Should I buy Bitcoin?

By

Garreth McDaid

December 2016

The rise of currency

In the beginning, we humans didn't need much. We left our caves in the morning, wandered around looking for something to kill, dragged it back to our caves, ate it and slept. The next day, we did the same thing. After about 30 years, if we hadn't been killed by another human, or a wild animal, we died from a degenerative disease or an infection.

As the centuries passed, our brains evolved. Our needs became more sophisticated. We began to farm, which required tools and seeds, which, if we couldn't make or produce ourselves, we had to acquire from others. For a time, we could swap what we produced ourselves for these items, but gradually the humans who had the things we needed no longer wanted the things we produced. We had to find some other way to transfer value to them.

Collectively, and subconsciously, we agreed that certain substances, like gold, had value. Gold was rare, it was finite, it was divisible, it was portable, it was recognisable and it was durable. We agreed that gold had perennial value. If you wanted to acquire something, like a tool, or an animal, the person who possessed that thing would transfer it to us for some gold, not because they had a particular need for a piece of gold, but because they knew that they could trade that piece of gold for something they needed at some future date.

But while gold was divisible, it was still a lump of rock, and was not practical for use in the ever increasing number of transactions that were happening as we started to travel and acquire goods from places that were far removed from where we were born and lived.

In an attempt to solve this problem, we started to produce coins. At first, these were made entirely of gold, but there wasn't a sufficient supply of pure gold to produce all of the coins that were needed all over the world.

Around the same time, we also started to organise ourselves politically. The small tribes that we had belonged to when we lived in caves had become larger. To protect our land and livelihoods, our tribes began to form alliances with other tribes. Tribal leaders established power through force or consensus. These leaders began to organise their now larger tribes to maintain control. They dictated laws, they administered justice, they levied taxes.

Over time, through just and productive leadership, or force, they established political authority. They became princes. When they decreed that something should be done, it was done. They also recognised that their authority was dependent on their subjects being both happy and afraid at the same time, which meant they needed to housed and fed, but also taxed, which meant their subjects needed to have incomes. Both of these needs required trade, and it was their responsibility to ensure trade flourished, which meant they had to provide a means for people to transfer value, a means of exchange, a common currency.

But the scarcity of gold to make portable coinage was still an issue. To resolve this problem, they produced coins that contained a small of amount of gold, which were still recognisable and durable. They stamped an image of their face on them, so that people would know that they stood over the value of the coin, and that the coin could be traded for its equivalent value in gold at any time at their Treasury. If people trusted their leader, they trusted his currency, and trade flourished.

As it did, it was no longer practical to include any gold in coins, and they were produced

instead from less expensive but equally durable medals. The fact that the coins had no real value did not deter people from using them. They had been using the currency for years, and still trusted that their value in gold was redeemable from their political masters. For the first time, the value of a currency was entirely derived from *trusting a political authority*.

Currency, which was still linked to the value of the gold reserves held at the Treasury, could now be produced in abundance. Successful traders, and warlords, began to accumulate vast quantities of it. They did not have the time or inclination to manage it themselves, nor keep it secure, and employed others to do this work for them.

The number of these people, who *banked* the currency of others, began to grow. They began to offer services for more than one customer, and to merge their resources to form larger banks. To make life easier for their customers, they offered them the ability to carry their wealth in more portable form, as pieces of paper that were signed and sealed by the bank to guarantee that the bearer could redeem the note at their bank for “hard” currency.

The merchants and warlords carried these notes on their travels, and used them in place of the heavy coins they had previously carried. The people who accepted them still trusted the the notes had redeemable value, and were happy to accept them. Gradually, these notes became as frequently traded as the coins. The banks continued to merge, and get bigger, and establish themselves in different parts of the world. The bigger and more visible the bank became, the more likely people were to trust its notes.

The growth in the size of the reserves of cash being held by banks presented a new opportunity. The bankers released that it was highly unlikely that all their notes would be redeemed at the same time, and that provided that held a minimal reserve of currency to satisfy any requests for redemption, they could loan the remainder of the reserves to others in exchange for an interest payment. They obviously needed permission for this, and proposed to the owners of the currency that they would pay them some of the interest they received from the lenders. The difference between interest paid by the lender and the interest paid to the depositor was profit for the banker. Everybody won. Everybody was happy. Lending flourished.

Political organisation began to change around this time too. Principalities began to combine into larger principalities, and ultimately countries. Treasuries became larger, and harder to manage. Seeing that the notes produced by the private bankers were trusted in the same way as coins, the national Treasuries also began to issue notes. These notes soon became the most common form of paper currency, and so the private banks stopped issuing their own notes, and used the notes produced by the national Treasuries instead. The national Treasuries also saw the potential of lending, and began to lend currency to the private bankers, who in turned loaned it to their customers.

Other political developments were also taking shape. With the advent of the printing press, people had more information, and became less content that they had no say in how their lives were run. They rebelled against their leaders, and formed new political systems based on input from the people, through the appointment of people's representatives to political assemblies. Control of national Treasuries transferred from the princes to the people's representatives. This gave those representatives great power, because they could manage the Treasury in a way that made them popular and more likely to be chosen again by the people to represent them.

They could regulate the flow of currency into the economy through setting the interest rate at which currency was loaned to private banks. They also had to be trusted to ensure that no more notes or coins were issued than could be backed by the store of gold held in the Treasury. Doing so might make them popular in the short term, but if people stopped trusting the value of the currency, damage would be done to the economy of the country.

After some mishaps in this regard, most notably in Germany after the First World War, established political practice required the Treasury to be managed independently from the assembly that governed the country. If the people who managed the Treasury were not representatives, and did not want to be representatives, they had no incentive to manage the Treasury in any way other than the best interests of the country.

By this stage, the regulation of currency had become the most important function of economic management in the world economy. To maintain control of economic activity, every country issued its own currency. Depending on how stable and successful individual countries were, people regarded their currencies with different degrees of trust, and therefore value.

In the aftermath of the Second World War, the United States of America emerged as the world's most powerful and economically successful country. Their currency, the US Dollar, became to most trusted currency in the world, to the extent that people in other countries preferred to trade is US Dollars than their own currencies.

At this time, the US Dollar was still linked to the value of gold held by the the US Government at their Treasury at Fort Knox. The Treasury was not allowed to issue any more currency that existed at Fort Knox, and any holder of US Dollars could still present at Fort Knox and redeem those dollars for gold. Similar arrangements were still in place in the majority of the world's developed economies.

But the extent to which the US Dollar was becoming the currency of choice for the rest of the world was becoming a problem for the US Government. Demand for US Dollars was so high that borrowing US Dollars from banks meant paying very high interest rates, which was stifling economic activity in the US, and contributing to high levels of unemployment.

The ability of others to deplete the gold reserves of the US was also a security concern for the US Government. They weren't comfortable with the idea that their rivals in the Soviet Union or China could undermine the economic foundation of their country.

At the same time, they recognised that the US Dollar was widely trusted, and that there was no other currency in circulation that could compete with the US Dollar in terms of trust.

As such, in 1971, they decided to break the link between the US Dollar and the gold in Fort Knox. From then on, you could not present your US Dollars for an equivalent value of gold at Fort Knox. Instead, the US Dollar would be allowed to "float". It would have no equivalent value in gold. Its value would be entirely determined by supply and demand, or in other words, the trust that people had in the stability of the US economy. If the US economy was stable, the US Government would have no reason to issue more US Dollars, and the value of the dollar would hold.

Other countries now had to consider their position. If their currencies were linked to their gold reserves, they would be more valuable, and therefore more expensive, making it more expensive to buy goods and services in their countries. They would not be able to compete with the US, and were forced break the links between their currencies and their reserves too.

Over the following decade, every major currency was reconfigured to have a floating rather than fixed value. The value of currency, which had previously been based on having redeemable value in gold, was now based both on trust in political authority *and* on economic stability. We had moved from our starting position where currency had actual value, to an intermediary position where currency had guaranteed value, to our current position where currency has no value, other than our faith that somebody else will have faith in its value.

Terminology is important here. At no stage prior up to this have I used the word money. There is a fundamental and important difference between currency and money. Currency is what we have discussed so far. It is that note or coin that is issued by an authority that we trust to maintain its value, and that we use to complete transactions with others when we wish to exchange goods or services.

Money is something more basic. Money is a commonly agreed store of value. Currency is money, but so are other things.

In considering the value Bitcoin, the key point to understand for now is that currency is not the only form of money. Provided we commonly agree that something has value, it can be money. It does not need to be issued and controlled by an authority that is separate from ourselves.

The other important lesson in this introductory section is the inverse relationship between economic and political sophistication and the real value of currency.

As economic activity has increased and become more complex, and government has become more elaborate, the further we have moved from our starting point of using a currency that has

actual value.

In the 21st century, in which we have reached a point where currency exchange is more developed and complex that at any time in human history, centrally managed currencies, or *fiat* currencies as they are known, have moved beyond having limited intrinsic value, and now have non-existent intrinsic value. The next question that arises is can we continue using currencies that have zero intrinsic value while the complexity of our economic and political systems continues to intensify.

The automated economy

Moore's Law is named after one of the co-founders of Intel, Gordon Moore, and states in its most basic form that computing power doubles approximately every 2 years. Moore made this prediction in 1965, which at the time of writing is over 50 years ago.

That doesn't sound like anything particularly important, but lets consider what would happen it we applied the same principle to a car.

If a car, from a starting point of 2km/h, were to double its speed every 20m, after 1km (i.e. 50 times), it would be traveling at 1,048,576 km/h.

Now, lets go back to computers. Moore was correct in his prediction. The computing capacity of the world has been doubling every 2 years for over 50 years. This means that Artificial Intelligence, or AI, is more advanced than ever, and likely to become even more advanced as time passes.

But AI isn't new. As far back as 1997, IBM had developed a robot ("Deep Blue") which beat Grand Master, Gary Kasparov, in a chess match. What has changed is the amount of data that is available to facilitate the synthetic learning that forms the basis for AI, which is being generated by the ever expanding number of devices through which humans are recording their behaviors.

In the past, AI could replace behavior in which variations from what was routine were minimal; now, with almost endless amounts of data from which it can learn, AI can replace any behavior that is predictable within a very wide range of variance.

What this means is that the technology which once was a tool for humans to increase their productivity and income thereof, is now becoming a replacement for humans. To state this in more fundamental economic terms, where industry once involved 2 inputs, namely: Labour and Capital, it now more frequently only requires 1: Capital.

Examples of this are everywhere. Think of Satellite Navigation. This was a technology that added value to supply chain logistics, saving time and money for truck and van drivers trying to deliver goods from point A to point B. But the owner of the trucking company still had to invest in Labour (the driver) and Capital (the truck). Now technology has advanced to the point where the truck can drive itself, removing the requirement for the owner of the trucking company to make any Labour investment to get his trucks from point A to point B.

Another emerging trend in economic automation is notable at this point. In the past, automation was only pervasive in manufacturing industries, where robots did routines tasks on assembly lines and humans bookended the process by turning the robots off and on.

Now automation is moving more and more into the services sector, which to date has absorbed the surplus of Labour made available by automation in manufacturing, and where the majority of non-skilled workers now find jobs in western economies.

The example of the driverless truck has already been given, but automation is going even deeper than that. We've all seen self-service checkout facilities in supermarkets, pulled up at petrol stations where you pay with your card at the pump and deliver the petrol to the car yourself, listened to robots on the telephone telling us what our banks balances are; but now we're also going to have to deal with robots that do physical tasks that we would never have imagined anything other than a human doing.

The fast food industry is perhaps the best example of this. With its low wages and minimal entry requirements, the fast food industry is essentially the safety net you have to fall through

before you finally get to the safety net of state welfare. Workers who can't make it in the fast food industry will generally not find employment anywhere else.

The number of people employed in the industry is huge. McDonalds alone employs 1.8m people in 34 countries. But if you go into any McDonalds now, there is a good chance that you will not give your order to a human standing behind a counter, but to a machine. Your only contact with a McDonalds human will be when they bring your food to your table.

Automation in fast food isn't only occurring in the dining area. Fast food corporations are now being offered the services of a robot that can prepare, cook and pack food items like hamburgers. The robot can even cook the meat to a certain specification, and can do all this in a much smaller space than a human, without the health and safety regime that would protect a human and without the inclination to boredom, dissatisfaction, ill health and general grumpiness that would be normal for any human charged with the task of of producing hamburgers without interruption for 24 hours a day, 7 days a week, 365 days per year.

None of this is idle speculation. The trend can be backed up by economic data. As technology assumes more and more of the workload previously borne by humans, and in particular in the service sector, return on investment to capital has increased while return on investment to labour has declined. Between 1973 and 2013 in the United States, the purchasing power of the average worker has decreased by 13%, despite productivity levels (i.e. return on investment) having risen by 107%. Perhaps even more worryingly, no net new jobs were created in the decade between 2000 and 2009, which is the first decade in which this happened since the end of World War II.

Conversely, more wealth in now concentrated in the hands of the top 5% of income earners than at any time since the decline of Europe's monarchies.

At the same time, the population of the world is increasing an an exponential rate, and people are living longer, creating more and more demand for an ever shrinking pool of human employment. The has been accommodated to a certain extent by depletion of natural resources and the availability of cheap energy, but again, these bandages are beginning to peel away. Developed democratic nations are no longer tolerant of the high environmental cost of cheap energy, and even the threat of Climate Change is starting to creep into public policy.

These changes are creating enormous challenges for Governments across the world. The post-war decades were a golden era for western democracies. Not only was the world at peace, but growth and productivity, assisted in no small measure by technology, were expanding at phenomenal rates, delivering real spending power to workers, on which they built lifestyles that their parents could only dream off. Any political movement that could not guarantee the survival of the new order was not going to survive.

But sustaining that progress was never going to be possible. The developing world would not remain in a developing state forever, and ultimately they too would require their share of the world's bounty.

The plan was that liberalising trade between parts of the world that had previously sought to protect their economies from competition would create new opportunities, more demand, more supply, more growth. The transition phase would be drawn out, and relatively smooth.

But Moore's Law has put paid to that hypothesis, and governments in western economies are now struggling to replace the strategies they thought would work with ones that actually will.

Unfortunately, the only ones that are available to them are ones that the media-run democracies of the 21st century will not entertain, and that has profound implications for the value and stability of fiat currencies.

The dictatorship of the articulate

At its most basic level, in either the democratic or totalitarian context, Government has a simple aim: to keep people happy enough or scared enough not to revolt.

In the democratic context, which prevails in most of the developed world, Governments have 2 tools in this regard: fiscal policy, which deals with how much they raise in taxes and spend

on providing services and social protections, and monetary policy, which deals with the way they regulate the supply of currency in their economies.

Because electoral democracy is effectively a popularity contest, use of these policies always refers to the impact they will have on the ability of a sitting Government to be re-elected.

Governments like to spend currency, but hate raising taxes. To fill the gap, they borrow currency, and only agree to pay it back over an extended time period, so that when it comes to paying it back, some other Government will have to take responsibility.

Except when that day arrives, the subsequent Government doesn't pay it back either. They just borrow more currency to pay off the original debt and the cycle continues. Over time, the debt just builds and builds, and never actually gets paid back.

That said, every now and then there are times when a Government needs to borrow so much currency that the rate lenders want to charge them is simply to high. When this occurs, they revert to monetary policy, which means they reduce their value of their currency rather than taking on more debt.

They normally do this be reducing the interest rate on their currency, making it less valuable. As we noted earlier, this function is normally reserved by independent central banks. Most Governments cannot directly instruct their Central Banks to reduce interest rates, but when Governments can't borrow, and therefore spend, economic activity contracts, reducing the value of the currency in that economy. Inability to borrow on the part of the Government is also an indication of lack of faith in the economy they manage, which also reduces the value of their currency. Given that Central Banks are charged with maintaining the value of a currency within a certain inflationary band (e.g. 1-2% per year), in order to preserve the stability of the currency they manage, they will normally respond to deflationary pressure (i.e. reduced economic growth) by reducing interest rates. The logic here is that if they reduce to cost of currency, and reduce the return available on saving, they will encourage greater spending, which will then boost the inflation rate back into the 1-2% inflationary band.

They essential point here is that the need for a Government to reduce interest rates and the need for a Central Bank to reduce interest rates generally arises at the same time.

Reducing interest rates makes its easier to pay back existing debt, and, in the short terms, makes the goods and services produced within a particular economy cheaper for foreign buyers (because the money to buy those goods and services is cheaper). But both Governments and Central Banks prefer to use this as a last resort, because they know the more currency they create (by devaluing the individual unit of that currency), the more they undermine the trust that people place in that currency, which has long term implications for its value.

What Governments almost never do is actually stop spending more currency than they collect in taxes. They generally understand that this is what they should do, but also understand that if they do this, they will not get re-elected, which defeats the basic purpose of political involvement.

To date, that cycle has continued without serious interruption. Every year, the US Congress ties itself in knots about whether or not to increase the Federal Deficit, but always does. What keeps this cycle going is that there are always people with currency (the wealthy elite who continue to accumulate wealth from automation in the economy) who need to preserve the value of that currency by obtaining a return on it. They trust that Governments will repay any currency they borrow, so loaning money to Governments is always seen as a safe bet.

But as the debt of Governments increases, the cost of servicing that debt increases, and as more and more people need assistance from the State (the workers whose real incomes continue to decline through automation of the economy), the more of an issue the cost of that debt becomes.

In parallel with this, privately owned media organisations (and publicly owned media organizations who compete with them) understand that their revenues are correlated with the anger and resentment that their subscribers feel towards the monolithic political and economic elite whom they feel are to blame for all their problems.

Political opportunity now starts to blossom. If the people are angry, the politician who can best articulate that anger will prosper, and it is far easier to articulate simplistic solutions to topical

issues than actually engage with people about the complexity of the world in which they find themselves.

As the articulate opportunists prosper, so the traditional political powers react. They too engage in the over-simplification and populism that their opponents are using to eat into their support. Gradually, the mundane business of sound Government is replaced with high-profile short-termism designed to appease the disaffected. When that doesn't work, more short-termism is applied. The hole gets deeper and deeper, and the only way to hold on to the shovel is to keep digging.

Eventually, the end game is reached. So much debt has been accumulated that further borrowing opportunities are unavailable, and interest rates have been reduced to zero, making it impossible to reduce the value of a currency any further.

The Government now has 3 choices. The first of these is the obvious and responsible one: to match spending with taxation, either by reducing spending or increasing taxation. Neither is popular, and in doing so, they understand that they will no longer hold power.

The other 2 choices are more dramatic: they can repudiate all their existing debt, or they can create new currency by actually increasing the supply of of the units of currency that are circulating in the economy. Both of these options have short-term appeal, probably enough to get them over the next electoral hump, but these options also have a far more serious consequence: the remove the trust that forms the basis on which people use a currency as a store of value for trade.

All of what we have discussed in this section so far is theoretical. But lets overlay with some of the events and trends that we know are taking place in Europe and the US.

European and US citizens have accumulated more State-backed debt than at any time in human history. Between 2007 and 2014, several European countries were frozen out of the sovereign debt markets, requiring bailouts from their more prudent neighbours and the IMF to allow them keep providing public services. Most of them emerged from this arrangement, but only by converting their debt to longer repayment schedules rather than actually paying it off. Public debt in the US has reached equally epidemic levels.

Worrying trends are also apparent in respect of monetary policy. The interest rate on the Euro is at 0.15% at the time of writing, its lowest ever level and as close to zero as makes no difference. The interest rate on the US Dollar is 0.5%, and hasn't risen in 2 years. Every suspicion that it might possibly rise sends US equity markets into a panic, indicating that investors believe the US economy is surviving on cheap currency rather than productivity.

Politics is also following the theoretical blueprint outlined above.

Extremes of both Left and Right, offering simplistic and seemingly obvious solutions, all of which project blame elsewhere and eschew any idea of sacrifice, are prospering.

In the UK, UKIP won 11% of the vote in the most recent General Election, and are the largest UK party in the European Parliament. In Spain, Podemos, have become the 3rd largest party in less than 5 years. In Italy, the 5 Star movement has won widespread support. In the US, Donald Trump, a former TV celebrity and property mogul, has become President. There are numerous other political movements with the same profile who are prospering across the developed world.

The traditional political parties appear to have no answer to the wave of populism that is washing over democratic nations. In the recessionary period that followed the global property and banking collapse of 2008, the Governments which had previously been formed by these traditional parties reacted by cutting spending, by introducing what their opponents called “austerity”. Dramatic electoral loses followed, not to their traditional opponents, but to the new forces of populism that had emerged as the recession unfolded. The lesson was learned that promoting fiscal prudence, which, while never universally popular, could always command enough grudging support from the core of the electorate to uphold a party's support, was now anathema.

Central Banks were also introduced to new realities. As the global recession continued and growth rates plummeted, the decision makers at the ECB, Federal Reserve and Bank of England watched as the prospect of negative inflation, or deflation, became more and more apparent. Interest rates were reduced to record lows, to levels where they were functionally non-existent. When this

didn't stem the tide, a new tactic, Quantitive Easing, was introduced. This involved Central Banks buying debt instruments issued by private corporations, to incentive borrowing on the part of the private sector, which the Central Banks hoped would promote growth. Vast amounts of currency were introduced into these troubled economies as a result, and a measure of stabilization was achieved. Inflation and growth halted their decline and began to grow again, albeit very slightly.

But the problem that Central Banks, and Governments, now faced was that they had used almost all the tools available to them to reverse the recession, but the recession itself hadn't fully gone away. Yes, growth had returned in small measure, but employment as still lagging behind productivity. The jobs that had been lost during the recession were been replaced with capital investment in automation. Market indicators also seemed to suggest that whatever growth existed was highly depended on the economic medicine of low interest rates, quantitive easing and liberal Government spending (i.e. borrowing) , none of which could continue in perpetuity.

Which brings us to the point where we are now. We have Governments that are mortally afraid of fiscal prudence. We have Central Banks who cannot reduce interest rates any further, or introduce any new currency via Quantitive Easing, and economies that are shedding Labour in favour of automation, and addicted to the life support that is being provided by economic agencies.

The question that arises is what happens when we have to deal with the next economic shock and the recession that follows in its wake, which could be even more dramatic than the most recent one as automation continues to eat into labour demand in the services sector?

Will centrist political parties risk losing power to even more extreme elements of the populist left and right? Given the reaction to the election of Donald Trump that seems unlikely, which means that reduced spending/borrowing and more prudent fiscal management are unlikely to arise as responses to any such crisis.

In the absence of renewed support for fiscal prudence, and the inevitable inability of Governments to borrow money during a recession, the only response that remains rests with world's Central Banks.

This option is what is know as “Helicopter Money”. It involves Central Banks increasing the actual supply of currency in the economy and distributing that directly to citizens in the form of actual cash payments. It is an extreme form of Quantitive Easing. Supporters of “Helicopter Money” argue that Quantitive Easing is ineffective, as private corporations use cheaper borrowing to pay off existing debt rather than make new investments. They argue that giving money directly to citizens is the most effective way to get it circulating in the economy, as the individual is more likely to spend a windfall than a corporation.

Opponents of “Helicopter Money” recognise that this is a valid argument, but oppose it from a political rather than economic point of view. Giving money directly to citizens would obviously be political popular, but anything that is political popular can't normally be reversed, and Governments would come under increasing pressure to deliver more “Helicopter Money”, even when there is no economic rationale to do so.

The ultimate question this is leading us to is what all this means for the traditional fiat currencies that are centrally managed and which we all use in our everyday lives. Recalling our history of how these currencies came into being, we are reminded that their value is entirely based on the trust we place in our institutions not to abuse them.

For how long can this trust last if Central Banks start sending cheques in the post to citizens? And if that trust breaks down, with what form of money will our currencies be replaced?

What is Bitcoin?

Bitcoin is a digital currency. That means it exists only on computer networks, and that you need a computer to use it, like email.

Bitcoin is money, because it is a commonly agreed store of value. You can use it to buy things. Bitcoin is also a currency, but it is not a *fiat* currency, because there is no central authority

that controls Bitcoin. For some, this is a concern, but for people who use Bitcoin, this is its biggest selling point. They understand that its value can never be increased or diminished for political or economic gain. Instead, Bitcoin's value is entirely derived from its finite supply and the amount of people who want to use it in their economic transactions. In this, Bitcoin shares exactly the same characteristics as gold.

If you research Bitcoin on the Internet, you will probably find images of piles of coins emblazoned with a “B” symbol.

But in trying to understand Bitcoin, you should expel from your mind the notion that a Bitcoin has any physical manifestation, or existence in any sort of unit, notional or physical. Bitcoin is essentially a record of transactions. Your holding of Bitcoin is the sum of your Bitcoin transactions, not some tangible or even intangible asset. You don't need to understand the full import of that definition right now, but you should remember it.

Lets leave the technical stuff aside now and provide an example.

Lets say Alice has acquired 100 Lydos (a fake currency that I have just made up, which are actual physical coins). Alice gives 50 Lydos to Bob. Bob gives 30 Lydos to Catherine. Catherine gives 10 of those Lydos back to Alice. All of these transactions are recorded in a journal, which Alice, Bob and Catherine each have a copy of and agree is accurate.

At this point, everyone agrees that Alice has 60 Lydos. Dan now comes along, and takes a copy of the journal. Alice records in the journal that she has given Dan 20 Lydos. Everybody's copy of the journal is updated, so if Dan now gives Bob 10 Lydos, Dan, and every else, is happy that Dan has 10 extra Lydos.

Now lets do something crazy. Lets do the whole things again, but this time without the actual coins. Lets just make sure every transaction is just recorded in the journal, and that a really secure and trusted system exists to share and protect the journal, and that everyone agrees that the journal is accurate. Now if Dan wants to give Bob 10 Lydos, he just has to write it in the journal, and everyone has to agree that the journal is accurate after Dan has made the update. Once everybody is happy that the journal is secure, everybody can just keep updating and sharing it and agreeing that it is accurate. No actual coins are needed. If somebody else comes along, they can take their copy of the journal and start recording transactions in it and sharing that information with the others.

If you can understand this in principle, you can understand Bitcoin.

But here's the next question: where do the Lydos come from in the first place? This is where is gets a bit tricker to understand.

For most people, if you want to earn currency, you have to do some work. In Bitcoin, its the same. Agreeing on the accuracy of the journal, making sure it is secure and distributing it to everybody who wants to participate in the system requires work, by computers that are owned by humans. The humans that run the computers that do this work also know that Bitcoin is designed to have finite supply, so there is an incentive to get in there and do the work before the supply of Bitcoin runs out.

All of the transactions that are made in the journal are divided up into blocks of transactions. After a certain number of transactions are entered in the journal, a new “block” of transactions is declared, and that block is then “frozen” so that it can no longer be altered, which is a key component in everyone agreeing that the journal is accurate. If everyone understands that a block of transactions can never be altered after it is finalised and agreed, everyone will be more likely to trust the journal.

To freeze the block, it has to be locked with digital encryption. A very high level of trust is required, so the effort to perform this encryption is significant. The computers that participate in the network race to complete the encryption task. The computer that wins this race gets to add an extra transaction to the block before sealing it. That transaction records an allocation of Bitcoin value to that computer, which all of the other computers agree can be used by that computer.

So to answer the question simply, it is the work involved in maintaining and and securing the journal, which is called the Blockchain, which generates the Bitcoin. This process is what is

referred to as Bitcoin Mining.

If you're still getting this you're doing really well, but there are still a couple of things that are essential to understand. We'll break this part into questions.

I still don't get the thing about Bitcoin only being a record of transactions, and not an actual unit of money. I see goods and services that are priced in units of Bitcoin. There is a US Dollar and Euro exchange rate for Bitcoin. How can that be if there is no "unit" of Bitcoin?

Bitcoin is complex, and to facilitate wider adoption, it is given artificial characteristics that are familiar to people who don't have the time or inclination to understand its complexity. If I state that I own 200 Bitcoins, what that means is that the sum of all my transactions in the Blockchain (what I have been given less what I have given away) is equal to 200 Bitcoins. When someone charges me 5 Bitcoins for a service, I send a transaction to the Blockchain that reduces my holding of Bitcoin and increases their holding of Bitcoin. I don't actually send them Bitcoins, although that is normally the phraseology used.

If the Blockchain states that I have 1 Bitcoin that I can transfer to someone else, how do I identify myself to the person to whom I want to send that 1 Bitcoin?

Entries in the Blockchain do not contain the names and addresses of people making transactions. A transaction is recorded as 2 alphanumeric strings, one for the sender and one for the recipient. These alphanumeric strings are cryptographic hashes. The hashes can only be created (encrypted) by the people involved in the transaction, but can be read (decrypted) by anyone. This part of Bitcoin is actually a lot more complex that this, but to feel comfortable with the security of the Blockchain, all you need to understand is that everybody can verify you have Bitcoin value to spend, but no one other than you can spend Bitcoin value that is allocated to you. You effectively have a "lock" on any transactions in the ledger that involves you in the transaction. Only you can update these transactions (by creating new transactions) to create new value elsewhere in the Blockchain.

If each new block adds more Bitcoin to the pool, won't their value diminish over time?

Bitcoin technology is designed so that only 21 million Bitcoins will be issued. After that point, it will no longer be possible for computers to add extra transactions to the Blockchain that add Bitcoin value for them. Computers will continue to be incentivized to participate in maintaining the Blockchain by charging transaction fees. These are fees that are deducted from the value of a transaction that is added to the Blockchain. These fees are already charged, but are small in comparison to the value of the transaction value that computers can currently add to the block when they win the race to encrypt the block.

What if one dishonest computer wants to alter the Blockchain to say that it has more Bitcoins to spend than it really has?

Every block in the Blockchain has a relationship with every other block. Each new block is started with a value derived from the previous block. To alter the Blockchain, for example to say that you had not transferred some Bitcoin to someone else, you would have to re-encrypt the Block in which that transaction occurred, and every other subsequent Block. Blocks are created approximately every 10 minutes. The computing power required to alter an entire series of Blocks would cost far more to acquire and maintain than any possible value that could derived from altering the Blockchain, so there is no financial incentive to attempt this. This is true even if the value of Bitcoin rises to extraordinary levels, as the more valuable Bitcoin is, the more incentive there is for computers to participate in the network, making it harder and harder to maliciously alter

existing blocks.

End of questions.

To deliberately labour the point, Bitcoin technology is very complex. It is the product of some of the most gifted and creative minds in computing and cryptography. Understanding its intricacies is optional, and really only necessary if you want to participate in its development or forecast its long term technological trajectory.

In every day life, it is simple to use. Bitcoin users have wallets like users of regular currencies, except that their wallets are software rather than bulges in their pockets. They keep these wallets on their phones or their PCs, or sometimes they get a service provider to manage them for them. Their wallets allow them to receive Bitcoins from others, and send Bitcoins to others, and, by being in constant communication with the Bitcoin network and the Blockchain, automatically update the value of Bitcoin that is available to the owner of that wallet to spend. The wallet is essentially a key, that allows the user to lock and unlock their transactions in the Blockchain to distribute and acquire Bitcoin value.

Bitcoin has been around since 2009. It was created by a single software engineer, whose identity is unknown, and is now maintained by thousands of developers all over the world. Nobody owns Bitcoin. The design of the technology means that it can only exist on a distributed network. If anybody attempts to own it, it becomes worthless, so there is no inventive to own it.

Its growth since 2009 has been phenomenal. At the time of writing, over 300k Bitcoin transactions are executed each day. It has also experienced some significant reverses, all of which have been to do with improper management of wallets by service providers. The core technology has never been compromised. Few technologies in history have been subjected to the level of skepticism and attack that has been experienced by Bitcoin, but it is more valuable against traditional currencies today than at any time in its history.

Why could go wrong?

Bitcoin isn't perfect. The question is whether or not it can replace the existing imperfect fiat currencies that we use, or at least become an alternative to them. Whether or not it can will depend on technical, societal and political considerations. Let's consider these in turn.

Bitcoin itself is highly secure, to a far greater degree than centrally managed currencies. However, to bring Bitcoin into general usage, particularly among non-technical users, individuals and companies have to offer services that allow for the creation, exchange and storage of of Bitcoin. This is generally where the security issues arise. However, traditional currencies are also exposed to huge security vulnerabilities, like Credit Card fraud, and online banking fraud, and basic theft, the risks which people accept and live with.

Capacity is another issue for Bitcoin. Currently, a Bitcoin transaction can take up to 10 minutes to be processed, which means you're not going to be able to use Bitcoin in a supermarket or petrol station any time soon. This is a major technical challenge for the Bitcoin community, and there is no consensus how to proceed. Some users want to change the technology to allow more transactions be processed in each block, but other argue this will undermine the security of the Blockchain. Other users want to build an intermediary layer between the end-user and the Blockchain, that can process immediate transactions and then pass them off to the Blockchain for processing after the fact. Until some sort of consensus is reached, the future technical direction of Bitcoin is uncertain, and that will weigh on its value.

Bitcoin only has value if people use it. If a lot of people are going to use it, it needs to establish trust and respect.

But in its early years, one of the principle uses of Bitcoin was on the “Dark” Internet, where the anonymity of transactions made it ideal to deal in drugs and arms, or anything else that was illegal to trade.

One of the largest sites engaged in this activity was called the Silk Road, which hosted millions of dollars worth of illegal transactions, using Bitcoin, before its owner was eventually tracked down and arrested in 2014. This created a lot of bad publicity for Bitcoin, and caused a lot of financial institutions to stop dealing with companies whose businesses were based on Bitcoin. It took several years for Bitcoin to establish the level of trust it had had built up prior to the collapse of the Silk Road. What is interesting about the episode is that when the Bitcoins that were seized from Silk Road were later auctioned by US authorities, the price they achieved was greater than the price of Bitcoin before the scandal broke.

Bitcoin is not the only digital currency on the market today. In fact, there are about 700 different digital currencies. Most of these arose out of the success of Bitcoin, but few have achieved anything like the level of traction and popularity enjoyed by Bitcoin. However, there are some which have prospered, and according to certain experts in the field, are better than Bitcoin from a purely technologically point of view.

The danger for Bitcoin is that one of these currencies, for example Ethereum, could outstrip the popularity of Bitcoin, and given that Bitcoin value is entirely based on the number of people using it, this would lead to a rapid decrease in Bitcoin's value.

However, to date, there has been no sign of this happening. What is becoming clear to observers in the digital currency world is that value is tied a lot more closely to trust than technological perfection, and because Bitcoin has established such solid foundation of trust, it is highly unlikely that any specific technological feature of an alternative currency will affect that.

Fear of Government regulation is one of the reasons why Bitcoin was invented, why its popularity grew and now, ironically, one of the potential brakes to its growth. If Governments begin to sense that Bitcoin is a threat to their fiat currencies, they may move to regulate the use of Bitcoin. The technical challenge involved in this would be immense, and in all probably, they would be unsuccessful, but the signal this would send to the financial community would be damaging. Bitcoin needs to have legitimacy. It can't survive if there is a persistent fear that the State will quash it, even if the State's ability to quash it is very limited. This would manifest itself in banks refusing to deal with Bitcoin companies, or major retailers refuse to buy and sell in Bitcoin.

To date, the response of the State to Bitcoin has been mixed. On a positive note, US authorities have taken steps to officially recognise the use of Bitcoin as a currency. However, the Inland Revenue Service has also made demands of Bitcoin exchanges to release personal information about users.

In China, where Bitcoin has established particularly rapid growth, there are persistent rumors that the Central Bank of China is about to step in and regulate Bitcoin. This is attributed to the growing use of Bitcoin as a means for wealthy Chinese to transfer their wealth from the Yuan to western currencies, in that capital controls apply in respect of the Yuan. A similar situation exists in India, and several South American countries. As of yet, no attempt has been made in these countries to regulate Bitcoin. The explanation for this is unclear. Some of it is probably to do with the uncertainty in relation to what is possible, some of is political, and some of it is probably just good old kicking the can down the road.

Should I buy Bitcoin?

To answer this question, we must recap what has been discussed thus far.

We use currency as a store of value. Originally, that currency had real value. Now, it has no value, other than the trust we put in political authorities to maintain its value.

As economic activity becomes more and more automated, and the world's population increases, the ability of Governments to provide income to voters contracts, necessitating expansion of currency supply to maintain order.

As currency expansion becomes the norm, so the trust placed in currency recedes, ultimately devaluing currency to the point where it no longer retains trust.

At this point, a new store of value will be required. That store of value will have to retain all

the characteristics of gold, but also must be highly divisible, digitally enabled and beyond the reach of Governments.

It is at this point that Bitcoin becomes the world's reserve currency.

This is a simplistic prognosis. It is unlikely that a transition will be that seamless, complete or imminent. But this is the *trend*, and if events keep unfolding as they currently are, it is likely that some version of this prognosis will ultimately come to pass.

However, until we get to the point where trust in fiat currencies begins to degrade, other forces will have to sustain Bitcoin. At the time of writing, approximately 300,000 Bitcoin transactions per day are entered on to the Blockchain. That's a huge number relative to Bitcoin's maturity, but it is tiny compared to the number of transactions in fiat currencies.

Equally, while Bitcoin does have critical mass in terms of person to person transactions, there are relatively view outlets where users can trade Bitcoin for goods and services. For Bitcoin's incubation period to continue, it is therefore vital that people continue to make long term investments in Bitcoin's future.

This is where the FinTech industry comes into play. FinTech describes the use of technology in finance. For example, PayPal is a FinTech company, and Apple Pay is a FinTech product. FinTech is a huge growth area, and investors are staking large amounts of cash on its future. They foresee the continuing migration of commerce into the digital world, and the continuing struggle with problems such as fraud and security, and recognise the enormous opportunity this presents.

For these investors, the Blockchain has particular appeal. The Blockchain is a revolutionary technology, and has been central to Bitcoin growing to where it is today, and surviving the many challenges it has faced.

But while Bitcoin technically depends on the Blockchain, the Blockchain does not technically depend on Bitcoin. It can be detached, and used for other purposes; for example, to securely record trades in stocks and shares. FinTech companies and investors have been quick to latch on to the potential of the Blockchain, and there are now myriad companies working on non-Bitcoin applications of the underlying Blockchain technology.

What this means for Bitcoin is that awareness of, and trust in, the Blockchain will continue to grow, which by extension means that awareness of, and trust in, Bitcoin will continue to grow. Over time, they will develop a symbiotic relationship: if trust in Bitcoin suffers, so will trust in the Blockchain; if trust in the Blockchain suffers, so will trust in Bitcoin. This means that the number of people who have an interest in Bitcoin succeeding will grow exponentially, driving them and others to force Bitcoin in the realm of the traditional fiat currencies.

In conclusion, if this text has convinced you that the nature of our economies and politics is changing, and that this will bring to an end the primacy of the fiat currency, however long that takes, then, yes, you should buy Bitcoin.