this facilitates low costs transactions and hence micropayment business models. Bitcoins are stored in "wallets": effectively a cryptographic public key (about 33 digits) hosted on web, pc or phone, or even paper printouts [8]; loss of the "wallet" e.g. by throwing a pc away can be irrecoverable. It is estimated that up to 4% of created bitcoins have been lost due to errors and theft, but that is just similar to a normal wallet [9].

Double spend

The need to eliminate the possibility of double spend is a challenge to all virtual (non analog/no physical exchange) currencies. Consensus to changes and transactions is achieved through public key cryptography community verification (by the miners) of proof of work [1], and having a distributed open ledger to which transactions are checked [10]. The community acts as the recording body [11].

Mining

Bitcoins, whose supply has been deliberately fixed at 21m, are created by being mined through "operator miners" solving increasingly complex problems, and hence requiring increasing computing resources [12]. The more bitcoins are brought into existence the harder become the algorithms [1]; some commentators forecast that the last bitcoin will be mined in 2140 [10].

2.2 Exchanges

Bitcoin can be converted to national currencies (leaking out into the "real world" [9]) through exchanges [11]. At any one time there may be as many as 50 exchanges [2]. Less popular exchanges suffer from high closure rates (nearly 50% over 3 years) with more popular exchanges suffering a higher ratio of security breaches [13], such as malleability

attacks [14]. The closure and bankruptcy of Mt.Gox (which had around 600,000 users/customers) was a blow to confidence and price stability, [2] although it should be noted that the system survived. Bitcoin is resilient due to its distributed nature [11].

2.3 Anonymity

Like cash, transactions carried out in bitcoin are claimed to be anonymous. In actuality, the correct aspect is "pseudonymous" [15] [10]; although some claim that these pseudonyms can be traced back to named individuals depending on the processes users have gone through to establish them. It is estimated that 40% of user profiles could be identified even if the users had followed bitcoin procedural advice [16].

There is a counterintuitive by-product of the protocols in that while *ownership* may be anonymous, the *flows* are globally visible [17]. The impact of this pseudo-anonymity, again like cash (more specifically high value paper), is the use of bitcoin in alleged criminal activity. The nature benefits of anonymity can lead to criminal or secretive activity [18]; which also leads to difficulty in enforcing regulatory anti-money laundering or "know your customer rules" where detailed data has to be given to intermediaries [19].

2.4 Crime

Crime may take place *in* bitcoin and *on* bitcoin. Bitcoin offers opportunities for fraud and tax avoidance[11]. It has become the money laundering route of choice for cyber criminals not wishing to deal in cash [20], although some traders in the dark web and "Silk Roads" have expressed concerns over bitcoin instability [21], leading to an alternate view that the concern is over technology rather than the law. Black markets often exist to circumvent discriminatory or discretionary corporate and government practices [22]. There are claims that Bitcoin and its associated exchanges have become a virtual "wild west "with its own breed of bank "heist"; and two of the larger exchanges to close appear to have been robbed or subject to fraud.

But Bitcoin also has legitimate users and these and their aspirations should not be bundled in with its criminal associations [5]; as has been noted, crime also exists in and on analog currencies. However there is concern over whether Bitcoin will work at scale and the length of time taken to validate transactions using existing proof of work protocols [17], [23], and when sufficient network scale and associated ecosystems of payments services and wallet firms can be created [24]. Bitcoin could flourish under circumstances where existing systems are untrusted or expensive [25] [26].

3 Bitcoin: the bubble?

3.1 Bitcoin: the asset

As an asset, the price is highly variable though the trend is upwards from its inception. The Bank of England report notes that price rose by 5,000% in two years. A logarithmic price chart shows a steady rise in value [1]. The value of any commodity is a reflection of supply and demand and because it is perceived to be a source of value [27]. Its reliability as a store of value remains a risk to those who hold it [2].

3.2 Bubbles

Bitcoin trading and price volatility has been likened to "tulip mania in" C17th Holland, where an established but small futures market in spices and tea spread over into tulips and subsequent speculation involving practically the whole nation in the domestic production of a "previously exotic import" led to rapidly rising prices followed by equally rapid collapse; the final settlement value of most contracts being less than 5% of face value [28]. The failure of Mt Gox led to a halving of Bitcoin value in a week [22].

Others have described Bitcoin as a giant "Ponzi" scheme [8]. There is some evidence of a linkage between google searches and value movements [29], [30]. There is also evidence that such bubbles are being socially created and given the data, now more easily researchable [31].

However the activity levels around bubbles can develop markets and infrastructure as well as raising public awareness, if not interest. A rapidly rising price leads to both an increased number of speculators and entrepreneurs developing new products and services [24]. The volumes and volatility around speculation could also be considered to be a good means of stress testing [10].

3.3 Bitcoin: the mainstream investment

Serious institutions are taking Bitcoin seriously, in their investment advice and in their trading. Banks like Goldman Sachs and Merrill Lynch are now covering Bitcoin, with investment companies raising specific funds to invest in Bitcoin [8], as consumer confidence increases [32]. Venture Capitalists are showing both speculative and payments services interest [24]; there has been an estimated $200m of VC investment in 2014 [2]. Bitcoin has been shown to benefit theoretical portfolios if held in small percentage quantities. Accountants are beginning to run courses on Bitcoin [33]; some are recommending its use in estate planning, where its fluctuating value could bring benefits [32]. The S.E.C. in the U.S. has issued warnings not about its use or existence, but in the potential for fraudsters to target now wealthy individuals holding bitcoins.

Losses on exchanges can be insured against, and a hedge fund is being developed to counter large value fluctuations [24]. Risks from price volatility maybe less than those experienced by investors in e.g. sub-prime mortgages and associated derivatives, a trade that was very destructive of bank, corporate, and personal capital [11].

A limited supply and no central governmental authority (which may be open to temptation to over create fiat money [34]) should mean that the currency bitcoin will not be devalued [10]; possibly quite the converse. The fixed amount promotes "upside potential" [27]. Bitcoin may fall beneficial victim to Gresham's Law: bad money drives out good (from use as a circulating currency), as investors and speculators gravitate towards it when the mining-go-round stops.

"Whether Bitcoin is a bubble is too early to tell. It does demonstrate however that anything can be a currency and that emotion can overload even the most mathematical of formulations" [35].

4 Bitcoin: Currency or Commodity?

Virtual currencies like Bitcoin exist in a "gray area" of being able to be considered as both a currency and a commodity [2], so inevitably questions arise as to how Bitcoin should be treated for governance, regulation and taxation purposes.

4.1 Regulation

The views on regulation reveal inter and intra national differences. The US and Canada treat bitcoin as property (commodity/asset) for taxation purposes [3]. However, in spite of this, in June 2014 California removed a ban which prevented the use of currencies other than dollars [3]. It is equally unclear whether transactions are liable to sales tax [11].

The E.U. position is equally confused. Within the European Union, The Payment Services Directive and E-money Directive form the legal framework for consumer protection in mobile payments, but does not cover Bitcoin [36]. Germany treats bitcoin as private money and a financial instrument, while Denmark considers it as neither currency nor an asset [2], the Danish central bank likening it to "glass beads", remarking that it was not a

currency because there was no issuer and no utility value, a particularly analog viewpoint. China acted to reduce its use and restrict trade in the currency, as a precursor to an outright ban. France and Korea do not treat it as legitimate [3]. The Japanese central bank suggested that bitcoin was an asset, rather than a currency or financial instrument, and that its use did not constitute banking.

Perversely dealers and exchanges are pushing for regulation as a way of building trust. There is a dichotomy for some users of bitcoin in the issue of regulation. On one hand it can be seen as interference and increasing unnecessary oversight and transaction costs, (e.g. through the need for personal record keeping); on the other it could confer respectability and a degree of legitimacy and support [11]. Whether officially supported or not, it is worth noting that the U.S. government was quite sanguine about potentially benefitting from the sale of 30,000 bitcoin confiscated from the closure of Silk Road 1.

4.2 Central bank support

A specific role of the modern central bank is to underwrite its currency and prevent large and erratic fluctuations in its value, and acting as "the ultimate rich uncle" in its support [37]. Bitcoin is not dependent on a central bank or a government standing behind it, but relies on the community to underwrite it. In the absence of centralized support it is claimed that the value fluctuations being experienced will continue and run the risk of the entire system collapsing [27]. However the collapse of Mt Gox whilst affecting value significantly does not appear to have altered fundamental beliefs in its future.

But the issue of central bank involvement runs deeper than underwriting. Central Banks and governments use control over the money supply as a means of managing (for better or worse) inflation, as can be seen with quantitative easing, and promoting growth. The existence of a currency or currencies outside this sphere of influence could lead to such efforts being less successful. National sovereign debt currency crises, like those in Argentina Russia and Thailand Ireland and Greece, leave a lasting political legacy and fiduciary implications [22].

5. Bitcoin: the Blockchain

The Bank of England report considers the impact of the blockchain in some detail; even mooting the possibility of the Bank operating a similar distributed ledger [1], and suggesting the blockchain as the basis of an "internet of finance".

5.1 The Blockchain

Bitcoin is as much about "on line" as it is about currency; it has myriad uses in and expanding mobile commerce [38]. Bitcoin is about online transactions [5]. It can serve as a "platform" "for financial information"[24]. It "contains the digital blueprints for a number of useful financial and legal services: information can be embedded in the blockchain, such as contracts, bets, and other sensitive or time based material e.g. fines for non performance" [10]. This may be useful for "mutually distrusting parties" engaging in exchange [39]. Because of validation by the community the "fairness" of the contract process can be guaranteed by its protocols [39].

The Bank of England report proposes the possibility, given that the records for most financial assets are now held in electronic form, (albeit centrally in a tiered structure - individual accounts with banks, bank's reserve accounts with the central bank), of this entire current structure of payments services and banking being ultimately replaced by distributed systems [1].

Other potential features include (beyond the obvious micropayments) dispute resolution, assurance contracts, and smart property; this could pave the way for enhanced crowd funding

applications, translation services and instantaneous processing [10]. Under the Bitcoin protocol legitimacy of transfer and ownership is established beyond challenge [8]. Bitcoin is the "foundation upon which other layers of functionality can be built" [10]. This could easily extend beyond finance providers to providing all the necessary accounting, banking and tax movements on each transaction, either purchase or perhaps on use or consumption in real time. This would give the opportunity for new service providers to disintermediate a range of financial services.

5.2 The internet of transactions

In the "internet of things" Bitcoin could be used by two entities to exchange value thus potentially creating a market for sensor data, "exchanging (electronic) data for electronic cash" [40]. The extensive digitisation of data plays a part in this. This is less about how can the data be monetized, a bit of an analogue hangover, but how it can be exchanged in non monetary ways or ways which reduce cost but increase outcome. However "if the web through the internet of things begins to intrude on increasingly more aspects of human and social activity, the issue of security or freedom, the compatibility and how much of each, will need to be addressed" [41].

6 Discussion

Bitcoin acts in one guise as both a currency and a payments system, and in another guise, like any good commodity, as an asset. The blockchain could change the way digital records (of any transaction or asset) are made and kept. Much of current literature is centred on the currency and cryptography, and although it is noted that there has been little research into the economics of Bitcoin [9], there has been even less on what might be referred as the "ethics" of Bitcoin.

6.1 Payments Systems and Disruption

Bitcoin is as much a payments system as a currency. Being virtual, non-denominated and non -intermediated, it is extremely efficient to use in micro or low value payments [38]. But it is potentially an attractive new business model, given that disruption often occurs at the margins [42]. Some speculate that virtual currencies like bitcoin could ultimately replace government forms of fiat money [43], even in the face of government opposition. Opposition may also come from large corporations. Apple withdrew bitcoin apps shortly before announcing their own payments services and Amazon may be considering starting payments services [11] [44]. This poses a potential choice between community intermediation or "big silicon" control.

Could Bitcoin or something like it become the "Napster for finance?" [11]. The disruption is not limited to products and processes but, as has been described above, could extend to markets and rules and tax revenues [11]. The Bank of England report remarks that some commentators suggest that bitcoin could become the "internet of money", or even the "internet of finance" [1].

There is a fear that regulation will kill the experiment, for whatever motives [27]. This clash of digital disruption with analog regulation and mind-sets highlights issues of the legitimacy of state regulation itself [11]. But if Bitcoin is a reaction to a lack of liquidity or transparency, some have argued that these underlying causes should be addressed rather than attempting to inhibit Bitcoin's development [22]. Removing the ability of a government to control its currency "can change the economics process and drive deep wedges between various social and political elements" [22]. But there may be effects beyond the potential disruption to financial services and economic structures.

6.2 Law in "Mixed Reality"

The virtual and real worlds increasing mix and confound each other [43]. "If drug or other illegal activity is conducted on the dark web in bitcoin, neither of which is mediated or controlled by government, issues of law enforcement come to the fore" [45]. But what sort of law will regulate these places? There is a lack of current law available to deal with virtualisation technologies where there is "the emergence of a "mixed reality" of virtual and realspace features and geography" [46]. Noting that most virtual world's research is concerned with the impact that "real world" regulations have on online communities, it is important to decide whether, in a world of mixed reality, (real and cyberspace), online or offline law will cover rights of users over property and data [46]. Interestingly, since Bitcoin is essentially a kind of transaction log, where past transactions are public and known to the world, it is of great interest to prosecutors, who have called the coins 'Prosecution Futures' [42].

6.3 What is money?

Trust and the nature of money

Trust is "essential for virtually all economic activity" [37], be that in the "real/analog" world, (the quality of my cup of coffee, and the paper note with which to pay for it) and the virtual. There needs to be a belief in stated explicit or implicit promises, backed up where necessary by practice and legal frameworks; and there needs to be trust that central bank knows what it is doing in maintaining the value of the currency and of the economy [37].

Money is not the only currency

Certain South Sea islanders use stones as currency, with transactions and ownership being recorded in collective memory [47]. England used wooden sticks, (tallies), as a proxy for money for more than half a millennium and these sticks were very effectively used for taxation purposes [35]. Money is a fairly recent invention, whereas trading debt and credit are not [48].

"Identity is the new money"

This quote, suggesting a fundamental change in the nature of currency, is attributed to Sir James Crosby (quondam Chief Executive of HBOS) [47], It indicates the potential for new forms of exchange to emerge as a result of digital disruption. Leading industry commentators [47], see a possible return to those earlier community memory based versions of currencies as stores of value and media of exchange; these would not involve the physical transfer of analogues (e.g. coins or cards). Such developments have the potential to lead to an individual's digital reputation, or access to scarce resources (such as car parking spaces in cities), being of value and tradable directly as a generally accepted means of exchange [47].

Money can be both a series of promises or a fact (like a tally) [35]. If money is about relationships, then the "bitcoin project can best be thought of as a process of financial and communicative experimentation" [10]**.** Some authors have suggested Bitcoin, a community currency not an individual state mediated one, is a similar concept to Simmel's idea of "perfect money" within a "perfect society", ideals closely aligned to socialist principles [49].

Money can be described as alternately, a promise, a series of relationships and an analog or digital fact. "Perhaps the real problem is money itself" [50]. In existing systems privacy and liberty are allegedly at risk as is the value of the currency itself, due to government or corporate intervention. Bitcoin offers a "practical materialism" reminiscent of previous debates around "privacy, labor and value" [50]. "What is a debt anyway? A debt is just the perversion of a promise. It is a promise corrupted by both math and violence, mediated by state and capitalist institutions" [48].

6.3 Revolution and motivations

Some commentators [51] have argued that the blockchain system is only, so to speak, being experimentally trialed as a currency, and could be extended beyond the uses already seen, and they envisage the possibility of further innovation in and on the Bitcoin protocol [10]. Bitcoin allows companies and everyone to be peer to peer and distributed not just the currency [1]. It has been claimed that by not relying on trust or asymmetric power relationships, Bitcoin is somehow more "ethical" [52].

What will represent the nature of real and virtual boundaries inside which privacy is shared and outside which anonymity is guaranteed? The Snowden revelations have shown that decisions in this area about trade-offs are hard to make, with privacy too often treated as a "transactional personal good" when it might be considered to be more of a shareable public good [17]. The Bitcoin philosophy may be a way to offer an alternative to excessive surveillance.

Bitcoin appears to have an overtly "political" or ideological motivation: the initial "genesis block" in the block chain includes a newspaper headline covering the bail out of the UK banking system [1]. It has attracted strange bedfellows and combinations of technocratic programmers, cypherpunks and crypto-anarchists [2], neo liberals and "crypto-libertarians" [53] .

Some "cypherpunks" have intimated that bitcoin is the first step in a much larger project by its founder [51]. This project aims to prevent both private and public fraud by limiting monetary supply and removing the need for a central authority, and having the community authentic transactions and freeze history. These "3 centralities" to Bitcoin could, they argue, be extended to establish a "universally consistent history" in which falsification cannot exist, and separate classes of data emerge [51]. This could for example be an answer to the veracity issue faced for example by big data. Others venture that the "interesting experiment" may form a part of "distributed capitalism" [54], with the recording of "property" and "trust" dis-intermediated and established by the community.

7 In Conclusion

Why use bitcoin when you can use dollars? "Its limited supply and perceived freedom from human interference in a recent era where trust in the traditional monetary system are powerful assets that have transformed an interesting intellectual experiment into a living economy" [35], but how will Bitcoin make it further into the mainstream? This may be achieved by the fuller development of a supportive and innovative ecosystem [24], which will aid the innovation and experiment inherent in the Bitcoin approach to demonstrate ways it could develop [10]. The support, or at least the acquiescence (or absence of outright hostility) of regulatory authorities will be important here [10], [53]. Governments need to support its growth and provide the right legal support; that of course relies on those authorities coming to terms with the potential development of a parallel economy [11], the "internet of finance" [1]. Currencies are the "heart and soul" of society and the governments that rule them [22]; states and "currency" often emerge together, though the recording of debt and obligations precede both [48].

A digital world needs a digital currency but how is living in a non-material world to be managed? Some commentators see the development of Bitcoin as the" beginnings of the struggle" for control over the internet in a new environment but one in which the "age old dilemma" of security against freedom must still be debated [41]. "[T]he idea that any digital currency is to be fully liberated from government or central bank is fascinating; it's like the Fed meets the wild west" [55]. Bitcoin the currency, Bitcoin the blockchain, and Bitcoin the philosophy.

References

1. Ali, R., Barrdear, J., Clews, R. & Southgate, J.: Innovations in payment technologies and the emergence of digital currencies. Bank of England Quarterly Bulletin 54, 262-275, (2014)
2. Cofnas, A. B. E.: Bitcoin: Currency or commodity? Futures: News, Analysis & Strategies for Futures, Options & Derivatives Traders 43, 10-12, (2014)
3. Blundell-Wignall, A. (2014)
4. Baek, C. & Elbeck, M.: Bitcoins as an investment or speculative vehicle? A first look. Applied Economics Letters In press, (2014)
5. Turpin, J. B.: Bitcoin: The economic case for a global, virtual currency operating in an unexplored legal framework. Indiana Journal of Global Legal Studies 21, 335-368, (2014)
6. Courtois, N. T., Grajek, M. & Naik, R.: Optimizing SHA256 in bitcoin mining Communications in Computer and Information Science (2014)
7. Van Alstyne, M.: Why Bitcoin Has Value. Communications of the ACM 57, 30-32, (2014)
8. Levin, R. B., O'Brien, A. A. & Osterman, S. A.: Dread Pirate Roberts, Byzantine Generals, and Federal Regulation of Bitcoin. Journal of Taxation & Regulation of Financial Institutions 27, (2014)
9. Wu, C. Y. & K., P. V.: "Breaking News.". . Timeline (2014)
10. Brito, J. & Castillo, A.: BITCOIN: A PRIMER FOR POLICYMAKERS. Policy 29, 3-12, (2013)
11. Smith, A. & Weismann, M. F.: Are You Ready for Digital Currency? Journal of Corporate Accounting & Finance (Wiley) 26, 17-21, (2014)
12. Dev, J. A.: in Canadian Conference on Electrical and Computer Engineering (2014)
13. Moore, T. & Christin, N.: Beware the middleman: Empirical analysis of Bitcoin-exchange risk Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) (2013)
14. Decker, C. & Wattenhofer, R.: Bitcoin transaction malleability and mtgox Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), (2014)
15. Miers, I., Garman, C., Green, M. & Rubin, A. D.: Zerocoin: Anonymous distributed e-cash from bitcoin Proceedings - IEEE Symposium on Security and Privacy (2013)
16. Androulaki, E., Karame, G. O., Roeschlin, M., Scherer, T. & Capkun, S.: Evaluating user privacy in Bitcoin Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) (2013)
17. Meiklejohn, S., Pomarole, M., Jordan, G., Voelker, G. M. & Savage, S.: A fistful of bitcoins: Characterizing payments among men with no names Proceedings of the ACM SIGCOMM Internet Measurement (2013)
18. Peck, M. E.: The cryptoanarchists' answer to cash IEEE Spectrum, (2012)
19. Moser, M., Bohme, R. & Breuker, D.: An inquiry into money laundering tools in the Bitcoin ecosystem eCrime Researchers Summit, eCrime (2013)
20. Shoshitaishvili, Y., Invernizzi, L., Doupe, A. & Vigna, G.: Do you feel lucky? A large-scale analysis of risk-rewards trade-offs in cyber security Proceedings of the ACM Symposium on Applied Computing, (2014)
21. Van Hout, M. C. & Bingham, T.: Responsible vendors, intelligent consumers: Silk Road, the online revolution in drug trading International Journal of Drug Policy (2014)
22. Andelman, D. A.: Currency Wars. World Policy Journal 31, 115-124, (2014)
23. Singh, P., Chandavarkar, B. R., Arora, S. & Agrawal, N.: Performance comparison of executing fast transactions in bitcoin network using verifiable code execution. Proceedings - 2nd International Conference on Advanced Computing, Networking and Security, ADCONS 2013 (2013)
24. Cusumano, M. A.: The Bitcoin Ecosystem. Communications of the ACM 57, 22-24, (2014)
25. Surowiecki, J.: Economics: Cryptocurrency Technology Review 114, 107-107, (2011)

26. Surowiecki, J.: Economics: Cryptocurrency Technology Review 114, 106-107, (2011)
27. Lemieux, P.: Who Is Satoshi Nakamoto? Regulation 36, 14-15, (2013)
28. Davies, G.: A History of Money. (2014)
29. Bhattacharya, J.: Minting pure reason. Economic and Political Weekly (2014)
30. Kristoufek, L.: BitCoin meets Google Trends and Wikipedia: Quantifying the relationship between phenomena of the Internet era Scientific Reports (2013)
31. Garcia, D., Tessone, C.J., Mavrodiev, P., Perony, N.: The digital traces of bubbles: Feedback cycles between socio-economic signals in the Bitcoin economy. Journal of the Royal Society Interface 11, 0623, (2014)
32. Parthemer, M. R. & Klein, S. A.: Bitcoin: Change for a Dollar? Journal of Financial Service Professionals 68, 16-18, (2014)
33. Barry, J. S.: Lawsky Makes a Bet on New York. CPA Journal 84, 5-5, (2014)
34. Rogojanu, A. & Badea, L.: The issue of competing currencies. Case study-Bitcoin. Theoretical and Applied Economics 21, 103-114, (2014)
35. Swarup, B.: Money Mania. (2014)
36. Vandezande, N.: Between bitcoins and mobile payments: Will the European Commission's new proposal provide more legal certainty? . International Journal of Law and Information Technology (2014)
37. Coggan, P.: Trust (not money) makes the world go 'round. OECD Observer, 75-76, (2014)
38. Hurlburt, G. F., Bojanova, I.: Bitcoin: Benefit or curse? IT Professional 16, 10-15, (2014)
39. Andrychowicz, M., Dziembowski, S., Malinowski, D. & Mazurek, Ł.: Modeling bitcoin contracts by timed automata Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) (2014)
40. Wörner, D. & Von Bomhard, T.: When your sensor earns money: Exchanging data for cash with Bitcoin UbiComp 2014 - Adjunct Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing (2014)
41. Doguet, J. J.: The nature of the form: Legal and regulatory issues surrounding the bitcoin digital currency system Louisiana Law Review, (2013)
42. Ford, P.: Marginally useful. Technology Review 117, 80-82, (2014)
43. Castronova, E.: Wildcat currency: How the virtual money revolution is transforming the economy. (2014)
44. Wiener, H., Zelnik, J., Tarshish, I. & Rodgers, M.: Chomping at the Bit: U.S. Federal Income Taxation of Bitcoin Transactions. Journal of Taxation of Financial Products 11, 35-47, (2013)
45. Barratt, M. J., Lenton, S. & Allen, M.: Internet content regulation, public drug websites and the growth in hidden Internet services Drugs: Education, Prevention and Policy (2013)
46. Michailaki, A.: Mixed reality through the internet of things and bitcoin: How laws affect them. Communications in Computer and Information Science, 165-169, (2014)
47. Birch, D. G. W.: Tomorrows Transactions: the 2014 Reader. (Mastodon Press)
48. Graeber, D.: Debt: The First 5000 years. (2014)
49. Dodd, N.: Simmel's Perfect Money: Fiction, Socialism and Utopia in The Philosophy of Money Theory, Culture and Society, (2012)
50. Maurer, B., Nelms, T. C. & Swartz, L.: When perhaps the real problem is money itself!": The practical materiality of Bitcoin Social Semiotics (2013)
51. Smith, A.: in Sunday Times Magazine (Sunday Times, London, 2014)
52. Angel, J. J. & McCabe, D.: The Ethics of Payments: Paper, Plastic, or Bitcoin? Journal of Business Ethics in press, (2014)
53. Van Alstyne, M.: Economic and business dimensions: Why bitcoin has value Communications of the ACM (2014)
54. Kostakis, V. & Giotitsas, C.: The (A)political economy of bitcoin. TripleC 12, 431-440, (2014)
55. Schulaka, C.: Worth a Few Bitcoins? Journal of Financial Planning 27, 11-11, (2014)

Commentary on Review Points

Firstly let me thank both reviewers for their very supportive and encouraging marking, and the helpful comments which will improve the paper. I set out how I have dealt with the 3 recommendations below:

1. Abstract *"the description is too short, please include a brief summary of the main contribution"*

I have inserted the following:

> The main contribution of this paper is to progress the debate around Bitcoin beyond the technical and towards legal and ethical issues and the nature of money and memory itself.

I have included the comment regarding its inception in the abstract, but have left it in the main body of text as well.

2. *"US Government as main backer /manipulator"*

I have inserted the following at the end of section 4.1 Regulation

> Whether officially supported or not, it is worth noting that the U.S. government was quite sanguine about potentially benefitting from the sale of 30,000 bitcoin confiscated from the closure of Silk Road 1.

3. *"Add an overview timeline of Bitcoin"*

> I have added a brief table in the introduction

Other comments:

I have taken the opportunity to correct a few proof reading errors which I noticed on re-reading the paper, and tidied up some of the grammar.

Also I have noticed a couple of errors in the references, which I will correct for the final proof version.