Submission to the Senate Economics References Committee

Inquiry into Digital Currencies

Author: Dr. Pj Radcliffe, RMIT University.

Table of Contents

Executive Summary

Digital currencies have potential to make it easier, quicker, and cheaper to purchase goods and transfer money but there are significant dangers. As digital currencies grow there is the potential for businesses and individuals to suffer losses, and this may produce a back-lash to any government that has even tacitly accepted a digital currency. The government may have further problems with a reduction in taxation income as purchasers avoid GST and engage in untraceable illegal behavior such as money laundering and drug dealing.

As an academic and engineer who is familiar with networking and software and their security, I am well placed to comment on the risks of digital currencies and to offer tentative solutions.

Digital currencies are in their "Wild West" phase but they could become a useful part of the economy if problematic features are eliminated and there is firm regulation which is enforced.

Problems with Digital Currencies

The literature is filled with examples of fraud and problems with digital currencies [1] [2] [3]. There are also examples of tax avoidance which has harmed the government's tax base. This section looks at the key properties of these currencies and why these problems exist.

Traceability: The structure of most digital currencies means that either all transactions are private and untraceable, or that the identities and the transactions are all public. Total privacy makes it almost impossible for fraud and illegal activities to be detected, traced, and prosecuted [4]. It is also impossible to levy tax on any such dealing. Full public disclosure would eliminate the privacy that most citizens desire.

In order to allow proper law enforcement and taxation there are two practical alternatives-

1. All digital currency addresses must be publicly linked to an individual or organization. The public will need to understand that the public record of their payments to suppliers is the price paid for a more secure system where fraud and misbehavior can be prosecuted.
2. It must be possible for at least law enforcement and government agencies to find the true identity of the user of a currency address. An individual's purchases will remain private using this approach but the government will have some role and cost in maintaining the identity system. Digital currency exchanges may be required to hold the information that would be accessible only to law enforcement, and the parties to a transaction.

Either alternative is likely to be fiercely opposed by the digital currency advocates who see anonymity as a key property of the system. If the anonymity issue is not resolved then digital currencies will remain in their "Wild West" phase and should not be embraced by the main stream financial system.

Taxation: a significant effect of the lack of traceability is that taxation based on money flows becomes impossible [5]. The government cannot see the expenditure from the purchase nor the income to the supplier. This makes it easy and low risk to avoid GST. Wide spread use of a digital currency would be a major threat to the taxation base of any country with a GST or VAT.

Security Alert System: The Internet is bedeviled by attempts to defraud, to steal information [6] [2], and denial of service attacks. There is a well proven process of providing security alerts so that providers have time to fix systems or create patches before the fault is widely known, and users can see what they have to update. A digital currency must have a very strong security alert system and a legal requirement for digital exchanges to implement fixes very quickly. To date there is no established alert system or process for digital currencies. It may be possible to use the same organizations and services that protect the Internet. The massive theft from Mt Gox in 2013 was in large part due to a failure to patch a well known defect [7]. It has been reported that 150 malware programs are aimed at stealing Bitcoin from users [8].

The government can help by producing a code of conduct for digital currency exchanges and digital currency programs which includes security alert and repair requirements. Digital exchanges and products would be able to advertise that they conform to such a code and so consumers would be more likely to deal with such an organizations or products.

Dominant miner: miners keep the public record of transactions (the block chain) in return for the reward of receiving "mined" digital coins. A miner who controlled more than 50 percent of all Bitcoin mining power could tamper with the public record and do things such as spend Bitcoins

twice. A Chinese group GHash.IO recently got over the 50% threshold precipitating a drop in Bitcoin value [9][10]. It may not be possible to tell if there is collusion between major miners and fraudulent behavior, until too late.

Governments may have a role in ensuring that no one group or cartel ever gets above 50% in Bitcoin based digital currencies.

Speculation: digital currencies have seen dramatic booms and busts in value [11]. The basic problem (apart from human nature) is that the currency is not used much for real financial activity, most of the activity appears to be speculation. Most digital currencies are based on Bitcoin which is inherently deflationary and so a Bitcoin will most likely be worth more in the future which only encourages speculation.

If more business start to accept Bitcoin then there will be more financial activity and speculation will be reduced. A significant barrier to wide spread use is the conversion cost from real currency to digital currency. If this can be reduced then more people will be willing to use digital currencies, and put a digital currency on their mobile devices and then spend it a shops.

Technical limitations: most digital currencies have a range of technical limitations which may limit their wide scale usability. These include-

- Upper limit: most currencies have a maximum limit on the number of "coins". Bitcoin for example has used up about 13 billion of a maximum possible 25 billion coins [12]. Estimates vary but at current trends there will be no more Bitcoins after about 2025. At this point the currency will be deflationary as Bitcoin get lost and no new Bitcoin are created. This will make Bitcoin a key speculation and investment vehicle.
- Who pays the miners? Digital currency "miners" maintain the public transaction records in return for a small payment [13]. When there are no more digital coins to be mined who will maintain these public records? Will a very small fee be required by a "miner" to update a transaction record? The fees system has been established for Bitcoin and the system will most probably cope.
- Fragmentation: a small purchase may be a fraction of a digital coin and so fractions of digital coin accumulate at both buyer and seller. It is not possible to arbitrarily join digital coin fragments and so in the future the system may get clogged with many fractional coins. It would be helpful if a digital exchange made it a practice to agglomerate digital coin fragments in its care to reduce this problem.
- Response time: some digital currencies take 10 minutes to 10 hours or more to complete a transaction so that it becomes irreversible, which makes them impractical for point of sale. This limits immediate sales to small value items where it is not worth the bother to try and beat the system.

Volatility: most digital currencies such as Bitcoin have significant variations in their value as can be seen on currency conversion charts [14]. The volatility of Bitcoin is much higher than gold and makes it difficult to do business. One solution is to quote prices in traditional currencies but pay in a digital currency. Bitcoin has an average price variation of 10% per day [15].

Impact and Competition: who will use Digital Currencies?

From the previous discussion, digital currencies are not well suited to point of sale due to the time taken to lock in the transfer and other factors. To date there are few shops willing to take the dominant digital currency Bitcoin [16]. The real advantage of digital currencies is the very low transaction costs which are much lower than current banking services. For example consider buying a product in another country and suffering the usual currency transfers fee of 4% [17]. On reflection such a fee is a very high impost levied by the banks and a real inhibitor of international trade. A typical digital currency transaction will have no fees or perhaps a very small fee. Even local purchases with a debit card attract monthly fees which may add up to a hundred dollars a year. Using a digital currency instead would cost nothing or a very small amount.

With the exception of activities that involve significant currency conversion there is a marginal advantage to a digital currency user (ignoring the ability to avoid tax). The overhead costs of a credit or debit card are not that high and so there would not be a large impetus for purchasers to move to a digital currency given that most purchasers will still own and use a credit card.

Digital currencies could compete strongly with international money transfers as run by wire transfer companies and banks. These organizations will see a threat to their profits and may act to oppose such currencies.

From a government perspective anything that enables competition and lowers costs to the consumer is a good idea and will stimulate the economy. The novelty and risks of digital currencies will make it very unlikely that existing organizations will be threatened though excessive fees may be trimmed due to competition.

Illegal activities: digital currencies have been used extensively for illegal activities such as selling drugs and laundering money[18] [4]. This is a big and profitable business and possibly one reason why there are some very voracious supporters of total privacy and no traceability.

Government policies should make it as difficult as possible for any digital currency that enables or facilitates such illegal activity. The notorious Silk Road drug market used Bitcoin and that impeded investigators from tracking down the illegal activity [19] [20]. The Bitcoin public transactions could not be used to locate the sellers or buyer of drugs, nor the source and destination of money laundering.

Tax avoidance: as noted earlier it may be impossible to tax any form of money flow with a digital currency. Anyone keen on avoiding tax may well be keen to use a digital currency.

Regulatory System & Leadership

This topic area is not a main area of expertise but it contains ideas that may prove useful.

Regulation: the US has done a lot of work on regulations and their experiences and rules should be closely examined [21]. Australia's ATO does not seem very worried [22] which may be a mistake.

Financial service: digital currencies are simply another form of a financial service much like credit cards. There is a whole body of legislation built up over many years to encourage this industry and protect the players. It would make sense to have digital currencies under the same umbrella as

much as possible. Such an approach may require small changes to existing laws, and a few specifics for digital currencies.

Code of conduct: Some of the problems with digital currencies can be eliminated or minimized if digital exchanges followed good practices. The Australian government can generate a code of conduct with both compulsory and recommended practices. Where possible the detection of problems must be open to the public not just government. A digital exchange may advertise that it meets this code of conduct and must also display and breaches and repairs. This would give consumers a great deal more confidence that the digital exchange is trustworthy.

Promote "acceptable" currencies: as discussed, current digital currencies have weaknesses related to technical issues, and the ease of avoiding tax and committing illegal activities. The Australian government can define what makes an "acceptable" digital currency that avoids these problems, and then allow a viable place for such currencies in the Australian market place while at the same time eliminating or limiting the role of unacceptable currencies. Given such an environment, innovators and organizations will take the opportunity to develop acceptable currencies within the Australian context and then spread their Australian businesses overseas. There is a limited window of opportunity here as the first successful product in such an area normally dominates the market. If Australia is to succeed in this area then the government must very quickly decide what constitutes an acceptable digital currency and how such a currency can be fitted in to the Australian financial environment so that there is an incentive to develop such a currency.

Besides the legal and regulatory barriers the government may erect against unacceptable digital currencies, it would be helpful to create incentives to help acceptable currencies. One possible incentive is to lower the cost of conversion between real currency and an acceptable digital currency. The previously discussed "code of conduct" is another advantage for acceptable currencies.

Conclusions

Digital currencies are a fascinating and surprisingly resilient invention. Given there is no central coordinating body and no real regulator or law enforcement system it is amazing that any digital currency has survived. This in itself should alert us that digital currencies have significant potential.

The major problem with current digital currencies is the way in which they facilitate illegal activities such as fraud, taxation avoidance, purchase of illegal goods, and money laundering. The inability to identify the participants in the transfer process is the root cause of this problem and so any digital currency that has this feature is not suitable for wide spread use. If anything governments should make it as difficult as possible for such currencies. There are other non-trivial problems with these currencies that must also be addressed.

Digital currencies do have the potential to reduce financial fees which can help stimulate the economy and facilitate international trade. On balance the government should set an environment that favors digital currencies that meet key criteria so that Australian entrepreneurs can develop such businesses within Australia and then spread their currencies overseas. There are several key activities for the government-

1. Define what constitutes an "acceptable" digital currency that avoids many of the problems identified.

2. Develop a legal and regulatory environment, and other incentives which encourages acceptable digital currencies and suppresses unacceptable currencies.
3. Develop codes of conduct for players in the digital currency arena.

Timing is very important as the first successful product in this area will most likely dominate the market. It would be beneficial to Australia if that dominant player were Australian.

Biography

Dr. Pj Radcliffe is a senior lecturer in the school of Electrical and Computer Engineering at RMIT University. He has had extensive industry and academic experience starting from 1979 in the areas of communications, networking, computing, software, and the Internet. He has written several popular articles on digital currencies and maintains a strong interest in the area. He does not own any digital currencies and has no personal stake that will be effected by the outcome of the senate inquiry.

References

[1] "An expensive lesson against selling bitcoin on eBay | PandoDaily." [Online]. Available: http://pando.com/2013/08/27/an-expensive-lesson-against-selling-bitcoin-on-ebay/. [Accessed: 01-Nov-2014].

[2] "Bitcoin Crime, Scams and Hacks - News on CoinDesk." [Online]. Available: http://www.coindesk.com/bitcoin-crime/. [Accessed: 01-Nov-2014].

[3] "Indictment In Bitcoin Bidding Scheme For Mitt Romney's Tax Returns - Forbes." [Online]. Available: http://www.forbes.com/sites/robertwood/2013/06/27/indictment-in-bitcoin-bidding-scheme-for-mitt-romneys-tax-returns/. [Accessed: 01-Nov-2014].

[4] "Arrest in U.S. Shuts Down a Black Market for Narcotics - NYTimes.com." [Online]. Available: http://www.nytimes.com/2013/10/03/nyregion/operator-of-online-market-for-illegal-drugs-is-charged-fbi-says.html?pagewanted=all&_r=0. [Accessed: 01-Nov-2014].

[5] "TaxProf Blog: Marian: Is Bitcoin the New Tax Haven?" [Online]. Available: http://taxprof.typepad.com/taxprof_blog/2013/08/marian--1.html. [Accessed: 01-Nov-2014].

[6] "Bitcoin related fraud offences, Hervey Bay and Kingaroy - QPS News." [Online]. Available: http://mypolice.qld.gov.au/blog/2014/06/25/bitcoin-related-fraud-offences-hervey-bay-kingaroy/. [Accessed: 01-Nov-2014].

[7] "What PayPal s Past Means for Bitcoin s Future - Bank Think Article - American Banker." [Online]. Available: http://www.americanbanker.com/bankthink/what-paypals-past-means-for-bitcoins-future-1065935-1.html. [Accessed: 01-Nov-2014].

[8] "Nearly 150 Breeds Of Bitcoin-Stealing Malware In The Wild, Researchers Say." [Online]. Available: http://www.forbes.com/sites/andygreenberg/2014/02/26/nearly-150-breeds-of-bitcoin-stealing-malware-in-the-wild-researchers-say/. [Accessed: 01-Nov-2014].

[9] "One group controls 51 percent of Bitcoin mining, threatening security sanctity | PCWorld."

[Online]. Available: http://www.pcworld.com/article/2364000/bitcoin-price-dips-as-backers-fear-mining-monopoly.html. [Accessed: 01-Nov-2014].

[10] "Let's face it, the protocol has major flaws | Elite Trader." [Online]. Available: http://www.elitetrader.com/et/index.php?threads/lets-face-it-the-protocol-has-major-flaws.281223/. [Accessed: 01-Nov-2014].

[11] "Bitcoin Market Price (USD)." [Online]. Available: https://blockchain.info/charts/market-price. [Accessed: 01-Nov-2014].

[12] "Bitcoin Total Bitcoins in Circulation." [Online]. Available: https://blockchain.info/charts/total-bitcoins. [Accessed: 01-Nov-2014].

[13] "How does Bitcoin work? - Bitcoin." [Online]. Available: https://bitcoin.org/en/how-it-works. [Accessed: 01-Nov-2014].

[14] "Bitcoin Price Index - Real-time Bitcoin Price Charts." [Online]. Available: http://www.coindesk.com/price/. [Accessed: 01-Nov-2014].

[15] "In Conversation with Bitcoin expert and NYU Professor David Yermack." [Online]. Available: http://theconversation.com/in-conversation-with-bitcoin-expert-and-nyu-professor-david-yermack-31048. [Accessed: 01-Nov-2014].

[16] "Real world shops - Bitcoin." [Online]. Available: https://en.bitcoin.it/wiki/Real_world_shops. [Accessed: 01-Nov-2014].

[17] "Money Transfers Abroad - Compare Foreign Currency Exchange Rates." [Online]. Available: http://www.bestexchangerates.com.au/transfer_money. [Accessed: 11-Nov-2014].

[18] "Holder Warns of Criminal Appeal of Bitcoin, Other Virtual Currencies - WSJ." [Online]. Available: http://online.wsj.com/articles/SB10001424052702304819004579489373683252290. [Accessed: 06-Nov-2014].

[19] "How the Feds Took Down the Silk Road Drug Wonderland | WIRED." [Online]. Available: http://www.wired.com/2013/11/silk-road/. [Accessed: 06-Nov-2014].

[20] "At Least Two Moderators Of 'Silk Road 2.0' Drug Site Forums Arrested." [Online]. Available: http://www.forbes.com/sites/andygreenberg/2013/12/20/at-least-two-moderators-of-the-silk-road-2-0-drug-site-forums-arrested/. [Accessed: 11-Nov-2014].

[21] "FIN-2013-G001." [Online]. Available: http://fincen.gov/statutes_regs/guidance/html/FIN-2013-G001.html. [Accessed: 01-Nov-2014].

[22] "ATO targets Bitcoin users." [Online]. Available: http://www.afr.com/p/technology/ato_targets_bitcoin_users_oawpzLQHDz2vEUWtvYLTWI. [Accessed: 01-Nov-2014].