THE BITCOIN PRIMER:

Risks, Opportunities, And Possibilities

by David Seaman

The Bitcoin Primer: Risks, Opportunities, And Possibilities

by David Seaman

What is this?

This is a free, expanded edition of my #1 Amazon bestseller, "The Bitcoin Primer." It is being provided as shareware which anyone is free to read, distribute, and reshare.

The book is designed as an easy way to familiarize yourself or friends and family with Bitcoin… unless you enjoy answering the same kinds of questions over and over again. Those who are already Bitcoin experts will likely find this work to be a bit pedestrian, as it doesn't go into hashing, speculation about future transaction capacity, or any other overly technical details. Toward the end, however, Bitcoin veterans will be rewarded in Part III with some informed speculation about where the Bitcoin economy could conceivably go (hint: Moon).

You sick anti-capitalist freak, cannibalizing the success of your own bestseller!

I am very much a capitalist. I host a popular news & politics podcast on iTunes and have released 160+ hours of content for free

over there. Far from forcing me to give sexual favors on an I-405 underpass to pay my rent, releasing content for free has allowed me to gradually build an audience - the only reason I have an Amazon bestseller in the first place! Free pays off.

Most people are happy to compensate content creators when they are able to, provided the content is good. If you enjoy this book and want to support the people who created it, a $2 contribution in BTC is suggested:

David Seaman (@d_seaman) - author

BTC Address: 16b2Gzf8U3DtBvucSkktaKytg8V9xLpUgh

Arianna Power (@streetstylish) - book designer, editor

BTC Address: 1JrTEfkqu6ddqyG3BWKoudfUaEUZ8qNumw

Without any more explanations, here's the book! Enjoy and thank you so much for being you.

This e-booklet is designed to bring readers up to speed on the rapidly growing Bitcoin global payment technology. The booklet discusses the origins of Bitcoin, why digital currency is becoming desirable, best practices for business owners and freelancers to accept Bitcoin successfully, where to buy/sell coins safely, as well as a wide range of security considerations — how to store your coins in a way that reduces risk of accidental loss, create offline paper backups, prevent theft, etc.

I first became interested in Bitcoin back in October 2012, when I had an early investor on my podcast. Since then, it has been a wild ride and I've learned a tremendous amount about the pitfalls and opportunities Bitcoin presents. Although this is simply my opinion, I feel Bitcoin is one of *the most important* technologies of our lifetimes — certainly right up there with the World Wide Web, email, and smartphones. The disruptive possibility of digital currency is difficult to overestimate.

When I began covering it, Bitcoin had a total market capitalization of around $1 billion USD. As of writing this, the total market cap is approaching $12.4 billion USD, and it is entirely possible this growth will soon turn Bitcoin into a hundred billion dollar market cap asset class... or much larger.

It is also possible Bitcoin will be left in the dust by a newer, as-yet-not-invented technology.

Since this booklet was inspired by getting many questions from listeners about Bitcoin, it takes the form of a casual Q&A. If any questions remain unanswered by the end, my contact information is provided. I always welcome questions about Bitcoin and love to spread the message of financial liberation.

There is nothing wrong with central planning, per se. It had its time and place. But given the widespread acceptance of the Internet for communications and financial data, to neglect this shift and to

stick to what is old and familiar is a bit like inviting friends over by drafting a letter in cursive using an ink well and quill, then sending it to them via horseback... instead of just sending your friends a text message!

What is Bitcoin? What's so novel about it?

Bitcoin is a peer to peer decentralized digital currency. It makes use of advanced elliptic curve mathematics and cryptography, as well as a globally replicated public ledger called the Blockchain.

Bitcoin was developed in 2008 and first introduced by Satoshi Nakamoto in 2009. Satoshi is believed to be a pseudonym and the Bitcoin community hasn't heard anything from him since sometime in 2010. It's an origin story worthy of a comic book plot: mysterious cryptography genius develops a brand new currency capable of altering the global financial landscape, publishes a white paper

explaining the technology, and then disappears from the discussion altogether as it begins to gain acceptance.

There are several things Bitcoin accomplishes that were previously not possible with e-currency.

OK. What are those things?

Bitcoin makes it impossible (or near impossible) for double-spend transactions to occur — in other words, when money leaves your possession, it is no longer yours. This was a huge challenge with digital currency because when you send a friend a music file, for example, how do you make it so that the file no longer exists on your computer? When transacting in a digital currency, it is imperative that the money leave your hands and go to the receiving party's -- a user must not be able to spend their money more than once. This is part of the reason why Bitcoin is often described by the press as "digital cash" — the bearer has complete control of it, and

permanently loses that control when they give it to another party. Transactions are irreversible.

Bitcoin also provides near instantaneous (within 10 to 30 minutes) undeniable confirmation that your money has been received or sent. No worrying about bounced checks.

Bitcoin also is impossible to counterfeit; a cash transaction or a transaction in gold could contain counterfeit bills or fake gold. There is no such thing as a fake Bitcoin.

Furthermore, there is no prolonged settlement period. Once the transaction is confirmed by an acceptable number of nodes across the network, that money is truly yours.

And finally, since all transactions are listed in a global public ledger known as the Blockchain, Bitcoin provides an invaluable defense against "big hat, no cattle" bullshitters. In other words, if

you're planning to do business with someone who claims to have X amount of money — rather than going on their word, or the kind of watch they wear or car they drive, or their credit history, etc. that individual can simply provide a public address for you to view their balance. Within seconds you know if the party has the money or not.

Bitcoin has no intrinsic value, why are people accepting it as currency?

Nothing in the physical universe has "intrinsic" value. Gold is a metal that humans have decided has transactional value due to its scarcity and interesting physical properties (doesn't oxidize, nice and heavy, looks pretty, good conductor of electricity). The US dollar is a piece of paper or digital ones and zeros backed only by the "faith and credit" of the US government — in the public's trust that the government can repay its debts and make good on any obligations.

When people claim Bitcoin has no intrinsic value, what they are usually trying to say is: "I don't like Bitcoin."

And it's fine to have a personal preference on something, so long as you acknowledge that your personal belief does not coincide with the currency's actual value.

Bitcoin has value because people are willing to buy and sell it at a certain price. That market is liquid thanks to a number of exchanges. As of writing this, one coin sells for more than $1,100. Bitcoin is also accepted by an ever growing number of businesses and workers as a form of payment.

I hear horror stories in the media about people's coins being stolen, lost, etc. I thought this thing was secure?

Bitcoin is truly digital cash. If you were to leave a backpack filled with cash in the mall food court, and then if that backpack were to

be taken by some stranger, it would no longer be yours. Similarly, if you were to put a million dollars under your kitchen floorboards and your home burned down, you would no longer have that money.

Whoever holds the private keys to a wallet's coins controls those coins. When the private keys are lost or destroyed, that money is lost.

Well that doesn't sound fun. Remind me why this is a good thing?

There is no central authority, no company or government in charge. When you buy something with a credit card, if you are not satisfied (the product doesn't arrive as promised, for example) you can appeal to the card company and initiate a possible chargeback. This provides a layer of comfort for consumers, and that comfort is financed by high merchant transaction fees (as much as 2 to 3 percent of the total amount) as well as things like annual fees, high

interest rates, etc. The bank needs to pay for the support costs as well as its financial liability (chargeback costs, unauthorized transactions, identity theft, and so forth). Also, the bank needs to pay marketing costs to remain profitable.

With Bitcoin, as with email, there is no company in charge. It is a global protocol for sending and receiving money. Transaction costs are a tiny fraction of existing bank transaction fees. The irreversible nature of Bitcoin lowers costs since merchants bear no risk of chargebacks or fraudulent transactions.

Didn't early adopters get a lot of coins with relative ease? How is that fair? How is that different from a 'pyramid scheme'?

Yes, miners (those who run software on their computers to help keep the Bitcoin network operating) generate coins over time — at the beginning, these coins were produced with relative ease, and over time less and less coins are produced and the process becomes

more difficult. Similarly, early adopters were able to purchase coins for as little as $0.01.

It's worth noting that Bitcoin wasn't always the golden standard of e-currency. As recently as May 2010, 10,000 coins could maybe buy you a pizza. And miners were regarded by many as gullible morons, giving away valuable computing resources in exchange for "fake Internet money" no one accepted or cared about.

It's only natural, then, that those who took the risk of creating or owning Bitcoin early on in the process should see a return on their "investment."

Many of these individuals did not hoard the coins, but rather used them to buy things online, or sold them at prices far below today's market value — when something cost you $0.01, a $10 price seems attractive.

There is evidence that ownership of the coins is less concentrated than it was toward the beginning. Also, anyone could become a miner or buy the coins. It wasn't a closed club of insiders — it's just that most of the public didn't believe in the idea.

Can you explain how this is fair? Some people still have a lot more than others.

Bitcoin is mathematically pure and anyone can read the source code that makes the system operate. It isn't proprietary and no person or entity can inflate the market by creating new coins out of thin air (as a central bank would do). The creation of Bitcoin follows a mathematical "schedule" and will top out at 21 million coins by the middle of the next century. This scarcity ensures that an individual's purchasing power and stored value is not diluted by a politician's decision to print more currency (that's the idea, at least). No one can decide to print more Bitcoins.

Will early adopters become rich?

Based on my research, it is certainly possible that early adopters will become billionaires — if Bitcoin becomes the global standard for digital transactions in the same way that email became the global standard for digital communications, such an outcome is not ridiculous. It is also possible that early adopters will lose up to 100% of their "investment" if Bitcoin becomes compromised in a critical way or if the public's interest rapidly switches to an as-yet-unknown alternative protocol.

Aside from its appeal as an alternative to Visa, MasterCard and PayPal, some Bitcoin users claim it helps protect their money from inflation. Can you explain what this is about?

Inflation is one of the oldest problems facing any currency issued by a government or central authority. The ancient Romans did it, the Chinese did it, the Americans (and nearly everyone else) are doing it today. Provoking inflation is very tempting for the

establishment because it allows for a) a subtle tax on your citizens' wealth b) financing public projects — roads, healthcare, wars — that would otherwise be economically impossible to pull off.

An article from the popular financial blog Zero Hedge a couple years ago sums up the practice of currency devaluation, closely related to inflation, quite well:

"...as most monetarists know too well, it was the Romans who engaged in the first act of voluntary currency devaluation-cum-dilution, by progressively reducing the silver content (yes, even back then currencies were backed by precious metals: and guess what - no CDOs squared, cubed, or quadratic, were conceived by the local office of Goldmanus Sachus) until such time as it hit zero... and the Roman empire was no more. Ironically, the nearly 100% devaluation of the currency in Roman times took just over 2 centuries. This compares somewhat favorable to the 97% drop in the purchasing power of the US currency since the inception of the Federal Reserve."

(Read the rest of the article at http://www.zerohedge.com/article/chart-day-currency-devaluation-old-school-style)

So, as you can see, what our government is doing today hardly qualifies as a new practice. The ancient Romans, unfortunately, didn't have the Internet and decentralized currency to protect against currency dilution.

If you have $1,000 in a bank account, you still have $1,000 in that account next year — but the actual value of that money, the *purchasing power*, may decrease substantially. When the Federal Reserve decides to print more money, there is greater supply of dollars for the same amount of demand. Therefore, your money becomes a little less special, worth a little less. This, however, helps the government and other debtors to pay off their debts — they still owe the same nominal amount, only now they can pay back the debt in dollars worth less.

Can't this happen to Bitcoin also?

No. No emperor, chancellor, or Federal Reserve Chairman can arbitrarily decide to dilute the value of each Bitcoin in the hopes of "stimulating the economy" or financing a war or expanding welfare programs. The maximum number of Bitcoin is 21 million by the middle of the 22nd century. This limit is baked into the mathematical models that make Bitcoin run. Right now, a little more than 12 million coins have been "mined" and put into the world for use.

Damn. The government will try to shut this down then, right?

An article on NBC News' web site recently noted that Bitcoin has gained more than 7,600% in value this year.

"Many analysts and investors have labeled bitcoin's unfettered rise a bubble, yet greater awareness of digital currencies and last

week's U.S. senate seal of approval, paved the way for fresh gains," the article stated.

That's it right there: the U.S. Senate hearing was surprisingly positive and sane. For someone who has been quite critical of Congress' reactionary approach to Internet technologies lately, I was pleased — astounded, actually! — that the law enforcement officials and elected members present gave such sober and reasonable assessments of what Bitcoin is and is not.

This was the biggest cloud hanging over the digital currency's head: would the U.S. government take aim at Bitcoin and shut it down? The answer is, apparently, no.

Another piece of fantastic luck that headed Bitcoin's way in November: BTC China went online, a Bitcoin exchange in mainland China, and the response from Chinese consumers was BUY, BUY, BUY.

The majority of new Bitcoin orders since then has come from China, not the West.

The Chinese, like us, have a large middle class population eager to diversify — they want their hard-earned money to weather any regional economic storms. Keeping all of your money in US dollars, or Chinese yuan, or Swiss francs... is the financial equivalent of "all your eggs in one basket." Something could go wrong. There's also that whole inflation problem!

Part II: Buying, Selling, Securing

"We wants it, we needs it. Must have the precious. They stole it from us. Sneaky little hobbitses. Wicked, tricksy, false!"

— Gollum, from The Lord of the Rings: The Two Towers

Bitcoin consists of a public address and a corresponding private key. A new address and corresponding private key can be created with a single click, as many times as you'd like for new transactions.

Think of a public address as your mailing address if someone were to send you a check in the mail. The public address is what you want to give to anyone who plans to send you money. And think of the private key as the combination to your mailbox where you receive the check. Do not ever share or post your private key with anyone.

Allow me to repeat that: DO NOT EVER SHARE OR POST YOUR PRIVATE KEY WITH ANYONE.

In fact, whenever private keys are stored on your computer, that computer should (ideally) never be online -- and if it must be online, those private keys should be stored in a password-protected folder. And that password should be long and salty. (i.e. instead of

mydogsname, your password could be salted as such: mYd0gznAm3!)

Wallet security is one of the most important aspects of mastering Bitcoin, and failure to do your homework before loading money onto a wallet can lead to disaster — as it has for many newcomers. It's heartbreaking to see these stories of ruin in the Bitcoin forums. Almost all of them could have been easily avoided.

When storing Bitcoin, you should use a wallet client on your own computer — the major online-hosted Bitcoin wallets I simply would not trust with anything above a very trivial sum of money. The companies are too new, and they paint a target on their backs by having so much aggregate wealth on a single service. The major hosted wallet services undoubtedly have hackers trying to find a vulnerability around the clock, 365 days per year. And that company need only let down its guard for a millisecond to lose most or all of its customers' holdings.

Whereas a wallet client on your computer is just one target, and one that hackers would hopefully not be aware of in the first place.

Of all the wallet clients I have tried, Electrum is the best — nice combination of ease of use, simplicity, and security.

Read the documentation on Electrum at Electrum.org. The client is free open-source software which can be downloaded from that web site as well.

Ideally, you should disconnect your computer from the Internet when you first boot up Electrum. The first time you boot up Electrum, it provides you with a **wallet seed** during the set up process. This is phenomenally important, and will be explained in a moment, so you want to do everything in your power to prevent this wallet seed from being compromised by keylogging malware or by malware that takes screenshots.

If your computer has been used to surf the Web for a while, it's highly probable your computer has some malware on it. "Not *me*, I only go to safe web sites!" Yes, you, me, *almost everyone*. Malware is insanely prevalent on personal computers. In the recent past, such malware was usually used for things like spam, serving unwanted ads, etc. But as Bitcoin continues to increase in value and acceptance, it motivates malware designers to sniff for your coins.

An asset that can be instantly stolen is tempting to the kinds of people who design malware.

If you plan on loading a significant amount of money onto your wallet, you should go out and buy a dedicated new computer that never touches the Internet. You can get a decent low-end laptop or netbook for less than $400 today. "Time to go mobile!" as Bane would say...

When you set up a Bitcoin wallet that is never online, it's called a **"cold wallet."** A cold wallet, if set up properly, cannot lose coins — but it can generate new public addresses to give to people who want to send you money.

A wallet connected to the Internet, which can send coins as well as generate public addresses, is called a **"hot wallet."**

All of this is explained well on Electrum's web site. Another good resource is http://reddit.com/r/bitcoinbeginners. If you ask a question on there, remember that no matter what someone says, **DO NOT GIVE THEM any of your private keys and DO NOT GIVE THEM your wallet seed.** Anyone who has either of those things can spend your coins -- it's as if you have given them the password to your bank account.

Draconian security measures are not as important when dealing with small quantities of Bitcoin — say, enough to buy a used

book or a TV on Craigslist. But when the amounts get larger — amounts stored in the hopes of providing for your heirs or yourself in the future (which some people are doing; more on that later) — you *need* to be "productively paranoid." Think as a Bitcoin thief would: if something can be compromised, it will be. If something *could have been* exposed to a third party, assume it has been, and act accordingly. Move your money onto a new public address, after ensuring you have saved the private key for it properly. And back up that private key (or memorize the parent wallet seed). And password-protect the file that contains your private key.

Again, this stuff sounds a little out there, but as the market cap of Bitcoin continues to grow and each BTC becomes more and more precious, the incentive for malware developers is nearly limitless. It is relatively easy to develop a program that sniffs for your private key file and, if not properly password-protected (or kept offline altogether), to jack that information.

Bitcoin is cash for the digital era. And just as you wouldn't put $100,000 in a neon fanny pack and walk through a crowded marketplace known for pickpocketing, you shouldn't play too fast and loose with your Bitcoin security routine. As with any routine, good habits established now will lead to good habits forever.

There's also the fascinating issue of Bitcoin appreciation; many have speculated (so far, correctly) that the way Bitcoin is set up leads to deflationary pressure over time. In other words, since I believe 1 BTC will be worth more in US dollars (or euros, or francs) tomorrow than it is today, why would I spend it today? I'll wait until tomorrow. And the same issue arises tomorrow.

As such, even a small amount of Bitcoin set aside today could conceivably be equivalent to a whole year's salary in the not-so-distant future.

Aside from that, the value of Bitcoin benefits from a phenomenon I've dubbed **"coin rot."** Over time, a certain percentage of users forget their passwords, lose their private keys, or their computer hard drives die without proper back ups in place. Although this money is still a part of the Bitcoin ecosystem in the sense that it contributes to the total market capitalization of the currency, it is effectively null and void: that money will never be used in a transaction again. So if a party wants to transact in Bitcoin, they are likely buying newer coins, not coins from the earliest days of Bitcoin.

We could debate the intriguing merits and drawbacks of a deflationary currency until the end of time, but ultimately this pressure has minimal impact on Bitcoin's ability to be the global digital transaction protocol of choice, since both parties can jump in and out of Bitcoin within seconds thanks to the liquidity provided by exchanges.

I like to think of the US dollar as a "local currency" at this point, and Bitcoin as an emerging international super currency. Local currencies won't disappear any time soon, as they provide regional convenience, but for large *and* small international transactions the clear choice is Bitcoin. Think of Bitcoin as the cloud drive for our financial system, and local currencies as CD-ROMS or thumb drives that can be used to transport a consumer's money regionally.

OK, got it. So what is this wallet seed you were mentioning earlier? Sounds important.

Good question. So, when choosing a Bitcoin client I recommend Electrum because it provides an elegant solution to the problem of keeping track of all your addresses and private keys — at first start-up, it generates a 12 word mnemonic (something you memorize) based on 128-bit entropy (i.e. a very high degree of computer randomness).

Write this 12 word string down. Double check that you have written it down correctly. Then check one more time. And another time. This is one of the most important moments of your Bitcoin life, so it's appropriate to be careful here.

After writing down the 12 word mnemonic properly, work on memorizing it. You can memorize this within a few days to a week by reading it off the paper to yourself repeatedly. And it's even easier to remember if you use the 12 words to build a fun little visual story in your mind.

After committing your unique mnemonic to memory, put the written back-up copy in a safe place. Put a second written copy in a different physical location, in a Zip-loc bag in case of water damage.

The beautiful thing about this wallet seed is that even if you lose everything else — all your private keys, your password, your addresses... or even if your computer hard drive gets corrupted and

stops working, or is destroyed in a fire or earthquake... you can instantly recover everything by typing that wallet seed into Electrum using the Restore option.

In fact, the wallet seed is the only piece of information you NEED to retain in order to keep control of your coins.

That's intense. How does this work?

It is intense! Wallet seeds will make you feel like a Bitcoin-slinging James Bond. And you will quickly realize that this stuff is way more advanced than "traditional" banking. There's no friendly teller lady at the local branch to help you recover your password. The benefit of this, of course, is total freedom and total access to your own money.

The wallet seed works because Electrum creates what is called a **deterministic wallet**. All addresses and private keys it provides

you with are generated from that seed, and can be recreated knowing only the seed.

Think of it as a buried treasure map. Please note that the keys must be generated natively within Electrum to be regenerated by your seed. If, for example, you import private keys from elsewhere into Electrum those will obviously not be "stored" by your wallet seed.

Deterministic wallets are a relatively new innovation in the Bitcoin world.

Here's how Bitcoin Magazine describes them: "Unlike old-style Bitcoin wallets, which generate new Bitcoin addresses and private keys randomly as needed, in a deterministic wallet all of the data is generated using a specific algorithm from a single seed. That is to say, if you write down the seed to your deterministic wallet, and then after six months your hard drive gets corrupted and the wallet

unrecoverable, you can simply create a new wallet using the same seed and all of the addresses and private keys from your old wallet will come back again exactly as they were before. This trend in wallet development has received near-universal praise, and nearly every Bitcoin client that intends to handle multiple addresses either already has a deterministic wallet implemented or is planning to create one."

(Read their whole analysis at http://bitcoinmagazine.com/8396/deterministic-wallets-advantages-flaw/)

This isn't the final word on creating a wallet or wallet security. You should spend some time reading up on Electrum online, and then play with only small amounts of Bitcoin within your wallet, until you are confident in its features and have tried regenerating your addresses and balances from the seed at least once.

And in the future, better wallet clients may come along. (Armory is another client that has been very well-received by the Bitcoin community, but it's a more complex client offering the absolute highest level of security. For most users, this is probably not necessary, but you may prefer that one.)

Cool, I'll start experimenting with wallet clients. Where do I buy my coins?!

Here's the fun part. Bitcoin exchanges allow you to buy and sell coins at a real-time market price, plus the exchange's fee. I have had mixed experiences with exchanges — some of them are simply growing too fast to provide reliable, professional services.

The only excellent one I have used so far, that is consistently reliable, is Coinbase. They are based in the United States, follow all regulatory and financial compliance guidelines, are backed by more

than $6 million in tech start-up funding... in short, they are exactly what you would want in a reputable coin seller.

Although Coinbase takes admirable steps to protect their customers' funds, including storing approximately 90% of all Bitcoin holdings in an offline paper wallet (printed private keys) in a bank vault, it is still not wise to keep your coins there for a long period of time. Send coins there only when you plan to sell them and coins you've bought there should be sent to a wallet client on your computer ASAP. There's nothing wrong with their business practices, it's just pure math: exchanges are a huge target for hackers, as I mentioned earlier. And exchanges, due to unexpected volatility and the resulting surge in capital required to meet customer demands, can freeze up or go under altogether.

To reiterate: Buy your coins there. Sell them there. But keep your long-term coins somewhere else.

Follow this link to sign up for Coinbase and you'll receive $5 worth of free Bitcoin added to your account, so long as your purchase is for at least one full coin: http://bit.ly/1iysEi9

I'm a small business owner, and I am more interested in receiving coins than buying them on an exchange. How do I do this?

The very simple answer: setup a wallet client such as Electrum, generate a new public address, and give that address to customers when it's time for them to pay — include it on invoices, etc. Roughly the same process for accepting donations if you're an interest or independent content creator: post your public address and politely encourage fans and friends to send Bitcoin there.

There are obviously more advanced implementations. For a physical storefront, for example, you may want the computer at your store to have Electrum running from your Master Public Key, rather than from your wallet seed. The instructions for doing this are on

Electrum's web site documentation section. With this, your employee can generate new public addresses as desired so that individual customers can settle their balances, but there is no security risk since the employee only has "watching" access to your coins — since it wasn't restored from the actual seed, he or she cannot transfer coins out of your possession. They can only generate new public addresses. Pretty cool feature!

Where does it go from here… if you had to guess?

Now's probably a good time to throw in some legalese: Nothing in this booklet is meant as investment advice, make your own decisions only after consulting a financial professional, I assume no liability, Bitcoin is risky and can lose value, etc. Basically: if you lawyer up because you did something dumb and lost all your coins, I will be very annoyed! Adults should take responsibility for their own actions — free will is pretty sweet. With all that said, I personally own Bitcoins

because I believe deeply in the technology and I think we are in the very beginning of this transformation.

The U.S. Senate's positive hearing was HUGE.

The Chinese explosion of interest was equally HUGE.

Bitcoin wasn't invented yesterday: it's been around since 2009. And despite a rocky road, the exchanges and services today are more professional and stable than ever before. More merchants accept Bitcoin than ever before. And public interest in this technology is greater than ever. Bitcoin captivates the imagination, intrigues the tech savvy, and seduces the business-minded. The more control we have over our own money, the faster transactions can be, the less we pay in fees — these are all exciting developments.

In five years, the businesses and individuals who accepted Bitcoin early on could be in an enviable position. Hell, we're *already* in an

enviable position because this is fun and more efficient than legacy payment systems that were developed decades before the first webpage was uploaded. We’re pioneers.

Part III: Pure (Informed) Speculation

Now that you've got all the basics, let's have some fun. Life is short and a life without imagination is not exciting.

I got into Bitcoin somewhat early, although obviously not as early as billionaires in the wings like Roger Ver and Trace Mayer. Those are the real true believers. (I've had both on the podcast; definitely worth a listen as they are oddly psychic about everything that has come to pass in the Bitcoin world.)

Given the fact that the overwhelming majority of stores still do not accept Bitcoin, and many people still have not even heard of Bitcoin, I simply do not agree at all with people who regard Bitcoin as

a "bubble about to burst." Was email in 1995 a bubble about to burst? Was Google in 2002 a fad? These were seemingly credible questions at the time, but given what we know now, they are hilariously shortsighted.

Money is, at a most fundamental level, an agreement between people. We touched earlier on the idea that nothing has true "intrinsic" value; all value for our species is relative and derived. Certainly, if anything had *intrinsic* value, it would probably be something like a can of soup or a Swiss Army knife or sex. But we don't have a financial system based on Swiss Army knives and Campbell's soup as the transactional unit (thankfully). Instead, we have instruments like the dollar, gold, and — inevitably — Bitcoin.

The dollar, and other government-mandated fiat currencies, are an agreement between people FORCED upon us. "You have to agree to use this as money." No intention of making this an ideological book, and it's clear that there was a time where such mandates made sense.

But the Internet alters that landscape in a way that governments can simply not undo.

Money today can be an agreement between people, made voluntarily. "Yes, we agree to use Bitcoin as money, because Bitcoin is money." And *of course* I agree with you that's a circular argument. It's a self-reinforcing feedback loop. She's famous *because* she's famous, which leads to her becoming more famous. That's something I've seen firsthand in LA.

Currency is not so different, then, from fame. Something can go from nothing to something, and once it does stagnant stability or meteoric growth are far more likely outcomes than overnight ruin.

Bitcoin is something that you trust more as you research it more. The underlying math is fundamentally pure and actually *beautiful*. That you can give out a public address without in any way revealing the

private key, that a nearly infinite number of new public addresses can be created at will, that the entire social contract of Bitcoin exists at all times on the Blockchain... which is essentially a global decentralized cloud for financial agreements.

There's a beauty to it that outstrips, in every way, the existing establishment financial network.

Will this new order overtake traditional banking? Absolutely.

To predict anything else would be absurdly, almost criminally, shortsighted.

Traditional banking is far behind Bitcoin; the only thing your neighborhood Too Big To Fail branch has to offer you — other than monthly service fees and anemic interest rates — is *comfort*. The comfort that you can't really lose your money, as it can be reversed.

The comfort provided by the bank teller lady asking how your day was and commenting on the weather.

The same comfort was provided by travel agencies.

No one uses travel agencies any more, because Travelocity and the other travel booking web sites made the industry easier, faster, and more competitive.

In the same way that travel agencies are now a boutique experience for the very wealthy, the very incompetent, and the offbeat — bank branches will be precisely the same.

With Bitcoin, *you are your own bank*, and the collective hallucination of currency is played out in a way arguably more fair and transparent than at any other time in history.

Will Bitcoin become a trillion dollar technology? I don't know. It might. There are enough reasons to suggest yes: strong first mover advantage, a market cap and transaction volume far higher than any of the competing "me too" digital currencies that emerged shortly after it.

Or Bitcoin could flop. Critical flaws could be revealed. Something more refined, refined in a way we don't yet realize we want, could come along. But what's certain is that the cryptocurrency math it is built on, in some form, is here to stay. It has forever changed the way we think about currency. The mostly useless serial numbers and bizarre busts of dead presidents on our paper currency seem positively prehistoric compared to the unbreakable, non-counterfeitable nature of Bitcoin.

If Bitcoin becomes as successful as I think it will, in a few years' time thinking of Bitcoin wealth in terms of dollars will be outmoded as well. Just as we wouldn't compare the money in our bank accounts to

an equivalent number of animal pelts or Native American sea shell currency units.

I'll see you on the Moon. (Or in the madhouse.)

Contact information

My Twitter is https://twitter.com/d_seaman and Google+ is http://google.com/+DavidSeamanUS

If you can't get ahold of me there, my personal email is davidseamanmobile@live.com — please put "Bitcoin" in the subject line, as I get a few hundred emails per week. Always thrilled to answer simple questions and point people in the right direction. I also selectively take on new consulting work if your business needs help implementing a Bitcoin acceptance strategy. I cannot answer questions such as "Where will the price of Bitcoin be a week from now? Should I buy now?" I have no idea. I am in this for the long haul.

Thanks so much for reading, best of luck in your wild Bitcoin journeys, and please take a moment to review this booklet on Amazon. My previous e-book, **Total Abundance, Total Power,** is now also available in the Amazon Kindle Store. It is a longer, more structured read — the book discusses how disruptive changes in technology are leading to greater abundance and power for the individual. Bitcoin is one such technology explored. Read reviews here: http://www.amazon.com/Total-Abundance-Power-Little-Ideas-ebook/dp/B00CF897Q8/

My web site: http://davidseaman.net