OECD publishing

Please cite this paper as:

Blundell-Wignall, A. (2014), "The Bitcoin Question: Currency versus Trust-less Transfer Technology", *OECD Working Papers on Finance, Insurance and Private Pensions*, No. 37, OECD Publishing.
http://dx.doi.org/10.1787/5jz2pwjd9t20-en

OECD Working Papers on Finance, Insurance and Private Pensions No. 37

The Bitcoin Question

CURRENCY VERSUS TRUST-LESS TRANSFER TECHNOLOGY

Adrian Blundell-Wignall

JEL Classification: E5, F39, F65, G19, G2

OECD WORKING PAPERS ON FINANCE, INSURANCE AND PRIVATE PENSIONS

OECD Working Papers should not be reported as representing the official views of the OECD or of its member countries. The opinions expressed and arguments employed are those of the authors.

Working Papers describe preliminary results or research in progress by the author(s) and are published to stimulate discussion on a broad range of issues on which the OECD works. Comments on Working Papers are welcome and may be sent to the Directorate for Financial and Enterprise Affairs (daf.contact@oecd.org), OECD, 2 rue André-Pascal, 75775 Paris Cedex 16, France.

OECD Working Papers on Finance, Insurance and Private Pensions provide timely analysis and background on industry developments, structural issues, and public policy in the financial sector, including insurance and private pensions. Topics include risk management, governance, investments, benefit protection, and financial education.

The papers are generally available only in their original language, English or French, with a summary in the other if available.

OECD WORKING PAPERS ON FINANCE, INSURANCE AND PRIVATE PENSIONS
are published on www.oecd.org/daf/fin/wp

This document and any map included herein are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

Ce document et toute carte qu'il peut comprendre ne préjugent en rien du statut de tout territoire, de la souveraineté s'exerçant sur ce dernier, du tracé des frontières et limites internationales, et du nom de tout territoire, ville ou région.

© OECD 2014
Applications for permission to reproduce or translate all or part of this material should be made to: OECD Publishing, rights@oecd.org or by fax 33 1 45 24 99 30.

The Bitcoin Question:
Currency versus Trust-less Transfer Technology

by
Adrian Blundell-Wignall, OECD*

ABSTRACT

The financial crisis has led to a widespread loss of trust in financial intermediaries of all kinds, perhaps helping to open the way towards the general acceptance of alternative technologies. This paper briefly summarises the crypto-currency phenomenon, separating the '*currency*' issues from the potential technology benefits. With respect to crypto currencies, the paper argues that these can't undermine the ability of central banks to conduct monetary policy. They do, however, raise consumer protection and bank secrecy issues. The valuation of Bitcoins and price volatility issues are discussed, as well as electronic theft, contract failures, etc., all of which could result in large losses to users and hence ultimate costs to the taxpayer (e.g. the failure to provide adequate private pensions resulting in increased reliance on public pensions). The anonymity features of the crypto-currencies also facilitate tax evasion and money laundering, both of which are major public policy concerns. The technology associated with crypto-currencies, on the other hand, could ultimately shift the entire basis of trust involved in any financial transaction. It is an innovation that creates the ability to carry out transactions without the need for a trusted third party; i.e. a move towards trust-less transactions. This mechanism could work to eliminate the role of many intermediaries, thereby reducing transactions costs by introducing much needed competition to incumbent firms. The generic issues that policy makers need to examine are summarised.

Authorised for publication by Gabriela Ramos, OECD Chief of Staff and Sherpa to the G20.

JEL codes: E5, F39, F65, G19, G2

Keywords: Bitcoin, Gold standard, trust-less transaction, payment technology, intermediaries, legal tender, plenary powers, monetary policy

* Adrian Blundell-Wignall is the Special Advisor to the OECD Secretary-General on Financial Markets and Acting Director of the OECD Directorate of Financial and Enterprise Affairs (www.oecd.org/daf/abw). Paul Atkinson and colleagues in the OECD Secretariat provided comments on earlier drafts of this paper, though all errors and omissions remain those of the author.

Table of Contents

I. INTRODUCTION

"Money" has three broad characteristics: a store of value, a unit of account and a medium of exchange - though "money" doesn't have to be legal tender. On the face of it crypto-currencies could be thought of as meeting all of these "money" roles. They are (as are many things) a potential store of value, albeit a very unstable one. They could be used as a unit of account and, as the earliest known use of a Bitcoin retail transaction was to buy a pizza, they can be used as a medium of exchange for anyone willing to accept them. In this latter role they have significant advantages, as they can be divided digitally for any size of transaction and they avoid the high fees charged by credit card companies. But it is likely that the main reason crypto-currencies are 'taking off' in acceptability as a means of payment is due to the anonymity feature. The high degree of anonymity feature has great advantages for illegal activities such as money laundering, avoiding financial regulations, terrorist financing and evading taxes.

The financial crisis led to a loss of trust in many financial intermediaries, trading platforms and payment systems. The main innovation of crypto-currencies is the feature of trust-less transactions (the ability to avoid the need for a trusted third party). Barter is always possible – window cleaners could negotiate with shops, doctors' surgeries and farms to exchange hours or cleaning for goods and services. However, barter is a poor medium of exchange and cleaning cannot be meaningfully stored (and hence isn't a store of value). Casino chips, airline miles, Amazon credits, Disney money could also be used for some functions outside of their primary intended use, but not with the potential usability features of crypto-currencies in the digital age.[1]

Crypto-currencies can never become an alternative to legal tender, for the simple reason (as will be explained below) that people have to pay their taxes. This protects existing fiat currencies from being displaced, and the fear of loss of monetary control should not be used as an argument to prevent Bitcoins from circulating as parallel currencies. However, the technology of the digital payment protocols should not be confused with the parallel currency issue. With respect to the currency function, there are two potential policy issues: (a) consumer protection issues: e.g. electronic theft; a collapse in value of crypto coins say due to the emergence of substitutes; the use of government plenary powers to ban them, etc.; and (b) anonymity features permitting an expansion of socially unacceptable activities such as tax evasion and money laundering. The digital transfer technology, on the other hand, could play highly-socially useful roles. The basics of crypto-currencies are set out in section II using Bitcoin as the main example. How to think about their value is discussed in section III. Theft, substitutes and plenary powers are discussed in section IV. Contract law and the relevance of the need to pay taxes are set out in section V. The use of the governments' plenary powers is discussed in the context of the abandonment of the Gold Standard in section VI. The 'useful technology' issue is discussed in section VII. Finally, some concluding observations on policy issues are offered in section VIII.

[1] These parallel currencies have an exchange rate with the dollar, and this is also possible with Bitcoin by using a broker like *Coinbase* which provides easy to use Bitcoin wallets linked to bank accounts not unlike Paypal.

II. WHAT IS A CRYPTO-CURRENCY?

With respect to Bitcoin, the founders "seeded" the market by providing algorithms to early "miners" who accumulated the first stock of Bitcoins; and holders of such stock benefited from subsequent price increases. By using computers intensively and incurring high electricity costs, subsequent participants could mine for Bitcoins, of which a total of 21 million is the fixed supply. The supply function for the coins is reputedly spread out by reducing the size of blocks to be found and via an algorithm that makes finding them dynamically more difficult if they are found too quickly. It may take many years to mine them all. Bitcoins trade on an online market and anyone can buy them at the going exchange rate with the dollar on Bitcoin broker platforms (like *Coinbase),* though the price has proven to be very volatile to date. Part of the reason for this is that there is no clear intrinsic value or agreed valuation method, and certainly no Bitcoin central bank prepared to intervene to make the price more stable, which would violate the fixed supply element.

The digital transfer technology is very interesting. There is an open source key cryptology, one public and one private. Bitcoin transactions transfer ownership of a 'coin' from one public address to another, but a private key is required to de-crypt the Bitcoins and spend them. Public and private keys are alphanumeric strings based on sophisticated encryption: random numbers and letters are derived from public keys by the application of a "hash" function (a process that takes an arbitrary block of data and returns a fixed size bit string). Authentication is like *fingerprinting* - there can only be one generator of transfers with a given address (though of course storing private identification strings online opens the way for stealing and fraud as with anything where money and the internet is involved). Bitcoins in the form of public keys are stored in "wallets", on a computer's hard drive and can only be accessed with the private key. Safety against hacking is increased by the use of off-line "cold storage", and such services are provided by broker platform intermediaries. Wallets stored with an internet connection, or linked with a smartphone application are akin to cash, and Bitcoins can be moved from cold storage to mobile wallets as required.

Transactions are recorded in the "Block Chain" which is the key innovation in this technology – that is, a technology that removes the need for a trusted third party and the intermediary costs associated with such institutions (banks, credit card companies, payment companies, non-bank financial intermediaries). The Block Chain is a public database (giant ledger book), openly maintained by computers all over the world – it is a sequential record of all transactions and current ownership. This tracking and verification of transactions is supported by the decentralised computing power generated by the activity of 'mining', and this activity is rewarded in Bitcoin fees. The Block Chain allows participants to check whether transfers are coming from actual owners of coins and it avoids problems like "double spending" – you can't spend the same Bitcoin fraction more than once.[2]

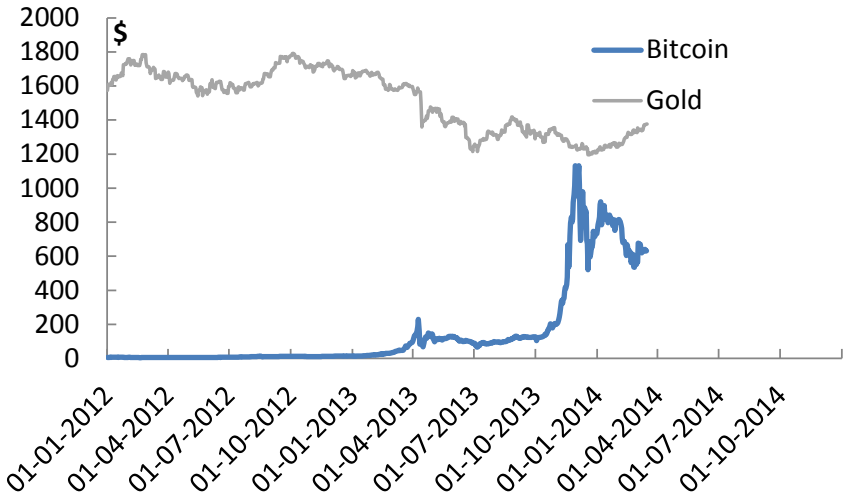
This Bitcoin technology has spawned a rapidly growing industry of crypto-currency innovations that use independent block chain methods (e.g. Bitcoin, Litecoin, Dogecoin, NXT, BitShares and Ethereum). Other protocols are built on top of the Bitcoin Block Chain to do new interesting things, like tokens being identified with specific assets for trading purposes (Coloured Coins, Mastercoin, and Counterparty). The Block Chain technology does have an important scalability problem, however, related to the computing power required to re-calculate the history of all transactions (discussed below), a problem which grows larger the more widespread the use of Bitcoins.

[2] Problems with this could arise if one miner controlled 51% of the computing power, which would attacks on the Block Chain.

III. VALUING BITCOINS

Figure 1 shows the Bitcoin price compared to the gold price. The price is single digit in 2012, around $100 for much of 2013 and then it moves up quickly to $1100 at the end of the year and collapses to the $500-$800 range for the early months of 2014.

Figure 1. **Bitcoin Prices versus Gold**



Source: Datastream, Bitcoincharts.com.

Such extreme high prices might be explained by strong inelastic demand and tight supply. Assuming that anonymity is important for some market participants to evade taxes or to launder money, the demand can well exceed mining supply. The supply side too may be a factor. For example, the difficulty of mining might suddenly accelerate, or miners might engage in cartel-like behaviour. Alternatively, speculative demand might enter the market, with each trader believing that buying at 10 or 20 times the mining cost doesn't matter, as long as someone else is willing to pay more than that – the '*greater fool'* theory. Judging by the sudden and extreme pick up in the volume of trading around the time of the price surge, the greater fool theory is probably the best contender for explaining the surge[3]. The recent price volatility certainly seems to have little to do with fair value – and part of the problem in valuing a crypto-currency is that it is a technology and not a business with a reported balance sheet or a currency backed by a commodity.

Attempts to value Bitcoins are highly unsatisfactory. Bank of America's David Woo tries to do so by using a potential market capitalisation approach, putting a value on each of the following components:

[3] Though several news headlines in late 2013 helped to legitimise Bitcoin to the man in the street: the purchase of a large quantity of Bitcoins by a well-known executive; the BTC market in becoming the largest exchange in China possibly resulted in speculation about the potential for Bitcoins in China; perception of support by politicians after the first Congressional hearings; etc. All of these may have encouraged investor interest.

medium of exchange (B2C); means of payment (C2C); and store of value.[4] The values are based on heroic assumptions that add up to about $15bn (2012 prices), and with the coins in circulation at the time a Bitcoin would be worth about $1300. For the medium of exchange component he uses macro assumptions for consumption and money, assuming that ultimately Bitcoins will be responsible for 10% of world transactions (he gets a $5bn number). But this set of arbitrary assumptions ignores the potential role of competitors: barriers to entry in starting up a new crypto-currency are relatively low, regulation and a number of other factors that could just as easily make the coins worthless. For a means-of-payment value, Bitcoin is given a market cap in line with the three big money transfer companies: Western Union, Moneygram, and Euronet (about $4.5bn). However Bitcoin is not a company with payment system spreads that generates revenues for shareholders. Indeed the main socially-beneficial feature of the Bitcoin is that it is a technology that has low transactions costs. As a store of value Woo uses silver as a guide (about $5bn). This seems highly unrealistic as silver has intrinsic value whereas Bitcoins do not – they are not backed by anything.

An alternative way of thinking about fair value is to focus only on the medium of exchange role of Bitcoins: recognising the potential value of the technology of trust-less exchange, but also incorporating some of the risks. Let M reflect the (constant) electricity, hardware time and human capital cost of mining a Bitcoin, and ε is a random add-on to that cost depending on the degree of difficulty of the algorithm at the time, random 'luck' and other one-off factors. This is the underlying value to which market prices should gravitate, with the mining supply of Bitcoins rising or falling in response to whether the market price sits above or below it – provided of course that the crypto-currency is always 'acceptable' with no risk of being worthless due to fraud; a better substitute coming along; technological scalability issues; or government policy banning them. However, since all of these risks are present, the fair value of the coin could be thought of as the present discounted value of the variable mining cost with a probability "p" of a fatal risk event in any period. Using (say) a 5-year horizon:

$$PV = (1-p_1)(M+\varepsilon_1)d_1 + p_1(1-p_2)(M+\varepsilon_2)d_2 + \cdots + p_1p_2p_2p_4(1-p_5)(M+\varepsilon_5)d_5$$

Where: $d_i = 1/(1+r)^i$, r is the riskless bond rate and i=1…5.

For example, if the mining cost of 1 Bitcoin happened to be $100 exactly in every period, the risk free rate for the discount factor is 4% and the probability of a risk event is 50% in each period, then the value would be $85. Since $100 per coin might be thought of as a high mining cost, it is difficult to understand how values of over $1000 can be achieved. If there is no earnings stream for a payment system role and no intrinsic value (such as for gold or silver), or the 'good faith and credit' of a government (as for a fiat currency)[5], then the price should gravitate to the discounted medium-of-exchange (only) value. If the probability of a fatal event were to rise to 90% each period, the price would fall to $26; for 100% the price would fall to zero.

Unlike gold, there is no intrinsic value for a Bitcoin. Gold is a rare substance with a long history of discovery and a high cost of production. Gold's main use historically has been as money, and the move towards fiat currencies began only from 1914. Gold also has a strong store-of-value role as a hedge against inflation and other risks as well as industrial and decorative uses. Bitcoins have a supply function and a demand curve derived from the advantages they convey. But if governments take away those advantages, the coins are stolen via fraud or an alternative better crypto-currency emerges, Bitcoin prices would fall to zero and the recovery value for the stock of 'coins' too would be zero.

[4] See Sharf (2013). B2C stands for business-to-consumer, and C2C for consumer-to-consumer.

[5] Even gamblers in a casino have the good faith and credit of the casino when they use its chips.

IV. CONSUMER PROTECTION AND RISK EVENTS FOR CRYPTO-CURRENCIES

Dabbling in crypto currencies with extreme volatility raises consumer protection issues that bear some scrutiny by the relevant authorities, since unsophisticated investors could become involved and provide the 'greater fools' to the market. Since major losses by a household could ultimately result in the state having to pay higher benefits (e.g. failure to provide for an adequate pension as a result of large Bitcoin losses) the state should provide clear guidelines on registration and *know-your-customer* issues. The structure of the Bitcoin and other networks is not well set up for this due to the decentralised and anonymous nature of the participants.

Market volatility and fairness

The potential for market volatility and contract litigation issues seems large. For example, a real estate sales company starts taking Bitcoins to pay for houses from persons unknown and of dubious origins. They fail to convert the Bitcoins into legal tender for the client just prior to a major dip in price, or an event that takes their value to zero. The coins are not backed by anything and the network has no capital or obligations. The client has signed a contract accepting the risks and takes a massive wealth loss, while the money launderer now owns a building. Who does the house seller litigate against? Presumably the real estate agent, as the buyer is unknown. The real estate entity fails, and it has other links with banks and the financial system, creating losses and instability elsewhere in the financial system.

Fraud

This requires little elaboration. The Mount Gox episode illustrates that it is certainly possible for the coins to be stolen in a digital attack, and an exchange shut down, with the likelihood of all ex-owners losing their "money". Such episodes will likely incentivise other exchanges for crypto-coins to improve their security practices.

Substitutes

Bitcoins already have their imitators and innovators: e.g. Litecoin, Worldcoin, Mastercoin, Coloured Coins, Dogecoin and others – barriers to entry do seem to be very low. There is no reason why good or better crypto-currencies won't drive out bad ones, including Bitcoin itself. An initial widespread use of Bitcoins could emerge as a parallel currency only to be replaced by a better one. It would not be the first time that second-mover advantages outweigh those of first-movers.

Regulation

Some governments have already moved in some jurisdictions to regulate Bitcoins. China has banned yuan to Bitcoin deposits into BTC China (its largest exchange) and banned the use of the QQ exchange which had been used to buy real goods and services. Germany, France, Korea and Thailand have also indicated a repudiation of Bitcoins as a currency. Other countries are yet to follow. However, while some form of regulation of crypto-currencies will be important due to the anonymity issue, it is not at all necessary to ban their use as a private currency on the grounds of loss of monetary control, for reasons that will be explained in the following section.

V. CONTRACT LAW, LEGAL TENDER AND PAYING YOUR TAXES

The government decides what can or cannot settle a legal monetary contract. In most civil societies that consists of legal tender or cheques and other transfers drawn on a bank that is regulated by the government and is a part of the payments system - in normal circumstances a bank deposit is transferable into legal tender (since the bank deposits are insured and/or the bank can obtain cash through the lender-of-last-resort function). The government enforces all legal contracts through the civil legal code.

Some might argue that a crypto-currency is also transferable into legal tender. Stocks and securities of all forms are all transferable into legal tender, but they cannot serve as legal tender.

The ultimate reason for this is a certain government monopoly within the payments system. Everyone has to pay their taxes, and hence anyone's bank has to be able to clear with the government's bank, most often the central bank. The government will only accept legal tender for this purpose, which is precisely the leverage over the financial system that ensures that the government can affect interest rates in the entire economy. The government's bank will not accept Bitcoins in the clearing process. As the central banks own liabilities are the (rare) legal tender, no bank can exchange legal tender for Bitcoins within the payments system. A non-bank Bitcoin seller can receive a cheque or cash from a non-bank buyer, and then deposit dollars in his or her bank within the normal clearing system, as is also the case with stocks and bonds. But it is not "money". No matter how acceptable Bitcoins are amongst its enthusiasts, it can in no way impact the ability of the government to conduct monetary policy because everyone at the end of the day has to pay their taxes and must obtain central bank liabilities to clear with the central bank.

In the case of the '*dollarization*' phenomenon (e.g. Zimbabwe) this conclusion is not changed. While good US dollars drive out de-based local currency, dollarization involves the government accepting US dollars in the payment of taxes fees and fines, and hence the dollar's acceptance into the payment system. At this point the government has effectively decided to import US monetary policy as an explicit decision. No government should accept Bitcoins into the payment system and thereby lose control of the money supply and interest rates.

Taxes and money laundering issues are more substantial

While paying taxes involves clearing with the central bank and that ensures in general that monetary policy cannot be undermined, the issue of how to treat capital gains and losses for tax purposes in the crypto currency world and the problem of using anonymity to evade taxes are legitimate policy issues.

There appears to be a move by some countries to treat Bitcoin as a 'commodity' in terms of taxation. In November, the Canada Revenue Agency issued a news release which stated that any gains or losses from trading a digital currency would be considered taxable income or capital for the taxpayer. This tax treatment is similar to a capital asset (stocks, bonds, commodities, etc.), which are traded in the open market. The United States, Internal Revenue Service has taken a similar position for tax purposes. In other words, the position is that Bitcoin is not a currency, but that it will be treated as a commodity which can be traded with resulting gains or losses and which can be used to pay for goods and services with valuations for tax purposes being whatever the value of the Bitcoin is on the date of the payment or receipt.

The use of Bitcoins for tax evasion is a potentially very significant policy issue. Bitcoins, like cash transfers, cannot be traced by third parties and are essentially invisible to tax authorities. Everyone can see the public key accounts and all transactions, but not the identity attached to it. This makes taxation at source and information exchange agreements largely irrelevant, and similar issues would apply for money laundering. The Financial Crimes Enforcement Network (FinCen) of the US Treasury determined in March 2013 the circumstances under which Bitcoins would come within the Bank Secrecy Act. They have guided that Bitcoins are *'convertible virtual currencies'* and should be treated like a currency for the purposes of US anti-money laundering laws in the cases where Bitcoin money service providers can be classified as "*money transmitters*" (where Federal and State registration, recording, reporting and '*know your customer'* rules come into play)[6]. This is not inconsistent with the above treatment of Bitcoins as a commodity for tax purposes – it is akin to a currency with an exchange rate to the dollar the gains and losses from which are taxable.

A paradox

If a *raison d'etre* for Bitcoins is to carry out illegal activities due to the 'anonymity factor' it is likely true that the means is easily found to convert them back into legal tender. But there is a paradox here. The more successful the crypto currencies become at fraud, money laundering and/or the undermining of the tax system, the greater will be the incentive for the government to use its plenary powers to abandon its hitherto 'light-touch' in dealing with the crypto-currency phenomenon. Exchanges dealing in illegal activities have already been closed down and in the limit the government may use its plenary powers simply to ensure that any form of legal contract involving Bitcoins is unenforceable. All contract clauses in Bitcoins could be abrogated and unenforceable by the action of lawmakers. History is replete with examples, but none better than with the abandonment of the gold standard.

[6] That is, a business of administration of Bitcoin activities with a central repository which is transmitting something of value from one location to another where third parties to an initial transaction are involved. See FinCen (2013). In January 2014 it was further clarified that individuals and companies obtaining Bitcoins for their own use, or as investments, does not constitute being a money transmitter under the Bank Secrecy Act.

VI. PLENARY POWERS AND THE ABANDONMENT OF THE GOLD STANDARD IN 1933

Prior to 1933 the Gold Standard was the basis of the world monetary system. In the UK a *gold specie standard* was in place from 1821 when the Royal Mint began producing gold sovereigns until the outbreak of World War I. At that time the specie standard was abandoned and was replaced by Treasury notes backed by gold specie (i.e. redeemable in gold specie) – but with the Bank of England using patriotic motivations to avert the need for actual redemptions in gold specie. This in itself caused no legal issues as gold clauses in contracts could still be binding. In 1925 Britain formally returned to a gold bullion standard – the law compelled the authorities to sell gold at a fixed price in terms of the pound sterling. Any form of cash outflow from a country would cause them to begin losing gold stocks, the money supply would contract, and policies to reduce demand would be implemented to restore external balance. This caused intolerable economic hardship in the 1930's, and Australia and New Zealand were the first to leave the gold standard. Britain followed in 1931.

When Franklin D. Roosevelt came to power in the midst of the Great Depression, he immediately closed the banks under the Emergency Banking Act. Executive order 6102 then required the surrender of all gold bullion, coins and gold certificates to the government by 1 May 1933, in exchange for dollars at the rate of $20.67 per troy ounce.[7] However, many legal contracts were written with gold clauses, based on the legal tender at the time they were written. So Congress passed a resolution cancelling all gold clauses in both private and public contracts. The sense of the resolution was that gold clauses interfered with the power of Congress to regulate the US currency.

This was challenged in the High Court in a number of cases (Norman versus The Baltimore and Ohio Railroad; The USA versus Bankers Trust Corporation, 1935; Nortz versus the United States; and the Unites States versus Perry, 1935). The court decided in a 5-4 majority in all of these cases that: "*the power to regulate money is a plenary power*". The abrogation of all gold clauses was considered to be within the powers of Congress when such clauses presented a threat to Congress' control of the monetary system. In short, contracts specifying payment in a fixed quantity of gold were not enforceable in law. If Bitcoins begin to undermine the financial and tax systems they will be shut down and all contracts between traders would be unenforceable.

[7] See Friedman and Schwartz (1963) and, for a short summary, Richardson, Komai and Gou (2013).

VII. THE TECHNOLOGY WITHOUT ANONYMITY

Crypto-currencies solve an important problem: the safe transfer of ownership without the need of a middleman or trusted third party. This technology has the potential to reduce transactions costs for retail spending with credit cards, E-commerce costs and money transfers. Goldman Sachs (2014) uses the Coinbase fee of 1% for providing these services with Bitcoin and compares this to the 2-3% fees on credit cards, the 2.9% average fee for E-commerce and the 8.9% average fee for money transfers. Future regulatory costs could of course push up the cost of this example. But such companies are intermediaries too, and it should not be forgotten that competition in the crypto-currency world is fierce, and new decentralised technology innovations may reduce costs dramatically.

The biggest problem for the Bitcoin approach is the need to re-calculate the full Block Chain history to verify the validity of all current transactions – which becomes increasingly computer intensive and costly – if full security is to be assured. While miners are rewarded in this verification activity, other approaches are looking to provide new alternatives to the Block Chain. This scalability problem is something Bitcoin will have to solve but it isn't yet clear how this can be done.

The *Ripple* protocol is interesting in this respect and solves the scalability problem of Bitcoin. It is a trust-less transfer technology based on a network of servers that enables trading in different currencies. While it does have its own currency (XRP), this is mainly for system protection reasons. XRP is not required to be the store of wealth, unit of account and medium of exchange, and at least one global bank has begun to use the technology in the payment system to cheapen costs and reduce exchange risk. The equivalent of the block chain is a public ledger shared by a *unique node list* (UNL) of members' servers. The ledger is a record of all Ripple accounts – the '*last closed ledger'* is the last validated set of Ripple accounts. A set of new transactions arrives as proposals to change the ledger and forms a *candidate set* which is distributed to all external servers – those not on the UNL list are discarded and a set of iterations begins to match the transactions in the current candidate set. Once voting of server nodes reaches a consensus of 80% (after reformulating the candidate set and discarding invalid transactions at each stage) validation is declared, a new last closed ledger forms and the process starts again. This takes minutes only, and the voting procedure removes the huge electricity cost of mining activities associated with recalculating the Block Chain in the Bitcoin world. There is a small transaction fee in XRP (all members must hold at least 20 XRP) so that the cost in XRP can respond to any flooding scams and essentially block it.[8] This approach doesn't require the huge private centralised servers used by credit card companies, and ultimately this type of technology should act to undermine their expensive systems in the long run if they do not adapt to use it themselves. One German online bank has already adopted the Ripple protocol, allowing it to do trust-less transfers with partners greatly reducing payment costs. The speed of transactions greatly reduces currency risk during the payment process.[9]

[8] Ripple is said to deduct only 0.00001 of one unit of its currency XRP as a transactions fee, and one XRP in early 2014 was in the 30 to 40 cents range – tiny.

[9] In the current banking world a transfer order is made, and a cumbersome process with correspondent banks begins. The client is informed later of the price at which the exchange took place. The Ripple protocol allows an almost instantaneous transfer at the current price.

Whether or not the Ripple protocol is the ultimate winner remains to be seen, but policymakers should welcome the exploration of the use of new technology to improve efficiency and provide competition to high-cost incumbent intermediaries in the financial system. Policymakers do need to focus on how to ensure that the new technologies operate in the most socially-useful way. That is, it should be possible to make use of a new technology to facilitate the medium-of-exchange transporter and ledger functions and increase competition in financial services, while eliminating the 'anonymity' problems. In the above description of Ripple, for example, the nodes are clearly money transmitters, and so full registration should be required for all nodes. Such a system can have members that use their own unit of account and store of wealth – such as gold for example. It is not difficult to imagine an entire network using the technology of trust-less transfer amongst all sorts of assets based on an exchange rate with gold, or some other commodity priced in real time or a fiat currency like the dollar – banks, payment system companies, fund managers, insurance companies etc. transacting directly between members without requiring trusted third party intermediaries.

The technology is not a currency, and even if networks do use gold, Bitcoins, XRP coloured coins and the like, this could not interfere with monetary policy and would help to provide much needed competition for credit cards and other payment system functions.

VIII. CONCLUDING COMMENTS

There are genuine policy issues with existing crypto-currencies, including consumer protection and socially unacceptable activities related to tax evasion and money laundering. The payment technology itself, however, could play and important useful role in the financial system.

The generic policy issues that need to be addressed are:

- A general ban on any form of use of crypto currencies in the clearing system between banks and the central bank – to ensure that the monetary system is not undermined.

- Recognition that a trust-less transfer and ledger technology is separable from the idea of a crypto-currency and is potentially very useful for future competition in the financial system.

- Some form of agreement for best practice registration that permits consumer protection, tax and anti-laundering authorities to verify the owner's identity.

- A level playing field for all players in the financial system is important, so balance sheet reporting and income statements for all networks and other appropriate regulations would be important.

- Some amount of capital should be held by exchanges on the balance sheet (perhaps in the form of legal tender) for fraud and technological failures.

- Some form of backing for crypto-currencies may be wise – such as gold.

- The use of government plenary powers to close down all non-complying networks.

The general aim of policy should be to encourage technologies that improve competition in the payments system, and to ensure that the use of crypto-currencies remove anonymity where money transmission is concerned (to avoid the darker aspects of Bitcoin use) and to meet minimum requirements for consumer protection.

REFERENCES

FinCen (2013), "Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies", 18 March.

Friedman, M. and A. Schwartz (1963). *A Monetary History of the United States, 1867-1960*. Princeton: Princeton University Press.

Goldman Sachs (2014), "All About Bitcoin", in *Top of Mind*, March 11.

Richardson, G., A. Komai and M. Gou (2013), "Roosevelt's Gold Program: Spring 1933", in: 100 Years of the Federal Reserve System, http://www.federalreservehistory.org/Events/DetailView/24.

Sharf, Samantha (2013) "Bitcoin Gets Valued: Bank of America Puts a Price Target on the Virtual Tender", Forbes Magazine, 12 May 2013.

WORKING PAPERS PUBLISHED TO DATE

The full series is listed below in chronological order. Prior to March 2010, the series was named *OECD Working Papers on Insurance and Private Pensions*. All working papers can be accessed online at: www.oecd.org/daf/fin/wp.

2013

WP 36 Institutional investors and infrastructure financing

WP 35 Institutional investors and green infrastructure investments: selected case studies

WP 34 Promoting Financial Inclusion through Financial Education

WP 33 Financial Education in Latin America and the Caribbean

WP 32 Pension Fund Investment in Infrastructure: A Comparison between Australia and Canada

WP 31 Policyholder Protection Schemes: Selected Considerations

2012

WP 30 The Effect of Solvency Regulations and Accounting Standards on Long-Term Investing

WP 29 Trends in Large Pension Fund Investment in Infrastructure

WP 28: Communicating Pension Risk to DC Plan Members: The Chilean Case of a Pension Risk Simulator

WP 27: The Role of Funded Pensions in Retirement Income Systems: Issues for the Russian Federation

WP 26: Infrastructure Investment in New Markets: Challenges and Opportunities for Pension Funds

WP 25: The Status of Financial Education in Africa

WP 24: Defining and Measuring Green Investments: Implications for Institutional Investors' Asset Allocations

WP23: The Role of Institutional Investors in Financing Clean Energy

WP22: Defining and Measuring Green Investments: Implications for Institutional Investors' Asset Allocations

WP21: Identification and Assessment of Publicly Available Data Sources to Calculate Indicators of Private Pensions

WP20: Coverage of Private Pensions Systems: Evidence and Policy Options

WP19: Annual DC Pension Statements and the Communications Challenge

WP18: Lessons from National Pensions Communication Campaigns

WP17: Review of the Swedish National Pension Funds

WP16: Current Status of National Strategies for Financial Education

WP15: Measuring Financial Literacy: Results of the OECD International Network on Financial Education (INFE) Pilot Study

WP14: Empowering Women through Financial Awareness and Education

WP13: Pension Fund Investment in Infrastructure: Policy Actions

WP12: Designing Optimal Risk Mitigation and Risk Transfer Mechanisms to Improve the Management of Earthquake Risk in Chile

2011

WP11: The Role of Guarantees in Defined Contribution Pensions

WP10: The Role of Pension Funds in Financing Green Growth Initiatives

WP9: Catastrophe Financing for Governments

WP8: Funding in Public Sector Pension Plans - International Evidence

WP7: Reform on Pension Fund Governance and Management: The 1998 Reform of Korea National Pension Fund

2010

WP6: Options to Improve the Governance and Investment of Japan's Government Pension Investment Fund

WP5: The New IAS 19 Exposure Draft

WP4: The EU Stress Test and Sovereign Debt Exposures

WP3: The Impact of the Financial Crisis on Defined Benefit Plans and the Need for Counter-Cyclica Funding Regulations

WP2: Assessing Default Investment Strategies in Defined Contribution Pension Plans

WP1: Framework for the Development of Financial Literacy Baseline Surveys: A First International Comparative Analysis

OECD Working Papers on Insurance and Private Pensions

2010

WP41: Policy Action in Private Occupational Pensions in Japan since the Economic Crisis of the 1990s

WP40: Pension Funds' Risk-management Framework: Regulation and Supervisory Oversight

WP38: Managing Investment Risk in Defined Benefit Pension Funds

2009

WP37: Investment Regulations and Defined Contribution Pensions

WP36: Private Pensions and Policy Responses to the Financial and Economic Crisis

WP35: Defined-contribution (DC) arrangements in Anglo-Saxon Countries

WP34: Evaluating the Design of Private Pension Plans

WP33: Licensing Regulation and the Supervisory Structure of Private Pensions

WP32: Pension Fund Investment in Infrastructure

WP31: Pension Coverage and Informal Sector Workers

WP30: Pensions in Africa

WP29: Ageing and the Payout Phase of Pensions, Annuities and Financial Markets

2008

WP27: Fees in Individual Account Pension Systems

WP26: Forms of Benefit Payment at Retirement

WP25: Policy Options for the Payout Phase

WP24: National Annuity Markets

WP23: Accounting for Defined Benefit Plans

WP22: Description of Private Pension Systems

WP21: Comparing Aggregate Investment Returns in Privately Managed Pension Funds

WP20: Pension Fund Performance

WP19: Coverage of Funded Pension Plans

WP18: Pension Fund Governance

WP17: Funding Regulations and Risk Sharing

WP16: Evaluating the Impact of Risk Based Funding Requirements on Pension Funds

WP15: Governance and Investment of Public Pension Reserve Funds in Selected OECD Countries

WP14: Sovereign Wealth and Pension Fund Issues

2007

WP13: Reforming the Valuation and Funding of Pension Promises

WP12: Pension Fund Investment in Hedge Funds

WP11: Implications of Behavioural Economics for Mandatory Individual Account Pension Systems

WP10: Portfolio Investment in an Intertemporal Setting

WP9: Collective Pension Funds

WP8: Pension Fund Regulation and Risk Management

WP7: Survey of Investment Choice by Pension Fund Members

WP6: Benefit Protection

WP5: Benefit Security Pension Fund Guarantee Schemes

WP4: Governments and the Market for Longevity-Indexed Bonds

WP3: Longevity Risk and Private Pensions

WP2: Policy Issues for Developing Annuities Markets

2006

WP1: Funding Rules and Actuarial Methods