Bitcoin Doesn't Exist – Five Parts – All You Need To Know

By Raul I Meijer – The Automaticearth.com

Part 1

Dr. D: Bitcoin is all the rage today, and as it crosses over $10,000, a 10-bagger for the year, we should look at what it is, what it isn't, and why it's become so popular. Note my observations are those of a layman – which may be more useful than those of a programmer – but also those of a skeptic, which I'll get to at the end.

First, what is Bitcoin? Well, the idea of digital money goes back to the first digits, financial mainframes. In fact, the "money" in use today throughout the financial system have long been no more than virtual 1's and 0's on a spinning hard drive somewhere, but the idea of Bitcoin-money, private-money, goes back further still. I mean, what is "money"? At its core, it's no more than the most-tradable good in a given society, a trading chit we use as a measurement tool, a token recording how much value we created or are owed. Arguably the first money was not gold, not seashells or even barter, but a promise. Let me borrow your net and I'll give you a couple fish from the work. Why? Because you might break the net or I might use it, so I need to get paid for my risk, reward for my effort in making and storing the net to begin with.

So money at its most austere is simply a promise. But a promise to whom for what? And that's the problem. No matter what good you use, people place differing values on it, different time-preferences, and most especially ways to cheat, game the system, and renege. This is bad among businesses, banks – who are after all only men – especially bad among governments, but worst of all among government and banks combined. Because, should the banks lie, renege, default, abuse their privilege, who then would hold them to task?

In the past, over and over, groups have created their own "money". The whole 19th century was marked by general stores extending credit, bank notes issued by thousands of private banks, each with their own strength and solvency and geography and discounted accordingly. In the 20th century, with central banks controlling money, many cities issued local "scrip" – promises to pay – in Detroit in the Depression, or California in the budget crunch of 2009, or "Ithaca Dollars" in NY as a sort of ongoing Ivy League experiment. But the problem with these only highlight the problems with money generally:who can issue them? Everyone? A central authority? Can they deliver goods? And what can they buy, not just in value but in location?

Ithaca Dollars or California Tax Vouchers are not much good to buy oil from Texas or tea from China. People will always prefer a good that is accepted everywhere, with no decay and no discount, because ultimately the money flows away, offshore or to central taxation, which makes local currencies ever-

less valuable. But even if successful it leads to a new set of problems: if Detroit or Ithaca Dollars were in high demand, there would be ever-stronger incentive to counterfeit, cheat, and double-spend them. Thus from the Renaissance to now we used reputable banks backed by force of governments, through the Gold standard and the Fiat age until today.

Enter the hackers.

It's not that these problems are unknown, or haven't been approached or attempted before. Every generation, when they find the banks + government take a percentage for their costs to insure the system, thinks how can we do away with these guys, who both take too much and end up in an unapproachable seat of power? I mean, aren't we supposed to be a Democracy? How can we have a fair society if the Iron Bank is both backing all governments at once, on both sides of a war? What good is it to work if compounding interest invariably leads to their winning Boardwalk and Park Place 100% of the time? But despite several digital attempts – some immediately shut down by government – no one had a solution until Satoshi Nakamoto.

We don't know who Satoshi Nakamoto is, but since several of the well-meaning developers were immediately jailed for even attempting private money on reasons arguably groundless, we can suppose he had good incentive to remain anonymous. And speculation aside, it doesn't matter: Satoshi's addition was not "Bitcoin" per se, but simply an idea that made private currency possible. The domain Bitcoin.org was registered in 2008, showing intent, and the open-source code was promoted to a small cryptography group in January 2009. But what was it? What did it solve?

Double-spending. Basically, the problem of money comes down to trust. Trust between individuals, between the system, but also partly trust in non-interference of governments or other powerful groups. Bitcoin is a trust machine.

How does it work? Well, the basic problem of cheating was one of not creating fake, hidden registers of value, as the U.S. Government, J.P. Morgan, and the Comex do every day. If they asked Yellen to type some extra zeros on the U.S. ledger, print a few pallets of $100 bills to send to Ukraine, who would know? Who could stop them? So with Bitcoin, the "value", the register is created by essentially solving a math problem, akin to discovering prime numbers. Why do something so pointless? Simple: math doesn't lie. Unlike U.S. Dollars, there are only so many prime numbers. We can be certain you won't reach 11-digits and discover an unexpected trove of a thousand primes in the row. Can't happen. However useless, Math is certainty. In this case, math is also limited. It's also known and provable, unlike the U.S. budget or Federal Reserve accounting.

The second problem of cheating was someone simply claiming chits they did not own. This was solved by having the participants talk back and forth with each other, creating a public record or ledger. In fact, Bitcoin is nothing more

than a very, very long accounting ledger of where every coin came from, and how every coin has moved since then, something computers do very well. These accounting lines register amongst all participants using a process of confirmed consensus.

Double-spending is when someone writes a check either against money they don't have (yet) and round-robin in the money for the one second of clearing, or else write a check against money they DO have, but then cancel the check before it clears, walking away with the goods. In a standard commerce, the bank backfills fraud and loss and the government arrests, tries, and imprisons people, but it's no small cost to do so. Although there is still a small possibility of double-spending, Satoshi's plan effectively closed the issue: the ledger is either written, or unwritten. There is no time in the middle to exploit.

Great for him, but if I buy coins by Satoshi and the original cryptogroup, won't I just be transferring all my value to make them rich? Although Bitcoin supply may be limited by mathematics, this is the issuer problem. It is solved because as a free, open source code, everyone has an equal opportunity to solve the next calculation. Bitcoin starts with the original 50 coins mined in 2009, so yes, early adopters get more: but they took more risk and trouble back when it was a novelty valuable only as proof-of-concept. The original cash transaction was between hackers to buy two pizzas for 10,000 BTC ($98M today). Why shouldn't they get preference? At the same time, we are not buying all 20 Million eventual coins from Satoshi and his close friends, which is arguably the case with the Federal Reserve and other central banks. Bitcoin is bought and created from equal participants who have been actively mining as the coins appear, that is, from doing electronic work.

This leads to the next challenge: why would anyone bother keeping their computers on to process this increasingly long accounting ledger? Electricity isn't free. The process of "mining" is the recording of Bitcoin transactions. The discovery of coins therefore effectively pays for the time and trouble of participating in a public accounting experiment. Even should that stop, the act of using Bitcoin itself cannot be accomplished without turning on a node and adding lines to process the ledger. So we can reasonably expect that people will keep Bitcoin software "on" to help us all get Bitcoin work done. That's why it's a group project: public domain shareware.

What if they shut it down? What if it's hacked? This leads to the next problem: resiliency. You have to go back a step and understand what Bitcoin is: a ledger. Anyone can store one, and in fact participants MUST store one. If Bitcoin were "shut off" as it were, it would be stored with each and every miner until they turned their computers back on. If it's "off" there's no problem, because no one transferred any Bitcoin. If it's "on" then people somewhere are recording transactions. Think of it like a bowling group keeping a yearly prize of the ugliest shirt. Is there an actual shirt? No, the shirt is not the prize. Is there a gold trophy? No, "prize" is simply the knowledge of who won it. There is no "there", no physical object at all. Strangely, that's why it works.

This is important for the next problem: intervention. Many private monies have been attempted, notably e-gold within Bitcoin's own origin. But the problem was, if there was anything real, like a gold bar, it could be encumbered, confiscated, and stolen. You'd have to trust the vault, the owner, the auditor and we're back in the old system. At the same time, if Satoshi were keeping the Bitcoin record and had any human power over it at all, government could imprison him, pass a law, create a cease-and-desist, or demand he tamper with the record, which they did with e-gold. **But Satoshi does not have that power, and no one else does either.**

Why? Precisely because Bitcoin DOESN'T exist. It's not a real thing. Or rather, the only "real" thing is the ledger itself which is already public to everyone everywhere. You can't demand the secret keys to Bitcoin privacy because it's already completely, entirely public. What would a government demand? Suppose they ordered a miner to alter the record: the other miners would instantly reject it and it would fail. Suppose they confiscated the ledger: they now own what everyone already has. Suppose they unplugged it: they would have to unplug the entire internet, and everything else on it, or every Bitcoin node, one-by-one, worldwide. If any nodes were ever turned on, all Bitcoin would exist again.

Can they track them down? Not really. In theory, Bitcoin can be written on paper without an Internet. In practice, any public or private keys certainly can be. So even chasing down the Internet it would be very difficult to stop it given sufficient motivation, like the Venezuelan hyperinflation where they are chasing down miners, wallets, and participants, and failing despite overwhelming force.
What about privacy? A completely public ledger recording every person and every transaction seems like a police state's dream of enforcement and taxation. Is it private? Yes and no. The Bitcoin ledger is not written like "Senator Smith spent .0001 BTC on August 21st, 2015 to buy a sex toy from Guangzhou," but Wallet #Hash2# transferred .00017 BTC to wallet #Hash3# at UTC 13:43:12 21:11:2017 – or not even that: it's encrypted. Who is #Hash2#? You can go back, but it will only say #Hash2# exists and was created on Time:Date. Who is #Hash3#? The ledger only says #Hash3# was created a minute ago to receive the transaction. In fact, #Hash2# may have been created solely to mask the coin transferred from #Hash1#. So is it anonymous? Not exactly. Given enough nodes, enough access to the world's routers, enough encryption, you might see #Hash2# was created in Pawtucket, and if #Hash2# is not using active countermeasures, perhaps begin to bring a cloudy metadata of #Hash2# possible transactions into focus, tying it to Amazon, then a home address, but the time and resources required to break through would be astronomical.

What about theft? Yes, like anything else it can be stolen. If you break into my house and tie me up, you can probably get the keys. This is also true online as you must log on, type a password that can be logged on a screen that can be logged over a network that can be logged, but think again about what you're doing: does it make sense to break into every participant's computer one by one? Most Bitcoin is held by a few early adopters, and probably those wallets

were lost when their hard drives crashed, the users lost their passwords, or died before this computer experiment had any value. We know for a fact that all of Satoshi's original coins, 2.2 million of them, have NEVER been spent, never moved on the ledger, suggesting either death or the austerity of a saint.

So even today hacking a wallet, is far more likely to net $1.00 than $1M. Take a page from Willie Sutton: when asked why he robbed banks, he said, "that's where the money is." So today. Where is the real money stolen, transferred? From the '08 bailout, the kiting of fake bonds in the market, the MF Globals, the rigging of LIBOR or the fake purchase of EU bonds. You know, where the money is. At $160B market cap, Bitcoin is still one week's purchase of central bank bond buying, i.e. a rounding error, no money at all. Hack a home wallet? I guess, but hacking Uber or Equifax once is a lot easier than hacking 100,000 wallets on 100,000 different computers. At least you know you'll get something. But MT Gox was hacked and 650,000 coins went missing. Surely Coinbase, Gemini, Poloniex are the same. Well…not exactly.

Bitcoin Doesn't Exist – 2

Dr. D: You have to understand what exchanges are and are not. An exchange is a central point where owners post collateral and thereby join and trade on the exchange. The exchange backs the trades with their solvency and reputation, but it's not a barter system, and it's not free: the exchange has to make money too. Look at the Comex, which reaches back to the early history of commodities exchange which was founded to match buyers of say, wheat, like General Mills, with producers, the farmers. But why not just have the farmer drive to the local silo and sell there? Two reasons: one, unlike manufacturing, harvests are lumpy. To have everyone buy or sell at one time of the year would cripple the demand for money in that season. This may be why market crashes happen historically at harvest when the demand for money (i.e. Deflation) was highest. Secondly, however, suppose the weather turned bad: all farmers would be ruined simultaneously.

Suppose the weather then recovered: the previous low prices are erased and any who delayed selling would be rich. This sort of random, uncontrolled, uninsurable event is no way to run an economy, so they added a small group of speculators into the middle. You could sell wheat today for delivery in June, and the buyer would lock in a price. This had the effect of moderating prices, insuring both buyers AND sellers, at the small cost of paying the traders and speculators for their time, basically providing insurance. But the exchange is neither buyer, seller, nor speculator. They only keep the doors open to trade and vet the participants. What's not immediately apparent is these Contracts of Wheat are only wheat promises, not wheat itself. Although amounts vary, almost all commodities trade contracts in excess of what is actually delivered, and what may exist on earth. I mean the wheat they're selling, millions of tons, haven't even been planted yet. So they are synthetic wheat, fantasy wheat that the exchange is selling.

A Bitcoin exchange is the same thing. You post your Bitcoin to the exchange, and trade it within the exchange with other customers like you. But none of the Bitcoin you trade on the exchange is yours, just like none of the wheat traded is actual wheat moving on trucks between silos. They are Bitcoin vouchers, Bitcoin PROMISES, not actual Bitcoin. So? So although prices are being set on the exchanges – slightly different prices in each one – none of the transfers are recorded on the actual Bitcoin Ledger. So how do you think exchanges stay open? Like Brokers and Banks, they take in the Bitcoin at say 100 units, but claim within themselves to have 104.

Why? Like any other fractional reserve system, they know that at any given moment 104 users will not demand delivery. This is their "float" and their profit, which they need to have, and this works well as far as it goes. However, it leads to the problem at Mt. Gox, and indeed Bear Sterns, Lehman and DeutscheBank: a sudden lack of confidence will always lead to a collapse, leaving a number of claims unfulfilled. That's the bank run you know so well from Mary Poppins' "Fidelity Fiduciary Bank". It is suspected to be particularly bad in the case of Mt. Gox, which was unregulated. How unregulated? Well, not only were there zero laws concerning Bitcoin, but MTGOX actually stands for "Magic The Gathering Online eXchange"; that is, they were traders of comic books and Pokemon cards, not a brokerage. Prepare accordingly.

The important thing here is that an exchange is not Bitcoin. On an exchange, you own a claim on Bitcoin, through the legal entity of the exchange, subject only to jurisdiction and bankruptcy law. You do not own Bitcoin. But maybe Mt.Gox didn't inflate their holdings but was indeed hacked? Yes, as an exchange, they can be hacked. Now you only need infiltrate one central point to gain access to millions of coins and although their security is far better, it's now worth a hacker's time. Arguably, most coins are held on an exchange, which is one reason for the incredibly skewed numbers regarding Bitcoin concentration. Just remember, if you don't hold it, you don't own it. In a hack, your coins are gone.

If the exchange is lying or gets in trouble, your coins are gone. If someone is embezzling, your coins are gone. If the Government stops the exchange, your coins are gone. If the economy cracks, the exchange will be cash-strapped and your coins are frozen and/or gone. None of these are true if YOU own your coins in a true peer-to-peer manner, but few do. But this is also true of paper dollars, gold bars, safe deposit boxes, and everything else of value. This accounts for some of the variety of opinions on the safety of Bitcoin. So if Polinex or Coinbase gets "hacked" it doesn't mean "Bitcoin" was hacked any more than if the Comex or MF Global fails, that corn or Yen were "hacked". The exchange is not Bitcoin: it's the exchange. There are exchange risks and Bitcoin risks. Being a ledger Bitcoin is wide open and public. How would you hack it? You already have it. And so does everybody else.

So we've covered the main aspects of Bitcoin and why it is eligible to be money. Classically, money has these things:

1. Durable- the medium of exchange must not weather, rot, fall apart, or become unusable.
2. Portable- relative to its size, it must be easily movable and hold a large amount of value.
3. Divisible- it should be relatively easy to divide with all parts identical.
4. Intrinsically Valuable- should be valuable in itself and its value should be independent of any other object. Essentially, the item must be rare.
5. Money is a “Unit of Account”, that is, people measure other things, time and value, using the units of value to THINK about the world, and thus is an part of psychology. Strangely that makes this both the weakest and strongest aspect of Bitcoin.
6. “The Network Effect”. Its social and monetary inertia. That is, it’s money to you because you believe other people will accept it in exchange.

The Score:

1. Bitcoin is durable and anti-fragile. As long as there is an Internet – or even without one – it can continue to exist without decay, written on a clay tablet with a stylus.

2. Bitcoin is more portable than anything on earth. A single number — which can be memorized – can transport $160B across a border with only your mind, or across the world on the Internet. Its portability is not subject to any inspection or confiscation, unlike silver, gold, or diamonds.

3. Bitcoin is not infinitely divisible, but neither is gold or silver, which have a discrete number of atoms. At the moment the smallest Bitcoin denomination or “Satoshi” is 0.00000001 Bitcoin or about a millionth of a penny. That’s pretty small, but with a software change it can become smaller. In that way, Bitcoin, subject only to math is MORE divisible than silver or gold, and far easier. As numbers all Bitcoin are exactly the same.

4. Bitcoin has intrinsic value. Actually, the problem is NOTHING has “intrinsic” value. Things have value only because they are useful to yourself personally or because someone else wants them. Water is valuable on a desert island and gold is worthless. In fact, gold has few uses and is fundamentally a rock we dig up from one hole to bury in another, yet we say it has “intrinsic” value – which is good as Number 4 said it had to be unrelated to any other object, i.e. useless. Bitcoin and Gold are certainly useless. Like gold, Bitcoin may not have “Intrinsic value” but it DOES have intrinsic cost, that is, the cost in time and energy it took to mine it. Like gold, Bitcoin has a cost to mine measurable in BTU’s. As nothing has value outside of human action, you can’t say the electric cost in dollars is a price-floor, but suggests a floor, and that would be equally true of gold, silver, copper, etc. In fact, Bitcoin is more rare than Rhodium: we mine rare metals at 2%/year while the number of Bitcoins stops at 22 Million. Strangely, due to math, computer digits are made harder to get and have than real things.

5. Bitcoin is a unit of account. As a psychological effect, it’s difficult to quantify. Which comes first, the use of a thing, or its pricing? Neither, they grow together

as one replaces another, side-by-side. This happened when gold replaced iron or salt or when bank notes replaced physical gold, or even when the U.S. moved from Pounds and Pence to Dollars and Cents. At first it was adopted by a few, but managed to get a critical mass, accepted, and eventually adopted by the population and entirely forgotten. At the moment Bitcoin enthusiasts do in fact mentally price things in Bitcoins, especially on exchanges where cross-crypto prices are marked vs BTC. Some never use their home currency at all, living entirely according to crypto-prices until home conversion at the moment of sale, or as hundreds or thousands of businesses are now accepting cryptocurrencies, even beyond. For them it is a unit of account the way Fahrenheit is a unit within the United States.

6. Bitcoin has the network effect. That is, it is widely accepted and publicly considered money. It's in the news, has a wide following worldwide, and exchanges are signing up 40,000 new users a month. It's accepted by thousands of vendors and can be used for purchases at Microsoft, Tesla, PayPal, Overstock, or with some work, Amazon. It's translatable through point-of-sale vendor Square, and from many debit card providers such as Shift. At this point it is already very close to being money, i.e. a commonly accepted good. Note that without special arrangements none of these vendors will accept silver coins, nor price products in them. I expect if Mark Dice offered a candy bar, a silver bar, or a Bitcoin barcode, more people would pick the Bitcoin. In that way Bitcoin is more money than gold and silver are. You could say the same thing about Canadian Dollars or Thai Bhat: they're respected currencies, but not accepted by everyone, everywhere. For that matter, neither are U.S. dollars.

Note what is not on the list: money is not a unit created or regulated by a central authority, although governments would like us to think so. In fact, no central authority is necessary or even desirable. For centuries the lack of monetary authority was historic fact, back with medieval markets through to private banks, until 1913, 1933, 1971, and the modern evolution into today's near-total digital fiat. Besides the technical challenge, eliminating their overhead, oversight, control and corruption is the point of Bitcoin. And right now the government's response to Bitcoin is a strange mixture of antipathy, ignorance, oppression, and opportunity. At $160 Billion it hardly merits the interest of a nation with a $500 Billion trade deficit, and that's spread worldwide.

This leads into one of the spurious claims on Bitcoin: that it's a refuge for drug smugglers and illegal activities. I assure you mathematically, that is not true. According to the U.N. the world drug trade is $435B, 4 times the total, and strictly theoretical value of Bitcoin, coins locked, lost, and all. Besides if you owned $160B coins, who would you transfer them to? You're the only user. $435B/year can only be trafficked by major banks like as HSBC, who have paid public fines because money flows that large can't be hidden. This is so well-known the U.N. suggested the drug-money flows may be one reason global banks were solvent in '08. Even $160B misrepresents Bitcoin because it had a 10-fold increase this year alone. So imagine $16B total market cap. That's half the size of the yearly budget of Los Angeles, one city. Even that overstates it,

because through most of its life it's been around $250, so imagine a $4B market cap, the budget of West Virginia.

So you're a drug dealer in illicit trades and you sell to your customers because all your buyers have Bitcoin accounts? Your pushers have street terminals? This doesn't make sense. And remember as much as the price of Bitcoin has risen 40-fold, the number of participants has too. Even now, even with Coinbase, even with Dell and Overstock, even with BTC $10,000 almost no one has Bitcoin, even in N.Y.C. or S.F.. So who are these supposed illegal people with illegal activities that couldn't fit any significant value?

That's not to say illegal activities don't happen, but it's the other half of the spurious argument to say people don't do illegal acts using cash, personal influence, offshore havens, international banks like Wells Fargo, or lately, Amazon Gift Cards and Tide Detergent. As long as there is crime, mediums of value will be used to pay for it. But comparing Bitcoin with a $16B market cap to the existing banking system which the U.N. openly declares is being supported by the transfer of illicit drug funds is insanity.

Let's look at it another way: would you rather: a) transfer drugs using cash or secret bank records that can be erased or altered later or b) an public worldwide record of every transaction, where if one DEA bust could get your codes, they could be tracked backwards some distance through the buy chain? I thought so. Bitcoin is the LEAST best choice for illegal activities, and at the personal level where we're being accused, it's even worse than cash.

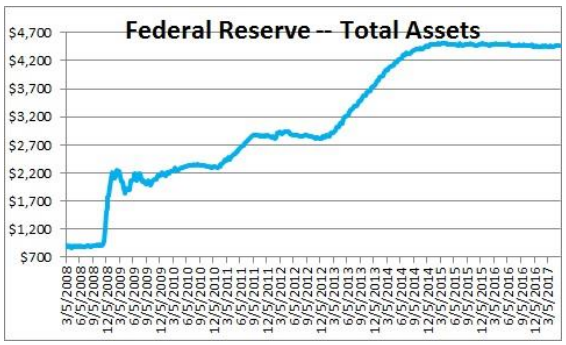
We showed that Bitcoin can be money, but we already have a monetary and financial system. What you're talking about is building another system next to the existing one, and doubling the costs and confusions. That's great as a mental exercise but why would anyone do that?

In a word: 2008.

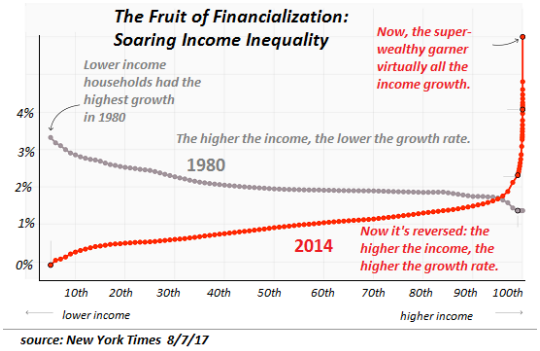
It's probably not an accident Bitcoin arrived immediately after the Global Financial Crisis. The technology to make it possible existed even on IRC chat boards, but human attention wasn't focused on solving a new problem using computer software until the GFC captured the public imagination, and hackers started to say, "This stinks. This system is garbage. How do we fix this?" And with no loyalty to the past, but strictly on a present basis, built the best mousetrap. How do we know it's a better mousetrap? Easy. If it isn't noticeably better than the existing system, no one will bother and it will remain an interesting novelty stored in some basements, like Confederate Dollars and Chuck-e-Cheez tokens. To have any chance of succeeding, it has to work better, good enough to overcome the last most critical aspect money has: Inertia. So given that Bitcoin is unfamiliar, less accepted, harder to use, costs real money to keep online, why does it keep gaining traction, and rising in price with increasing speed? No one would build a Bitcoin. Ever. No one would ever use a Bitcoin. Ever. It's too much work and too much nuisance. Like any product, they would only use Bitcoin because it solves expensive problems

confronting us each day. The only chance Bitcoin would have is if our present system failed us, and fails more every day. They, our present system-keepers, are the ones who are giving Bitcoin exponentially more value. They are the ones who could stop Bitcoin and shut it down by fixing the present, easy, familiar system. But they won't.

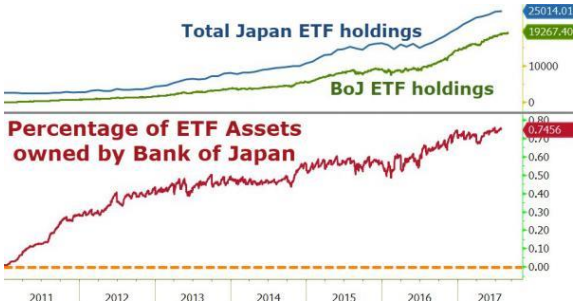
Where has our present system gone wrong? The criticisms of the existing monetary system are short but glaring. First, everyone is disturbed by the constant increase in quantity. And this is more than an offhand accusation. In 2007 the Fed had $750B in assets. In 2017 they have $4.7 Trillion, a 7-fold increase. Where did that money come from? Nowhere. They printed it up, digitally.



The TARP audit ultimately showed $23 trillion created. Nor was the distribution the same. Who received the money the Fed printed? Bondholders, Large Corporations, Hedge Funds and the like. Pa's Diner? Not so much. So unlike Bitcoin, there not only was a sudden, secret, unapproved, unexpected, unaccountable increase in quantity, but little to no chance for the population to also "mine" some of these new "coins". Which leads to this:



Near-perfect income disparity, with near-perfect distribution of new "coins" to those with access to the "development team", and zero or even negative returns for those without inside access. Does this seem like a winning model you could sell to the public? Nor is this unique to the U.S.; Japan had long ago put such methods to use, and by 2017 the Bank of Japan owns a mind-bending 75% of Japanese ETFs:

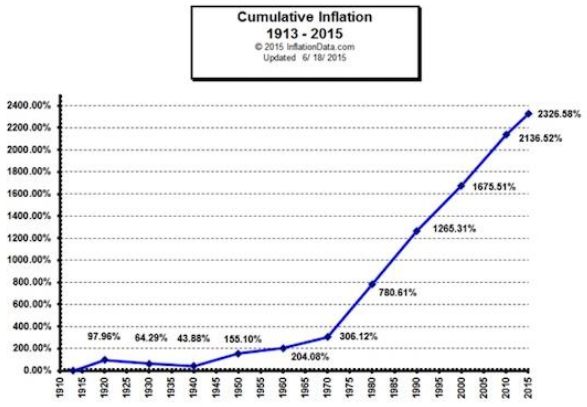


So this unelected, unaccountable bank, which creates its coin from nothing without limit or restraint, now owns 75% of the actual hard labor, assets, indeed, the entire wealth HISTORY of Japan? It took from the Edo Period in 1603 through Japan-takes-the-world 1980s until 2017 to create the wealth of Japan, and Kuroda only 6 years to buy it all? What madness is this?

Nor is Europe better. Mario Draghi has now printed so much money, he has run out of bonds to buy. This is in a Eurozone with a debt measuring Trillions, with $10 Trillion of that yielding negative rates. That's a direct transfer from all savers to all debtors, and still the economy is sinking fast. Aside from how via these bonds, the ECB came to own all the houses, businesses, and governments of Europe in a few short years, does this sound like a business model you want to participate in?

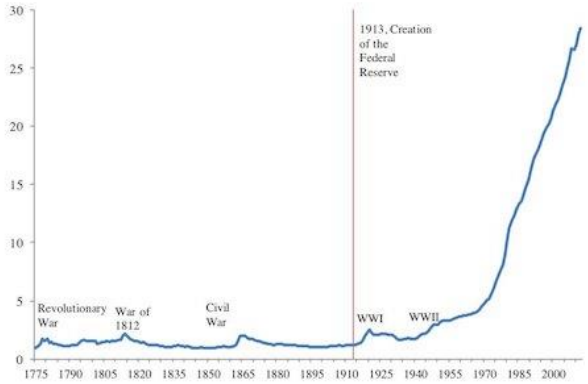
So the volume of issuance is bad, and unfairness of who the coins are issued to is as bad as humanly possible, giving incredible advantages to issuers to transfer all wealth to themselves, either new or existing.

But if the currency is functional day-to-day, surely the issuance can be overlooked. Is it? Inflation is devilishly hard to measure, but here's a chart of commodities:



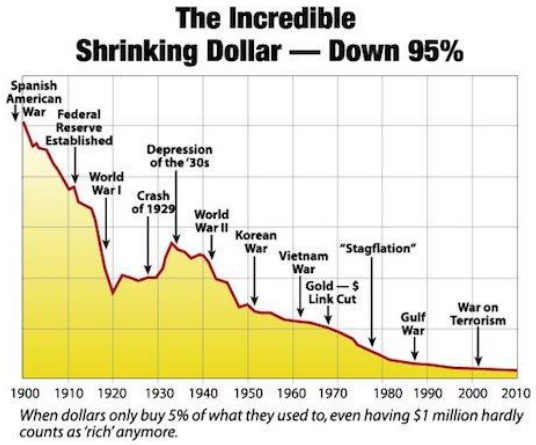
CPI:

Figure 1. Consumer Price Index, United States, 1775-2012
(level, 1775=1)

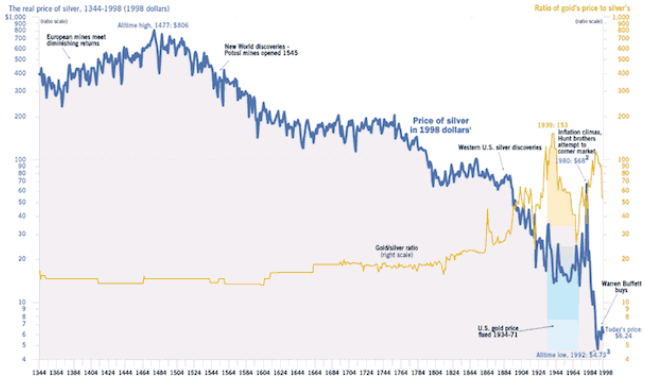


Sources: Bureau of Labor Statistics, Historical Statistics of the United States, and Reinhart and Rogoff (2009).

The US Dollar:



or vs Gold (/silver):



Does that look stable to you? And not that Bitcoin is stable, but at least Bitcoin goes UP at the same rate these charts are going DOWN. One store coupon declines in value at 4% a year, or may even start negative, while the other gives steady gains to loyal customers. Which business model would you prefer?
But that's not all.

Bitcoin Doesn't Exist – 3

Dr. D: The money, the unaccountable, uninhibited release of tokens can do more than just buy centuries of hard labor in seconds, it's also a method of control. Banks, our present issuers of money, can approve or destroy businesses by denying loans. They can do this to individuals, like denying loans to unpopular figures, or to whole sectors, like gun shops. They can also offer money for free to Amazon, Facebook, and Tesla, which have no profitable business model or any hope of getting one, and deny loans to power plants, railroads, farms, and bridges as they fall into the Mississippi.

The result is banks and their attending insiders are a de facto Committee of Central Planners in the great Soviet style. What is fashionable and exciting to them can happen, and what they dislike or disapprove of for any reason can never happen. And once on a completely fiat system, this is how capital is allocated through our entire system: badly. What's worse has been a 20-year turn toward Disaster Capitalism, whereby loans are extended to a business, sector, person, or nation, and then suddenly cut off, leading to the rapid foreclosure and confiscation of companies, assets, or continents by the "Development Team."

Imagine a Bitcoin where Satoshi could erase your coins in your wallet for giving him a bad haircut. Or because he likes your wife. Nor is there any help for independent nations like Iran, or even nuclear powers like Russia. Both have been cut off, their funds suspended at a whim with no recourse. Even being a fellow insider is no insurance, as the NY banks cut off Lehman from funds they were owed, driving it into bankruptcy to buy the pieces in receivership. Unpopular Billionaires are treated likewise. This is a system with no justice, no order, no rules, and no predictability. Anyone within it is at grave and total risk. And yet before Bitcoin it was the only system we had, short of returning to the 19th century, it was the only way for modern commerce to deliver food, water, power, or function at all.

This is seen in its abuses, but also by its effects. The present system not only controls whether you are a winner or loser, whether you may go or stay, whether you may live or die, but also tracks every purchase, every location, in effect, every action throughout your entire life. These records will describe what books you read, what movies you watch, what associates you have, in real time Already these daily actions are being approved or denied. Take out a variable-rate jumbo loan? We'll give you 110% of the value, paying you to be irresponsible (we'll foreclose later). Want to buy gas when driving through Cheyenne 3:30 at night? Sorry, we disabled your card as a suspicious transaction. Sorry about you dying there of crime or of cold; we didn't know and didn't care. All your base are belong to us.

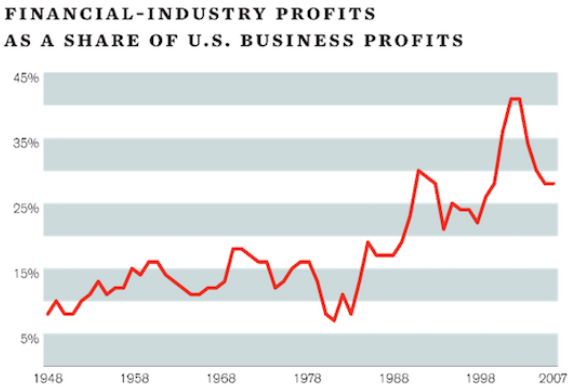
You say you don't care if JP Morgan has your pay stubs to disturbing porn sites and Uber purchases to see your mistress? Well the future Mayor of Atlanta will, and he hasn't graduated college yet. With those records it's child's play to blackmail policemen, reporters, judges, senators, or generals, even Presidents.

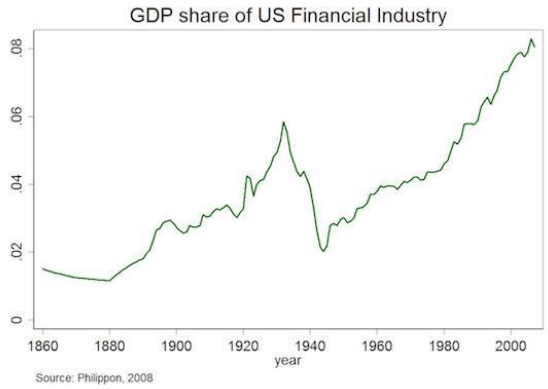
And all those future Presidents are making those purchases right now, the ones that can be spun into political hay, real or unreal. So if you don't worry what everyone knows about you, that's fine, but imagine reading the open bank records, the life histories of every political opponent from now until doomsday. Then Don't. Do. It. The people who have those records – not you – then have not just all the assets, not just all the money, but all the power and influence.

Forever!

Are you signing up for that? Bitcoin doesn't. Bitcoin doesn't care who you are and with some care can make it very difficult to track you. And without tracking you, it makes it impossible to boycott you. And without a central repository, it's impossible to march in with tanks and make them give you the records, turn money on or off, to make other people live or die and bend to your will by violence.
No one will care about that, because no one cares about it now unless, like Russia or China, it's directed at them personally and then it's too late. The real adoption of Bitcoin is far more mundane.

The long-term interest rate is 5%. Historically banks would lend at 8%, pay at 4%, and be on the golf course by 5. No one thought much about it because like a public utility, banking was a slow, boring affair of letting business do business. You know, farming, mining, manufacturing, all that stuff we no longer do. For decades, centuries even, banking was 5%-15% of a nation's GDP, facilitating borrowers and lenders and timescales, paying for themselves with the business efficiencies they engender.





All that changed after WWII. Banks rose in proportion to the rest of the economy, passing the average, then the previous high, then when that level reached “Irrational Exuberance”, Greenspan started the printing presses, free money was created, and Senators and Presidents whose bank records were visible suddenly repealed Glass-Steagall. An economy stretched to breaking with free, centrally-allocated and misallocated money crashed and shrank, yet the banks– now known as the FIRE stocks: Finance, Insurance, and Real Estate – kept growing. How can banks and finance keep growing with a shrinking economy? By selling their only product: debt.

How do you sell it? Reduce the qualifications past zero to NINJA-levels, and use your free money to FORCE people to take it via government deficits and subsidized loans. No normal economy could do this. No normal business model could do this. Only a business now based on nothing, issuing nothing, with no restraint and no oversight. And the FIRE sector kept growing, through 15%, 20%, 25% until today most of U.S. GDP is either Finance selling the same instruments back and forth by borrowing new money or GDP created by governments borrowing and spending.

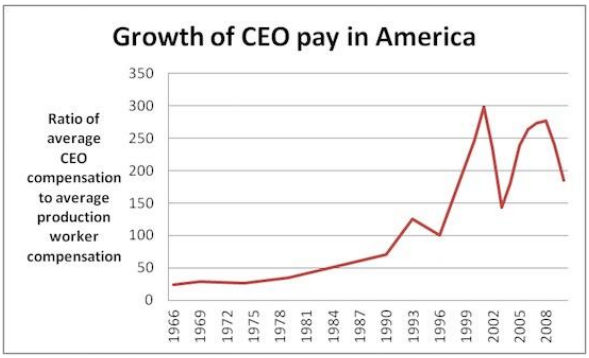
Remember when we started, banks paid 4% and charged at 8%. Now they openly take savings with negative interest rates, and charge at 30% or higher on a credit card balance averaging $16,000. And still claim they need bailouts comprising trillions a year because they don’t make money. The sector that once facilitated trade by absorbing 5% of GDP is now 5x larger. There’s a word for a body whose one organ has grown 5x larger: Cancer. Unstopped, it kills the host.

What does this have to do with Bitcoin? Simple. They’re charging too much. They’re making too much both personally and as a group. They’re overpriced. And anything that’s overpriced is ripe for competition. And the higher the markup, the more incentive, the more pressure, the more profit there is to join the upstart. Bitcoin can economize banking because what does banking do? It saves money safely, which Bitcoin can do. It transfers money on demand, which Bitcoin can do. It pays you interest, which mining or appreciation can do.

It also can lend, register stocks and ownership, rate credit risks, and allocate capital which other non-Bitcoin Tokens can do. In short, it can replace the 25%

overpricing of the financial sector. If it could reduce the overhead of outsized profit, the misuse of expensive brainpower, of Wall Street and London office space, and reduce financial costs to merely 10% GDP, it could free up 20% of GDP for productive purposes. Why did you think Detroit and Baltimore fell in on themselves while N.Y. and D.C. boomed? That's the 30% they took, $4B a year, from every other state, every year for 40 years.

That money and that brainpower could be much better allocated elsewhere, but so long as the Finance sector can print free money and buy free influence, they will never stop on their own. Only an upstart to their monopoly can cure the cancer and bring them back to a healthy size and purpose. Bitcoin can do this only because they charge too much and do too little. Of course, they could go back to paying 4% and charging 8% with a CEO:employee pay ratio of 20:1 but history says it will never happen. Only a conflict, a collapse, or competition can reform them, and however long it takes, competition is by far the best option.



So why would people pick Bitcoin? It costs less and does more. Amongst adopters, it's simpler and more direct. It pays the right people and not the wrong ones. It rewards good behavior instead of bad, and can help producers instead of parasites. It's equitable instead of hierarchical. What else? While not Bitcoin proper, as a truth machine Blockchain technology is the prime cure for the present system's main problem: fraud. There is so much fraud at the moment, libraries of books have been written merely recording the highlights of fraud since 2001. But merely recording the epic, world-wide, multi-trillion dollar frauds clearly does not cure it. Like other human problems, no one cares about your problems, only your solutions, and Blockchain has the solution.

While the details of fraud are complex, the essence of fraud is quite simple: you lie about something in order to steal it. That's it. It could be small or large, simple or complex, but basically fraud is all about claiming what didn't happen. However, the Blockchain is all about truth, that is, creating consensus about what happened, and then preserving it. Take the Robosigning scandal: accidental or deliberate, the mortgage brokers, banks, and MBS funds lost the paperwork for millions of houses. A house could be paid off could be foreclosed, as happened, or it could be owned 5 times, as happened. Like the Sneeches, no one knew which one was who, and the only certainty was that the official authority – county courthouses – did not know because to register there would have cost Wall Street and inconvenient millions or billions in shared tax stamps.

The system broke down, and to this day no one has attempted to define ownership, choosing instead to usher all the questionable (and therefore worthless) material into the central bank and hiding it there until the mortgage terms expire, forcing the taxpayers to bail out a multi-trillion dollar bank fraud at full value. And this is just one messy example. The S&L crisis was not dissimilar, nor are we accounting for constant overhead of fees, mortgage transfers, re-surveys, and title searches nationwide.

With Blockchain it's simple: you take line one, write the information, the owner, title, date, and transfer, and share it with a group. They confirm it and add mortgage #2, then #3 and so on. It's a public ledger like the courthouse, but the system pays the fees. It also can't be tampered with, as everyone has a copy and there is no central place to bribe, steal, and subvert as happened in 2006 but also in history like the 1930s or the railroad and mining boom of the 1800s. If there are questions, you refer to the consensus If it's transferred, it is transferred on the ledger. If it isn't on the ledger, it isn't transferred, same as the courthouse. Essentially, that's what "ownership" is: the consensus that you own something. Therefore you do not have a mortgage due disappear, or 4 different owners clamoring to get paid or take possession of the same property, or the financial terrorism of shattering the system if you even attempt to prosecute fraud.

It's not just mortgages: stocks have the same problem. Since the digital age began, the problem of clearing stock trades has steadily increased. Eventually, the NYSE trading volume was so large they couldn't clear at all, and the SEC let trading houses net their internal trades, only rectifying the mismatches between brokerages. Eventually, that was too large, and they created the DTCC as a central holder and clearing house. Yet, in an age of online trading and high-frequency trading mainframes, it became apparent there was no way to clear even residual trades, and they effectively no longer try, and the SEC, instead of forcing them to compliance, lets them. There are 300M failed stock trades a day and $50B a day in bond failures, or $12 Trillion year in bonds alone. And so? If you sell your stocks and bonds, the brokerage makes it come out whole, so what?

Bitcoin Doesn't Exist – 4

Dr. D: Well, all parts of the system rely on accurate record-keeping. Look at voting rights: we had a security company where 20% more people voted than there were shares. Think you could direct corporate, even national power that way? Without records of transfer, how do you know you own it? Morgan transferred a stock to Schwab but forgot to clear it. Doesn't that mean it's listed in both Morgan and Schwab? In fact, didn't you just double-count and double-value that share? Suppose you fail to clear just a few each day. Before long, compounding the double ownership leads to pension funds owning 2% fake shares, then 5%, then 10%, until stock market and the national value itself becomes unreal. And how would you unwind it?

Work backwards to 1999 where the original drop happened? Remove 10% of CALPERs or Chicago's already devastated pension money? How about the GDP and national assets that 10% represents? Do you tell Sachs they now need to raise $100B more in capital reserves because they didn't have the assets they thought they have? Think I'm exaggerating? There have been several companies who tired of these games and took themselves back private, buying up every share…only to find their stock trading briskly the next morning. When that can happen without even a comment, you know fraud knows no bounds, a story Financial Sense called "The Crime of the Century." No one blinked.

But it doesn't stop there. You don't only buy stocks, you sell them. And you can sell them by borrowing them from a shareholder. But what if there's no record of delivery? You can short or sell a stock without owning any. And the more you sell, the more it drives the price down and the more money you make. In fact, profits are infinite if you can sell enough that the company goes bankrupt: you never have to repay the stock at all. And this "naked" short selling can only occur if there's openly bad recording and enough failures-to-deliver to hide it. You could literally own nothing, borrow nothing, post nothing, and with no more than insider access to an exchange, drive a company out of business. That's how crucial recording is.

And while for appearance's sake, they only attack and destroy small plausibly weak stocks, Overstock.com with a $1.45B market cap fought these naked short sellers for years. Publicly, openly, vocally, with the SEC. Besides eroding their capital, besides their legal fees, besides that e.g. Amazon could pay to have their competition run out of business with fraudulent shorting, the unlimited incentive to short instead of long on small companies could suppress the entire stock market, indeed the national wealth and GDP. It may account for some of the small caps underperforming their potential for years, and why an outsized portion of stock value to be in just the 5 protected FAANG or DOW 30 stocks. …We don't know, because we have no honesty, no accounting, and nothing to compare it to. But no one cares, because it's been going on for 20 years, and if they cared, they'd do something about it. Again, no one cares about your problems, only your solutions. Even if the nation falls.

Look at it from their point of view: if you're a business owner, now you can't rationally list your corporation. Your stock could be manipulated; your business could be bankrupted for no reason at all. We've seen the NYSE shrink as businesses start to list in more honest jurisdictions, and even Presidents can't convince them to come back. Traders and Fund Managers retire in public interviews, telling the world there is no longer any sense or price discovery, and therefore there is market madness.

Yet we just said that to clean up the market would discover 10%, 20%, 40% fake shares, fake business values, fake pension values, therefore fake GDP values, and fake GDP to Debt ratios, and therefore would perhaps lead to an accurate Debt to GDP of 140%, which would crash the U.S. dollar and possibly the nation. Would a complete U.S. financial collapse lead to a nuclear war? And

it all goes back to fraud we didn't stop 20 years ago. How do you solve the problem? The only way out without collapse is to build an honest system parallel to the existing system and slowly transfer assets from the rotten, sinking ship to the new one. The captains of the old ship may not like it, but look at the incentives. No one can tolerate the old ship except the pirate captain; even the crew, the stock traders, don't want or control it any more.

However, what if you created an honest stock market Blockchain that actually had the stock certificates and actually transferred them, cheaply and reliably without false duplication? This is what is happening in the Jamaican Stock Market. A new company can choose to list on the stock Blockchain and avoid the old system. Other companies or even the whole exchange can clean up the books, slowly, stock by stock, and move it to the new honest system. Because they're honest? No way! No one cares about truth or honesty, clearly. Because they can sell their stock exchange as superior, solving the existing problems. Stopping fraud, theft, the stealing or crippling of companies, fake voting, depression of Main Street and outsiders in favor of Wall Street and insiders, this is what Blockchain can do. In short, it would work better, cheaper.

What else can Blockchain do?

Blockchain is just software written by programmers so it's as versatile as any other software. So why not program things into it with a "Smart Contract"? Suppose you make a bet: IF the Packers beat the Lions on November 12, 2017, THEN I will pay you $50. You set up the contract, and the bot itself can look for the headlines and transfer the money when the conditions are met.

That's pointless but how about this: You run a jewelry business on Etsy and need to buy $500 in beads from Hong Kong. Normally, you would need to pay an importer, a currency exchange, bank account, tire transfer, escrow account, and a lawyer, or their proxies within the system, plus two weeks' clearing time. That's a lot of overhead for a small transaction. In contrast, a smart contract such as Ethereum could post the value of the coin (escrow), and when Long Beach or FedEx confirms delivery, releases the Ethereum, a coin of value, to the seller in Hong Kong. Instantly. Why? The existing financial system is charging too much and doing too little. That's a huge incentive to get around their slow, overpriced monopoly.

Once you cut the costs, have a more direct method, and reduce the time to minutes, not weeks, the choice is obvious, which may explain why Microsoft, Intel, and others are deep in ETH development. Why overpay for bad service, and support the overpriced bonuses of men who will use their power to turn on or shut off your livelihood at will? Blockchain costs less and does more. Being just software, there are many other software products serving hundreds of other business plans. These use-coins are generally called "Tokens", whereas"Coins" are meant to be pure currencies. There are Tokens for a wide variety of business purposes: online gambling? Yes. Tokens to buy marijuana in certain states? Sure.

But how about a Token like Populous that contains the credit information of small businesses worldwide, so you can make modest income lending against their accounts receivable? You get more income, business worldwide gets better service and lower costs. Why? The existing financial system is charging too much and doing too little. How about a Token like Salt for personal loans and perfecting collateral? They will lend cash against your Cryptocurrencies, because if your loan falls short, they can sell your collateral instantly. No foreclosures, no repossessions, no overhead.

This is what banks do when they hold your savings and checking accounts, yet sell you a personal loan. But the banks are giving you no interest on savings, while charging origination fees and high interest. They're charging too much and doing too little. Well, you say, this sounds too good to be true: a parallel system to replace our existing corrupt, broken, overpriced one. One that doesn't have to confront existing power or reform the system, but beyond price appreciation has its own incentives to join? Surely there are problems.

Oh, yes. So many problems. The first is often mentioned: it's fine that Bitcoin is a finite commodity with only 22M coins, and if Bitcoin were the only coin, that would work. But there are over 1,000 coins now, and more every day. Isn't that just another avenue to unlimited issuance and inflation by unlimited, unregistered people? Well, yes and no. It's true that anyone can start their own Bitcoin – Litecoin for example is a faster duplicate of Bitcoin – but it's also true that anyone can start their own Facebook. MySpace certainly did.

So why don't they? Basically because of financial inertia, the Network Effect, a coin you start and only you use is worthless. The value is in the belief that other people will use it. Without that, you're banished to MySpace Siberia. Still, with a 1,000 coins, don't they all compete? Yes, and that's a good thing, not bad. This is no different than the competing Bank Notes of the 19th century. If you like this bank and believe in them, you prefer their notes to others. Or you might use one note in Missouri and another in Louisiana. So with Cryptos. You might choose Bitcoin, with slow traffic and **high costs to pay for a house**. But you would choose Litecoin to pay for coffee.

You already do this, no different than using cash to buy a hot dog, your debit card for groceries, and a bank transfer for a car. It's overlooked because they're all called "dollars," but they're not. One is currency, one is a short-term credit, and one is a banking ledger. Because of the Network Effect, you can't have 1,000 equal coins and have them all work. The market will prefer some over others until there are only a few, just as AskJeeves and Infoseek gave way to Google, which may someday give way to someone else. Just as you can't start a new Google today, there are only a few top coins, easily updated, and little space for new coins.

In addition, the "1,000 coins" are not actually coins. Most of the new coins are Tokens, which are not "currencies" like Bitcoin and a means of exchange, but business models and services. Like Bank Notes, the market is self-limiting, but evolving. But if there are a variety of coins, and like Litecoin they can suddenly

appear and change, what reassurance do you have that your Bitcoin “money” is worth anything? Like 19th century Bank Notes or AskJeeves, your responsibility is to be aware of the market and the changing values and react accordingly. And in a mature market, “everyone knows” the histories and reputations, but in a young market, like Dell and Gateway in 1992, no one knows. But that’s also why there is more profit now as well as more risk. But we’re also watching volatility and risk in Pounds, Lira, Gold, or even outright defaults like Argentine Pesos or Rubles. We already carry that risk, but it’s familiar and taken for granted.

If coins can just “change” and “fork” whenever they want, then isn’t it like buying Australian Dollars, then waking up and finding they’re Yen? Yes and no. Like other cryptos, Bitcoin is just software written by men. So a group of developers may think Bitcoin should remain the same while the old team thinks it should be improved so much that they do the work, write the updates, and release it. Well you have a “fork”, but what happens next is the Network Effect. So you’re a miner and a user of Bitcoin. You now have a choice: do you use the new software, the old software, or both? Everyone expected one to be adopted, and the old one to wither into oblivion. Since a Fork gives you one unit of each, the eventual outcome was a wash within the user group. But that doesn’t seem to be happening.

Ethereum forked, and Ethereum Classic still exists, and trades steadily but far less. Bitcoin Cash Forked and although 1/10th the price, both are trading briskly. No one knows what will happen, because it’s never existed before. So yes, you could wake up and find you don’t like what Bitcoin decided to do, just as you could wake up and not like your new bank manager or CFO of Dell, and then you sell that asset and choose another. That’s your responsibility. That’s competition.

Besides unexpectedly finding both forks have value, there is an upside to the downside. If some new advance in speed or encryption appears in Litecoin or Dash, Bitcoin can also adopt it. This not only improves the market, but reduces sudden upsets as new advances shouldn’t unseat popular coins but are adopted by them. Indeed, this was the purpose of Bitcoin Cash fork: to improve speed and cost. Yet now they both exist for different purposes in the market. Another objection is that cryptos depend on electricity and an expensive, functioning Internet. True. But while I’m no fan of technology, which is full of problems, so does everything else. Without electricity, the western world would stop, with no water, no heat, and no light.

Without Internet, our just-in-time inventory halts, food and parts stop moving, banking and commerce fail. You’re talking Mad Max. TEOTWAWKI. That’s a grave problem, but not unique to Bitcoin.

Bitcoin Doesn’t Exist – 5

Dr. D: Bitcoin can be stolen. Although "Bitcoin" can't be hacked, it's only software and has many vulnerabilities. If held on an exchange, you have legal and financial risk. If held at home, you could have a hard drive fail and lose your passwords. If it's on a hardware fob like a Trezor, the circuits could fail. For a robust system, computers themselves are pretty fragile. You could write down your passwords on paper, and have a house fire. You could print out several copies, but if any of the copies are found, they have full access to your account and stolen without you knowing. You could have your passwords stolen by your family, or have a trojan take a screen or keystroke capture.

Hackers could find a vulnerability not in Bitcoin, but in Android or AppleOS, slowly load the virus on 10,000 devices, then steal 10,000 passwords and clear 10,000 accounts in an hour. There are so many things that can go wrong, not because of the software, but at the point where you interface with the software. Every vault has a door. The door is what makes a vault useful, but is also the vault's weakness. This is no different than leaving blank checks around, losing your debit card, or leaving cash on your dashboard, but it's not true that there are no drawbacks. However the risks are less obvious and more unfamiliar.

Bitcoin isn't truly anonymous. If someone, the NSA, wanted to track your drug purchases on SilkRoad, they could follow the router traffic, they could steal or work out your keys, they could eventually identify your wallet, and from there have a perfect legal record of all your transactions. Defenders will say that wallets are anonymous, that like Swiss accounts, we have a number, but not a name, and you can create new numbers, new wallets endlessly at will. Fair enough, but if I can see the transfers from the old to the new, it can be tracked. If I can get your account number by any means, I can see the flows. To some extent it's speculation because we don't know what technology they have available to crack codes, to see into routers, Internet traffic and servers.

Could there be a hidden exploit not in "Bitcoin" but in AES256 or the Internet itself? Maybe. Are there secret code-breaking mainframes? Possibly. But given enough interest, we can be sure that they could always get a warrant and enter your house, hack your computer, and watch your keyboard. However, this is no different than cash. If necessary, they can already track every serial number of every bill as it leaves an ATM or a drug sting. Then you follow those serial numbers as they are deposited and reappear. I expect Bitcoin is not very different, and like cash, is only casually anonymous. But is this a problem with cash? Or with Bitcoin? Your intent as a citizen is to follow the law, pay your taxes, and not hurt others. If government or other power centers are willing to expend that much effort to track you, perhaps the problem should be addressed with proper oversight on warrants and privacy.

Bitcoin is slow and expensive. Very true. Bitcoin Core has gotten so outsized from its origins that it may soon cost $5 to buy a $1 coffee and 48 hours to confirm the purchase. That's clearly not cheaper, faster, OR better. It's worse: far, far worse. Nor can it improve. Since Blockchain writes the ledger, the longer the ledger, the bigger it is. Technically, it can only clear a few transactions per second. This problem may not doom it, but it would relegate it to only huge,

slow transactions like moving container ships. That is, a form of digital gold note. We don't actually ship gold or whatever to pay for transactions; it just sits in the background, an asset. Per Satoshi, Bitcoin is a "Digital Asset."

And the core team seems to like this more secure, higher value direction, where these obstacles are acceptable. But without a larger, deeper market, it's the plaything of billionaires and then who sets the price? It becomes another experiment, an antique. Luckily, the story doesn't stop there. Because it's only software, you can always change it if you can convince the participants to use the new version. Bitcoin Cash is a fork that it larger, faster, and cheaper, reducing the limitations for now. And it can become Segwit2 or Cash2 later if the community agrees. But by design Bitcoin is not meant to be instant nor free, and probably never will be. Like gold, it is meant to be expensive, vaulted, and rarely moved. If you want fast and cheap, LiteCoin, Dash, and many others are vying to be the digital silver or digital payment card. That's not very different from the gold standard, or even payments today.

Bitcoin is a huge electric and Internet drain. This is true. However, it's also misrepresented. What is the electric overhead of every bank, every terminal, every mainframe on the NYSE, every point-of-sale card machine, every cash register and router in retail? Don't we use an awful lot of electric to keep those running? What about their cost, the repairmen, the creation of new systems every year from mine to market, from idea to update release, to replace them? We also personally have our computers and routers, the whole Internet on and idling. What's the base cost? Is it fair to compare as if it were a pasture before Bitcoin arrived?

We built the existing system this way because it gained efficiency. Time in the clearing, price in not running typewriters and mail worldwide, and of course taxes. We're talking about creating a parallel financial system here. If the old one is replaced, is the new one better, or worse? Mining takes a lot of power, but the math in Bitcoin is meant to get increasingly harder to compensate for increasing computer speed. The computers are supposed to be on to confirm transactions. That means that the more people use it, the more power consumed, but that's true of everything. The more people that drive cars, the more gas is used. So is the car doing something useful and being used well? Is it replacing a less efficient horse, or just wasting energy better used elsewhere? These are complex questions.
At the least, Bitcoin uses far, far too much energy in the design, and because of the speculation, far too many people are mining it without using it. However, all of the subsequent coins were concerned about this, and their power consumption is far, far less. As Bitcoin is near its hardest stage and stops at 22 Million, power consumption is near peak, but should stabilize, or even fork to a low-energy proof-of-stake model. As Bitcoin is not well-suited to worldwide transactions, it should be replaced with less-power intensive alternatives, and because of this, may get smaller. And if it replaces some of the existing system, it can generate an offset. But yes, if it uses too much power, is too inefficient by design, it will be too expensive, abandoned, and fail.

Are Cryptos a scam? Probably not: we pointed out some legitimate uses above for both coins and tokens. But there's one coin that arguably is a Ponzi, a dozen coins that are scams, scores that are terrible ideas like Pets.com and will fail, and another dozen good, well-meaning tokens that are honest but ultimately won't succeed. Yet, like the .Com 90's, there are probably some like Apple that rise far more than it seems they should, and by surviving, effectively give 16% compounded returns for 40 years, front-loaded. That's the nature of business. But are many coins and tokens open scams that run off with your money? Yes. Are others worthless? Yes. It's also true of the stock and bond market and can't be helped. Buyer beware.

Is Bitcoin a Ponzi? It's not a Ponzi by definition because there is no central thief, nor are new investors paying off old investors. So is it a fraud, misrepresenting a few hours of electricity as worth $10,000? Well, that depends on what you think its value is. Is it providing value, a service? If so, what is that service worth to you? We already said it has the operational elements of money, with the addition of being extremely transmissible and transportable. If that has value to you, fine, if not, perhaps gold or bonds are more appropriate. But that's the problem of what gives Bitcoin value.

A stock or bond you can look at the underlying asset, the profit or income flows, the book value. But Canadian or New Zealand dollars? What gives them value? They're also backed by nothing. What gives gold value? It has no income, just popularity. Likewise Bitcoin: what gives it value is that other people want it. If they stop wanting it, it has no value, but that's psychological and can't be directly measured. With that in mind, is its fair value $1K or $1B? No one knows. Can its value fall from $10k to $5k? Yes, and it has many times. Only the market, that is, we can decide what it's worth to us, and the market is small and immature, with no price history and prone to wild swings.

Shouldn't the exchanges set the price? Yes, and they do, but how is that accomplished? We already said the Exchanges do internal trading off-ledger, outside Bitcoin. So aren't they setting the price on the exchange instead of the people setting the price peer-to-peer? It would seem so. So aren't they subject to market manipulation? Although at the moment they have a fairer design, and smaller pipelines to the larger market of money, yes. So if they launch a Bitcoin future, a tracker, a triple-short ETF, internally inflate their holdings, wouldn't that make it subject to corruption and thus back into the existing system?
No one knows: it's never been done before. I suspect not, but only because the people want Bitcoin specifically because it is Outside-system, Anti-fraud and watch these things carefully. But it's run by humans and reflect human nature: that means over time some new form of exchange and corruption can grow up around it as before. While the ability to rig Bitcoin is limited because the quantity of Bitcoin is limited and riggers must first buy Bitcoin fairly, the Exchanges and the price-setting are an issue, and especially into the future.

Central Banks and existing powers can outlaw or replace it. Bitcoin is still small, almost irrelevant, yet it has been driven down or outlawed in several places, for example North Korea, Venezuela, and New York. That's right New York, you're

in proud company. North Korea outlaws everything and there is little internet access, so that's no example. New York is simply regulating Bitcoin which creates business obstacles, but is still available via the few companies willing to do extensive paperwork. Venezuela, however, is actively suppressing Bitcoin which competes with the Bolivar, and is in fact seeking out and shutting down miners.
They do this on the premise that Bitcoin is consuming valuable (and free) national electric that could be better used powering a small town. Point taken. However, Bitcoin users are able to defend themselves against a terrible, lingering hyperinflation that is starving the nation to death, cutting off food, medicine, and services. Mining Bitcoin with national electric – or even having any – can be the difference between life or death. With Bitcoin, you can order food and medicine on Amazon. Without it, you can't. So a ferocious national government has attempted to halt Bitcoin at gunpoint from both the users and the vendors. Like other currency oppressions, the USD in Zimbabwe for example, it hasn't worked. Bitcoin is suppressed, but when the need for commerce is high enough, people make a way.

So maybe they will replace it with their own coin. Go ahead: this is a free market, freely competing. Banks already made a coin called Ripple, which trades in volume on exchanges, but is not open and public. If people choose it, I can't stop them. Suppressing Bitcoin may make the incentives to choose the legal option far higher. But ultimately the point of Bitcoin is to be open, fair, and uncontrolled. A coin that is closed, controlled, and operated by some untrustworthy men has no incentive. But it can happen: people have chosen against their better interest before.

And that's my real reservation. Suppose Bitcoin works. Suppose it replaces currency. Suppose it is adequately private. Suppose can be made fast enough, cheap enough, and slim enough. Suppose the old system fades and we all get used to having our lives entirely on the Blockchain. Your every post is perfectly recorded and provably yours on Steemit. Your every photograph is saved and stamped to you. Every medical experience is indelibly written. Every purchase, every trade, it's all on a blockchain somewhere. And even suppose it's private. What then? I mean, isn't this the system we had in 1900, under the former society and former gold standard? So what happened?

Being comfortable and familiar with Blockchain ledgers, taking them as for granted as Millennials do Facebook, and someone says, "Hey, rather than waste power on this inefficient, creaking system of writing everywhere for a fraction of the power the Federal Reserve Block can keep it for you. Think of the whales." Sound silly? That's exactly what they did in 1913, and again in 1933 – replace a direct, messy, competitive system with a more efficient one run by smarter men. The people didn't protest then any more than they do now, so why would we expect them to in 2050 or 2070? No one cares about corruption and murder: we're only moving to this system now because it's better and cheaper. If the Fed Reserve Block is cheaper, won't we move then?

I can’t solve the next generation’s problems. We’ll be lucky to survive our own. But I can warn you that even now this generation will never accept a digital mark without which you cannot buy or sell, not voluntarily and not by force. It’s too far to reach and social trust is too compromised. But could they get us halfway there and just make it official later, when everything’s fixed again? I think absolutely.

Once that’s in, you can finish all the plans written in the bank and government white papers: perfect, inescapable taxation. Perfect, indelible records of everyone you talked to, everything you said, everything you bought, everywhere you were, everyone you know. Not today, but in the future. And that is the purgatory or paradise they seek today. The price of Liberty is eternal vigilance. The system we have wasn’t always bad: a small cadre of bad men worked tirelessly while complacent citizens shirked their duty. So when we move to a new system softly, without real purge, real morality, real reform, what makes you think the same thing won’t happen to your new system? Only far, far more dangerous. But I can’t prevent that. Think, and plan accordingly.