SPECIAL ESSAY FROM THE OWNER/AUTHOR: THE UNBREAKABILITY OF BITCOIN

Go to www.bitgoldwallet.com for information on what bitcoin is and how to safely buy, use and store it, and how to choose a secure and memorable password

Saturday 24 February 2018

Foreword...

This article was first prepared in January 2017 and the values in it are now inaccurate. I have only just decided to share it with readers now. The article is almost identical to when it was first written with only some minor editing. The financial figures have not been changed in order to highlight the growth potential of crypto-currencies. The current total marketcap of bitcoin is \$175 billion USD and the total marketcap of altcoins is \$284 billion USD. Up to date figures can be found via an online search.

The Unbreakability of Bitcoin...

Why is bitcoin worth anything?

Why is bitcoin worth anything? Why has it gone from being worth \$0 USD total in January 2009 to being worth over \$10 billion USD total as of January 2017?

I remember when I first heard about it. I don't even remember quite when but I clearly remember my absolute dumbfounded reaction to it. It was not a positive reaction. It was wholly of disbelief and the feeling of total absurdity at the idea. Total absurdity and the total unquestionable belief that it would not succeed, and that the individuals who created such a thing were doing it just for fun. How wrong I was.

Fast forward to October 2016. I revisited the idea of Bitcoin to see how things were going. True enough, bitcoin was still obscure and not yet mainstream, but boy had it grown. It was now clearly out of harms way of disappearing from existence at any single time. It had become a child of about 7 years of age, able to walk on its own and existing in the world in its own right. It had the immune system of an entity that had taken its fair share of hits and knocks and was as strong as ever.

What was more profound was just what it was worth. Any doubts I ever had about its potential evaporated. I made it a firm resolution never to blindly doubt bitcoin again and so I got about learning more about it, about how it worked and why it was worth so much. What I learnt led me to make my first purchase of bitcoin and eventually led me down the road of becoming more involved in the bitcoin system and the promises of riches it offered. I will say that I am converted and it takes a lot to convert me to a big idea. Having said this, nothing impresses me more about Bitcoin than its future potential and guaranteed place in this world as a king of wealth.

Bitcoin can currently be seen as being just a guppy in a tank full of fish. It is one financial form of wealth among many others. It exists both as a form of currency like the US dollar and as a form of wealth preservation like gold. In these two markets alone (currency and gold) it is tiny. In Dec 2015, according to 'The Money Project' all the world's gold was worth \$7.8 trillion USD and all of the world's easily accessible money (which includes coins, paper money and bank account deposits) was worth \$28.6 trillion USD. This makes Bitcoin's \$10 billion USD, amount to less than 1/3650th of this. If bitcoin was to grow to take up merely 1% of this total amount, each single bitcoin you hold would be worth over 36 times what it is worth now. If it was to grow to be worth half the total market value of gold, it would be worth over 380 times what it is worth now.

Which leads me back to the original question I asked which is: why is bitcoin worth anything?

The short answer to this is that bitcoin is worth what it is worth because it has most of the characteristics that makes currency valuable and most of the characteristics that makes gold valuable. These things derive their primary value from the fact that they are an exceptional medium of exchange and a great store of wealth. In my opinion, bitcoin could be called bitgold as well as bitcoin.

Why is gold valuable?

Gold cannot be forged Gold is very durable Gold is easily recognized as gold Gold is portable and value dense Gold can be separated into smaller parts Gold has a limited supply Gold is tradable

Why is a well managed currency valuable?

Currency is hard to forge Currency is durable Currency is very easily recognized as currency Currency is portable and value dense Currency can be separated into much smaller parts Currency has controlled limited supply Currency is tradable

So now finally, why is bitcoin valuable?

Bitcoin is impossible to forge:

Gold is impossible to forge but it is possible to make fairly hard to detect fake replicas of, especially in the case of gold coated tungsten coins and bars. Paper money is hard to forge but by no means is it impossible. Digital currency is likely hard or impossible to counterfeit illegally but by no means is this assured. All it may take is a very sophisticated computer hacker. Additionally, certain forms of digital money are rather easy to create legally by banks out of thin air via unsecured loans and other means.

Bitcoins however, are impossible to forge. Every single bitcoin that was ever added to the blockchain or will ever be added to the blockchain is an original, impossible to fake, impossible to counterfeit, impossible to manipulate unit of bitcoin. This has been proven in the 8+ years it has been around. No individual or organization can create more bitcoins out of thin air without doing it through the proper process. No bank or government can simply add more bitcoin to the money supply on a whim after creating it out of thin air. No bank or government can create fake stores of bitcoin like they can with gold or currency, and present bitcoin as being real when it is not on the blockchain. With gold and currency it is wise to entrust large amounts of these for storage with another organization (such as a bank) since gold and paper currency is easily stolen and hard to store large amounts safely. With bitcoin, we do not have this problem. Your personal storage of bitcoins can be as good and secure as that of a large organization. Not to mention, gold and currency can be costly to store whereas bitcoin is not.

To sum up, every bitcoin currently stored at a bitcoin public address is impossible to forge.

Bitcoin is indestructibly durable:

Exists only as information which can never be destroyed. Your bitcoin private key is essentially a completely random number from an unimaginably massive list of possible numbers.

Although it can never be destroyed, like all other forms of wealth, it can be lost. Even gold and currency can also be lost. Bitcoin is more resistant to lost however because copies where the information is recorded can be backed up.

Bitcoin is easily and definitively recognized as bitcoin:

As long as you have internet access you can check that you have bitcoins. You can be sure the coins are real because you hold the private keys to the address/s. If the main site that shows you the record of the bitcoin blockchain that proves your funds are there goes down, there will be other sites you can check or new websites will spring up. Or you can simply download a wallet program that has the full copy of the blockchain via decentralized file sharing systems like torrents. Bitcoins can be verified with 100% accuracy anywhere where there is an internet connection. That is the only thing that is really needed.

Gold is easily recognized as gold. Currency is very easily recognized as currency. Gold does an adequate job in this respect and currency does a great job. Gold can be made to be easier to recognize through the process of minting and other means and this has been used throughout the ages...

Bitcoin is portable and value dense:

Bitcoin is more portable than gold and paper money and can be transported completely anonymously and internationally without physical restriction. Currently, 1 million USD worth of gold will weigh over 20 kilos. 1 million worth of cash will take up significant space in a suitcase and will weight a fair bit. 1 million USD or more worth of bitcoin will weigh as little as a usb drive or SD card, or even less. Bitcoin is always portable. Not to mention transporting it can be much more anonymous than transporting gold or currency.

Bitcoin is more portable than other digital currencies because it is a universal currency usable all over the world. For a digital currency (such as the Chinese yuan) to travel from one country to another country requires it to be transferred from one bank account to another bank account. Governments may impose restrictions on this happening and banking institutions may charge high fees. With bitcoins, the first can't exist and the second is always reasonable. You don't really need to transport bitcoins anywhere in the first place because it is useable all over the world. You could if you wanted, store it completely on the internet and avoid carrying it anywhere.

Bitcoin can be separated into much smaller parts:

Gold can be broken into smaller parts however throughout most of its existence this size has been limited to a size where the volume and weight of the gold can still be reliably measured. These volume and weight measurements are needed to ensure the authenticity of the gold otherwise it would be useless as a medium of exchange if its authenticity can not be confirmed. This means that gold cannot simply increase in value indefinitely while at the same time decrease in size and volume to meet demand for it as a medium of exchange. Governments around the world have tried doing this many many times by mixing other metals into gold coins and the effect has always been the same – inflation to the point where the gold coins become useless. In the 19th centuries and before, if 10 grams of gold was the minimum measurable size and weight and was worth for example \$200 USD, then this did not mean that a one gram bar of gold was worth \$20 and could be traded as such. This was because there were no scales or volume measuring devices that could check accurately enough that the one gram bar of gold was in fact authentic. The minimum unit of gold that could be weighed and measured maybe needed to be about 10 grams. Now these amounts are arbitrary but the point is that a lower limit value exists. Nowadays, with our sophisticated scales and other measuring tools, that lower unit value is probably in the tenths of a gram but there is still a lower limit value.

This problem does not exist with Bitcoin or with other digital currencies. Generally bitcoins can be broken down into as small a unit as is necessary as the bitcoin value increases. If the 16 or so million bitcoins currently in existence were to grow to the value of 100 trillion, which is about 3 times the estimated value 'The Money Project' calculates all the world's 2015 gold supplies and easily assessable money to be worth, then one satoshi, the smallest unit of bitcoin would be worth about 10000 times what it is worth currently, which would be about 10 USD cents. 10 cents is still a very usable value. In essence, bitcoin can be separated into much smaller parts if needed. A major benefit with bitcoin over currency in this respect however is that bitcoin's supply is strictly limited and can never exceed 21 million coins in circulation. This means that it cannot experience hyper inflation.

Bitcoin has exact limited supply: 21 million maximum. Every 10 minutes or so a set amount is added to the system (currently 12.5 coins) based on the authentication process. The difficulty level of this process is set by the protocol (software program) in such a way where it will always take around 10 minutes on average to complete. This is irrespective of how many computers are currently taking part in the authentication process (known as mining). This is in contrast to gold mining or currency printing where the level of new gold or new currency that enters the world is always different and has been different throughout the ages. These differences can have a significant effect on the value of the gold or currency especially if they are sudden and large. In the case of gold, it is estimated that about 3000 metric tones in 2016 was mined. For the case of currency this amount is closely related to the inflation rate and depends mainly on the governments and banks that issue the currency (not to mention the counterfeiters!).

If the supply of a currency or medium of wealth storage is always at a stable level, this goes a long way to ensuring that the value of the currency or medium of wealth storage is stable. This limited supply is one of the main things which has made gold so useful as a currency through most of known history or as a backbone value throughout most of known history. Gold has been used effectively as a standard because it does such a great job as a medium of exchange and as a store of wealth.

Bitcoin is tradable:

It cannot be understated how big a factor this plays in making a commodity a valuable medium of exchange and store of value. This is possibly the primary factor that separates bitcoin from all of the other cyptocurrencies (called altcoins) currently in existence. Bitcoin came out first and it became widely traded. This head start has made all the difference. It developed the user base and the authentication base it needed to grow to become a world product. Its tradability factor in many ways surpasses traditional digital currencies and this is a key reason for its continued success. It has enabled countless unbanked individuals in the developing world to spend and store digital money. It is a perfect value storage method for refugees and those people seeking to flee from their home countries. It is an ideal form of currency for prison inmates, and yes, online prohibited trading. It is great for use as casino chips for online gambling websites due to its anonymity factor. It can be and has been used as a way of accepting donations when no other method of donation may be available. It can be sent and received via sms or wallet app for anyone with a phone.

Its use was validated in the USA after the FBI auctioning of the silk road confiscated bitcoins, and after this, many corporations sprung up.

Bitcoin is traded and accepted worldwide. It is completely neutral in its position as a currency. It does not favor one geographic or political region over another. It does not discriminate on who can use it or how it can be used. Whether it is used in online gambling websites or by prison inmates or by reputable business establishments makes no difference. Bitcoin can be traded by all.

It could be observed that gold really started to made its mark on the world in early the 19 hundreds when trade restrictions were reduced and gold become a much more easily traded commodity.

Bitcoin will always be tradable. The reason is: its marketplace is global and it is a commodity that is traded via the internet. Unlike physical gold which must be traded at a physical location which may allow for governments or other organizations to impose trade bans or manipulate local prices, bitcoin is without

boundaries. Bitcoin bypasses governments. A government cannot ban bitcoin trading much like it cannot ban MP3 sharing from peer to peer sites or it cannot ban people from sending emails to each other. There is no central location where all trades are performed. Bitcoin.com and Bitcoin.org are merely websites that allow people to monitor and download the current state of the bitcoin blockchain. Localbitcoins.com is merely one online trading platform where buyers and sellers of bitcoin can meet. If these sites are shut down, others will take their place. Any attempt to ban bitcoin would much more likely have the effect of making it more popular as it will draw people's attention to it which may have not have been there before.

Tradability can also mean how simple it is to buy, store and spend bitcoin. With gold, you simply go to a gold dealer. With currency you simply hand over paper money to another person or you use a bank or bank instrument like a credit card or bank account. At the moment, for bitcoin, this process is not the simplest to do securely. A lot of it has to do with the excessive government regulations surrounding it. Or maybe even the inadequate government regulation surrounding it. A lot of it has to do with the fairly technical aspects of the technology which may not be easy for the layperson to understand. During its 8 years or so of growth, bitcoin has made many leaps and bounds in this and many other respects and the technology as a whole has become much more assessable and useful to humans in general. This trend will continue into the future until it becomes as easy to use as email.

Summary:

In summary, as you can see, bitcoin is currently a good medium of exchange and a good store of wealth which explains its current value in the world. Having said this, there is nothing about it that will limit its potential to become an exceptional medium of exchange like a well managed currency or a good store of wealth like gold. In fact, it can surpass both currency's medium of exchange factor and gold's wealth preservation factor. It is global in a way that currencies cannot be global and gold cannot be global. It is a store of wealth in a way that currency cannot be a store of wealth and gold cannot be a store of wealth. When bitcoin moves from being good at these things to being great at these things, a large minority of people in the world will notice. When bitcoin moves from being great at these things to being exceptional at these things, the majority of people in the world will notice... and life will never be the same again.

DISCLAIMER

This document is not financial advice. It is not investment advice. It is not legal advice. These notes represent only the opinion of the author and is not an offer to sell bitcoin or anything else. Everything offered here is presented as is, purely for information purposes, and the author and anyone affiliated with this work accepts absolutely no liability whatsoever for any circumstance, action, or loss that may arise out of the information provided. The reader of this information does so entirely at their own risk. They must take full responsibility for their own actions and should do their own research on the appropriate topics.

^{***}Go to www.bitgoldwallet.com for information on what bitcoin is and how to safely buy, use and store it, and how to choose a secure and memorable password***