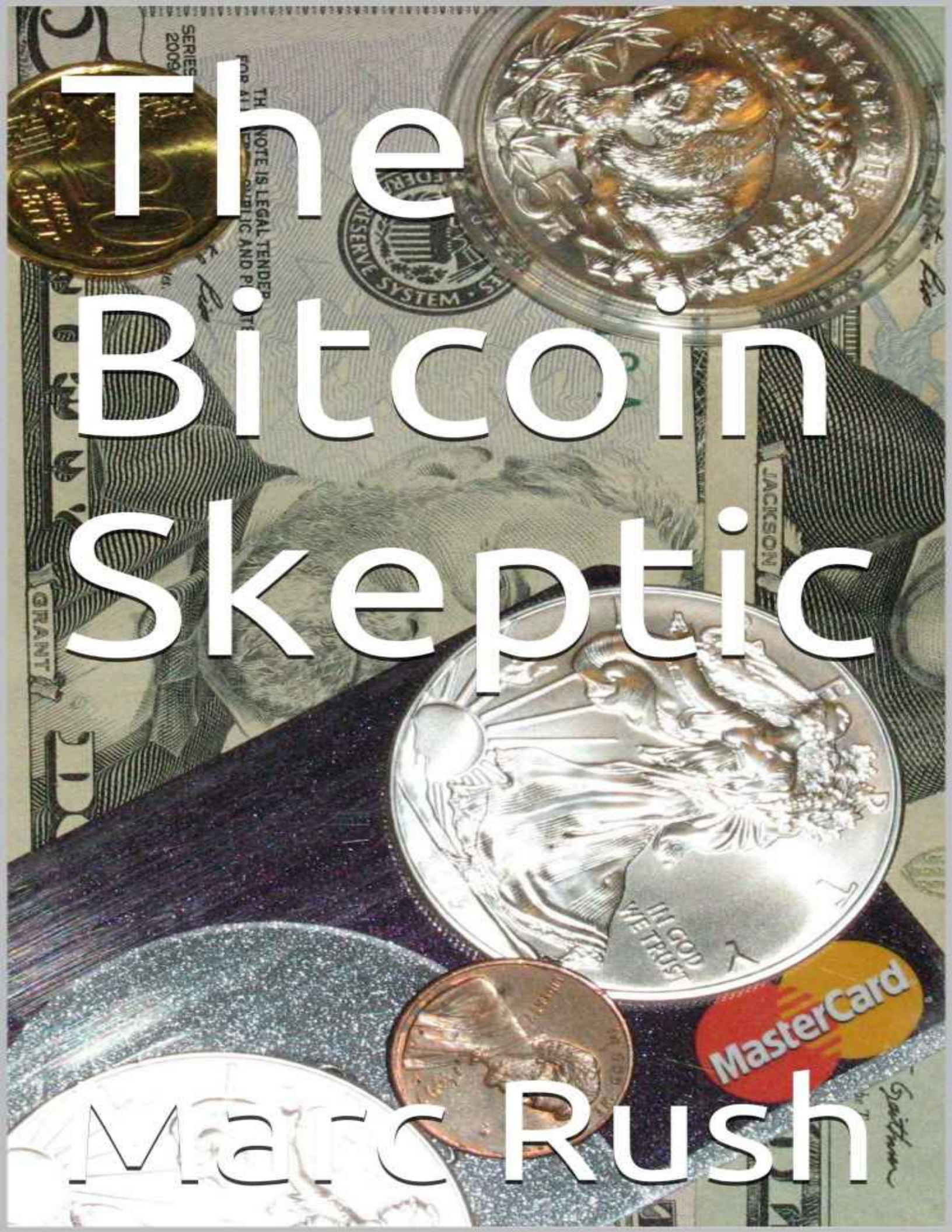
The Bitcoin Skeptic
Marc Rush
JACKSON
GRANT
IN GOD WE TRUST
MasterCard

THE BITCOIN SKEPTIC CONSIDERATIONS BEFORE YOU PROCEED

Marc C. Rush

 To All Those Who Don't Believe The Banksters And Are In Search Of A Safer, Better And More

Effective Store Of Value
This book should in no way be construed as financial/investment advice. Consult your financial advisor (and/or your thinking cap) before making any financial decisions.
Contents

Introduction

It is completely understandable that people are looking for new places to put their money.

Central banks are printing money at an unbelievable rate, and running up debt to astronomical levels. This calls into question not only the sustainability of such actions, but the value and sustainability of these currencies themselves.

Interest, even on a long-term certificate of deposit is under 2 % which means, when inflation (especially food and energy) is taken into account, you are losing money by leaving it in a bank. In such an environment, it is only natural for people to look for a better hedge against inflation.

And then there is Cyprus. The original plan to bail-out the banks there included taking money from depositors, even insured depositors. The final plan spared the insured depositors, but there are capital controls limiting how much money depositors can withdraw from the banks. A logical question is where else could this happen next?

Also, the government, especially post9/11 is tracking everything. Your phone calls, emails and certainly your financial transactions. Oh how nice it would be to give Uncle Sam a great big middle finger and say, "Sammy, you can't track me now. Ha ha ha."

For all of these reasons, it is understandable that people would be looking for some place new to put their money, especially a place that is more financially secure and somewhat anonymous.

Enter Bitcoin (BTC). If you believe the proponents of it, BTC solves all these problems, and (because they say there will be a finite number of them) will continue to increase in value long into the future.

Recent history suggests that BTC is not the panacea its proponents would have you believe. We will get back to this in great detail, but first, by way of background and necessity, will be a very brief description of what BTC is and how it works.

BTC was created in 2009 by someone using the name Satoshi Nakamoto. He used cryptography to create a digital currency.[1]

The creator designed BTC with a proofof-work component whereby people voluntarily allow their computers to be used as part of a verification process.[2]

In exchange for this, the people who successfully crack the code can receive free BTCs, although they are not really free when one takes into account the $1000 plus cost of the necessary computing equipment and the electricity to run it. The other way people can obtain BTCs is by buying them from an exchange or elsewhere.

Once one has BTCs, they can redeem them for currencies or spend them at merchants who accept them. In order to spend or redeem BTCs, once has to prove he is the rightful owner of them.

To prove this, the owner of the BTCs has a 51 character secret number called a private key.[3]

[1] http://en.wikipedia.org/wiki/Bitcoin
[2] http://bitcoin.org/bitcoin.pdf
[3] https://en.bitcoin.it/wiki/Securing_your_wallet

This key can be kept by the individual owner on their computer, on removable media like a flash drive, or even written on a piece of paper. BTCs can also be kept on a third party website referred to as an exchange which would allow deposits, withdrawals and payments.[4]

The promises of BTC are an electronic payment system, privacy/anonymity and nowadays many claim it is a hedge against inflation or even an investment.

THEFTS/HACKS

One reason people put money in a bank, and do not leave all of it under their mattress is they are concerned it might be stolen if they leave it at home. Granted we can have a discussion about whether a bank paying you one-percent interest which does not keep up with inflation is its own sort of theft, as well as concerns about uninsured deposits being confiscated in Cyprus, but generally speaking, in most instances, one of the reasons you put money in a bank is for reasons of security. Does BTC provide the same level of security?

In September of 2012, $250,000 worth of BTCs were stolen from a America called Bitfloor.[5] BTC exchange in

Bitfloor closed operations as a result of this theft, and customers lost all their BTCs stored on this exchange.

[4] https://en.bitcoin.it/wiki/Ways_to_store_Bitcoins [5] http://www.economist.com/node/21563752

Subsequent to this, Bitfloor began operating again, with a commitment to try and return users funds, and that the exchange now has greater security.[6] How reassured are you?

Mt. Gox is estimated to handle over 80% of all BTC trade.[7] In June 2011, on this most popular BTC exchange, the price of BTCs went from $17 to less than a dollar in minutes.[8]

At that time, trading was suspended and Mt. Gox blamed the crash on a compromised user account. As a result of this hack, Mt. Gox users had their usernames, email addresses and passwords put on the internet for all to see.

Earlier in the same week, a weakness with Mt. Gox was reported in which an attacker could take over a user's account.[9]

In March of 2012, $228,000 worth of BTCs were stolen from eight customers of a popular webhosting company by taking advantage of a vulnerability.[10]

[6] http://bitcoinmagazine.com/bitfloor-back-inbusiness/
[7] https://mtgox.com/
[8] http://arstechnica.com/tech
policy/2011/06/bitcoin-price-plummets-oncompromised-exchange/
[9] https://bitcointalk.org/index.php?topic=18709.0

The webhosting company put out a statement advising that security was their top priority and they would be reviewing procedures to prevent a reoccurrence.[11]That's good enough for me.

In May of 2012 the exchange Bitcoinica was hacked and $90,000 worth of BTCs were stolen.[12] Instead of being able to access their accounts, users of this exchange were redirected to a porn site. Bitcoinica is no longer in business.[13]

In March of 2013, an account at BTC payment processor Bitinstant was hacked and $12,000 worth of BTCs were stolen.[14]

In a blog post about the theft, Bitinstant said in part, "The attacker is not highly technically skilled." That makes me wonder how extensive the financial loss could have been and

[10] http://arstechnica.com/business/2012/03/bitcoinsworth-228000-stolen-from-customers-of-hackedwebhost/
[11] http://status.linode.com/2012/03/managersecurity-incident.html

[12]

http://www.theregister.co.uk/2012/05/15/bitcoinica _hack/
[13] https://en.bitcoin.it/wiki/Bitcoinica
[14] http://techcrunch.com/2013/03/08/hacker-steals12000-worth-of-bitcoins-in-brazen-

dns-based-attack/

could be from someone who is highly technically skilled.

Also in March 2013, the largest BTC exchange in Brazil was hacked, taken offline and users were not guaranteed of getting all of their funds returned.[15] The owner of the exchange sent an email to users stating that he would try to pay back what he could, whatever that means.

What are we to make about the hacks/thefts of BTCs? One proponent of BTC dismissed such concerns stating, "Don't worry about the occasional BTC hack, pioneers always end up with a few arrows in their back…"[16]

Do you want to be a pioneer?
As unenthused as one could be about bank accounts, they have their advantages. If your bank goes bust, your insured deposits are protected (barring the unthinkable). If someone steals your credit cards and runs up bills, you are protected. If someone steals money from your bank account you can go to local, state and federal law enforcement for assistance.
When someone steals your BTCs who are you going to call? The Ghostbusters?

15

http://www.reddit.com/r/Bitcoin/comments/1b8mtn /
16 http://maxkeiser.com/2013/03/08/roger-vercharlie-shrem-2013-bitcoin-symposium nhlibertyforum/

Yes in theory theft is theft and you could attempt to get help from law enforcement. What if the hacker is in Russia, China, or North Korea? Who will you go to for help?

While we are on the subject of thefts and hacks, what is to prevent an exchange from claiming they were hacked or victims of some other kind of theft even if there was no hack/theft? Let me be clear. I am not suggesting that this has happened to date, but rather suggesting there is virtually no oversight of these exchanges, so who could prove otherwise.

With banks, they have a regulator who is auditing their books, and there is insurance for depositors. What is to stop someone from waking up tomorrow, starting a BTC exchange, getting a significant amount of deposits, and then simply claiming they were hacked and telling the users too bad, so sad, bye bye?

The startling lack of oversight is reminiscent of the Seinfeld episode where Kramer tells Jerry and George that he is going to start a make your own pizza business and George informs him that you can't have people shoving their arms into 600 degree pizza ovens. Kramer's response: "It's all supervised."

PRICE FLUCTUATIONS

In its brief history, BTC has seen some rather wild and unsettling price fluctuations. If you are a gambler you may think that is great because it means the possibility to make a lot of money. It also means the possibility to lose a lot of money. Also, if BTC is to be regarded as a currency, how highly can it be regarded if there are dramatic price swings?

We already covered the hack at Mt. Gox which resulted in a price swing from $17 to pennies in one day. Defenders of BTC might say that that was only on Mt. Gox exchange, and that the drop was not as severe on other exchanges at that time.

That is true. Prices at a competitor exchange only dropped 25% that day. Do you want your currency to drop 25% in one day? Also, remember that Mt. Gox is estimated to handle about 80% of BTC trade, so if you become involved in BTC, you will likely deal with them. Even if you don't it could happen at other exchanges.

There have been other price fluctuations. In April 2011 the value of one BTC was a dollar. By June it was more than $30.[17] Later in June it fell to $10 and then went back up to $20.

In April 2013, the price was over $100.[18] Life is good, and everything must be ok with BTC.

[17] http://arstechnica.com/tech policy/2011/06/bitcoin-price-plummets-oncompromised-exchange/
[18] http://arstechnica.com/business/2013/04/bitcoinvalue-triples-in-a-month-to-all-time-high-of-morethan-100/

Maybe this is the case, but less than a month prior, the price fell 23% in one day, and transactions at Mt. Gox were temporarily halted.[19]

What caused that swing? In introducing BTC we talked about how people voluntarily allow their computing systems to be used to crack the code. The price drop was the result of a disagreement about whether some had in fact cracked the next step in the

code or not.

The price eventually recovered, and transactions resumed, but is this where you want to put your retirement nest egg?

HOARDING/SPECULATION

The price of BTC has risen significantly. Some consider this more for purposes of hoarding then because of plans to actually use BTC as a currency.

Prices of products measured in BTCs have plunged as the value of BTC has increased. Accordingly, the tendency is to hold onto BTCs instead of spending them.[20]

[19] http://arstechnica.com/business/2013/03/majorglitch-in-bitcoin-network-sparks-sell-off-pricetemporarily-falls-23/

[20]

http://krugman.blogs.nytimes.com/2011/09/07/gold en-cyberfetters/

To reiterate, one of the main purposes of BTC is as a medium of exchange. However, if everyone thinks the value will keep going up, there is a tendency to hold onto them and not spend them. Under this phenomenon, there will be less in circulation, and it is less likely for most consumers and businesses to view BTC as a credible currency.[21]

This could happen with any conventional currency, but likely not to the extent of BTC. If the U.S. Dollar goes down in value, most people still need to spend some on food, rent and other necessities. The same is not necessarily true with BTCs.

There is evidence that this has already happened. In the middle of 2011, even as more BTCs were coming into existence, the number of transactions and the value of them in BTCs were shrinking.[22]

The problem of course is this hoarding and speculation comes to an end at some point. Ask those who paid $145 for a barrel of oil in July 2008 how that worked out.

What happens if large numbers of people try to redeem their BTCs at the same time? There are examples where the price crashed when this happened.

[21]

http://www.technologyreview.com/review/425142/c ryptocurrency/

[22] IBID

In fact, on March 13th, 2013, Mt. Gox announced withdrawal limits on BTCs due to, "Recent events in the Bitcoin community and the spike in the Bitcoin price."[23]

How nice. At least they are warning you that if you have large amounts "invested" in BTCs on their exchange. Don't expect to cash out all at once.

ANONYMITY

This was also highlighted as a major advantage of BTC. The reality is today there is not so much anonymity gained by using BTC.

For those of you who want to buy your home grown on the Silk Road, pay with BTC and be assured of anonymity, things are not like the good old days.

Mt. Gox now requires verification of who you are.[24] It is true that you could try to conduct your transactions strictly on a peer-to-peer basis, but most are not done this way.

Also, in March of 2013 the U.S. Treasury Department extended their reporting requirements for cash transactions to exchanges that deal in BTC.[25] This includes mandatory

[23] https://mtgox.com/press_release_20130313.html [24] https://bitcointalk.org/index.php?topic=49439.40[25]

http://online.wsj.com/article/SB10001424127887324
373204578374611351125202.html
reporting requirements for transactions over $10,000 as well as other requirements.

WHY DOES BITCOIN HAVE VALUE?

Obviously some people simply have faith in BTC. They are true believers. But beyond this group, what is it about BTC that makes it intrinsically valuable?

The most valuable criteria that proponents of BTC always point to is that there will be a finite number of BTCs. Eventually there will be 21 million BTC.[26] In theory this should limit the amount of inflation in BTC. It sounds good.

Then again, at one time, the U.S. Dollar was on the gold standard. Then one day, it

wasn't.
Proponents of BTC would have you believe that their rules cannot change. The only problem with this bold pronouncement is that the rules have been changed before.[27] Not only can the rules change but this limit of 21 million BTCs is misleading as all hell because each BTC is divisible into 100 million

26

http://bitcoin.stackexchange.com/questions/161/ho w-many-bitcoins-will-there-eventually-be

27

https://bitcointalk.org/index.php?topic=145475.msg1 543280#msg1543280

pieces.[28] The bottom line is don't get caught up in the proponents hype about how finite BTC is.

Ultimately, we are left with faith and nothing more as a reason for BTC value. I would argue that faith is misplaced based on the numerous and dramatic price fluctuations BTC has had in its brief history.

OPPORTUNITY COST OF INVESTING IN BITCOIN

Opportunity cost means that if you do one thing (in this case invest a certain amount of money in BTC), then you cannot do something else (invest that same money in something else).

What if instead of investing in BTC you buy gold, silver, a rental house or a business? If the proponents of BTC are right, you may not make as much money as you would have if you bought BTC.

Of course you may make more money with these investments. BTC has gone to almost zero. Gold never has and never will, and in terms of being finite, God isn't making any more gold or land.

28

http://www.youtube.com/watch?feature=player_em bedded&v=yi2WgeJ73IE at 14.52 minute mark SHUT DOWN THE INTERNET

A popular line of reasoning by BTC proponents is to raise the possibility that since the government cannot control BTC, once BTC presents a real threat to the existing order, the government may simply shut down the internet.[29]

Really? This is the best they have? Could they possibly come up with a more unlikely scenario? In the dictionary under straw man, this argument is located.

If BTC were to become more and more popular and used as a medium of exchange this would present an existential threat to central banks around the world.

However, they would not need to go anywhere near shutting down the internet (which would have its own devastating economic consequences) to deal a death blow to BTC.

Recall the massive drops in the price of BTC when there was just one hack in one day on one exchange. Now picture a hundred guys with PhDs in cryptography at Fort Meade, Maryland doing a hundred hacks a day for the foreseeable future. That solves the BTC problem from the government's perspective.

[29] http://www.huffingtonpost.com/max-keiser/howlong-before-bitcoin_b_2979396.html

E-GOLD

E-gold was a digital gold currency that was in operation from 1996-2009.[30] It was backed entirely by gold and silver. At one time it was used by millions of people in over 100 countries.[31]

It was founded by an oncologist who sold his medical practice, drained his retirement accounts and charged credit cards in order to raise over a million dollars to fund the business.

The founder was eventually charged with money laundering and conspiracy among other charges. He entered a plea deal and what remains of e-gold is a buyer and seller of gold.[32]

Proponents of BTC would argue that what happened to e-gold could not happen to BTC because there is no storefront business, no office to raid, no one to arrest.

It is true there is no single "owner" of BTC to arrest. The government could raid and charge the owners of the BTC exchanges. If they raided multiple exchanges on the same day, that could have a chilling effect on not only the price/value of BTC, but the desire

for people to continue using it.

[30] http://en.wikipedia.org/wiki/E-gold[31] http://www.wired.com/threatlevel/2009/06/egold/

[32] http://egold.com/

The other likely scenario for destroying BTC if the government deems it necessary is computer based attacks on the exchanges and users of it.

CONCLUSION

The desire for an alternative currency is understandable. Right now dollars, euros, and pounds are all questionable.

It is totally understandable for people to try to avoid fiat currencies and pursue something safer. Someone buying gold, silver, real property or a business makes perfect sense. However, it is a big stretch from that to buying into a computer generated, peer-to-peer, code that theoretically represents money and is backed by nothing more than its limited quantity (even though the supposed limit, is not much of a limit).

Governments can shut down BTC anytime they want. Remember what has happened to the value when there was only one hack. Imagine if there were more than one in a short period of time. The National Security Agency could do a hack a day, a hundred hacks a day or a thousand hacks a day, all while having total deniability. Governments can make BTC functionally obsolete anytime they want. They don't need to right now because at this point BTC is like a mosquito bite to central banks. To pursue it at this point it to give it attention/credibility that they view it as not deserving.

If BTC ever reaches a point in popularity/usage that governments regard as a threat, then that is when they will crush it. If and when they do crush BTC, you will wish you had bought 100 fortune cookies or 1000 units of rubber dog shit instead of 1 million BTCs.