Jan Kregel[*]

CAN DIGITAL CURRENCY SAVE THE WORLD FROM FINANCIAL CRISIS?

Hy Minsky famously remarked that it was not surprising that economics had little to say about financial crises since mainstream theory was based on the demonstration that the unimpeded operation of competitive market forces would produce equilibrium. As disequilibrium was obviously not a normal result crises were thus relegated to acts of God, external shocks, or statistical anomalies such as black swans and five-hundred-year floods. But reality has continued to contradict this theory and crises have become increasingly frequent, indeed endemic in the real world of capitalist financial systems. The problem, Minsky argued, was our inadequate understanding of the behaviour of the white swans, not the black ones. Of why crisis is not considered a natural result of the capitalist system.

One of the problems with mainstream theory was that it reasoned in real terms and relegated money to "applied" economics of business cycles. For most economists the role of money was represented by the accounting equality given by the Equation of Exchange, or by Marshall's analysis of the demand for money based on a desired cash ratio. Despite Keynes's final rejection of the Quantity theory in both forms, it regained new life as the result of Milton Friedman's *Monetarist counter-revolution* critique of the Keynesian fine-tuning approach to the "stagflation" of the late 1950's and 1960's.

But the emphasis on analysis in real terms had a more important omission, the absence of debt in early neoclassical synthesis Keynesian models developed in the 1960s. Minsky argued that even if the real economic variables were growing peacefully in equilibrium, there was an undergirding of financing relations that might become increasingly fragile, rendering the real equilibrium moot. If money is a commodity, or is supposed to be managed

[*] Linceo. Ragnar Nurkse Department of Innovation and Governance, Tallinn University of Technology

as if it were a commodity, then capitalist financing could be explained in real terms on the basis of the traditional loanable funds theory. Here money is embedded in a Say's Law world in which a reduction in consumption is offset by the real saving necessary to provide the loanable funds necessary for investment to expand. In such a world financial innovation is relegated to the creation of paper bank notes as a substitute for gold coin – which Adam Smith praised because they made it unnecessary to use gold for liquidity reserves and it could instead be used to finance business investment. Smith was not concerned that paper money might produce excess money creation, arguing that if business did not need the paper notes they would be returned to the banks.

Such a world is far from Minsky's favourite description of capitalism echoing the early work of Marx and Schumpeter who proposed realization crises and creative destruction as the natural result of bankers' ability to "create money out of nothing." As Schumpeter and other German and Austrian economists studying monetary cycles including Hayek and Hahn and others argued, it was this power that generated capitalist development punctuated by periodic financial crises. Even Hayek and Hahn held this view for a short period.

Minsky had a very insightful way to explain endemic financial crisis by noting that in a capitalist system the control and ownership of assets is obtained by issuing debt. He used a term of financial jargon to represent this relation: he defined "position" as the acquisition of an asset by incurring debt. A speculative position can be described as "selling what you don't have" to "buy what you don't need" because you expect the price of the former to fall so you can buy it back at a lower price, and the latter to rise so you can sell it at a higher price, reversing the position at a profit. This is just the contrary of the traditional description of finance which is to produce more than you need to acquire the funds to fund what you don't have. Here, every produced good has a destination in providing the ability to exchange in order to acquire what you don't have.

Of course, the goal of every capitalist position is speculative, that is to close your position with a profit which means selling the output created from the acquired inputs at a price which is enough to recover costs with a remaining surplus. Here higher prices increase output and vice versa, leading to equilibrium. But as noted above, it is also possible to profit by expecting to buy in what you don't have at some future date at a lower price and to sell what you don't want at a higher price. Here market exchanges produce adjustment counter to the traditional theory of price stabilization: if I sell in the expectation of falling prices, a fall in prices may induce me to increase the sale of things I don't have; if I expect prices to rise and my expectation in confirmed, I may buy more of what I don't want. The result

is that price signals and expectations are no longer homeostatic, but instead may become pathogenic. Thus, instead of falling prices reducing supply and increasing demand, just the opposite may occur.

As every economist knows, every trade has a buyer and a seller – and in most cases the seller expecting prices to fall has a bear position and the buyer, expecting prices to rise, a bull position. The expectations of one or the other must be disappointed. As prices move, the balance of bull and bear sentiment will move as profits are made and losses are suffered, and prices adjust as expectations are revised.

But there is an asymmetry between the bull and bear positions that emerges when we remember that control or ownership of assets is acquired by issuing debt. Minsky described this alternative response mechanism as dominant in financial crisis. For example, if you have borrowed to finance the acquisition of an asset with the expectation of appreciation, then if the price rises this increases your collateral and allows an increase in the leverage of your "position", you can borrow more to buy more without requiring any additional saving. This is a point that George Soros developed into his theory of "reflexivity" and which he has used with great success. While you are not obliged to take on more debt as prices rise, the confirmation of your expected profit makes this appear less risky and increases the incentive to do so.

On the other hand, if your expectation of a rise in price is disappointed, then the value of the asset held will decline and your lender may require additional security. If you cannot find accommodation then, in Minsky's terms you may be required to – "sell position to make position." You have no choice but to sell some of the asset to reduce your debt, to reduce your "position", indeed, your lender may do it for you. This means that when prices are falling there will be additional selling pressure on prices until prices no longer cover your outstanding debt, and you are insolvent. And here is the source of the financial crisis.

The dynamism also works if you are borrowing to sell in the expectation of buying back more cheaply and are disappointed; then you will have to buy in your position from those who hold the asset at a loss which may no longer cover your loans and erase your security and lead to insolvency. This is known as a "bear squeeze" which has a macabre twist at the end. If you were on the other side of this position and recognized a potential to increase your profits by buying as much of the asset available and refusing to sell to the bears to cover their position to make them bid up the price even higher – you may still lose, since your counterparties are bankrupt and cannot pay and you have accumulated a large long position at prices much higher than will continue to prevail. You would thus make losses as the market price collapses. In the mortgage crisis of 2007 and in more recent times

in the "Game Stop" crash this is what happened. Those who identified the "Big short" in the former and put on the "bear squeeze" in the latter risked losing their profits since their counterparties could not meet their commitments. It is important even in crisis for all the players to remain in the game, otherwise there is no game.

Irving Fisher, after assuring his clients that the market would automatically return to equilibrium after the 1929 stock market crash changed his approach and outlined a similar explanation of the negative impact of the collapse of stock prices under the name "debt deflation." Fisher's version differed in two respects – the generation of the crisis and the impact of falling prices on real purchasing power. For Fisher the initial fall in prices was the result of exogenous factors such as innovation from the 1920s (radio, airplanes) and the increase the real value of outstanding fixed in nominal terms, creating a vicious circle in which the real value of the debt to be repaid would increase faster than the position could be sold leading everyone to insolvency. Having lost his faith in the ability of the market to restore equilibrium Fisher became a believer in the necessity of "reflation", returning prices to precrash levels to restore equilibrium, only he now argued that government would be required to do what the market might not be able to do it on its own. It eventually took the New Deal to reverse the 1930 debt deflation.

Of course, the key to these price movements is in the initial assumption: the use of debt to acquire control of assets. Minsky went on to formulate his theory of financial fragility by classifying various types of borrowing to finance "position." In hedge finance the cash generated from the acquired liabilities far exceeds the interest costs of funding of the position; in speculative finance the cash may come up short, but additional short-term accommodation is available from lenders; in Ponzi finance the cash does not cover the interest carry cost and new funding is required to keep the position. Since there is no longer any profit being generated to repay lenders eventually the funding runs out or is called in by the lender and the entity has to sell position to make position and the crisis ensues. This is a system of slowly increasing leverage as the successful verification of expectations being met on hedge and speculative positions leads to increasing collateral values and debt finance and an increasingly fragile financial structure. A move in interest rates or funding conditions is enough to start the liquidation and a debt deflation.

Note that price response relative to expectations will always create winners' profits and losers' loss of capital. It is thus interesting that those who recognized the benefits of inflation and crisis to produce economic development when faced with hyperinflation reversed course and argued in favour of commodity money with zero leverage as supportive of equilibrium as a prerequisite for development.

This can be achieved by regulating the degree of leverage of private corporations or of banks, or creating competition which is to produce a preference for the most stable financial organisation. The latter initially considered a simple pro forma application of Hayek's theory to suggest competition in the financial sector, and since leverage in banking is created by the issue of banks' demand liabilities, this meant competition in the provision of money justified by the belief that providing a non-bank liability similar to cash would ensure price stability.

However, as Schumpeter pointed out – without leverage provided by the bankers the entrepreneurs never manage to acquire the commodities needed to make new innovations to increase income and employment. And the result is a stationary state, not a developmental state. So the conundrum - capitalist development requires leverage and leverage will always evolve from speculative to Ponzi finance and eventually produce a financial crisis in which the reversal of price expectations produce losses that exceed the net assets of investors.

Recently a number of proposals have been made to provide a replacement for bank liabilities to resemble bank notes or gold, but in a digital form. Indeed, the creator of one of the most prevalent digital currencies, bitcoin, [1] is interpreted by some as having believed he was proposing a solution to financial crisis and thus eliminating the need for government bailouts of the financial system.

The basis for this view is a message encrypted in the first bitcoin created, repeating a London Times headline from January 3, 2009 "Chancellor on brink of second bailout for banks." The idea is that it presents the project behind bitcoin as provision of a more fair and stable financial system based on a protocol that is pure computer code and thus immune from manipulation, fraud, bailout or rescue by any private financial institution or government agency or central authority [2] . The presumption is that a financial system based on bitcoin would have no leverage and no central authority

[1] Bitcoin: A Peer-to-Peer Electronic Cash System
Satoshi Nakamoto October 31, 2008https://nakamotoinstitute.org/bitcoin/

[2] The root problem with conventional currency is all the trust that's required to make it work. The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust. Banks must be trusted to hold our money and transfer it electronically, but they lend it out in waves of credit bubbles with barely a fraction in reserve. We have to trust them with our privacy, trust them not to let identity thieves drain our accounts. Their massive overhead costs make micropayments impossible.

Later, he wrote: Yes, [we will not find a solution to political problems in cryptography,] but we can win a major battle in the arms race and gain a new territory of freedom for several years. Governments are good at cutting off the heads of a centrally controlled networks like Napster, but pure P2P networks like Gnutella and Tor seem to be holding their own. See https://nakamoto.com/satoshi-nakamoto/

and thus could not become insolvent, fail and require government bailout or private loss. All transactions are the voluntary decisions of private individu-als to engage in transactions over the central organizing protocol embedded in the distributed ledger or block chain.

While this "creation myth" of the pursuit of a stable financial system may provide the explanation for the Nakamoto protocol which currently dominates other digital currencies, it fails as an explanation for the creation of digital financial instruments. Nor does it provide a solution to Minsky's proposed explanation of endemic financial fragility[3].

Many developers of alternative monetary frameworks have looked to the implications of the anonymity provided by the growth of the internet as the impetus for the development of digital currency. The locus classicus in this line of approach is found in Tim May's *Cryptoanarchy Manifesto*[4]. Crypto requires a new "Non-trust governance structure", based on the presumption that "Anonymous action will escape sanction and state control without the possibility of personal identification. Like a land of zombies. This raises the question of who will control information about actions. Combined with emerging information markets, crypto anarchy will create a liquid market for any and all material which can be put into words and pictures. Liquid markets in information".

But, in the development of the internet these "liquid markets" were not inherently anonymous. Indeed, their development on the basis of internet e-commerce has decreased invisibility and led to mechanisms for collecting and commercialising identity and private personal information. Indeed, only

[3] According to Craig Wright, «Bitcoin was not designed as a 'store of value', and it was not a built-in response to the global financial crisis. If somebody says it is, they are either an idiot/moron, a conman, or both». Craig Wright, *Bitcoin as a Security*, 25 July 2021, p. 11; re-published in CoinGeek, Editorial, 3 April 2022.

[4] «A specter is haunting the modern world, the specter of crypto anarchy. Computer technology is on the verge of providing the ability for individuals and groups to communicate and interact with each other in a totally anonymous manner. Two persons may exchange messages, conduct business, and negotiate electronic contracts without ever knowing the True Name, or legal identity, of the other. Interactions over networks will be untraceable, via extensive re-rout-ing of encrypted packets and tamper-proof boxes which implement cryptographic protocols with nearly perfect assurance against any tampering. Reputations will be of central importance, far more important in dealings than even the credit ratings of today. These developments will alter completely the nature of government regulation, the ability to tax and control economic interactions, the ability to keep information secret, and will even alter the nature of trust and reputation». The introduction to Tim May's *Crypto Manifesto*.

https://groups.csail.mit.edu/mac/classes/6.805/articles/crypto/cypherpunks/may-cryp-to-manifesto.html

The same themes are visible in the work of other cryptographers such as Whitfield Diffie. See Steven Levy, *Crypto: How the Code Rebels beat the Government—Saving Privacy in the Digital Age*, New York, NY, Penguin, 2001.

recently has the extent of identity transfer become obvious and required governments to impose privacy safeguards on participants in the global system.

Paradoxically, this expansion in private information in commercial transactions has led to the need for anonymity in the provision of digital currency. Robert Guttmann, writing in a 2002 book [(5)] noted that the "challenge to reviving the internet as a locus of commerce» after the dot.com collapse lies in the «question of how best to pay for purchases online". Although there were numerous attempts to provide digital currency, he notes that "something better is needed than cash, checks, bank wires or credit cards to pay for transactions on the internet". We can thus think of ebay auction markets, started in 1995, as the prototype of direct P2P commerce which needed an equivalent payment system which elicited an initial response in 1998 Confinity which became paypal absorbed by ebay, but was superseded by digital currencies such as bitcoin [(6)].

However, neither does history support this version of the impetus behind the search for internet cash as a secure and private message transmission linked to cryptography. The very first attempt at a secure messaging system that was extended to the creation of a non-commodity money apparently dates from the late 1960s [(7)]. It is due to a young graduate student grappling with the implications of the Bell theorem proving non-locality in quantum mechanics. Stephen Wiesner proposed a perfectly secure «quantum money» [(8)] that «it is physically impossible to counterfeit». The serial number expressed on each dollar bank note would carry a set of superpositioned photons inside special boxes. The issuing bank would insert the pho-

(5) *Cybercash: The Coming Era of Electronic Money*, New York, NY, Springer, 2002, p. 86.

(6) Although Nakamoto cites this approach in his Introduction »Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments." He proceeds to argue that it will be too costly for traditional financial institutions to provide trust by monitoring the "small casual transactions" required by internet commerce, thus requiring a "no-trust" system. His aim is to create the digital equivalent of small change! Craig Wright has also emphasized this aspect: «One reason why I created Bitcoin is directly linked to the nature of payments and the fact that the traditional internet payment mechanisms using credit cards didn't work for small-value transactions. Whilst large-value transactions in Bitcoin, and any related system, can be reversed, it is economically and computationally unfeasible to do so with small transactions. I never envisioned billion-dollar transactions as the use case of Bitcoin, for which it is a rather terrible system by itself. Instead, I saw the use of micropayments as small as a fraction of a cent and the ability to create small casual payments for systems such as online-gaming platforms. Such a methodology had value then, and it has value now» https://craigwright.net/blog/bitcoin-blockchain-tech/bitcoin-as-a-security/ p. 9.

(7) The system is fully described in Simon Singh, *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography*, New York, NY, Knopf Doubleday, 2011.

(8) Eventually published as S. Wiesner, *Conjugate coding*, ACM SIGACT News, Vol. 15, Issue 1 (Winter-Spring 1983), pp. 78-88.

tons in definite states of polarization (vertical, horizontal, right or left diagonal) and keep a sealed record in its archives of the arrays of polarizations that went with each serial number. Making a copy of the bill would require making measurements of each photon's polarization. If a photon in a box had been set in a diagonal polarization, but the counterfeiter chose to check for horizontal polarization instead, he would have a fifty-fifty chance of finding horizontal or vertical polarization, but not the correct diagonal since the filter would block the alternatives. For every unit of quantum currency, the counterfeiter would need to know the polarization of each photon before attempting to make a measurement or produce a copy. The bank, meanwhile, could easily check any bill against its own records to detect fakes. For the whole scheme to work, Wiesner had to assume that the pho-tons in the original dollar bill could not be duplicated without disturbing their original polarizations – an extreme assumption since the technology for placing photons in a particular polarized state for a sufficiently long period of time had not yet been developed. Even if the technology would have been available, it would be too expensive to implement it. It might cost in the region of $1 million to protect each dollar bill.

However, eventually a positive application was made in Vienna in April 2004 in which the city's mayor and the director of one of the city's larg-est banks collaborated with physicists from the University of Vienna and a spin-off company to produce the first electronic bank transfer using quantum cryptography. Specially prepared beams of light transmitted an unbreakable code – an encryption key – between the bank's branch office and city hall. If anyone else had tried to listen in on the signal, the eavesdropping would have been detected easily and unambiguously.

The real impetus for the cryptography that eventually allowed anony-mous digital currency development was the application of "one-way" func-tions by Whitfield Diffie (and we now know at least two other groups of researchers) which allowed asymmetric encryption. Again, these develop-ments had little to do with resolving financial crisis, save perhaps the family budgets of some of the researchers in the field who were facing difficulty in finding deep pocket funding outside National Security Administration. Further and they were not initially directed at the facilitation of online pay-ments which had yet to be implemented.

In the 1980s David Chaum produced a workable untraceable electronic currency system - digicash, [9] derivative of his work on blind signatures [10] to provide a voting system that could not be manipulated. The same prin-

[9] World's first electronic cash payment over computer networks DigiCash - 05/27/1994, available at https://chaum.com/ecash/

[10] David Chaum, *Blind Signatures for Untraceable Payments*, in: D. Chaum, R.L. Rivest, A.T. Sherman (eds), *Advances in Cryptology*, Boston, MA, Springer, 1983, pp. 199-203.

ciple, applied to payments, produced "ecash" which was first offered in the United States by Mark Twain bank where Hyman Minsky sat on its Board of Directors!

Wei Dai was the first to take May's challenge seriously, proposing a truly anonymous "b-cash" [11] based on two principles: "I am fascinated by Tim May's crypto-anarchy. Unlike the communities traditionally associated with the word "anarchy", in a crypto-anarchy the government is not temporarily destroyed but permanently forbidden and permanently unnecessary. It's a community where the threat of violence is impotent because violence is impossible, and violence is impossible because its participants cannot be linked to their true names or physical locations. Until now it's not clear, even theoretically, how such a community could operate. A community is defined by the cooperation of its participants, and efficient cooperation requires a medium of exchange (money) and a way to enforce contracts. Traditionally these services have been provided by the government or government sponsored institutions and only to legal entities. In this article I describe a protocol by which these services can be provided to and by untraceable entities".

Thus, while May assumed that the anonymity generated by the expansion of the internet was true, Dai and then Nakamoto after him tried to create the anonymity that was presumed to exist with the possession and use of physical cash bank notes by replicating them with digital money [12].

These developments were driven by two contrasting objectives. The first was derivative of May's manifesto – a purely unregulated, invisible mechanism which eventually served to provide liquidity to the Silk Road of money launderers and drug dealers which operated in the deep web independently of central institutions such as banks, or governments, or even other individuals. A system of "non-trust" which relied only on the individual [13].

[11] Wei Dai, *b-money*, Satoshi Nakamoto Institute, November 1998: http://www.weidai.com/bmoney.txt

[12] One reason why I created Bitcoin is directly linked to the nature of payments and the fact that the traditional internet payment mechanisms using credit cards didn't work for small-value transactions. Whilst large-value transactions in Bitcoin, and any related system, can be reversed, it is economically and computationally unfeasible to do so with small transactions. I never envisioned billion-dollar transactions as the use case of Bitcoin, for which it is a rather terrible system by itself. Instead, I saw the use of micropayments as small as a fraction of a cent and the ability to create small casual payments for systems such as online-gaming platforms. Such a methodology had value then, and it has value now. The Bitcoin was always designed to be, first and foremost, a micropayment system that could be extended beyond digital cash to the operation of other digital assets. …Given the state of the "cryptocurrency industry", both are the likely outcome.

[13] Opened in 2011. «In 2013, Silk Road founder and darknet drug emperor Ross Ulbricht, under the pseudonym Dread Pirate Roberts (DPR), seemed convinced that his website was destined to become

The other is clearly expressed by Craig Wright, who claims to have been, or have been part of the group that signed itself Satoshi Nakamoto: "The promise of Bitcoin lay never in removing government. The promise of Bit-coin lay in micropayments and a system that delivered an honest ledger" [(14)].

"In the past, eCash and related money-transfer systems were all based on a model of anonymity, aiming to make it private through encryption. I completely turned the model on its head, by not using encryption at any point within Bitcoin" [(15)].

It is here that the role of internet telecommunications and the search for an honest ledger come together with cryptography. A fair election requires verification of the individual vote but anonymity of the voter. An electronic voting system thus faces the problem of monitoring double voting. The same problem occurs with electronic money – physical notes can be counterfeit but that can be physically identified, while a digital note may be perfectly replicated. These are the types of questions that cryptography traditionally seeks to resolve, although usually reserved for government transmission of information. Chaum's problem of double voting, eliminated by blind signatures, or Wiesner's quantum money, solve the same problem as the elimination of counterfeiting, which the Bitcoin whitepaper presents as the problem of the "Double Spend". However, these initial solutions were not suitable because they relied on trust in a central authority or government for their organization.

Counterfeiting is a problem that needs to be eliminated for digital currency to replace existing physical notes, trust in centralised authority or government is not. The two basic characteristics of bitcoin that serve the second purpose but not the first are the blockchain and the proof of work provided by miners to convalidate "non-trust" in the system [(16)].

However, it is these two elements that provide the financial fragility inherent in the crypto protocol compared to the other digital cash proposals. It is perhaps paradoxical that it is in the most public aspects of the system,

the catalyst for a revolution. After all, his site linked nearly 4,000 drug dealers around the world to sell their wares to more than 100,000 buyers, and could you get you anything from falsified documents to heroin – even a rocket launcher».

https://www.oxygen.com/crime-time/ross-ulbricht-silk-road-darknet-dream-market-wall-street

"We're talking about the potential for a monumental shift in the power structure of the world", Ulbricht, still in the shadows as DPR, told Forbes, just months before he was ultimately arrested. "Sector by sector the State is being cut out of the equation and power is being returned to the individual".

(14) https://craigwright.net/blog/bitcoin-blockchain-tech/bitcoin-as-a-security/, p. 10.

(15) Wright, *Bitcoin as a Security*, cit., pp. 11-12.

(16) The original proposal circulated is *Bitcoin: A Peer-to-Peer Electronic Cash System*, by Satoshi Nakamoto, October 31, 2008 available at https://nakamotoinstitute.org/bitcoin/

rather than the anonymity of the agents provided by cryptography, that the systemic problems arise.

In the bitcoin system, instead of positing a decentralized system as having an advantage because of mistrust of government, the problem is posed in terms of the reversibility of transactions. In a traditional system this is taken care of via currency legislation. According to most legal systems currency is defined as that which provides a non-recourse liquidation of a debt. Thus, the purchase of stolen goods, if paid in currency, cannot be recovered in law by the rightful owner since it has been transferred to a new owner with payment in currency and is thus on a non-recourse basis. It is in this sense that a transaction cannot be reversed. In the case of digital cash, which would not be covered by currency legislation, a fraudulent transaction could be reversed if the system were run by a central authority. "Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party". So it is the possibility of reversal by the central authority that makes it necessary to provide an alternative mechanism of trust in the permanence of transactions. This is what bitcoin calls the “double spend” problem, which is similar to the counterfeiting problem in prior crypto research but not exactly the same. Both can be resolved by adjudication by a central authority, the double spend is a temporal problem because it is assumed a double spend must take place sequentially, rather than simultaneously which would be possible with a digital copy of the currency. It is the time stamp recording attached to each transfer of bitcoin that deals with the first problem, it is the recording in a consecutive ledger that solves the second. Together, the two problems are solved by a system of bookkeepers called “miners” who record and verify the temporal succession of transaction in a distributed (shared) ledger. Finally, the serial linkage of 100 consecutively registered and adopted ledgers makes any attempt to tamper with the time series of transactions of small sums becomes excessively costly – this is the temporally sequential linked series of distributed ledgers.

The double-spend problem thus also resolves the trust problem independently of any anarchic, decentralised or social preference governance

system in the form of a "peer to peer distributed time-stamp server" system. The non-reversible digital equivalent of cash called bitcoin in thus "an electronic coin as a chain of digital signatures".

At this stage we only have a definition of digital currency – but where does the digital money come from? The bitcoin world is composed of individual users, nodes and miners. Individual users create a digital identity by choosing a private key which is hashed into a public key and converted into a digital signature.

Pick at random a 256-bit value which creates a private key, an additional multiplication transforms the private key into a public key, which has your private key embedded, and an additional two transformations produces a digital code which is a bitcoin address. The use of one-way functions in the transformations means that knowledge of your bitcoin address cannot be easily derived from your public key. This creates privacy, but not with the objective of hiding identity but as security for your bitcoin.

But you only have an address, you have no coin. Where do they come from? How to you get one? Well to start you can receive one from someone who has one. A bitcoin owner signs his bitcoin with his private key and your public key and sends it to your address. At each transfer the coin acquires the recipients public key and the senders private key which is why it becomes a chain of digital signatures. You can now transfer the bitcoin to someone else by appending your private key and the recipients public key and sending it to their bitcoin address. Each transmission and the bitcoin's historical series are made public to all who have bitcoin addresses.

1. New transactions are broadcast to all nodes.
2. Each node collects new transactions into a block.
3. Each node works on finding a difficult proof-of-work for its block.
4. When a node finds a proof-of-work, it broadcasts the block to all nodes.
5. Nodes accept the block only if all transactions in it are valid and not already spent.
6. Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.

Now, all of this is required to provide decentralized trust in the form of avoiding reversals. The transactors are anonymous, but the addresses and public keys are visible, although the objectives of the transaction are not visible but known to each recipient. The history of each coin is visible, the nodes are all visible, as are those who verify the blocks representing the transaction ledger.

So back to the question of where the bitcoin come from if there is no government treasury or central bank or financial institution. In the American financial system cash is created by the Treasury and allocated to the private banks from the central bank in exchange for usually a government liability. So a liabilities on the government balance sheet, is acquired by a private bank who deposits it as collateral with the central bank in exchange for a reserve deposit which ca be converted to cash and distributed to clients who hold deposit accounts.

In the bitcoin system it is the bookkeeper accountants who manage the time stamp server. To manage the server they receive a payment or reward in bitcoin for performing what is called a "proof of work". The work is col-lecting the transactions distributed by the nodes and combining them into blocks with consistent time stamps. These participants are called miners but they would have nothing to verify if there are no bitcoin. It is perhaps easier to understand by following the paradigmatic story that it is a substitute for
Gold. You get gold by owning a mine and hiring labour to mine the gold; bit-coin can be "earned" by "proof of work" by a "miner" who receives a coin-base or "block award" (initially 50 bitcoin). So you don't need to own a gold mine, but you do need a sophisticated computer system. You also need an internet connection and a source of energy to run the computer system.

So the simple answer is that only miners can create bitcoin which they receive in payment for their "work" verifying transactions. Miners take the place of the traditional financial system. Why do we really need miners? As noted above this is to resolve the reversal or double spend or counterfeiting problem: trust. But this raises a chicken and egg problem. If only miners can create bitcoin by verifying transactions that they enter on a ledger block, where do the bitcoin used in the transactions that the miners verify come from? There had to be a first two transactors who existed before the first miners.

The creator(s) of bitcoin – Nakamoto – solved this problem using a system that has come to be called Patoshi which created the first 50 bitcoin coinbase (miner block reward) payment to the first miner. The trick was to allow the first miner to make a zero-value transaction, and the "work" was to validate that transaction (zero since there weren't any in existence yet) and to receive 50 bitcoin, recording it in single transaction Block 0 times-tamped on January 03, 2009 at 1:15 PM EST. So much for "non-trust", but every myth needs a garden of Eden.

As a result the initial block (called the *Genesis* block) in the first ledger of what would become the bitcoin block chain showed that the miner(s) of this block earned a total reward of 50.00 bitcoin consisting of a base reward of 50.00 bitcoin with an additional 0.00 bitcoin ($0.00) reward paid as fees of the 0.0 bitcoin sent in the block to the identifying address of the miner. The identity of the first bitcoin was technically the address of the owner (the miner) and the ledger showing its validation by the miner.

Schumpeter would be proud of this creation of bitcoin out of nothing, but perplexed that nothing was created out of the bitcoin except the blockchain – no creation, no destruction.

The first block which confirmed an actual movement of bitcoin from one address to another (they may have been the same owner) was number 170 sending 10 bitcoin of the 50 bitcoin fee to Hal Finney (long rumoured to be Nakamoto) on January 11, 2009 at 10:30 PM EST. The miner(s) of this block earned a total reward of 50 bitcoin. The next non-zero value transaction occurs in block 181 on January 12, 2009, followed sporadically by transactions in blocks 182, 183, 248, 545 and 546.

Aside from this initial period, there was no limit on miners who were intended to compete in providing block verification. Indeed, this competitive process is the representation of "trust" in the validation of the information in the system. Transactions are only confirmed after a miner has completed the proof of work and it is accepted by all according to the chain rule (it includes coins with the longest transactions histories) latency depends on miners' speed in confirming transactions and validating blocks of transactions and competing miners may choose which transactions to include in a block. Users are encouraged to include a "fee" for the miner of the successful proof of work to give miners an incentive to deal with their transaction first. This is a sort of "pay to play" incentive with the higher the fee the more rapid the transaction.

This is just a long story to demonstrate that all bitcoin in existence and will ever be created are created by miners in the form of block rewards. The finite limit on creation is achieved by imposing a halving rule which reduces the value of the block reward by half every four years. It is this factor which sets a maximum limit on the miners' ability to create bitcoin since the reward will eventually trend to zero. This regulation gives as a corollary the 21 million limit on total temporal creation of bitcoin. This is the money supply algorithm and is often presented as the monetary policy algorithm, which is a fixed money supply.

But this is not correct. Note that the first transaction referenced above also referred to a "fee." Above it was suggested that fees could be offered to miners to accelerate inclusion of a transaction in a validated block. The intention of the original protocol was rather to provide a transition from block rewards to transactions fees as the source of miners' remuneration. Thus there is a limit in which the mine is exhausted, and miners must impose transactions fees to validate transactions.

This raises the possibility that the bitcoin system will also be subject to instability. When the maximum creation of bitcoin is reached, every transaction will reduce the outstanding supply of bitcoin as users transfer bitcoin back to miners as transaction fees. The faster bitcoin comes to be used in

transactions the quicker the outstanding supply will decline and return to miners. Thus just as the beginning of the system required miners spending bitcoin with non-miners that they had received as block rewards the survival of the system will then depend on miners increasing their no-fee spending with non-miners. Again, it should be clear that the supply of bitcoin is not stable or given since it will depend on the relative propensities to transact of miners and non-miners and the size of fees. One possible result is the transfer of all bitcoin back to the miners. This is a possibility since the major expense of miners is not in bitcoin but in dollars or other traditional currencies.

In addition the supply conditions are tighter than those imposed by the miners' remuneration protocol. Of the 19 million bitcoin that have already been mined (by 2022) around 3 to 4 million are estimated to be unusable (because the owners or their keys have been lost) and an additional 10 to 12 million of the outstanding supply do not transact, that is they are held in the anticipation of price appreciation as speculative assets.

There is a second source of instability. If there is increasing use of bitcoin in transactions the most likely result is a temporal decline in supply and a trend deflation in bitcoin prices. Indeed, this is the reason bitcoin has been presented as an inflation hedge. But, recalling the intention to provide small change, it is interesting that each bitcoin is officially divisible into 100,000,000 "satoshis" which would allow for the possibility of declining goods prices. This does not, however, reduce the problem caused by deflation if time contracts are denominated in bitcoin.

In particular, this would mean the deflationary bias in prices denominated in bitcoin implies a transfer of real income from borrowers to creditors, from latecomer buyers to existing holders, and from lower to higher wealth holders. This calls into question another supposed tribute of digital currency that it is attractive to the "unbanked". It also means that miners will require higher fees since they have a currency mismatch – they earn declining bitcoin fees but have costs in traditional fiat currency. This would likely lead to even more miner pool concentration: currently half of blocks are currently mined by top 4 mining pools holding a 51% concentration of computing power. If energy and other costs do not fall miners might not be able to validate transactions and produce blocks in a timely manner. In which case bitcoin ceases to function and there is incentive to change the source code to secure dominance of miners. When miners with over 50% of computer power decide to cooperate instead of competing they can rewrite the block chain at their pleasure and benefit, and there is no longer any guarantee of non-trust.

All of this raises the question of whether bitcoin can ever become a dominant transaction currency and whether, if it did, it would be more stable than the traditional system it is meant to replace.