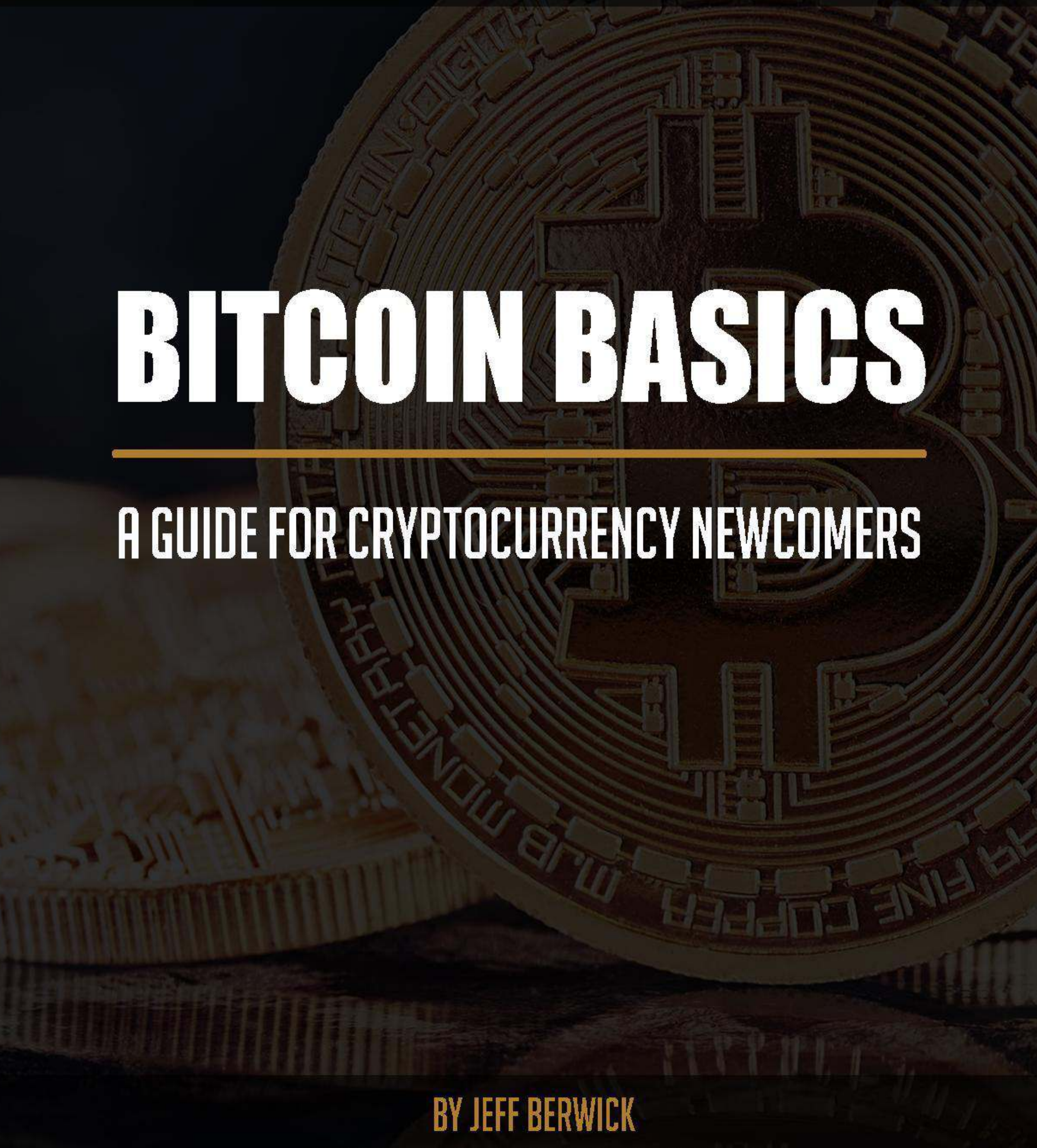
The DOLLAR VIGILANTE PUBLICATIONS



BITCOIN BASICS

A GUIDE FOR CRYPTOCURRENCY NEWCOMERS

BY JEFF BERWICK

FOUNDER OF THEDOLLARVIGILANTE.COM

FROM THE PREFACE

Bitcoin is a complete evolution in money and banking. By the time you are done reading this you will understand why. Bitcoin is to money and banking what the internet was to telecommunication - a massive paradigm shift that will change everything.

In this report, you will learn about the privacy, legal, security and ease of use implications of the best Bitcoin wallets and exchanges in the international Bitcoin market today.

Exchanges were analyzed on various grounds, specialty jurisdiction, anonymity granted to users and ease of funding, when purchasing Bitcoins.

Wallets were analyzed based on security, privacy, ease of use and platform availability.

-Jeff Berwick
Founder, TheDollarVigilante.com

This publication contains the opinions and ideas of its author and is designed to provide useful advice in regard to the subject matter covered. However, it is issued with the understanding that neither the author nor the publisher is engaged in rendering legal, accounting or other professional service. If legal advice or other expert assistance is required, the services of a competent professional person should be sought.

The involved in this book's creation and distribution specifically disclaim any responsibility for liability, loss or risk, personal or otherwise, that is incurred as a consequence, directly or indirectly, of the use and application of any of the contents of this book. Notwithstanding anything to the contrary set forth herein, TDV, its officers and employees, affiliates, successors and assigns shall not, directly or indirectly, be liable, in any way, to the reader or any other person for any reliance upon the information contained herein, or inaccuracies or errors in or omissions from the book, including, but not limited to, financial or investment data.

T.O.C.

PREFACE 5

1.INTRODUCING BITCOIN 8

2.UNDERSTANDING BITCOIN 14

3.HOW BITCOIN WORKS 20

4.GETTING STARTED 31

5. WALLETS & EXCHANGES 36

6. EXCHANGES 37

7. WALLETS 52

8. RESOURCES 67

PREFACE

By: Jeff Berwick

Whether you are a total bitcoin “newbie” or an intermediate or expert bitcoin user or programmer there is one thing that needs to be stated off the top.

Bitcoin is a complete evolution in money and banking. By the time you are done reading this you will understand why. Bitcoin is to money and banking what the internet was to telecommunications; a massive paradigm shift that will change everything.

Think back, if you were around, during the early days of the internet circa 1993-1995. I was personally there and immediately realized the power that was about to be unleashed on the world. Believe it or not, countless people were skeptical. Mainstream media reported on it as an oddity. Any sort of security breakdown was reported as being the end of the internet.

Sound familiar? Ponder for a moment about an investment in internet related companies in 1995 of a total of $250 million. A few short years later and hundreds of internet companies were valued in the hundreds of millions or billions. The same could happen with bitcoin related businesses.

Bitcoin is already changing the world. Nearly every government on the planet has commented on bitcoin. Clearly, it has been a disruptive technology.

The idea of bitcoin spread like wildfire. Within five years of its existence, mainstream media was covering it regularly. While at first they didn't quite understand it, it is clear that by 2014 things started to make more-and-more sense.

The technology itself is 21st century technology. This means that the elder generations might not fully understand what bitcoin is and why it is so important. For the younger generations, who live in a digital sea, bitcoin is something quite different – it is the easiest and simplest way to pay for things on the internet, where, as we have seen, more and more people are spending their money.

Much of the criticism of Bitcoin is that it is simply not real. But this is simply not true. It is, in fact, more difficult to counterfeit a Bitcoin than it is to counterfeit fiat currency. This in and of itself makes Bitcoin more valuable than paper money. The only thing which makes paper money valuable is that it has the state – a monopoly on violence – backing it.

PART ONE

1. INTRODUCING BITCOIN

One of the fascinations with bitcoin is its unknown origin. Nobody knows who created bitcoin. The pseudonym, Satoshi Nakamoto, either refers to the individual or group who created bitcoin. Whoever this party is, they/he/she do not appear to have been involved in the bitcoin software past mid-2010. Although Satoshi Nakamoto did resurface via one of his screen names to note that, in fact, Dorian Nakamoto – an individual Newsweek claims is the creator of bitcoin – is not *the* Satoshi Nakamoto.

In 2009, the first version of the bitcoin software was launched and thus the first coins were mined. This version was very complete, and if Satoshi worked solo, he spent a huge amount of time on bitcoin. Nakamoto remained active in modifying the bitcoin software and posting technical information on the Bitcoin Forum until he ceased contact with other bitcoin developers and the community began to fade in the middle of 2010. Since that time, much of the original protocol has been overhauled to be made more secure.

Bitcoin developer Mike Hearn, who worked for Google, once said, “Satoshi was clearly not an expert cryptographer. His interest in ECC went as far as saying 'this does digital signatures and takes less space than RSA'. He may or may not have chosen secp256k1 because he saw mention of performance - if he did, then he didn't mention that when I explicitly asked him about it. Alternatively, it could have been as simple as finding some example code somewhere on the net that happened to use that curve. He plugged it in, it worked, done. As it happens, whatever the reason for selecting that curve, it's worked out pretty well for us all things considered. Of all the issues bitcoin has, it turns out that ECC is not one of them."

Gavin Andresen has stayed very active as the lead developer for Bitcoin software. In July of 2012, he wrote an essay on his blog called "Is Store of Value Enough?" In it, he discusses the economics behind bitcoin speculation and transaction, and what we might see its price do in the bigger scheme of things:

Wallet security is a top concern for users and developers of bitcoin alike. Gavin Andresen has said that core developers of bitcoin are looking to implement multi-signature transactions which require more than one device to be signed. Many websites, like CoinBase, use similar technology to secure accounts. According to Andresen, "This will significantly reduce the effects if a computer gets compromised, considering this has been one of the biggest vulnerabilities over the last few years."

The Matthew Effect

And one thing is for sure. The bitcoin rich *are* getting richer. As the public bitcoin ledger inspired Daniel Kondor and others at Eotvos Lorand University in Hungary to download the complete list of transactions and reconstruct the entire financial history of each account in the bitcoin market, the mainstream press lambasted the currency as a haven for drug smuggling and money laundering. Their notion implied bitcoin was solely useful for its falsely-stated “anonymous” nature, and therefore it had much use in the shadowy underworld of black and gray markets.

With the data stored in the public ledger, the Hungarian team recreated the flow of digital cash through the network and studied the resulting patterns of wealth creation and accumulation. The aforementioned BitcoinTalk questioner’s fears had been affirmed. “We believe that this is the first opportunity to investigate the movement of currency in such detail,” stated researcher Kondor.

The recreation of the network consisted of each node representing a bitcoin address. The team drew links between two nodes if there was but one transaction between them. They then analyzed the way the network evolved.

The evolution clearly occurred in two phases, according to Kondor and his team. Pre-2011, the system was used by enthusiasts and the bitcoins had no real world value. There was little activity during this time and the network structure varied greatly.

With significant media coverage of 2011 enveloped in a feedback loop with a rise in the bitcoin price all the way to $30, bitcoin at the end of June tumbled to $2. People contended then that bitcoin was a bubble. However, they had seemingly forgotten that bitcoin had begun the year at a mere $0.50.

Bitcoin then began to attract a seemingly exponential number of users. The decentralized digital currency became more attractive after exchanges became more prevalent and practical, with Mt. Gox stealing the show as the top exchange in bitcoin's incipience. Not until 2013 would other viable options come online, like Coinbase.

In this second phase, bitcoins became like real world currency. The network grew by preferential attachment in the second phase, according to Kondor. In this model, a node with a large number of links is likely to attract more links than a node with fewer links. This is a well-known effect in network science. Economists refer to it as the Matthew effect after the biblical observation that the rich get richer.

The Matthew effect happens across networks. For example, popular websites are likely to grow more rapidly than less popular ones. Similar processes are thought to occur in real world economies where the rich get richer. So, the Matthew effect can be clearly demonstrated in the bitcoin network, as not only are popular nodes attracting more links, but their wealth is also growing quicker than less popular nodes.

What's likely, in a system as new as bitcoin, is that those nodes attracting more and more links are functional, growing businesses. “The ability to attract new connections and to gain wealth is fundamentally related,” according to the researchers. “The 'rich get richer' phenomenon is indeed present in the system.”

Kondor and his team speculate that the bitcoin network could be valuable for econophysicists wishing to evaluate and refine their models. There is no other system of currency in which it is possible to study what goes on in such detail as bitcoin. Erik Vorhees argues that the distribution of bitcoins is meaningless. Rather, the manner by which one is able to acquire them is what's important.

Another concern trumpeted by bitcoin skeptics is the digital currency's deflationary nature. This deflationary nature is in large part why the Matthew Effect applies to bitcoin. To be sure, many early bitcoiners are nearly disinterested in the economic facts about bitcoin. They are more piqued by the technological aspect; namely, the protocol itself.

Many contend the integrity of the protocol is infinitely more important than whether or not the money is deflationary. So, in this sense, when we talk about a bitcoin market, it is not necessarily like the sort of market in which stocks, bonds and other things are bought and sold. Bitcoin resembles more so, the market for energy than these products.

Further, bitcoin's nature automatically predisposes market participants to forward-think, as bitcoin is tightly interwoven with quickly evolving technology. That's okay, though, because bitcoin, like all software, can be updated. Having egged civilization and progress on, bitcoin's market will likely evolve like a runaway train, in very few ways taking on the form of a traditional market. How this all plays out will depend on how the bitcoin commons handle the stress of change. With that said, bitcoin obviously takes on the characteristics of both an asset and a currency.

So, back to deflation. Two vocal schools of thought on deflation and inflation are the Keynesians and Austrians. Keynesian economics, a school of thought in favor of government intervention in the economy and money supply inflation, are proponents of measures like the Federal Reserve's quantitative easing programs. Then, there is the Austrian school, which favors a free market with minimal to no government intervention, and generally believes inflation is bad and deflation is good. An Austrian might champion competing currencies, as opposed to fiat. (money by decree and consent)

The deflation/inflation argument is an innately economic debate, and not a debate about bitcoin.

It is true that, over time, mining bitcoin becomes more difficult. But, as bitcoin becomes more difficult to mine, one can be sure that technology could catch up to ensure relative ease of bitcoin mining. What this process helps to ensure, however, is the aforementioned Matthew Effect.

2. UNDERSTANDING BITCOIN

There is a lot to understand when using bitcoin. There is one highly important aspect of bitcoin. This aspect is how bitcoin gains much of its value (beyond convenience, etc.) Never will more than 21 million bitcoins come into existence. That this is the case makes the technology attractive to individuals who are prescient of the Federal Reserve's policies of printing billions of dollars per month.

The bitcoins are released over time at a declining rate by a mining complex comprised of volunteer miners, many of whom are not even making that much money, if any at all, after overhead costs are considered. At the same time, many miners are probably doing just fine, especially those who held the coins in anticipation of bitcoin's price appreciation.

New generation miners have come online recently, produced by Avalon. While Avalon has delivered some models after their pre-order periods (which garnered much interest), Butterfly labs has yet to deliver two years after initial orders. "BFL" became slang within the Bitcoin community for being ripped off.

As new coins are generated on the set schedule, they are given at random to those who contribute computing power towards securing the bitcoin network. This is referred to as "bitcoin mining" and is akin to an auditing process.

Those who contribute more computing power than others have better odds of receiving the new coins. The rate of new coin creation does not increase, but rather diminishes over time until 21 million bitcoins exist. Deflation is thus pre-programmed and decreasing toward zero.

- Each bitcoin is divisible by one hundred million. The smallest denomination of a bitcoin, known as a 'satoshi,' will become bitcoiner’s equivalent to nickels and dimes.

- Bitcoins are divided and combined easily in your account.

- It is nearly impossible to counterfeit a bitcoin due to cryptographic and mathematical limitations on the model.

- Bitcoin floats against all major currencies on the free market. The price has fluctuated monumentally, soaring all the way to $30 in June 2011; and then to $266 in April 2013. By the end of 2013, the price had peaked around $1,200.

- Like other currencies, bitcoins are freely traded on exchanges, most often located online. The most prominent exchanges are MtGox.com and Coinbase.com. The former has had numerous issues and also had to pay millions in fines to the US government due to having transmitted money as an unlicensed money transmitter. The latter has operated smoothly according to most reports.

Bitcoin Wallet

Bitcoin is a highly consolidated and streamlined currency option, as it also represents its own payment network. Therefore, bitcoin not only is a currency alongside other currencies – most often printed by the semi-sovereign nations of the world – but also is its own payment network like SWIFT or SEPA. Thus, bitcoin is not stuff or a thing. Rather, it is a ways and a means. It is a digital payment system.

This means that bitcoins are different from other fiat currencies because they do not need banks, inter-bank funding networks (such as SWIFT and SEPA), payment processors (like PayPal and WorldPay) and/or remitters (like Western Union).

Bitcoin powers its own network in order to create, store, account for, and transfer money. In order to use bitcoins, you download traditional software. This software is essentially your bank account. A secret code is stored on your computer, and this code enables funds to be spent from your bitcoin "bank account".

In bitcoin terminology, this is your wallet. Your wallet can exist in your computer (with all the associated security risks) and can be backed up with a USB or in the cloud and as soon as you have a wallet you can receive and send bitcoins to other wallet-holders anywhere in the world in five minutes or less. I do not recommend backing your bitcoins up to the cloud. A USB is safer and will suffice. For individuals maintaining large balances, to be sure, other options are available. We will go over these later.

To participate in bitcoin, there is no need for a name, an address, a social security number or any personal information of any kind, unless you use a major, US-based exchange (increasingly, any exchange worldwide). Still, bitcoin is not anonymous, but pseudonymous. Like its p2p predecessors, Bitcoin is free and open-source software available at Bitcoin.org. Transactions are sent and accounts are secured via “public key cryptography.”

Private and Public Keys

Every account has a public key and a private key, both of which are comprised of a long string of numbers and letters. Your wallet software knows your private key, which allows it to send money. To send money to an individual or business, all you need to know is their public key which functions essentially as a bank account number. Your private key will function as a password.

If you have your private key and their public key, a transaction can be initiated by you to them. If you post your bitcoin address anywhere on the internet, however, then it automatically becomes public. Because of the nature of bitcoin, one can have multiple addresses (basically accounts), some public and some private. Many websites use Bitcoin as a platform to process donations, and even a range of products, as can be found at CoinDL.

As stated, bitcoin is similar to popular p2p networks of the

Information Age. Instead of swapping things like movies, films and books, account holders can transfer another form of value: bitcoins. So long as your accounts' key remains private and divulged only to those who need it, one can maintain value relatively anonymously.

A constant refrain against bitcoin is that it is "fake" or intangible. But, let's take a look at a shorthand history of financial privacy and asset protection. Other than mathematics, there are other reasons why bitcoin has value. The "Swiss bank account" has been considered the gold standard for financial privacy. Nonetheless, anyone who holds such an account must come to terms with the risk associated in having a third-party institution hold onto their wealth.

In this day and age, the US government insists knowing the accounts of all their citizens, not only in Swiss accounts, but all over the world. Since the banking crisis in 2008, as well as with its public debt issues, "private" Switzerland has proven itself a myth, as banks surrender customer information to government authorities.

Bitcoin can be like a private, numbered Swiss bank account, only you manage it 100% by yourself. It is just you and a cryptographic environment axiomatically grounded by mathematics. So, the value in bitcoins is derived from their practicality and their built-in scarcity (the 21 million coin thing).

These are two of the axiomatic musts of a useful currency, and any currency that demonstrates these capacities will likely discover a price. As a sufficiently useful and sufficiently scarce sterile asset, bitcoin has floated in the open market with dependable price discovery. There is both a supply and a demand for Bitcoin.

3. HOW BITCOIN WORKS

"It seems to me that simple altruism can suffice to keep the network running properly." - Satoshi Nakamoto

This section gets a bit technical. Few truly understand how bitcoin functions, but by coming into contact, if even briefly, with the degrees of technology that go into powering a p2p network like bitcoin, one can have their mind expanded. To paraphrase Karl Marx, "the masses must live through the revolution in order to understand the revolution."

"Preliminary research" suggests that bitcoin is an autonomous thing. In other words, the bitcoin open-source community acts as one united soul - an institutional-entrepreneur - in which countless actions of individual agents converge over time to create the bitcoin hologram. The collective and neither the individual, nor a single organization, resolves the future of bitcoin. But, this collective is comprised of diverse individuals: of communists, of libertarians, of anarchists, of speculators and of the a-political. What inspired these individuals to create this community? Bitcoin.

Bitcoins are computer files, so they behave similarly to a music or a text file and can be destroyed or lost like any computer file. Many say bitcoin is digital cash. To be sure, bitcoin is not exactly like physical cash. When you lose cash, someone else can theoretically find it.

If you lose bitcoins, they are not readily available to another person unless you were hacked. Lost bitcoins are not just found in cyberspace by web-surfers. Also, your brain does not store a trail as to where your cash was last. If a $100 bill falls out of your pocket, you might not have access to any data whatsoever as to what-in-the-world happened. Potentially, when you lose bitcoins, a computer security expert can do research into the issue.

As Trace Mayer puts it, “Bitcoin is like a gold coin that you can e-mail.” As we've covered, the central aspect of bitcoin is that it is an open-source software and community, and open-source communities are strangers, from anywhere in the world with internet access, coming together and self-organizing around a shared interest so as to create value through sharing knowledge and innovation.

Undoubtedly, the community has not been able to tame the tide of misconceptions about bitcoin. Such as that bitcoin's are backed by nothing. Therefore, bitcoin is not a virtual gold. But, the value of gold is largely reflected in the amount of energy consumed in mining and refining the metal, which contributes just as much to gold’s value as does its suitability as money. As one individual once put it, “a gold coin represents a large amount of land, highly refined, with the input of a great deal of energy, labor and capital.”

In a similar manner, bitcoins represent the computing power, energy and capital required to create them. It takes specialized technology running for sometimes many days to create a bitcoin. This was even true many years ago. Like mining for precious metals, it is not easy to mine bitcoins profitably. Bitcoin mining is extremely competitive, as we will detail later, and it's rarely a profitable venture unless higher future prices in bitcoin are assumed. A main advantage of bitcoin is its peer-to-peer nature. This means that there is no "issuing authority" for bitcoin, and there are no central depositories or central banks.

Block Chain

The block chain is formed by a "peer-to-peer distributed timestamp server" which verifies that bitcoins have not been "double spent" - in other words, counterfeited. A timestamp records the exact time that a bitcoin is created or a transaction from one user to another transpires. The master list into which these timestamps are aggregated is the block chain.

The block chain, by using our private keys, tracks the wallets controlling the bitcoins. Using this same technology, a computer program could theoretically determine that a bitcoin represents a bond or a share in a company and with an additional layer of software, can easily track this via the BlockChain. In the tradition of bitcoin, these bonds and shares or whatever widgets, can be tracked without a third-party intermediary.

As Nakamoto wrote in 2008, the block-chain includes all past transactions. The software does retain the ability to abridge the chain if deemed necessary. The record of all current bitcoin owners' public keys will never be dropped from the chain.

There are many things that are best done off the Block Chain, such as micro-transactions or instant transactions. That means, essentially, that although you would like everything rooted on the Block Chain, the Block Chain is uneconomical for certain transactions.

In summation, the record of transactions is called the block chain, a sequence of record-keeping called 'blocks.' All computers participating in bitcoin (that download to their own computer their own wallet client, at least) have a copy of this block chain, which constantly updates as new blocks get confirmed.

Each block shows a group of transactions that have been sent since the prior block. The block chain is preserved as each block in the chain confirms the integrity of the prior block, a process that goes all the way back to the first block, “the genesis block.” Each block must meet requirements that make it difficult to generate a valid block. This disables an interested party from overwriting previous records by forking the chain, which we go over below.

Several cryptographic technologies come together to form bitcoin, the first being public key cryptography. Each bitcoin is tied to its current controller’s public ECDSA key. When you send bitcoins to another address, you create a message (transaction), which attaches the new owner’s public key to the right amount of coins, and the transaction is signed off with your private key.

This transaction gets broadcast to the bitcoin network, informing all nodes (users) who the new controller of these coins is. The entire history of transactions is kept by all users, and so anyone can verify wallets and how many coins they control.

Bitcoin hashrate

The generation of new bitcoins is made difficult by the Hashcash cost-function. Hashcash represents the first secure, efficient and verifiable cost-function or proof-of-work function, and it is non-interactive so it has no secret keys that must be managed centrally or by any party. In bitcoin, SHA-256 is the base cryptographic hash function.

A cryptographic hash function takes input data of essentially any size, and transforms it, in an essentially irreversible and/or unpredictable manner, into a more compact string. In the case of SHA-256, the hash is 32 bytes. Hashcash is fully distributed and infinitely scalable. Hashcash uses asymmetrical key cryptogaphy, namely a one-way hashcash function - typically either SHA1 or SHA-256.

And so, with a compact hash, you can confirm that it matches a certain input datum. Since bitcoin's input data is a block-chain, and much larger than the SHA-256 hash, bitcoin blocks don't have to contain serial numbers, because blocks can be identified by hash.

A hash is, in general, a way of taking an arbitrary piece of data, of arbitrary length, and then compressing it into a short summary of that data. An example of this is the set of books on your bookshelf. You might arrange them where all the titles are put together in alphabetical order. Your simple hashing algorithm is the first letter. The cryptographers have taken cryptographic hash functions that, when you run a function, a hash value is created (first letters of books, for example). A cryptographic hash function creates long numbers to do this same job.

The hash serves two purposes: identification and integrity verification. An identification string is called a self-certifying identifier. These functions and others enable verifiable ownership of bitcoins, and a distributed database of all transactions so as to prevent double spending.

Transactions as digitally signed announcements

The Bitcoin system defines a transaction as "digitally signed announcements [in which] the owner of some coins agrees to transfer them to a different owner." Just like in a real economy, the sender expects a product or service in return.

This would not work if the sender was able to broadcast a new, contradicting transaction which sent the coins back to themselves. This is a double-spend attack. A double-spend attack is a successful attempt to convince a merchant that a transaction has been confirmed, but then convince the overall network to accept some other, contradicting transaction. If this were the case, the merchant would be left with neither product nor payment, while the attacker keeps both.

This boils down to a question of synchronization on the network; i.e. there must be an accepted signal indicating that a transaction is confirmed and that no contradicting transaction can ever be accepted.

Blocks

Bitcoin solves this problem via a proof-of-work system: Computational effort, expressed by the calculation of hashes, acknowledges groups of transactions - known as blocks - and a transaction is considered confirmed once enough work has gone towards acknowledging the block which contains it.

Linking these blocks together then forms a chain, and over time the amount of work going into any given transaction perpetually increases. This makes it more difficult over time to broadcast a conflicting or false transaction that gets confirmed. Surely, in the event the attacker controls substantial computational power, he may succeed in doing this, but it is highly unlikely. Satoshi Nakamoto touched upon the statistical aspects of this problem in the original bitcoin white paper.

These blocks, which comprise bitcoin's transactions history, reference an earlier block by including the uniquely identifying hash of the earlier block in its header. There is one exception to this rule: the first block ever, the Genesis Block.

So, the blocks form a tree, with the genesis block as the root and each block thereafter a child of the block it references. A branch on this tree represents a path from a leaf block to the genesis block, and each such branch represents one version of the history of bitcoin transactions. Each node on the chain will consider the longest branch it is aware of as the valid chain; that is, the branch which represents the most proof-of-work (processing power).

The block chain represents bitcoin's common ledger. It details the controller of each bitcoin, or fraction thereof. The ledger of transactions is stored by broadcasting small pieces (known as "blocks"), each stating in its code that it continues the prior block. The block chain could split into a new branch – that is, two blocks can both point to the same parent block and contain some of the same transactions – and when this transpires each computer in the network must then decide which branch is "correct" and should therefore be accepted by the network.

In the future, due to bitcoin's adoption rate, block size limits will need to be increased by developers. At the time of writing, the blocks were 1 MB in size.

One question the network would have to address is how quickly this will happen. Gavin Andresen conjectured that around mid-2014 this 1 MB hard limit will be tested. (The hard limit was implemented to preclude someone from spamming the network when bitcoin was new, thus making the chain too large for download)

Cryptography

SHA-256 is the encryption used in bitcoin, and was developed by the NSA (similar to how the military-industrial complex created the internet). This basically means encryption by a 256 bit number; that is, a really big number. The cryptographers have designed the hashing algorithms in such a way that any data you put in will essentially create different numbers that are completely irreversible.

If you have the hash value, there is no way, as far as cryptographers know, to figure out what data went into that value. It is like a fingerprint or other specific data structure. Because of the mathematical properties one can know differences between specific fingerprints.

The only way to crack these are lookup tables; in short, by computing all hashes and putting them into a table, called a rainbow table, which means having access to dedicated time and storage. At 256 bits you can't really employ a lookup table to crack the code, because if you ran the numbers, you'd find that SHA-256 is comprised of more atoms than there are in the Earth. There is not enough computer memory in the world to store a 256-bit hash.

Forced work is basically having your computer prove it has performed a lot of calculations. The forced work in bitcoin is related to hashing. If you run a hashing algorithm, you get this big long 256-bit random number.

Bitcoin's execution is what separates it from past digital currency experiments. Since bitcoin arises out of the internet, there are certainly not only generation gaps in understanding, but also skeptics the world over who make good points about bitcoin's legitimacy and viability – something which became especially visible in the wake of Edward Snowden's National Security Agency revelation.

But, in the end, all that bitcoin is, is a protocol that helps route traffic and is at a layer of the internet "below" the http (for example, http://bitcoin.org) layer.

Bitcoin as auto-accountant

The bitcoin protocol, at its heart, has solved the double-spend issue. The Federal Reserve's quantitative easing program is an example of double-spend. What if there was a computer code that disallowed double-spending? Open-source code acts as a government essentially. Remember, bitcoin, being open-sourced, is available to peer-review. So, it could be argued that the open-source and communal nature of bitcoin represents a form of democratic self-governance.

The advancement in accounting which bitcoin employs is referred to as triple-entry accounting. In order to compromise the code, Trace Mayer estimates $30 billion worth of computing power would be needed, for at the time of writing, bitcoin is secured by processing power of over 250 pedaflops. The Department of Energy built a supercomputer for $1.2 billion that has 15 pedaflops. This gives you an idea of how big bitcoin is.

4. GETTING STARTED

One can acquire bitcoins by selling goods or services in exchange for bitcoins or by buying them at an exchange. “Exchanges” are websites where buyers and sellers come together to trade one currency for another. If you have an account with a certain exchange, you can use dollars to fund a bitcoin purchase.

These are obviously centralized online institutions and so it is recommended that if you choose to hold your bitcoins online, you do it with multiple wallet-services (for diversification's sake). For sure, there is no reason why, if you choose online exchanges, you shouldn’t also download the bitcoin client to store some of your bitcoin on a computer or USB. Of course, the constant internet connectivity of your daily machine is a security issue. To solve this, simply use a computer that is not connected to the internet, and don't connect it to the internet. Use a USB to transfer from the offline machine to the online machine.

Step 1) Download bitcoin client.

Step 2) Go to Local Bitcoins (http://localbitcoins.com) and attempt to find someone in your area selling bitcoins for a reasonable price. You can also visit Coinbase.com

Do you have your own blog, online store or brick-and-mortar store? Well, begin accepting bitcoin for your products or as a donation either with your own client, BitPay or Coinbase. Save some of your profits in bitcoin.

Step 3) If you purchased through an exchange, the bitcoins typically stay at the exchange account until you send them elsewhere (to a personal wallet or to a vendor or individual.)

If you want to sell your bitcoins for dollars, you merely send the bitcoins to an exchange, sell them at market price, and transfer the USD where you need it to go.

Unlike most markets, the bitcoin market is open 24/7, 365 days a year. The exchanges are accessible from anywhere in the world and support all major national currencies.

You could also accept bitcoin in exchange for goods and services, just like you sell goods or your labor for your dollars. All you have to do is put your public bitcoin address to your bitcoin wallet on your webpage or download the BitPay plugin in WordPress or other platforms.

Storage

The most secure way to store bitcoins is offline. This is referred to as "cold storage." This is the way in which leading exchanges store most of their bitcoins.

Although they usually offer an instant withdrawal feature, many of their bitcoins at any given time will be stored offline; that is, not present on a web server nor a computer with WiFi capabilities. The amount kept in so-called “hot storage,” or online, is only enough to cover anticipated withdrawals. Some methods of cold storage include:

•On a USB drive or other data storage medium in a safe place (e.g. safety deposit box, safe)

• On a paper wallet

• On a bearer item such as a physical bitcoin.

• Online, but on encrypted media where the encryption key is offline.

Another option for keeping bitcoin online is referred to as deep cold storage. A simple instance of deep cold storage is putting a USB stick with an encrypted wallet file on it in a safety deposit box. The public addresses (to receive) can be used anytime; however spending bitcoins would require physical access to the box and the encryption password. Certain precautions must be heeded when storing in this manner. Some issues with storing your USB in a place like this include:

• The box could be accessed by bank or maintenance personnel.

• The box could be stolen or destroyed in a disaster, or the media on the USB could become unreadable, so the box should not contain the only copy of the wallet.

• The trustee could die or become incapacitated. If access to the wallet or knowledge of its location is lost, or encryption passwords are lost, the bitcoins are gone forever. Provisions should be made so the box can be accessed by someone else, including encryption passwords.

A great device for storing bitcoins in cold storage is the Raspberry Pi. The Raspberry Pi is a credit-card sized single-board computer using a Broadcom BCM2835 system on a chip, which contains an ARM1176JZF-S 700 MHz processor. The unit has 512 megabytes of RAM and does not include a build-in hard disk for solid-state drive. Instead, the device uses an SD card for booting and long-term storage. The Raspberry Pi comes with Debian and Arch Linux ARM distributions for download. The Raspberry Pi is quite cheap, running for approximately $40. This price will likely come down in the future.

PART TWO

Bitcoin Wallets & Exchanges Report

5. WALLETS & EXCHANGES

The purpose of the following is to understand the privacy, legal, security and ease of use implications of the best Bitcoin wallets and exchanges in the international bitcoin market today.

Exchanges were analyzed on various grounds, especially jurisdiction, anonymity granted to users and ease of funding, when purchasing bitcoins. Wallets were analyzed based on security, privacy, ease of use and platform availability.

6. EXCHANGES

When it comes to privacy and security, there are relatively few options for exchanges in the Bitcoin space. This is due to the ease of use that debit cards, credit cards, and banking transactions bring, when purchasing larger amounts of Bitcoin.

This means users who wish to buy large amounts of Bitcoin quickly, will have two options. Submit to KYC and AML with a Bitcoin exchange, by verifying their identity and transferring funds directly from their bank accounts or using a bitcoin trading market place, like LocalBitcoins.com.

Privacy

The fiat financial system is built upon identity verification. This was safe during the analog era, when identity was stored in paper under a steel lock in the physical security of a bank. Today all of it is digitized, exposing users to ever increasing and stunning risk of identity theft, among other attacks. However, the system is slow to adapt and regulators wield great power, something that is unlikely to change given the political benefits of government dictated embargos.

As a result, almost all bitcoin exchanges require KYC and AML information, logging the identity of users and asking for banking style personal information.

Privacy however is not dead and Bitcoin does not care who you are. There are some ways to get bitcoin anonymously and there are some exchanges that respect user privacy more than others.

If what you want is high ease of use and high anonymity, well sorry, but I see no path to that today. However, below are some tools that can get you anonymity with some work, as well as high ease of use if you are ok with identity verification.

Privacy from best to worst.

1. Local Bitcoins
2. (The rest)
3. Bitstamp

Jurisdiction

Jurisdiction is another essential question for users, as some do not reside in USA and some prefer not to use American systems.

The question of jurisdiction however, can be analyzed in two ways; who owns the company and where can it operate. See specific exchanges to learn about who owns them.

The following are the best exchanges when it comes to anti-fragility to American power. In other words, they are exchanges that can be used inside and/or outside the United States.

1. Local Bitcoins
2. Kraken
3. Uphold

Ease of funding, CC and Debit

Credit Cards and Debit Cards are the most common and easy to use fiat technologies in the developed world. This makes them very useful for Bitcoin conversion, but their nature makes them very risky for Bitcoin sellers. Unlike bitcoin, credit and debit transactions can be reversed, exposing bitcoin sellers to chargeback fraud.

Because of this, CC and debit deposits are always secured by identity verification and are also heavily regulated. However, they are familiar means for users to pay online, making them the easiest means to get bitcoin.

When it comes to ease of funding, here's the best:

1. Uphold
2. Circle
3. Bitstamp

Closing thoughts: Over the Counter trading or OTC is also a substantial portion of bitcoin trading, usually for high volume trades and institutional interest, however, this is not represented in this research in any depth. It is also outside of the scope of this report. However, see this article for a good start into understanding the OTC, high volume BTC trading world.

https://www.buybitcoinworldwide.com/kb/buy-large-amounts-of-bitcoin/

Kraken

Well-funded American Bitcoin exchange Kraken, founded by Trace Mayer the same founder of Armory, a wallet long regarded as Bitcoin's Fort Knox (not further developed). Kraken, which was founded in 2011, claims a record of zero hacks.

Fees: up to 0.26% plus third party banking fees.

https://www.kraken.com/help/fees

Privacy: Medium. Allows trading Bitcoin to fiat (and some altcoins) without proving identity, but requires input of name, date of birth and phone number without proof of identity.

Fiat deposits or withdraws require further ID verification, such as residential address. See details here:

https://support.kraken.com/hc/en-us/articles/201352206-What-are-the-Verification-Tiers-

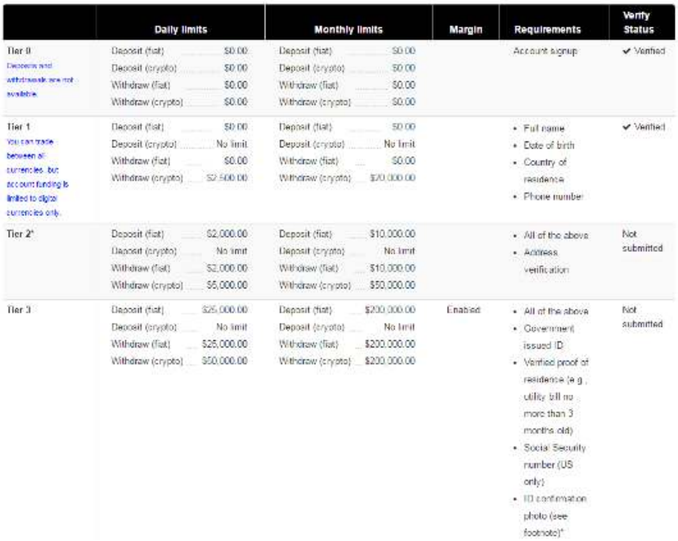
While it is possible to reach the second tier of verification without proving your identity or residence, (fake name, fake address etc.) it remains impossible to deposit fiat into their exchange without reaching Tier 3 - which does required ID and residential address proof. This consists of the typical, being a picture of state sanctioned ID, which they compare against information you have given them and against known databases of identity profiles and perhaps some manual checking of address integrity etc.

Once verified at Tier 3, it is possible to trade EURO, USD, CAD, GBP and YEN, by depositing with SEPA, Wire Transfers, SWIFT, EFT, INTERACT and presumably through an unnamed YEN method not revealed to Tier 2.

Jurisdictions: Presumably anywhere where the following banking rails are used, which covers a lot of countries, including the USA: SEPA, Wire Transfers, SWIFT, EFT, INTERACT (plus, unknown YEN deposit method).

CC Deposite: NO.

Limits: https://www.kraken.com/u/verify



	Daily limits		Monthly limits		Margin	Requirements	Verify Status
Tier 0 Deposits and withdrawals are not available.	Deposit (fiat) Deposit (crypto) Withdraw (fiat) Withdraw (crypto)	$0.00 $0.00 $0.00 $0.00	Deposit (fiat) Deposit (crypto) Withdraw (fiat) Withdraw (crypto)	$0.00 $0.00 $0.00 $0.00		Account signup	✓ Verified
Tier 1 You can trade between all currencies, but account funding is limited to digital currencies only.	Deposit (fiat) Deposit (crypto) Withdraw (fiat) Withdraw (crypto)	$0.00 No limit $0.00 $2,500.00	Deposit (fiat) Deposit (crypto) Withdraw (fiat) Withdraw (crypto)	$0.00 No limit $0.00 $20,000.00		• Full name • Date of birth • Country of residence • Phone number	✓ Verified
Tier 2*	Deposit (fiat) Deposit (crypto) Withdraw (fiat) Withdraw (crypto)	$2,000.00 No limit $2,000.00 $5,000.00	Deposit (fiat) Deposit (crypto) Withdraw (fiat) Withdraw (crypto)	$10,000.00 No limit $10,000.00 $50,000.00		• All of the above • Address verification	Not submitted
Tier 3	Deposit (fiat) Deposit (crypto) Withdraw (fiat) Withdraw (crypto)	$25,000.00 No limit $25,000.00 $50,000.00	Deposit (fiat) Deposit (crypto) Withdraw (fiat) Withdraw (crypto)	$200,000.00 No limit $200,000.00 $200,000.00	Enabled	• All of the above • Government issued ID • Verified proof of residence (e.g., utility bill no more than 3 months old) • Social Security number (US only) • ID confirmation photo (see footnote)*	Not submitted

Bitstamp

Based out of the ‘EU’, Bitstamp is a popular bitcoin marketplace founded in 2011. Though it has suffered at least one major hack, it remains standing and claims to be fully regulated, presumably in the EU.

https://www.crunchbase.com/organization/bitstamp#/entity

Privacy: Very low. Heavy compliance AML and KYC. Stories on reddit of compliance far beyond what is ‘normal’ in fiat finance. Though these are technically anecdotal and might be exaggerated.

Limits: Could not find clear description of limits and there may not be any. ID verification seems very stringent and they might simply not allow trade without verification.

Fee: 0.25% max plus third party banking fees.

https://www.bitstamp.net/fee_schedule/

Jurisdictions: Seems to serve many countries, including USA.

CC Deposit: YES https://www.bitstamp.net/article/bitcoin-purchase-with-credit-card-germany-italy/

Ripio

Bitcoin exchange run in Argentina and Brazil, owned by BitPagos, well known Latino American bitcoin payment processing company, funded by venture capitalists firms like Pantera Capital, with board members like latam fintech leader, Juan Llanos. https://www.crunchbase.com/organization/bitpagos#/entity

From basic testing seems straightforward and easy to use. Though some kind of number is needed to fund it with cash at a store front, this may not be released until ID verification.

Privacy: Low. KYC and AML compliance from the start.

Commission: 2.5% al 6% depending on form of payment.

User side Security: 2fa, password and email registration.

Jurisdiction: - Argentina, Brazil

Claims Basic 1k ARS requires name, address, phone number.
No ID. No proof asked.

Advanced 5k ARS with ID verification and higher with ‘full ID verification.

Max 50k/ month full ID. See for details:

https://www.ripio.com/en/faq/

CC Deposit: NO

How to buy: Cash at storefronts.

https://www.ripio.com/stores/mapa/

HQ: San Francisco, CA.

Circle

Circle is an American bitcoin exchange backed by the major

American Banks. That's right, Goldman Sachs, IDG Capital Partners, an Ex JPMorgan Exec, among others have been associated with this company, making it the "Death Star" of Bitcoin exchanges.

https://www.crunchbase.com/organization/circle-2#/entity

That said, it is incredibly easy to use, fast, and insured. And given the amount of high level backing it has received, you can expect that they have top notch security. Though either way, you should never leave your money in a Bitcoin exchange.

Purchase Limits: $300 USD a week unverified - $3000 USD a week verified.

Forms of Deposit: Debit, Credit Card, Bank account linking.

Deposits from friends: Similar to PayPal.

Privacy: Low. There is no way to buy with cash or cash deposit. Every form of fiat deposit associates your identity with them, providing a clear avenue for identification. Claims to not allow prepaid CC or Debit (older reports from 2014 contradict this, remains untested).

https://support.circle.com/hc/en-us/articles/205382324-Which-debit-and-credit-cards-can-I-use-

Jurisdictions: United States, UK only. Accepts debit deposits from international UK banks, fees may be charged by such banks.

HQ: Dublin Ireland.
CC Deposit: YES

Difficulty: Easy. Plug in debit/credit card number, pay and get bitcoin within half hour, with some exceptions that take 3 hours.

Security: Requires 2fa (two factor authentication) to withdraw more than $30 USD equivalent. It asks for your phone number during signup.

USD funds are insured by the FDIC, like other American Banks. Bitcoin funds insured by Marsh USA, a subsidiary of Marsh & McLennan.

Security procedures are likely to be top of the line, especially given that they are insured. This is one of the biggest American Exchanges, (I know this based on 2015 information, last time I looked closely at American exchanges. This may change after in-depth report.)

How to use Circle to buy Bitcoin quickly and easily. 3 minute video:

https://www.youtube.com/watch?v=S0OgXCkndH8

LocalBitcoins

LocalBitcoins is an international exchange that takes Bitcoin's decentralization to heart. Instead of trying to play middleman between traders, it lets them meet and coordinate among themselves, while providing reputation stats and escrow to facilitate trust.

Localbitcoins has been around since the early days of bitcoin and may have been inspired by similar trades happening on the bitcointalk forums. Traders often use pseudonyms and it is the most anonymous way I know of to buy bitcoin without doing too much work. It is however, more technical than bitcoin exchanges and requires some understanding of the financial system and bitcoin.

Lbtc is a grassroots organization, and according to techcrunch, it has not received any formal investment.

https://www.crunchbase.com/organization/localbitcoins#/entity

HQ: Helsinki Finland.

Purchase Limits: None - depends on payment methods, country and current supply.

Forms of deposit: All or most. May depend on the country of residence of the traders or where their bank accounts are if using the traditional financial system.

CC Deposit: YES, though more expensive due to fraud risk incurred by Bitcoin seller. Credit and Debit Card payments can be reversed, Bitcoin cannot.

Jurisdictions: International. Almost any country. Though some certainly have a lot more volume and traders than others.

Commission / Fee: Often higher prices than in centralized exchanges.

Privacy: Can be fairly anonymous. Getting bitcoin without revealing identity information is actually quite difficult. One way to do it may be to go to localbitcoins, find someone in your area willing to sell your bitcoin for cash, and then meeting them in a public place.

They'll get to see your face, unless of course, you say, wear a hat and shades, but you'll likely be sitting with them for a few minutes to half an hour, waiting for the bitcoin transaction to confirm.

It's generally advised that the meeting place be public, like a Starbucks or ironically, a bank. For extra control, you might suggest the meeting place, though consider that the seller will have similar security concerns as you.

To the best of my knowledge, the best way to do it might be through Cash deposit at a bank, using escrow for the bitcoin. Wear a wig or some kind of facial obfuscation for the cameras if you choose. Hats are often not allowed at banks though, so eyewear and fake hair might be the way to go, to get bitcoin 007-style.

The bigger the city, the more likely you will find someone to sell you large amounts of Bitcoin. It is a great way to meet bitcoiners. Just make sure they have a mostly positive and high reputation. Don't trade with people that have zero or negative reputation.

Difficulty: Medium to advanced: Requires understanding of payment methods. Some non-cash based payments are reversible while bitcoin is not. If you sell bitcoin in exchange for Paypal money, the buyer, may have Paypal do a chargeback after and take away your fiat. This creates risk, which in turn raises prices for certain payment methods. Though not all traditional payment methods are reversible. Cash deposits, and bank transfers are not according to localbitcoins.

For your first trade, request that the seller use the escrow. Localbitcoins will charge a small fee, but it will teach you an essential part of bitcoin and peer to peer trading. Knowing how this works will come in handy in the future.

Uphold

Uphold is a financial institution with loud and clear libertarian values. Within seconds of their flagship ad, they explain fractional reserve banking and how they 'never' do it. Calling themselves 'not a bank' but a full reserve financial services company. They represent

the movement to international low barriers to entry for sound finance. And to that end they enable conversion between sound currencies and fiat. Yes, gold, silver, bitcoin, Ethereum, Voxel and many others include those who are on top of cell phone minute systems. They even have their own app store previously known as BitReserve.
Uphold was Equity crowdfunded to the tune of 6.3 million.

https://www.crunchbase.com/organization/bitreserve#/entity

HQ: San Francisco, CA, USA.

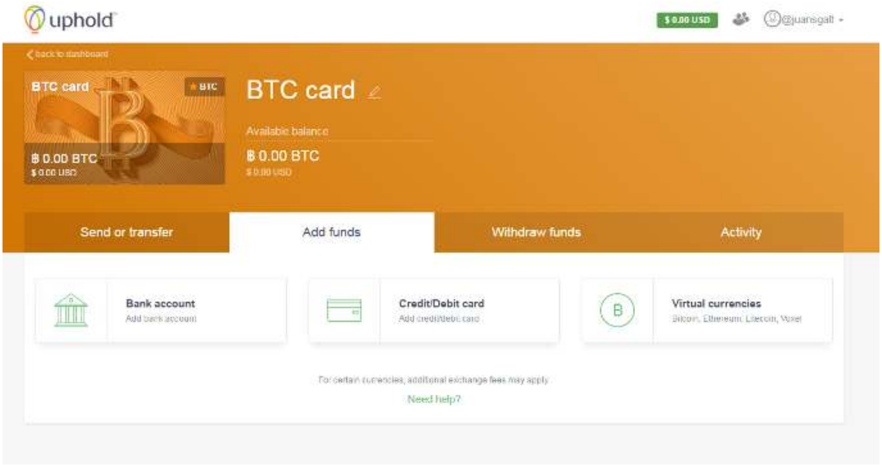
CC Deposit: YES.

Privacy: Medium.

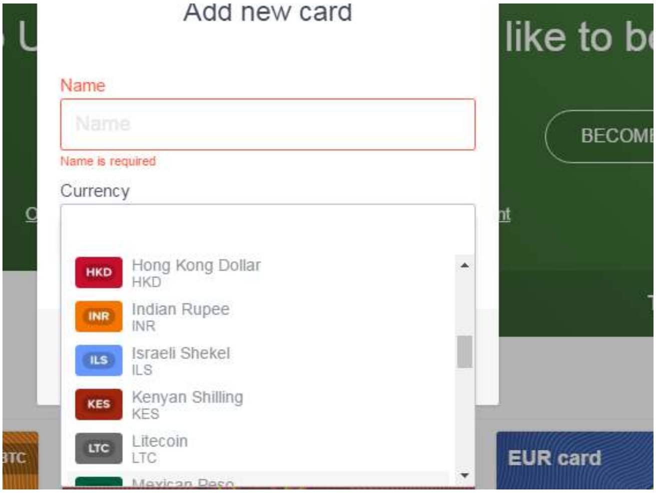
It requires identity verification to deposit CC, debit and linking of bank account.

Ease of use: High, big buttons, simple interface.

Forms of deposit: CC, debit, Link Bank account, Bitcoin, Ethereum, Voxel, Litecoin



Assets Traded: Gold, Silver, USD, EURO, CNY, JPY, GBP, BTC, LTC, ETH, VOX, and many more through custom cards which are super easy to make.



Limits: https://support.uphold.com/hc/en-us/articles/206118653

7. WALLETS

Bitcoin wallets are just that, wallets. They are containers for your bitcoin. This is what allows you to ‘be your own bank’ and with it comes a small learning curve and more responsibility, but also far more security and independence. Particularly from banks attacks like those seen in Cyprus or from exchange hacks like what happened with the legendary Mt. Gox.

Recommended practices:

- Use wallets that claim to be HD. This will protect you from public address reuse and dramatically enhance your privacy with ease of use.
- Don’t use web wallets, even client side encrypted web wallets like blockchain.info. While blockchain.info is considered secure, it is low on privacy and it has so many users that updates to its website are slow and so it is falling behind the competition.
- Do a back-up as soon as you can and follow the steps provided by the wallet of your choice. Never write the ‘seed’ on any computer. Store it physically by writing it on one or more pieces of paper and hiding them in secure locations.
- Use a PIN with wallets when possible and use a password or passphrase to lock your desktop. Even if it is somewhat easy to guess, it should give you enough time to restore your bitcoin from back up to a new wallet, before an attacker

breaks through your defenses. For more details on this, see my workshop on easy to use digital security and privacy at freedomhacker.tv/safe.

Basic Concepts

Security

Bitcoin security is one of the first questions new users will be faced with. Which wallet to use? What standards to follow?

The following products are among the best in the market as of the time of writing and include most common security procedures, for the most commonly used platforms. It does not cover industrial or business grade security practices in any depth, though some of these standards may be sufficient for such use cases. The difference between a private user and an organization or institution using Bitcoin is their risk profile and how visible they are to attackers. How often they must make transactions also has an effect on their security choices and thus on how protected they are.

There is no organization to my knowledge doing systematic ranking and analysis of Bitcoin wallet security standards, though most of the Bitcoin industry follows open source practices and developers tend to gather and communicate through the development of BIP (bitcoin improvement proposals).

With this in mind, here is the ranking hierarchy that I see based on my research since 2013. From least secure to most secure.

1. Web wallet. (a website has unencrypted control over your private keys, and you and the website must be online to move your bitcoin)
2. Web wallet with client side encryption (blockchain.info model. They do not control your bitcoin, but may be vulnerable to man in the middle attacks. Users can restore their bitcoin in other wallets)
3. Software product wallets. (Any wallet that requires a download of a software program, whether it be on mobile or desktop. This is among the most commonly used bitcoin wallet based on my personal experience.)
4. Hardware Wallets. (This is the next step for users in bitcoin security that is easy to use. It requires a small learning curve, but it brings bitcoin security to the physical world and goes to great lengths to isolate the private keys from internet access, by creating small independent micro computers in pocket size USB devices.)
5. Cold storage. (Considered to be among the highest standards of digital security, it brings the odds of digital internet based hacks to zero by generating and storing the Bitcoin private keys in hardware devices or paper wallets that are incapable of connecting to the internet. In exchange, having users secure these storage devices through physical security standards)

6. Multi-signature cold storage. (Multi-signature cold storage is a security standard usually used by institutional users and companies. It requires multiple private keys, up to 15 in Bitcoin, for a withdrawal to be made from a wallet. It requires clear understanding of bitcoin security from players involved and other human organization procedures, but provides the most decentralized bitcoin security approach and isolates bitcoins from digital internet hackers.)

Privacy

Bitcoin privacy is a concern and value of many Bitcoin early adopters. As such, it is a topic of common discussion and it is constantly developed at various levels. It matters because it is essential to Bitcoin's success as a currency given that in the digital world privacy is the same as fungibility. Privacy is often used to mean the same as anonymity, though technically they are different things. Anonymity concerns itself with hiding who is doing what. Privacy concerns itself with hiding what someone is doing, but not necessarily who they are.

Privacy rating standards in this report are provided by the Open Bitcoin Privacy Project, founded by Kristov Atlas. This open source, non-profit organization releases one report every year, does systematic technical analysis of bitcoin wallets and their privacy and ranks them on multiple grounds including; security from network observers, wallet providers, and physical observers, among others.

Ranking scores go up to 100, with 100 being perfect privacy, the highest achieved by any wallet during March 2016's ranking review is 50, by the hardware wallet Ledger Nano. For more details see their official website at www.openbitcoinprivacyproject.org.

Ease of use

As a general rule, ease of use is inversely related to privacy and anonymity. The easier to use a wallet, the less likely it is to be private and secure. As a result most users seem to gravitate towards wallets such as client side web wallets like blockchain.info and software wallets. With that being said, hardware wallets like Ledger Nano are bringing the Bitcoin wallet industry to a new era of high grade security with good ease of use.

As a general recommendation, users should not use web wallets, including blockchain.info. And instead should do some reading on bitcoin to climb the first steps of the bitcoin learning curve where needed and skip ahead to software wallets.

Mycelium Android

Mycelium is generally recognized as one of the most private and easiest to use Bitcoin wallets. It is available for Android devices.

Cost: Free

Privacy Rating: 37/100. It uses ‘HD wallet’ which means it creates a new public address per new transaction, going a long way towards protecting you from statistical analysis.

Difficulty: Easy to medium. User must learn to back up their wallet. (Follow the steps during the ‘back up’ phase, and write the ‘seed’ only in paper, not in a text note on your pc or any other part of your pc, unless you use a very secure password manager). Lite client, does not require downloading the full bitcoin blockchain.

Instant anonymous conversion to USD, EUR and JPY equivalent through coinapult.

https://www.youtube.com/watch?v=eT2CmOfXyH0

Security: Software wallet with integration to hardware wallets like Trezor and Ledger nano. HD privacy architecture.

Electrum Windows, OSX (Mac), Linux

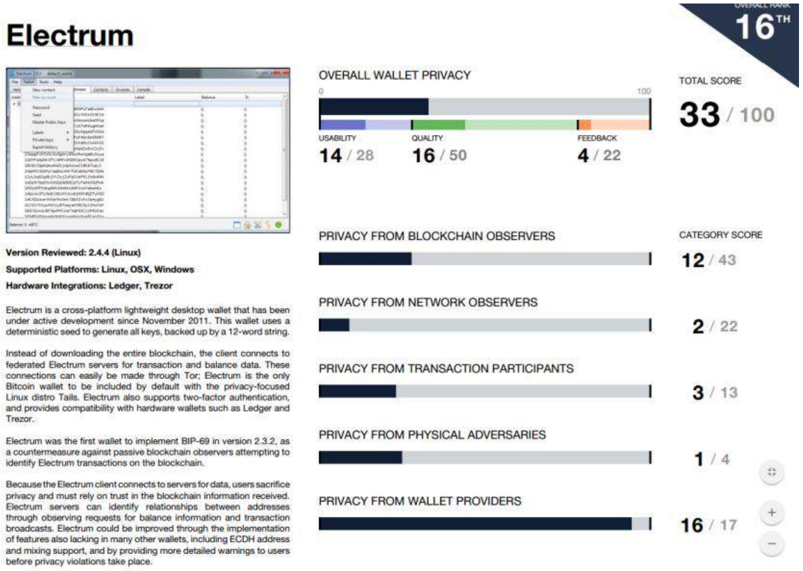
Classic and old school bitcoin wallet. Open source, and available on almost all platforms except iOS.

Cost: Free

Privacy*:* 33/100. It uses a ‘HD wallet’ which means it creates a new public address per new transaction, going a long way towards protecting you from statistical analysis.

Electrum comes installed by default with Tails Linux, an amnesic Linux distribution meant to be run from a USB, and designed for top grade anonymity and privacy. The recommended OS for dark web surfers and people seeking to obfuscate their location against well-funded actors.

Difficulty: Medium.



Electrum

Version Reviewed: 2.4.4 (Linux)

Supported Platforms: Linux, OSX, Windows

Hardware Integrations: Ledger, Trezor

Electrum is a cross-platform lightweight desktop wallet that has been under active development since November 2011. This wallet uses a deterministic seed to generate all keys, backed up by a 12-word string.

Instead of downloading the entire blockchain, the client connects to federated Electrum servers for transaction and balance data. These connections can easily be made through Tor; Electrum is the only Bitcoin wallet to be included by default with the privacy-focused Linux distro Tails. Electrum also supports two-factor authentication, and provides compatibility with hardware wallets such as Ledger and Trezor.

Electrum was the first wallet to implement BIP-69 in version 2.3.2, as a countermeasure against passive blockchain observers attempting to identify Electrum transactions on the blockchain.

Because the Electrum client connects to servers for data, users sacrifice privacy and must rely on trust in the blockchain information received. Electrum servers can identify relationships between addresses through observing requests for balance information and transaction broadcasts. Electrum could be improved through the implementation of features also lacking in many other wallets, including ECDH address and mixing support, and by providing more detailed warnings to users before privacy violations take place.

OVERALL RANK
16TH
OVERALL WALLET PRIVACY
0
100
TOTAL SCORE
33 / 100
USABILITY
14 / 28
QUALITY
16 / 50
FEEDBACK
4 / 22
PRIVACY FROM BLOCKCHAIN OBSERVERS
CATEGORY SCORE
12 / 43
PRIVACY FROM NETWORK OBSERVERS
2 / 22
PRIVACY FROM TRANSACTION PARTICIPANTS
3 / 13
PRIVACY FROM PHYSICAL ADVERSARIES
1 / 4
PRIVACY FROM WALLET PROVIDERS
16 / 17
+
−

Users must learn to back up their wallets. (Follow the steps during the ‘back up’ phase, and write the ‘seed’ only in paper, not in a text note on your pc or any other part of your pc, unless you use a very secure password manager). Lite client, does not require downloading the full bitcoin blockchain.

User interface can be confusing and it does not follow most modern design models.

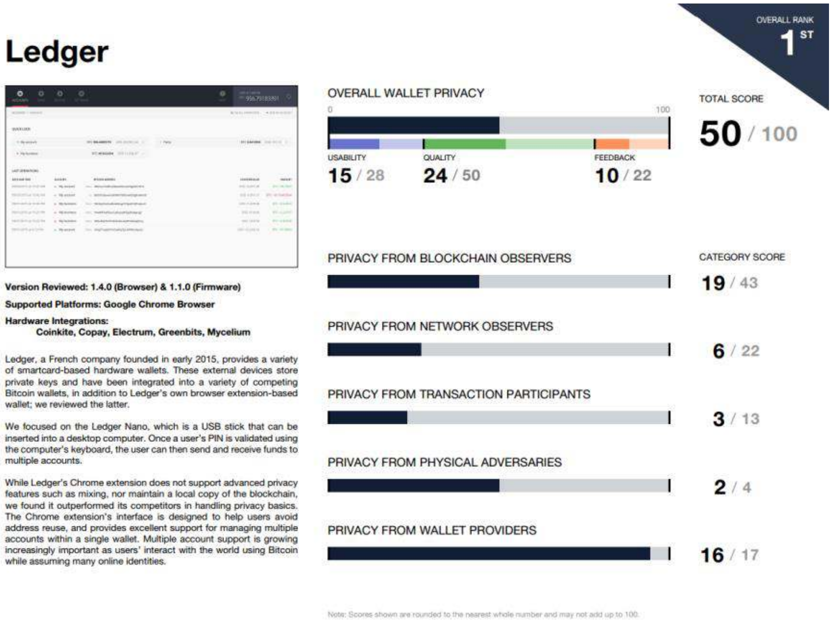
Security: Software wallet with hardware wallet integration. Syncs with Ledger Nano, and Trazer. Allows 2-factor authentication and multi-signature addresses. Uses HD privacy architecture.

Ledger Wallet Hardware

Ledger Wallet is on the cutting edge of hardware wallets. Which are believed to be much more secure than software wallets as the key components rest on a USB device with its own microprocessor. Ledger also uses a three factor authentication, which requires a pin, the USB device and a card that has an allegedly unique combination of numbers and letters, making up part of the encryption process. Long story short, Ledger is hard core and it is what I personally use. Learn more on their site.

Cost: $35 USD minimum. Latest model is $50 USD.
https://www.ledgerwallet.com

Privacy: 50/100 (winner of ranking march 2016 OBPP, uses HD Wallet and can be used with Mycelium. Combining two great technologies can be even more effective. It also has its own software wallet interface to help users interact with their hardware wallet.



Ledger

Version Reviewed: 1.4.0 (Browser) & 1.1.0 (Firmware)

Supported Platforms: Google Chrome Browser

Hardware Integrations:
Coinkite, Copay, Electrum, Greenbits, Mycelium

Ledger, a French company founded in early 2015, provides a variety of smartcard-based hardware wallets. These external devices store private keys and have been integrated into a variety of competing Bitcoin wallets, in addition to Ledger's own browser extension-based wallet; we reviewed the latter.

We focused on the Ledger Nano, which is a USB stick that can be inserted into a desktop computer. Once a user's PIN is validated using the computer's keyboard, the user can then send and receive funds to multiple accounts.

While Ledger's Chrome extension does not support advanced privacy features such as mixing, nor maintain a local copy of the blockchain, we found it outperformed its competitors in handling privacy basics. The Chrome extension's interface is designed to help users avoid address reuse, and provides excellent support for managing multiple accounts within a single wallet. Multiple account support is growing increasingly important as users' interact with the world using Bitcoin while assuming many online identities.

OVERALL RANK
1 ST
OVERALL WALLET PRIVACY
0
100
USABILITY
15 / 28
QUALITY
24 / 50
FEEDBACK
10 / 22
TOTAL SCORE
50 / 100
PRIVACY FROM BLOCKCHAIN OBSERVERS
CATEGORY SCORE
19 / 43
PRIVACY FROM NETWORK OBSERVERS
6 / 22
PRIVACY FROM TRANSACTION PARTICIPANTS
3 / 13
PRIVACY FROM PHYSICAL ADVERSARIES
2 / 4
PRIVACY FROM WALLET PROVIDERS
16 / 17

Note: Scores shown are rounded to the nearest whole number and may not add up to 100.

Difficulty: Medium. Once you do a backup of your 'seed' which is where you bitcoin rest. Then it's a matter of doing one transaction and you are good. The guide is very user friendly and teaches you how to use the Ledger hardware wallet. However, the multifactor security process means that it takes 2-4 minutes to prepare for a transaction depending on how fast you are. Not as fast as using a software wallet. A common approach seems to be to use higher security wallets for most funds, and a mobile software wallet for spending funds and smaller amounts.

Security: Multifactor authentication hardware wallet. (Requires users to have 3 items to sign transactions). The USB device, special card that has scrambled symbols, used to complete the encryption algorithm in the device and a pin number. Users are prompted to back up their HD seed during initial setup. If any of the items are lost, the bitcoins can be recovered with the seed + the pin.

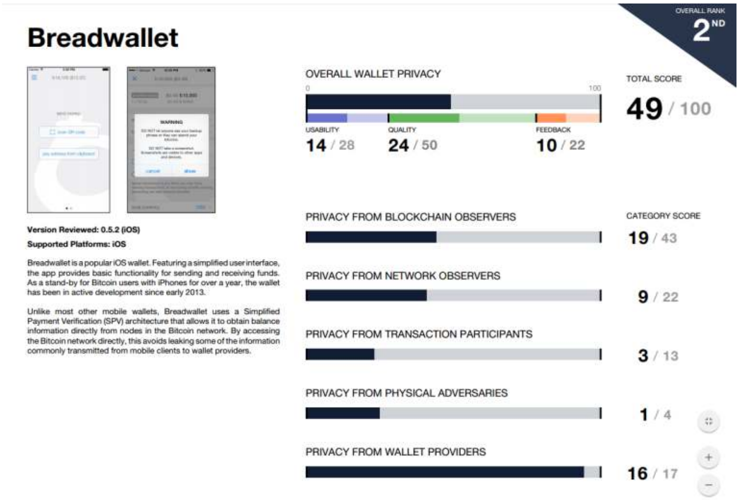
Has its own software wallet, but can be synced with Mycelium, Electrum, Greenbits and Copay.

Breadwallet iOS

Rated as the second most private bitcoin wallet by OBPP and recommended by friends as the way to go for iOS, Breadwallet seems to cover all the basics when it comes to bitcoin privacy, while keeping it simple and even going beyond the basics.

Cost: Free

Privacy: 49/10, ranked #2 in OBPP privacy rankings in March 2016. Breadwallet has been recommended to me as one of the best wallets for iOS.



Breadwallet

Version Reviewed: 0.5.2 (iOS)

Supported Platforms: iOS

Breadwallet is a popular iOS wallet. Featuring a simplified user interface, the app provides basic functionality for sending and receiving funds. As a stand-by for Bitcoin users with iPhones for over a year, the wallet has been in active development since early 2013.

Unlike most other mobile wallets, Breadwallet uses a Simplified Payment Verification (SPV) architecture that allows it to obtain balance information directly from nodes in the Bitcoin network. By accessing the Bitcoin network directly, this avoids leaking some of the information commonly transmitted from mobile clients to wallet providers.

OVERALL RANK 2ND

OVERALL WALLET PRIVACY

USABILITY 14 / 28

QUALITY 24 / 50

FEEDBACK 10 / 22

TOTAL SCORE 49 / 100

	CATEGORY SCORE
PRIVACY FROM BLOCKCHAIN OBSERVERS	19 / 43
PRIVACY FROM NETWORK OBSERVERS	9 / 22
PRIVACY FROM TRANSACTION PARTICIPANTS	3 / 13
PRIVACY FROM PHYSICAL ADVERSARIES	1 / 4
PRIVACY FROM WALLET PROVIDERS	16 / 17

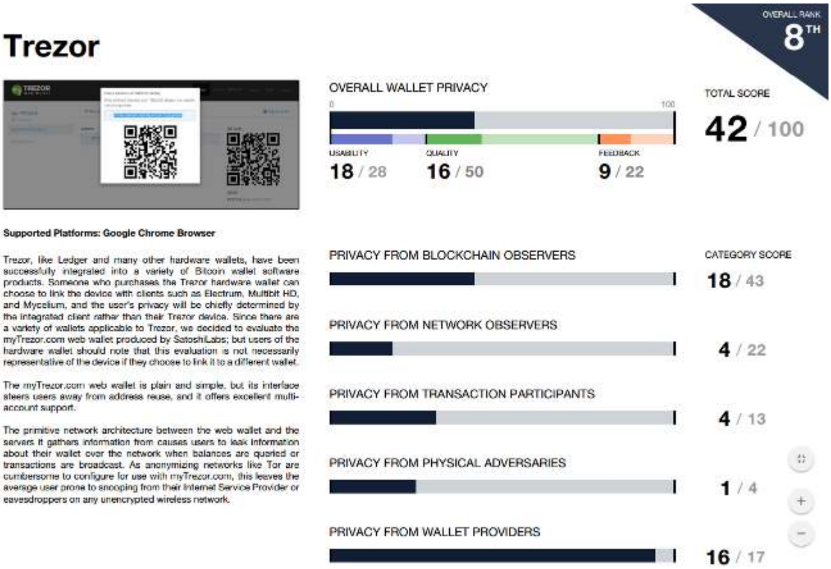
Security: Software wallet with HD privacy architecture.

Trezor Hardware

Trezor is one of the first hardware wallets to enter the Bitcoin market. Similar to Ledger Nano, it is designed to never expose your private key to the computers it connects to, so much so that the Trezor company goes as far as saying that it does not matter what computer you connect it to, even if it’s at an internet cafe. Trezor development is allegedly open source. I have not tested it personally.

Cost: $100 USD

Privacy: 42/100, ranking at #8 on March 2016’s OBPP report. Uses HD architecture which protects users from address reuse.



Trezor

OVERALL RANK 8TH

OVERALL WALLET PRIVACY

TOTAL SCORE 42 / 100

USABILITY 18 / 28

QUALITY 16 / 50

FEEDBACK 9 / 22

Supported Platforms: Google Chrome Browser

Trezor, like Ledger and many other hardware wallets, have been successfully integrated into a variety of Bitcoin wallet software products. Someone who purchases the Trezor hardware wallet can choose to link the device with clients such as Electrum, Multibit HD, and Mycelium, and the user's privacy will be chiefly determined by the integrated client rather than their Trezor device. Since there are a variety of wallets applicable to Trezor, we decided to evaluate the myTrezor.com web wallet produced by SatoshiLabs; but users of the hardware wallet should note that this evaluation is not necessarily representative of the device if they choose to link it to a different wallet.

The myTrezor.com web wallet is plain and simple, but its interface steers users away from address reuse, and it offers excellent multi-account support.

The primitive network architecture between the web wallet and the servers it gathers information from causes users to leak information about their wallet over the network when balances are queried or transactions are broadcast. As anonymizing networks like Tor are cumbersome to configure for use with myTrezor.com, this leaves the average user prone to snooping from their Internet Service Provider or eavesdroppers on any unencrypted wireless network.

	CATEGORY SCORE
PRIVACY FROM BLOCKCHAIN OBSERVERS	18 / 43
PRIVACY FROM NETWORK OBSERVERS	4 / 22
PRIVACY FROM TRANSACTION PARTICIPANTS	4 / 13
PRIVACY FROM PHYSICAL ADVERSARIES	1 / 4
PRIVACY FROM WALLET PROVIDERS	16 / 17

Difficulty: Easy. With a two button interface and multiple wallet options to sync to, it allows users to use wallet interfaces they are more familiar with and claims to keep the new hardware security steps simple.

Security: Hardware wallet. Trezor is widely regarded as a great innovation in financial security and the equivalent of a vault for your bitcoin. Similar to Ledger nano, if it is lost, the user can restore from an HD seed. To make a transaction, the user needs the Trezor device and a pin number. More complex setups can also be created through advanced settings, including secret wallets that are password protected.

Pin protection means that even if the Trezor wallet is stolen, it will take years for the hacker to guess the pin, as every guess increases the time he must wait before the new attempt, according to Trezor documentation.

AirBitz Android, iOS

Paper Wallet

Paper wallets were among the first cold storage solutions for Bitcoin security. Cold storage means that the private key that stores the bitcoins is generated on a device or some other mathematical method, which is disconnected from the internet. Without internet connection, the chances of external hacking goes to zero - something attractive to those seeking the highest standards of digital security.

In exchange for this digital security, users must then secure the paper wallet from physical attacks, if it is stored on paper. Or whatever the means of storing these data are. Protection from physical theft is generally considered a more intuitive and understood problem.

Cost: Free

Privacy: Low. It can be high, but requires transfer of all funds to new bitcoin paper wallet after every withdrawal. This being a manual and potentially laborious process makes its ease of use low. It also does not facilitate the generation of a new address per every deposit, so in general it is not the most private of bitcoin solutions.

Difficulty: Advanced. Requires basic understanding of bitcoin wallet cryptography. In essence, you must know that Bitcoin wallets are algorithms with a ‘public address’ and a ‘private key. These can be generated offline, using open source mathematical standards.

Requires basic understanding of web browsing among other technical concepts.

Security: Cold Storage, with multi-signature potential. It allows for cold storage and even better multi-signature cold storage, it is generally considered among the highest standards of digital security. In exchange, users must secure the paper wallets well from physical attackers, but that is generally considered easier and more intuitive for most people.

The following recommendation on how to create Paper wallets securely, was written by Bitcoin researcher Pontus Lindblom, on his website:

http://startusingbitcoin.com:

A paper wallet simply means that you store your secret private key either in plaintext or encrypted on a piece of paper. This is a good way to store large amounts of bitcoins safely in cold storage. You should always try out your storage method with a tiny amount of bitcoins before you transfer any larger amounts to make sure that everything works the way you intended and that you can transfer the bitcoins out to another address at a later time. For added security, you can also divide the keys and store them on different papers in different locations so that you need M of N (e.g. 2 of 3 or 5 of 7) of the partial keys in order to transfer the bitcoins out of cold storage. If you want to take this advanced approach you can split the keys using the Shamir's threshold secret sharing scheme using the open source tools available at PassGuardian. Here are two good sources for creating paper wallets.

https://www.bitaddress.org

This is a good open source tool for generating secure offline bitcoin wallets, but it doesn't explain best practices of doing so on the web page itself. Here is an excellent guide that walks you through all the steps and pitfalls that you should know about for generating paper wallets so that you end up storing your bitcoins safely.

https://bitcoinpaperwallet.com/

This is another good option which is open source and based on the above bitaddress.org open source code and it also explains how you should generate your paper wallets safely offline.

8. RESOURCES

Bitcoin Wikipedia on Satoshi Nakamoto

Available at: https://en.bitcoin.it/wiki/Satoshi_Nakamoto

Bitcoin London 2012: Mike Hearn

Available at: http://www.youtube.com/watch?v=mD4L7xDNCmA

Andresen, Gavin. “Is Store of Value Enough?” July, 2012. ç

Available at: http://gavinthink.blogspot.com/2012/07/is-store-of-value-enough.html

Omega Tau Podcast Ep. 59: Bitcoin: A Decentralized Currency, with Gavin Andresen

Available at: http://omegataupodcast.net/2011/03/59-bitcoin-a-digital-decentralized-currency/

O'Connell, Justin, “The Mathew Effect,” GoldSilverBitcoin, 2013

Available at: https://www.goldsilverbitcoin.com/mathew-1312-bitcoin-style-the-rich-get-richer/

Vorhees, Erik. “Bitcoin – The Libertarian Introduction,” *Evorhees*, April, 2012.

Available at: http://evoorhees.blogspot.com/2012/04/bitcoin-libertarian-introduction.html

Stacke, Jonathon. “Mapping Bitcoin Adoption,” *The Genesis Block* May, 2013.
Available at: http://thegenesisblock.com/mapping-bitcoin-adoption-a-global-perspective/

Reddit Post. Available at:
http://www.reddit.com/r/Bitcoin/comments/1do53k/at_this_very_moment_bitcoin_is_blowing_up_in/

SEC Filing, Winklevoss Trust.
Available at:
http://www.sec.gov/Archives/edgar/data/1579346/000119312513279830/d562329ds1.htm

Hashcash.org
Available at: http://www.hashcash.org/bitcoin/

Omega Tau Podcast Ep. 59: Bitcoin: A Decentralized Currency, with Gavin Andresen
Available at: http://omegataupodcast.net/2011/03/59-bitcoin-a-digital-decentralized-currency/

Krantz, Matt. SecondMarket Jumps To Give Bitcoin Legitimacy, *USAToday*. February, 2014.
Available at:
http://www.usatoday.com/story/money/business/2014/02/26/secondmarket-bitcoin-exchange-trading/5840593/

Brandon, Russell. A String of Thefts Hits Coinbase, *The Verge,* January, 2014.
Available at: http://www.theverge.com/2014/2/7/5386222/a-string-of-thefts-hit-coinbase-bitcoins-most-reputable-wallet-service

BitPayNews
Available at: http://www.coindesk.com/companies/bitpay/

Rubens, Paul. Bitcoins and virtual currency – how do businesses cope, *BBC,* January, 2014.
Available at: http://www.bbc.co.uk/news/business-25809011

Mt. Gox Continues To Crumble, *Silicon Angle,* March 2014.
Available at:
http://siliconangle.com/blog/2014/03/05/bitcoin-weekly-2014-march-5th-mtgox-continues-to-crumble-flexcoin-and-poloniex-hacked-zeroblock-gets-rtbtc/

Library of Congress Report, Regulation of Bitcoin In Selected Jurisdictions
Available at: http://www.loc.gov/law/help/bitcoin-survey/

FinCen Guidelines On Bitcoin
Available at:
(http://www.fincen.gov/financial_institutions/msb/materials/en/bank_reference.html)

9. CONCLUSION

This short book has been offered as a primer for those who want to know more about bitcoin. But in presenting it simply, I’ve purposefully not emphasized in detail the larger reasons why bitcoin and other upcoming cryptocurrencies are so important to our future and prosperity.

It’s not merely that bitcoin constitutes an effective alternative currency. It has to do with what bitcoin serves as an alternative TO. And that something is monopoly central banking in which a handful of people debase currency on a regular basis while pretending to help people build more wealth.

Bitcoin allows us to save, buy and sell “money” that is under our control not central banking’s. As our current group of currencies continue to devalue around the world, bitcoin and other cyrptocurrencies will accumulate value against them. This is yet another powerful reason to learn about bitcoin and beging using it.

In postings on my website, TheDollar Vigilante, we regularly discuss monetary affairs, especially from a central banking government spending and debasement standpoint.

If you’ve enjoyed this book and want to receive current bitcoin news as well as information about new and emerging cryptocurrencies, please visit *www.TheDollarVigilante.com/subscribe.*

Not only do we offer the most recent and pertinent geo-political and financial news, but when you become a member you will get access to specific portfolio recommendations with individual investment picks – some of which are cryptocurrencies.

We do a lot of the painstaking technical research so you don't have to. As we mentioned in the beginning of this book, block chain technology is much like the beginning of the internet, generally not many know about it or fully understand it.

With this "infancy" comes a myriad of investment opportunities. Part of our job is to help you sort through and narrow down your options to those that are most viable and worthwhile. You've finished this book, not put your newfound knowledge and heightened interest to good use. I'll look forward to you joining us.