[https://gegen-kapital-und-nation.org/en/bitcoin-finally-fair-money/]

Bitcoin - Finally, fair money?

In 2009 Satoshi Nakamoto invented a new electronic or virtual currency called Bitcoin, the design goal of which is to provide an equivalent of cash on the Internet.[1] Rather than using banks or credit cards to buy stuff online, a Bitcoin user will install a piece of software, the Bitcoin client, on her computer and send Bitcoin directly to other users under a pseudonym.[2] One simply enters into the software the pseudonym of the person one wishes to send Bitcoin and the amount to send and the transaction will be transmitted through a peer-to-peer network.[3]
What specifically one can get with Bitcoin is somewhat limited to the few hundred websites which accept them, but includes other currencies, web hosting, server hosting, web design, DVDs, coffee in some coffee shops, and classified adverts, as well as the ability to use online gambling sites despite being a US citizen and to donate to Wikileaks.[4] However, what allowed Bitcoin to break into the mainstream – if only for a short period of time – is the Craigslist-style website "Silk Road" which allows anyone to trade Bitcoin for prohibited drugs.[5]

On February 11th, 1 BTC exchanged for 5.85 USD. So far 8.31M BTC were issued, 0.3 Million BTC were used in 8,600 transactions in the last 24 hours and about 800 Bitcoin clients were connected to the network. Thus, it is not only some idea or proposal of a new payment system but an idea put into practice, although its volume is still somewhat short of the New York Stock Exchange.

The three features of cash which Bitcoin tries to emulate are anonymity, directness and lack of transaction costs, all of which are wanting in the dominant way of going about e-commerce using credit or debit cards or bank transfers. It is purely peer-to-peer just like cash is peer-to-peer. So far, so general.

But what makes the project so ambitious is its attempt to provide a new currency. Bitcoin are not a way to move Euros, Pounds or Dollars around, they are meant as a new money in itself; they are denominated as BTC not GBP. In fact, Bitcoin are even meant as a money based on different principles than modern credit monies. Most prominently, there is no "trusted third party", no central bank in the Bitcoin economy and there is a limited supply of 21 million ever. As a result, Bitcoin appeals to libertarians who appreciate the free market but are sceptical of the state and in particular state intervention in the market.

Because Bitcoin attempts to accomplish something well-known – money – using a different approach, it allows for a fresh perspective of this ordinary thing, money. Since the Bitcoin project chose to avoid a trusted third-party in its construction, it needs to solve several 'technical' problems or issues to make it viable as money. Hence, it points to the social requirements and properties which money has to have.

In the first part of this text we want to both explain how Bitcoin works using as little technical jargon as possible and also show what Bitcoin teaches about a society where free and equal exchange is the dominant form of economic interaction. In the second part we then want to criticise Bitcoin's implicit position on credit money. From this also follows a critique of central tenets of the libertarian ideology.

The first thing one can learn from Bitcoin is that the characterisation of the free market economy by the (libertarian) Bitcoin adherents (and most other people) is incorrect; namely, that exchange implies:

Mutual benefit, cooperation and harmony.

Indeed, at first sight, an economy based on free and equal exchange might seem like a rather harmonious endeavour. People produce stuff in a division of labour such that both the coffee producer and the shoemaker get both shoes and coffee; and this coffee and those shoes reach their consumers by ways of money. The activity of producers is to their mutual benefit or even to the benefit of all members of society. In the words of one Bitcoin partisan:

"If we're both self-interested rational creatures and if I offer you my X for your Y and you accept the trade then, necessarily, I value your Y more than my X and you value my X more than your Y. By voluntarily trading we each come away with something we find more valuable, at that time, than what we originally had. We are both better off. That's not exploitative. That's cooperative."[6]

In fact, it is consensus in the economic mainstream that cooperation requires money and the Bitcoin community does not deviate from this position: "A community is defined by the cooperation of its participants, and efficient cooperation requires a medium of exchange (money) …"[7] Hence, with their perspective on markets, the Bitcoin community agrees with the consensus among modern economists: free and equal exchange is cooperation and money is a means to facilitate mutual accommodation. They paint an idyllic picture of the 'free market' whose ills should be attributed to misguided state intervention and sometimes misguided interventions of banks and their monopolies.[8]

Cash

One such state intervention is the provision of money and here lies one of Bitcoin's main features: its function does not rely on a trusted third-party or even a state to issue and maintain it. Instead, Bitcoin is directly peer-to-peer not only in its handling of money – like cash – but also in the creation and maintenance of it, as if there was no Bank of England but there was a protocol by which all people engaged in the British economy collectively printed Sterling and watched over its distribution. For such a system to accomplish this, some 'technical' challenges have to be resolved, some of which are trivial, some of which are not. For example, money needs to be divisible, e.g., two five pound notes must be the same as one ten pound note, and each token of money must be as good as another, e.g., it must not make a difference which ten pound note one holds. These features are trivial to accomplish when dealing with a bunch of numbers on computers, however, two qualities of money present themselves as non-trivial.

Digital signatures: guarantors of mutual harm

Transfer of ownership of money is so obvious when dealing with cash that it is almost not worth mentioning or thinking about. If Alice hands a tenner to Bob, then Bob has the tenner and not Alice. After an exchange (or robbery, for that matter) it is evident who holds the money and who does not. After payment there is no way for Alice to claim she did not pay Bob, because she did.

Neither can Bob transfer the tenner to his wallet without Alice's consent except by force. When dealing with bank transfers etc., it is the banks who enforce this relationship, and in the last instance it is the police.

One cannot take this for granted online. A banknote is now represented by nothing but a number or a string of bits. For example, let us say 0xABCD represents 1 BTC (Bitcoin).[9] One can copy it easily and it is impossible to prove that one does not have this string stored anywhere, i.e., that one does not have it any more. Furthermore, once Bob has seen Alice's note he can simply copy it. Transfer is tricky: how do I make sure you really give your Bitcoin to me?[10]

This is the first issue virtual currencies have to address and indeed it is addressed in the Bitcoin network.

To prove that Alice really gave 0xABCD to Bob, she digitally signs a contract stating that this string now belongs to Bob and not herself. A digital signature is also nothing more than a string or big number. However, this string/number has special cryptographic/mathematical properties which make it – as far as we can ascertain – impossible to forge. Hence, just as people normally transfer ownership, say a title to a piece of land, money in the Bitcoin network has its ownership transferred by digitally signing contracts. It is not the note that counts but a contract stating who owns the note. This problem and its solution – digital signatures – is by now so well established that it hardly receives any attention, even in the Bitcoin design document.[11]

Yet, the question of who owns which Bitcoin in itself starts to problematise the idea of harmonic cooperation held by people about economy and Bitcoin. It indicates that in a Bitcoin transaction, or any act of exchange for that matter, it is not enough that Alice, who makes coffee, wants shoes made by Bob and vice versa. If things were as simple as that, they would discuss how many shoes and how much coffee was needed, produce it and hand it over. Everybody happy.

Instead, what Alice does is to exchange her stuff for Bob's stuff. She uses her coffee as a lever to get access to Bob's stuff. Bob, on the other hand, uses his shoes as a leverage against Alice. Their respective products are their means to get access to the products they actually want to consume. That is, they produce their products not to fulfil their own or somebody else's need, but to sell their products such that they can buy what they need. When Alice buys shoes off Bob, she uses her money as a leverage to make Bob give her his shoes; in other words, she uses his dependency on money to get his shoes. Vice versa, Bob uses Alice's dependence on shoes to make her give him money.[12] Hence, it only makes sense for each to want more of the other's for less of their own, which means deprive the other of her means: what I do not need immediately is still good for future trades. At the same time, the logic of exchange is that one wants to keep as much of one's own means as possible: buy cheep, sell dear. In other words, they are not expressing this harmonious division of labour for the mutual benefit at all, but seeking to gain an advantage in exchange, because they have to. It is not that one seeks an advantage for oneself but that one party's advantage is the other party's disadvantage: a low price for shoes means less money for Bob and more product for her money for Alice. This conflict of interest is not suspended in exchange but only mediated: they come to an agreement because they want to but that does not mean it would not be preferable to just take what they need.[13] This relation they have with each other produces an incentive to cheat, rob, steal.[14] Under these conditions – a systematic reason to cross each other – answering the question who holds the tenner is very important.

This systemic production of circumstances where one party's advantage is the other party's disadvantage also produces the need for a monopoly on violence of the state. Exchange as the dominant medium of economic interaction and on a mass scale is only possible if parties in general are limited to the realm of exchange and cannot simply take what they need and want. The libertarians behind Bitcoin might detest state intervention, but a market economy presupposes it. When Wei Dai describes the online community as "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."[15] he not only acknowledges that people in the virtual economy have good reasons to harm each other but also that this economy only works because people do not actually engage with each other. Protected by state violence in the physical world, they can engage in the limited realm of the Internet without the fear of violence.

The fact that 'unbreakable' digital signatures – or law enforced by the police – are needed to secure such simple transactions as goods being transferred from the producer to the consumer implies a fundamental enmity of interest of the involved parties. If the libertarian picture of the free market as a harmonic cooperation for the mutual benefit of all was true, they would not need these signatures to secure it. The Bitcoin construction – their own construction – shows their theory to be wrong.

Against this, one could object that while by and large trade was a harmonious endeavour, there would always be some black sheep in the flock. In that case, however, one would still have to inquire into the relationship between effort (the police, digital signatures, etc.) and the outcome. The amount of work spent on putting those black sheep in their place demonstrates rather vividly that it is expected there would be many more of them without these countermeasures. Some people go still further and object on the more principal level that it is all down to human nature, that it is just how humans are. However, by saying that, one first of all agrees that this society cannot be characterised as harmonic. Secondly, the statement "that's just how it is" is no explanation, though it claims to be one. At any rate, we have tried to give some arguments above as to why people have good reason to engage with each other the way they do.

Purchasing power

With digital signatures only those qualities of Bitcoin which affect the relation between Alice and Bob are treated, but when it comes to money the relation of Alice to the rest of society is of equal importance. That is, the question needs to be answered how much purchasing power Alice has. When dealing with physical money, Alice cannot use the same banknote to pay two different people. There is no double spending, her spending power is limited to what she owns.

When using virtual currencies with digital signatures, on the other hand, nothing prevents Alice from digitally signing many contracts transferring ownership to different people: it is an operation she does by herself.[16] She would sign contracts stating that 0xABCD is now owned by Bob, Charley, Eve, etc.

The key technical innovation of the Bitcoin protocol is that it solves this double spending problem without relying on a central authority. All previous attempts at digital money relied on some sort of central clearing house which would ensure that Alice cannot spend her money more than once. In the Bitcoin network this problem is addressed by making all transactions public.[17] Thus,

instead of handing the signed contract to Bob, it is published on the network by Alice's software. Then, the software of some other participant on the network signs that it has seen this contract certifying the transfer of Bitcoin from Alice to Bob. That is, someone acts as notary and signs Alice's signature and thereby witnesses Alice's signature. Honest witnesses will only sign the first spending of one Bitcoin but will refuse to sign later attempts to spend the same coin by the same person (unless the coin has arrived in that person's wallet again through the normal means). They verify that Alice owns the coin she spends. This witness' signature again is published (all this is handled automatically in the background by the client software).

Yet, Alice could simply collude with Charley and ask Charley to sign all her double spending contracts. She would get a false testimony from a crooked witness. In the Bitcoin network, this is prevented, however, by selecting one witness at random for all transactions at a given moment. Instead of Alice picking a witness, it is randomly assigned. This random choice is organised as a kind of lottery where participants attempt to win the ability to be witness for the current time interval. One can increase one's chances of being selected by investing more computer resources. But to have a decent chance one would need about as much computer resources as the rest of the network combined.[18] In any case, for Alice and Charley to cheat they would have to win the lottery by investing considerable computational resources, too much to be worthwhile – at least that is the hope. Thus, cheating is considered improbable since honest random witnesses will reject forgeries.

But what is a forgery and why is it so bad that so much effort is spent, computational resources wasted for solving the aforementioned mathematical puzzle, in order to prevent it? On an immediate, individual level a forged bank note behaves no different from a real one: it can be used to buy stuff and pay bills. In fact, the problem with a forgery is precisely that it is indistinguishable from real money, that it does not make a difference to its users: otherwise people would not accept it. Since it is indistinguishable from real money it functions just as normal money and more money confronts the same amount of commodities and the value of money might go down.[19]

So what is this value of money, then? What does it mean? Purchasing *power*. Recall, that Alice and Bob both insist on their right to their own stuff when they engage in exchange and refuse to give up their goods just because somebody needs them. They insist on their exclusive right to dispose over their stuff, on their private property. Under these conditions, money is the only way to get access to each other's stuff, because money convinces the other side to consent to the transaction. On the basis of private property, the only way to get access to somebody else's private property is to offer one's own in exchange. Hence, money counts how much wealth in society one can get access to. Money measures private property *as such*. Money expresses how much wealth as such one can make use of: not only coffee or shoes but coffee, shoes, buildings, services, labour-power, anything. On the other hand, money counts how much wealth as such my coffee is worth: coffee is not only coffee but a means to get access to all the other commodities on the market: it is exchanged for money such that one can buy stuff with this money. The price of coffee signifies how much thereof. All in all, numbers on my bank statement tell me how much I can afford, the limit of my purchasing power and hence – reversing the perspective – from how much wealth I am excluded.[20]

Money is power one can carry in one's pockets; it expresses how much control over land, people, machines, products I have. Thus, a forgery defeats the purpose of money: it turns this limit, this magnitude into an infinity of possibilities, anything is – in principle – up for grabs just because I

want it. If everyone has infinity power, it loses all meaning. It would not be effective demand that counts, but simply the fact that there is demand, which is not to say that would be a bad thing, necessarily.

In summary, money is an expression of social conditions where private property separates means and need. For money to have this quality it is imperative that I can only spend what is mine. This quality, and hence, this separation of means and need, with all its ignorance and brutality towards need, must be violently enforced by the police and on the Bitcoin network – where what people can do to each other is limited – by an elaborate protocol of witnesses, randomness and hard mathematical problems.[21]

The value of money

Now, two problems remain: how is new currency introduced into the system (so far we only handled the transfer of money) and how are participants convinced to do all this hard computational work, i.e., to volunteer to be a witness. In Bitcoin the latter problem is solved using the former.

In order to motivate participants to spend computational resources on verifying transactions they are rewarded a certain amount of Bitcoin if they are chosen as a witness. Currently, each such win earns 50 BTC plus a small transaction fee for each transaction they witness. This also answers the question of how new coins are created: they are "mined" when verifying transactions. In the Bitcoin network money is created 'out of thin air', by solving a pretty pointless problem – that is, the puzzle whose solution allows one to be a witness. The only point of this puzzle is that it is hard, that is all.[22] What counts is that other commodities/merchants relate to money as money and use it as such, not how it comes into the world.[23]

Thin air: Bitcoin, credit money and capitalism

However, the amount of Bitcoin one earns for being a witness will decrease in the future – the amount is cut in half every four years. From 2012 a witness will only earn 25 BTC instead of 50 BTC and so forth. Eventually there will be 21 million BTCs in total and no more.

There is no a priori technical reason for the hard limit of Bitcoin; neither for a limit in general nor the particular magnitude of 21 million. One could simply keep generating Bitcoin at the same rate, a rate that is based on recent economic activity in the Bitcoin network or the age of the lead developer or whatever. It is an arbitrary choice from a technical perspective. However, it is fair to assume that the choice made for Bitcoin is based on the assumption that a limited supply of money would allow for a better economy; where "better" means more fair, more stable and devoid of state intervention.[24] Libertarian Bitcoin adherents and developers claim that by 'printing money' states – via their central banks – devalue currencies and hence deprive their subjects of their assets.[25] They claim that the state's (and sometimes the banks') ability of creating money 'out of thin air' would violate the principles of free market because they are based on monopoly instead of competition. Inspired by natural resources such as gold, Satoshi Nakamoto chose to fix a ceiling for the total amount of Bitcoin to some fixed magnitude.[26] From this fact most pundits quickly make the transition to the "deflationary spiral" and whether it is going to happen or not; i.e., whether this choice means doom for the currency by exponentially

fast deflation – the value of the currency rising compared to all commodities – or not. Indeed, for these pundits the question why modern currencies are credit money hardly deserves attention. They do not ask why modern currencies do not have a limit built in, how credit money came about, if and how it is adequate for the capitalist economy and why the gold standard was departed from in the first place.[27] They are not interested in explaining why the world is set the way it is but instead to confront it with their ideal version. Consequently, they miss what would likely happen if Bitcoin or something like it were to become successful: a new credit system would develop.

Growth

Capitalist enterprises invest money to make more money, to make a profit. They buy stuff such as goods and labour-power, put these 'to work' and sell the result for more money than they initially spent. They go through cycles of buying – production – selling.[28] The faster each of these steps, the faster the advanced investment returns, the faster the profit arrives and the faster new investments can be made. Capitalist success is measured by the difference between investment and yield and not by the amount of money someone owns in absolute terms. Of course, the absolute amount of wealth a company owns is a relevant magnitude, because more money is a better basis for augmentation. Yet, in order to decide whether a company did well or poorly in the last quarter, the surplus is usually what counts. For a capitalist enterprise, money is a means and *more* wealth – counted in money – the end: fast growth – that is the mantra.

Libertarian Bitcoin adherents have no problem with this. While currently Bitcoin are mainly used – if at all – to buy means of consumption or as a hoard, they hope that one day something like Bitcoin will replace the US dollar and other central bank controlled currencies: Bitcoin or its successor as the currency to do serious business in. This sets Bitcoin apart from other virtual currencies such as Linden Dollars or World of Warcraft Gold. They are purely used to buy/sell in some limited realm of some virtual world, while Bitcoin are in principle usable for any purchase (on the Internet). Bitcoin want to be money, not just some means of circulation in a virtual reality.

Credit

If money is a means for growth and not the end, a lack of money is not sufficient a reason for the augmentation of money to fail to happen. With the availability of credit money, banks and fractional reserve banking it is evident that this is the case. Just because some company did not earn enough money yet to invest in a new plant, that does not mean it cannot – it would apply for a loan from a bank. That bank in the last instance may have borrowed that money from the central bank which created it 'out of thin air'. However, assume, for the sake of argument, that these things did not exist. Even then, at any given moment, companies (or parts thereof) are necessarily in different stages of their accumulation cycles: some are just starting to sell a large stock of goods while others are looking to buy machines and hire workers. Some companies have money which they cannot spend yet while other companies need money to spend now. Hence, both the need and means for credit appear. If some company A expects to make, say, 110 BTC from a 100 BTC investment but only has 70 BTC in its accounts, it could take a loan of 30 BTC from some company B with 10% interest rate and still make 10 - 3 = 7 BTC of profit. For the company B which lends A 30 BTC, this business – if successful – is also better than just sitting on those 30 BTC which earn exactly nothing. If growth is demanded, having money sitting idly in one's vaults

while someone else could invest and augment it is a poor business decision.[29] This simple form of credit hence develops spontaneously under free market conditions.[30] The consequences of this fact are not lost on Bitcoin adherents. As of writing, there are several attempts to form credit unions: attempts to bundle up the money people have in their wallets in order to lend it out to others – for interest, of course.

Furthermore, under the dictate of the free market, success itself is a question of how much money one can mobilise. The more money a company can invest the better its chances of success and the higher the yield on the market. Better technologies, production methods, distribution deals and training of workers, all these things are available – for a price. Now, with the possibility of credit the necessity for credit arises as well. If money is all that is needed for success and if the right to dispose over money is available for interest then any company has to anticipate its competitors borrowing money for the next round of investments, rolling up the market. The right choice under these conditions is to apply for credit and to start the next round of investment oneself; which – again – pushes the competition towards doing the same. This way, the availability of money not only provides the possibility for credit but also the basis for a large scale credit business, since the demand for credit motivates further demand.

Even without fractional reserve banking or credit money, e.g., within the Bitcoin economy, two observations can be made about the relation of capital to money and the money supply. If some company A lends some other company B money, the supply of means of payment increases. Money that would otherwise be petrified to a hoard, kept away from the market, used for nothing, is activated and used in circulation. More money confronts the same amount of commodities, without printing a single new banknote or mining a single BTC. That is, the amount of money active in a given society is not fixed, even if Bitcoin was the standard substance of money.

Instead, capital itself regulates the money supply in accordance with its business needs. Businesses ‘activate’ more purchasing power if they expect a particular investment to be advantageous. For them, the right amount of money is that amount of money which is worth investing; to have available that money which can be used to make more money. This is capital’s demand for money.[31]

Growth guarantees money

When one puts money in a bank account or into some credit union, or simply lends it to some other business, to earn an interest, the value of that money is guaranteed by the success of the debtor to turn it into growth. If the debtor goes bankrupt that money is gone. No matter what the substance of money, credit is guaranteed by success.

In order to secure against such defaults creditors may demand securities, some sort of asset which has to be handed over in case of a default. On the other hand, if on average a credit relation means successful business, an IOU – i.e., a promise of payment – itself is such an asset. If Alice owes Bob and Bob is short on cash but wants to buy from Charley he can use the IOU issued by Alice as a means of payment: Charley gets whatever Alice owes Bob. If credit fulfils its purpose and stimulates growth then debt itself becomes an asset, almost as good as already earned money. After all, it should be earned in the future. Promises of payment get – and did get in the past – the quality of means of payment. Charley can then spend Alice’s IOU when buying from Eve, and so forth. Thus, the amount of means of payment in society may grow much larger than the official money, simply by exchanging promises of payment of this money. And this happens without

fractional reserve banks or credit money issued by a central bank. Instead, this credit system develops spontaneously under free market conditions and the only way to prevent it from happening is to ban this practice: to regulate the market, which is what the libertarians do not want to do.

However, the replacement of cash by these securities remains temporary. In the most severe situation, in crisis, the means of payment available for the whole of society would be reduced back to hard cash again, which these credit tokens were meant to replace. Simply because people start distrusting the money quality of these promises of payment would lead to a collapse of trade which relies on these means of payment. In crisis, credit's purpose to replace money is void.

Central banks

This is where the central banks step in, they replace the substance of money with something adequate for its purpose: a money whose value is guaranteed by the growth it stimulates. With the establishment of central banks, the economy is freed from the limitations of the total social hoard of hard cash. If there is a lucrative business then there is credit: money which is regulated according to the needs of capital. Credit money as issued by a central bank is not a promise of payment of money, it is itself money. The doubt whether these promises of payments are actually money ought to be put to rest by declaring them as money in the first place.

Now, the value of modern credit money is backed by its ability to bring about capitalist growth. When it facilitates this growth then – and only then – money fulfils its function.

Hence, something capital did to money before, is now 'built in'. The central bank allows private banks to borrow (sometimes buy) additional funds – for interest – when needed. The money they borrow is created by the central bank 'out of thin air'. Hence, all money in society comes into being not only with the purpose of stimulating growth but also with the explicit necessity: it is borrowed from the central bank which has to be paid back with interest. While clearly a state intervention, the central banks' issuing of money is hardly a perversion of capitalism's first purpose: growth. On the contrary, it is a contribution to it.

Systematic enmity of interests, exclusion from social wealth, subjection of everything to capitalist growth – that is what an economy looks like where exchange, money and private property determine production and consumption. This also does not change if the substance of money is gold or Bitcoin. This society produces poverty not because there is credit money but because this society is based on exchange, money and economic growth. The libertarians might not mind this poverty, but those on the Left who discovered Bitcoin as a new alternative to the status quo perhaps should.

1This text is a slightly revised version of a text which first appeared on http://metamute.org and was written in collaboration with Scott Lenney.

2 The central white paper on Bitcoin is *Bitcoin: A Peer-to-Peer Electronic Cash System* by Satoshi Nakomoto, the Bitcoin creator. However, some details of the network are not explicitly described anywhere in the literature but only implemented in the official Bitcoin client. As far as we know, there is no official specification except for https://en.bitcoin.it/wiki/Protocol_specification.

3 A peer-to-peer network is a network where nodes connect directly, without the need of central servers (although some functions might be reserved to servers). Famous examples include Napster, BitTorrent and Skype.

4 Probably due to pressure from the US government all major online payment services stopped processing donations to the Wikileaks project (http://www.bbc.co.uk/news/business-11938320). Also, most US credit card providers prohibit the use of their cards for online gambling.

5 After Gawker media published an article about Silk Road (http://gawker.com/5805928/the-underground-website-where-you-can-buy-any-drug-imaginable) two US senators became aware of it and asked congress to destroy it. So far, law enforcement operations against Silk Road seem to have been unsuccessful.

6 https://forum.bitcoin.org/index.php?topic=5643.0;all

7 Wei Dai, *bmoney.txt*, http://www.weidai.com/bmoney.txt. This text outlines the general idea on which Satoshi Nakamoto based his Bitcoin protocol.

8 "The Real Problem with Bitcoin is not that it will enable people to avoid taxes or launder money, but that it threatens the elites' stranglehold on the creation and distribution of money. If people start using Bitcoin, it will become obvious to them how much their wage is going down every year and how much of their savings is being stolen from them to line the pockets of banksters and politicians and keep them in power by paying off with bread and circuses those who would otherwise take to the streets." – http://undergroundeconomist.com/post/6112579823

9 For those who know a few technical details of Bitcoin: we are aware that Bitcoin are not represented by anything but a history of transactions. However, for ease of presentation we assume there is some unique representation – like the serial number on a five pound note.

10 "Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. [...] Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. [...] 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." – Satoshi Nakomoto, op. Cit.

11 For an overview of the academic state-of-the-art on digital cash see Burton Rosenberg (Ed.), *Handbook of Financial Cryptography and Security*, 2011.

12 To avoid a possible misunderstanding. That money mediates this exchange is not the point here. What causes this relationship is that Alice and Bob engage in exchange on the basis of private property. Money is simply an expression of this particular social relation.

13 Of course, people do shy away from stealing from each other. Yet, this does not mean that it would not be advantageous to do so.

14 The Bitcoin designers were indeed aware of these activities of direct appropriation and the need to protect the possible victim . "Transactions that are computationally impractical to reverse

would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers." – Satoshi Nakomoto, op. Cit.

15 Wei Dai, op. Cit.

16 "The problem of course is the payee can't verify that one of the owners did not double-spend the coin." – Satoshi Nakomoto, op. Cit.

17 "We need a way for the payee to know that the previous owners did not sign any earlier transactions. For our purposes, the earliest transaction is the one that counts, so we don't care about later attempts to double-spend. The only way to confirm the absence of a transaction is to be aware of all transactions." – Satoshi Nakomoto, op. Cit. Note that this also means that Bitcoin is far from anonymous. Anyone can see all transactions happening in the network. However, Bitcoin transactions are between pseudonyms which provides some weaker form of anonymity.

18 On the Bitcoin network anyone can pretend to be arbitrary many people by creating many pseudonyms. Hence, this lottery is organised in such a way that any candidate has to solve a mathematical puzzle by trying random possible solutions which requires considerable computational resources (big computers). This way, being 'more people' on the network requires more financial investment in computer hardware and electricity. It is just as in the lottery: those who buy many tickets have a higher chance of winning. As a side effect, many nodes on the network waste computational resources solving some mathematical puzzle by trying random solutions to win this witness lottery.

19
For many people, this is where they content themselves with knowing that the value goes down without ever asking what this "value" thing is. However, changes in value only make sense if one knows what it is that changes. Furthermore, the relationship of money supply and inflation is not as it might seem: increased money supply does not necessarily imply inflation; only if it is not accompanied by increased economic activity.

20 From this it is also clear that under these social conditions – free and equal exchange – those who have nothing will not get anything, aka the poor stay poor. Of course, free agents on a free market never have nothing, they always own themselves and can sell their skin – their labour-power – to others. Yet, their situation is not adequately characterised by pointing out that nature condemns us to work for the products we wish to consume, as the libertarians have it. Unemployed workers can only find work if somebody else offers them a job, if somebody else deems it profitable to employ them. Workers cannot change which product they offer, they only have one. That this situation is no pony farm can be verified by taking a look at the living conditions of workers and people out of work worldwide.

21 The Bitcoin forum is – among other things – a remarkable source of ignorant and brutal statements about the free market, such as this: "If you want to live then you have to work. That's nature's fault (or God's fault if you're a Christian). Either way, you have to work to survive. Nobody is obligated to keep you alive. You have the right not to be murdered, you don't have the right to live. So, if I offer you a job, that's still a voluntary trade, my resources for your labor. If you don't like the trade then you can reject it and go survive through your own means or simply lay down and die. It's harsh but fair. Otherwise, I'd have to take care of myself and everyone else which is unfair. Requiring me to provide you a living is actual slavery, much worse than nonexistent wage slavery." – https://bitcointalk.org/index.php?topic=5643.0\%3ball

22 “The only conditions are that it must be easy to determine how much computing effort it took to solve the problem and the solution must otherwise have no value, either practical or intellectual” – Wei Dai, op. Cit.

23 Those who read Marx’s Capital might now object that this implies that Bitcoin is based on a concept of value whose substance is not abstract human labour. Instead it would rely on value which is abstract computer labour or something else entirely. This objection is based on a misunderstanding: computing power earns, if one is lucky, 50 BTC but this is just a number, it is meaningless. What 50 BTC buy, how much purchasing power or command over social wealth they represent is an entirely different question. 50 BTC have value because they command social wealth not because a computer picked the right random number.

24 “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.” – Satoshi Nakamoto quoted in Jashua Davis, *The Crypto-Currency: Bitcoin and Its Mysterious Inventor*, The New Yorker, 10 October, 2011.p. 62.

25 We stress that opposing states increasing the ‘money supply’ at will and fixing the absolute amount of money that can ever be created are not the same thing. One could just as well keep generating 50 new BTC every 10 minutes until the end of time or the Bitcoin network – whichever comes first.

26 “The steady addition of a constant amount of new coins is analogous to gold miners expending resources to add gold to circulation. In our case, it is CPU [central processing unit] time and electricity that is expended.” – Satoshi Nakomoto, op. Cit. Furthermore, the distribution of how Bitcoin are generated is inspired by gold. In the beginning it is easy to mine but it becomes harder and harder over time. Bitcoin’s mining concept is an attempt to return to gold money but on the Internet.

27 cf. our text “Public debt makes the state go round” available at http://www.junge-linke.org/en/public-debt-makes-the-state-go-round. It should be noted that Bitcoin is not an equivalent to a return to the gold standard but a return to paying with gold coins. Even under the gold standard there were many more dollars than the gold they represented, based on the assumption that people would not claim the gold worth of their dollars from the FED.

28 Some companies such as supermarkets do not have a production phase, they simply buy and sell. This difference does not matter for the argument presented here though.

29 Of course, there are also reasons keep a certain amount of money around, such as the uncertainties of the markets.

30 An even simpler form of credit exists between whole-sellers and producers. If, for example, the producer allows the whole-seller to pay later, he is effectively granting credit.

31 On a side note, if businesses which take out loans are successful on average, they produce more commodities: more commodities that confront the increased supply of purchasing power.

Hence, increases in the money supply, and hence purchasing power, does not necessarily mean inflation.