what the

GOVERNMENT

doesn't want you to know about...

BITCOINS

The Bitcoin Bible:

The Safest and Easiest Ways to Buy, Sell, Store, and Speculate

What Is Bitcoin?

The world of Bitcoin is today one of the most promising, confusing, erratic sectors of the emergent world economy. So it will be for years to come because Bitcoin is in its infancy. Currently, it operates as digital payment system. Its efficiency far surpasses any other method of sending and receiving money. Its operation makes PayPal seem old fashioned and clumsy.

But its potential is actually far greater. It seeks to be a competitor to all existing government currencies. Indeed, it could eventually replace them. In time, Bitcoin and other "crypto-currencies" could reinvent the monetary and financial world from the ground up — on the basis of human choice rather than government imposition. But for now, the primary users and enthusiasts of this nascent digital currency belong to the young generation raised in a world swimming in computer code.

How can we know it has a future?

Consider the modern trajectory of digital innovation. In the last 20 years, letters have become email, television has become YouTube, and telephones have left the wall socket and become pocket video phones. This is the digital revolution, and it has been accomplished by the free market, not by government. It was not a "plan"; it is something that came about through trial and error through the commercial marketplace.

Bitcoin is in a similar position to what email was like in 1990 or so. Hardly anyone understood how it worked or why we would need it. Most email addresses were long numbers like 34243920@compuserve.com. There were only a few commercial services around. You had to dial up and connect to send and receive. Servers crashed. Messages were awkward because people didn't know how to use email. Then the spam problem came. That was followed by the terrible problems with viruses.

The purpose of Bitcoin is to serve as a digital-age payment system, evolving one step at a time into an independent money to compete with that forced on us by the nation-state.

At any point in the evolution of email, there were people who doubted it would amount to anything at all. It would never replace the letter, people said. It was insecure, we were told. It was too much trouble, people thought. But gradually, over time, nearly every problem with email was solved, one by one. The technology stabilized. People discovered the great truth about software: A great technology is still great, even if the services using the technology need time to stabilize and get their act together.

Over time, of course, email won the day. Now it is indispensable. And there are new iterations that are making gigantic inroads, from Facebook and Skype messages to smartphone SMS systems. We navigate

the world with hand-held devices that speak directions and give real-time traffic data. We now take it all for granted. It wasn't always so. Not even the science fiction cartoon The Jetsons imagined the existence of email. But now it is a reality of the modern world. No one thinks a thing about it.

The next step is in this evolution is obvious: Money too needs to be reinvented. For a hundred years, the dollar has been essentially nationalized by the government and the central bank. Now there is market pressure for a money that leaves the world of government and enters the digital age. It needs to be liberated from the control of a politically appointed central bank and returned to the people.

Bitcoin is the most successful attempt so far to create such a currency. Silicon Valley venture capital is lining up behind it. Young people are saving in it and some are even earning salaries in it. It is subject of feature stories in every major newspaper. Websites that accept it are becoming more prominent and profitable. It is serving as a safe haven in economically unstable countries. Every day, more merchants are accepting it.

When it first appeared in 2009, people laughed and said it would go nowhere. Four years later, it is the subject of articles in all major financial publications. Transactions happen every second. Sums in the tens of millions are moved every day by individuals, and the entire market sector has a market capitalization exceeding $1 billion — a drop in the bucket as regard world finance, but far beyond what anyone believed was possible.

Most strikingly, no politician invented Bitcoin. No commission approved it. No central bank controls it. It has absolutely no political and bureaucratic vacuum. No social consensus came up with the idea. Its success or failure depends entirely on the market. It is not even owned or controlled by a single corporation. Its value is not tied to any existing currency, but rather seeks to be its own unit of account.

Bitcoin offers a path away from monetary controls. Once you move dollars into Bitcoins, the medium of exchange is released from the Fed's fetters. This has serious implications for the conduct of monetary policy. As *Time* magazine put it:

> If a future Fed chairman tries to repeat Ben Bernanke's policy of quantitative easing (effectively printing money), worried investors could start pulling their savings out of the dollar and send it streaming into the cloud so fast that the Fed would be forced to change course... Once alternative currencies are frictionlessly available on the Internet, every laptop will become its own Cayman Islands.

In short, if the promise of Bitcoin comes to fruition, we could be watching the birth of a new global currency, one that can compete with and even replace the failed experiment in government paper currency.

If it doesn't succeed, the experience of Bitcoin itself will inspire the creation of new attempts at creating digital currency units that trade on the free market, rather than depend on governments.

To properly understand Bitcoin, you must keep in mind that its purpose is not to serve as an investment vehicle. It is an entrepreneurial invention, somewhat like the steam engine, the railroad, steel, or email. It is a pure software, based on what is called cryptography (a lynchpin of Bitcoin because it allows for privacy and unique identifiers for both coins and owners).

That technology is a payment system that is evolving as a real money. Right now its most spectacular use is in transferring funds from one person to another. It is as easy as sending a text message on a phone.

That said, all technologies are introduced into society through the commercial marketplace. That means speculation will always be part of its development — just as it was with railroads. Also part of the market will be mistakes, surprises, failings, setbacks, but also progress, triumph, and ultimately greater human satisfaction.

All the while, there will be many people who see Bitcoin and all digital currencies as a get-rich-quick scheme. People will get rich while many others will lose their shirts. But who will see the bigger picture? The trend of economic history is clear. The pressure to replace government currency with a modern alternative is intensifying every day. There will be no stopping a technology whose time has come.

Background

Bitcoin is a decentralized electronic currency conceived in 2008 by a person or group known only as "Satoshi Nakamoto." His — or their — true identity is unknown. Nakamoto introduced the idea and the code, answered questions on an Internet forum. He wrote mostly about code but he sometimes branched out into economics and politics. His ideological orientation is indisputable: he is a believer in free markets and an opponent of government paper money. His invention was motivated by those convictions. Once his invention started to gain market traction, he disappeared without a trace.

Nakamoto designed the software that manages the currency network, along with the network that supports it. Anyone can look at the underlying code. It is not "owned" by any one group or business or individual. The Bitcoin network is controlled directly by the individual owners themselves, a system known as peer-to-peer (P2P).

The motivation being its creation tapped into a sense that most close observers have of government money. Nakamoto argued that government money relies too much on people's trust of their political elites and the system that they established. It is constantly mismanaged. No one knows what the banking elites are going to do next. It is not an open system. It is inflationary. It creates booms and busts. To top it off, it is expensive.

In contrast to the majority of other currencies, the functioning of Bitcoin is not dependent on a centralized institution. Anyone can start an exchange, retail shop, or website that tracks prices and exchanges. All of these draw from a database that is publicly distributed. The software designed by Nakamoto uses cryptography to provide security, such as the guarantee that Bitcoins may only be spent by their owner, and never more than once.

Bitcoin is one of the first implementations of the concept of crypto-currency, and without a doubt the most successful to date. Nakamoto's major achievement is the solution of the problem of double-spending in a decentralized system, which had been a major cause for concern for economists and programmers alike.

Even in the mid-1990s, programmers were talking about the need for a digital currency, but each attempt

faltered because there was no way to prevent the unit from being copied — that is, to prevent fraud.

The Internet specializes in making copies. But in the area of money, copies are the kiss of death. It leads to inflation and instability and finally destroys the value of all existing currency. What we need is a money stock that is fully transparent and predictably fixed at some point in time.

Bitcoin was the first successful attempt to control copying. To prevent a Bitcoin or any fraction of a Bitcoin from being spent more than once by the same person (in other words, to avoid fraud), the network uses what Nakamoto describes as a *distributed time-stamp server*, which identifies and sequentially orders the transactions. Every Bitcoin is assigned an owner. This prevents their modification.

The history of all Bitcoin movements remains stored in what's called the blockchain, a database that maintains a record of all transactions in the network. This information is stored in "nodes," which are nothing more than computers executing the Bitcoin software worldwide, connected to each other via the Internet. In other words, if you use Bitcoin, you are a node.

Even though Bitcoins are sent instantly and any operation may be monitored in real-time, the individual transactions are shown on screen when using the Bitcoin software that chronicles the clearing process.

Worldwide, there are between 25–50 million Bitcoin transactions taking place per day. That is small compared with government currencies, but not insubstantial. You can watch Bitcoin transactions in real-time at *blockchain.info*. For a fun site on which to listen to music made of Bitcoin transactions, see *ListentoBitcoin.com*.

These exchanges are confirmed and verified by the software. The greater the number of confirmations, the more remote is the possibility of being a victim of double-spending. When a transaction exceeds six confirmations by the network, a transaction is considered technically irreversible.

How reliable is it?

To date, there is not a single documented instance of double-spending in Bitcoin. It is possible for a computer attack to hit a particular exchange, but the system as a whole cannot be hacked. So far, no one has seen a way for it to be possible for more Bitcoins to be assigned to more owners.

As a payment system that transfers funds from one person to another, it is extremely efficient. The payment is logged by the software before the network verifies that it is real and sound and then confirms the transaction. The majority of receivers and retailers who accept Bitcoins are satisfied with one single confirmation. For small amounts, it's even reasonable to accept transactions instantly, even before they are confirmed by the network.

The information that allows users to control Bitcoins in their possession can be stored in any electronic medium, such as personal hard drive, memory cards and sticks, CD, Web mailbox, etc., or in websites that offer "Bitcoin accounts."

You can keep this information on printed paper. You can even carry around such pieces of paper and use them for tippigg the wait staff at a restaurant, for example. You can even keep it in your mental memory. Bitcoin ownership can be transferred through the Internet to anyone with a "Bitcoin address,"

similar to the way an email is sent to an email address.

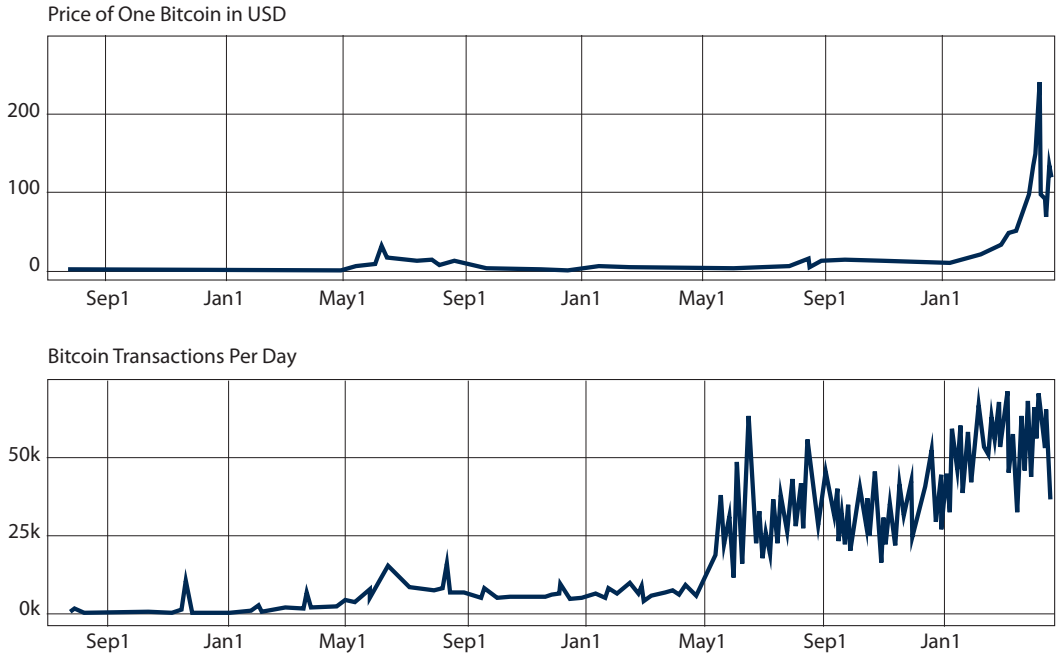
Thanks to Bitcoin's cryptographic architecture, a transfer between Bitcoin addresses is far more secure than a transfer between bank accounts (and that's not counting the risk implied by the mandatory third-party intrusion within the banking system).

As it develops, we will continue to see wild swings in the price as irrational exuberance gives way to despair and back again. Bitcoin has so far proven solid as a rock. The software infrastructure built around Bitcoin will grow, fail, develop, grow, and fail again. This will happen for a long time, just as it did with email, Web media, and cellphones.

Also, as is common in these cases, some people will write it off as a failed experiment on the first dip. This has already happened in the history of Bitcoin. In 2011, the price collapsed from $30 down to $2. Even technical publications wrote it off as a failed experiment. Then it went through a revival, shooting up astronomically until the existing Bitcoin exchanges couldn't handle the load. That led to panic selling again. This could happen many more times before the market completely shakes itself out.

Remember that Bitcoin does not trade at a fixed relationship to any other currency. It is designed to be a floating currency that competes with all others. For that reason, its value will be forever fluctuating. This feature is what alarms many potential users. It acts like a wild stock and no one has any solid basis for understanding its current and potential valuation. That said, plenty of venture capitalists and many large investors are already deeply involved in the Bitcoin market.

Here is a complete picture from July 2010 to the present (April 11, 2013). You can see the wild run-up, but then a settling down at an exchange ratio of eight times its price on Jan. 1, 2013. It's been a rocky road, but the overall increase of 800% is a phenomenal increase.



Such swings in a new market are to be expected. The first run-up and dip of Bitcoin happened as more retail outlets came online and silver fell in price. The huge run-up from $15 to $266 occurred in the midst of the Cyprus crisis and bailout. We can probably expect another upward sweep during the next

currency crisis, wherever it happens to be, followed by yet another sell-off. So far, each run up and down and resulted in a new stable zone higher than it was previously.

These are the convulsions of a new currency being born. Free markets are always in a state of flux, with buyers and sellers forever participating in the process of price discovery. This is particularly true in nascent frontier markets, where early adopters meet with future waves of market participants, each with their own unique set of desires and expectations. Bitcoin has been called the "Wild Wild West" of the currency world, so it is not surprising that we should see violent swings in its price and disruptive innovations in the infrastructure serving the economy.

Left alone, markets undergo the process of "creative destruction" at breakneck pace... and they are all the better for it.

The short price history is that Bitcoin languished for most of its three-year history until it suddenly took off in March 2013, mostly in conjunction with the banking crisis in Cyprus. It shot up and fell back, but still remains at a very high point relative to its history. These gyrations have confused many people. What is the correct dollar-to-Bitcoin exchange ratio? No one knows for sure right now, just as no one knows the correct dollar-to-euro or euro-to-yen exchange ratio. This is for the market — and the buyers and sellers involved therein — to decide.

Is It Money?

People who use Bitcoin everyday treat it like money. Those who have no familiarity with it dismiss it entirely. Other commentators like Paul Krugman agitate against it on grounds that nothing can be money unless it is "legal tender" and controlled by a central bank.

It is true that the "peer to peer" nature of the Bitcoin network makes it impossible to establish a centralized control of the whole system. This prevents the arbitrary increase of the quantity of coins in circulation (which would cause inflation) and any other type of manipulation of their value on the part of the authorities.

The Bitcoin software (also known as "Bitcoin client") installed in users' computers transmits each transaction to nearby nodes, which in turn propagate it throughout the network. Invalid transactions are refused by honest clients (those who comply with the protocol). As yet, most transactions may be carried out free of charge, but it is possible to pay a transaction fee so that miners prioritize (speed up) their processing.

Where do new Bitcoins come from? They are "mined" the same way that gold is mined. This mining takes place when a computer works to verify transactions by solving complicated math problems. In the early days, the mining was easy. But the program is designed to make mining harder as more computers get involved in the process.

The idea here is to strictly restrain money creation. Every 10 minutes, a new block is added to the overall blockchain. Currently, each new block contains 25 additional Bitcoins. Every time 210,000 Bitcoins are mined, the production rate is halved. But just as there is only so much gold in the world, there are only so many Bitcoins.

In 2140, the total number of Bitcoins in circulation will reach 21 million. Their supply grows as a geometric series (at a constant rate). Already, more than half the total supply has generated. In 2017, three-quarters of the total supply will already be in circulation.

Bitcoins are divisible down to eight decimal points, and potentially more, which removes the practical limitations to price adjustment. In other words, one Bitcoin can buy you a cab ride or it could buy you a condominium in Manhattan, depending on the market valuation. If the value of Bitcoin rises that much, it is easy to denominate goods and services in ever smaller decimal units. If Bitcoin matures enough, its value will become independent of any existing monetary unit.

As of this writing, Bitcoin has a $1 billion-plus market capitalization. Still, the Bitcoin economy is tiny compared with well-established economies. Even so, all types of goods and services are currently being exchanged for Bitcoins, and there are many websites offering the exchange of almost every currency for Bitcoins through different funds transfer systems.

We aren't ready to say that Bitcoin is already money, though clearly many people (perhaps half a million or so) already regard it as such. But for it to be a universal money, there would have to be more general interest in its value independent of other currencies, and pricing would need to take place not based on the exchange rate, but on its own. That said, we are watching its moneyness emerge slowly, but steadily, exactly as gold and silver emerged in the past.

Why Bitcoin Is Hard to Understand

Even the most qualified people have trouble understanding how Bitcoin works, just as it might have been difficult to explain email 20 years ago. The reason for this is that Bitcoin challenges a series of concepts that have rarely ever been questioned before. We need to unlearn these suppositions before adopting better ones.

Even knowing that Bitcoin is superior to any other monetary system, many people tend to prefer that with which they are familiar, rather than venturing into unknown territory. The eternal battle between the conservative — who supports the theory of "better the evil you already know" — and the adventurer — who would rather go for the "good that is yet to be known" — takes place within all of us.

But once the legacy of misconceptions has been rejected and the inertia of habit has been overcome, the path becomes far easier for the adventurer, who will also pave the way for the conservative.

What are the ingrained habits that make Bitcoin appear implausible?

- We are used to seeing the act of paying as separate from the act of recording the payment. Through Bitcoin, nobody pays (nobody sends or receives Bitcoins); instead people modify balances in a sort of decentralized ledger (which is sort of like a big book). Thus, the act of paying is indistinguishable from the act of recording the payment;

- We are used to thinking that the monetary system needs to be guarded by a privileged caste of central bankers and regulators. The Bitcoin protocol does not protect

someone or some group in particular, but rather protects the tool itself and, therefore, all those who use it;

- We are used to our bank accounts being linked to our identity. Bitcoin addresses are anonymous if their owners so wish;

- We are used to transactions that are known in detail only by those directly involved in them (plus the third-party payment processor). With Bitcoin, information about all transactions is public and easily accessible;

- We are used to money as a receipt with more or less backing. With Bitcoin, the unit and the receipt are the same "thing," and impossible to duplicate or to falsify.

Will There Be a Crackdown?

One possible failure scenario for Bitcoin is that of a worldwide governmental campaign against the software and the sites that accept Bitcoins. The Financial Crimes Enforcement Network has already intervened to insist that miners and exchanges register the same way any currency trader does. The FBI is carefully watching Bitcoin for fear that it is a vehicle for money laundering. Other government agencies will certainly get involved, wanting to regulate and control.

What about the ultimate fear that government will simply outlaw digital currency? Given the nature of the system, the total elimination of Bitcoin (as that of any other P2P network) does not seem either technologically or economically viable. It is just not possible to rid the world of particular combinations of 1s and 0s. Government is powerful, but not that powerful. Even if something called "Bitcoin" were made illegal, the currency could be reinvented under another name.

There are certain factors mitigating against even the attempt. Large corporations are already accepting it. Venture capital has already put vast sums into development. It is a global, not a national, currency, meaning the difficulties of unified laws and enforcement are vastly more.

There's an additional factor here too. Bitcoin is the greatest tool ever invented for passing money from one party to another without a paper trail. This is something that politicians, bureaucrats, and government employees of all sorts in all lands desire very intensely — even more than regular citizens. It might remain untouched for that reason alone.

Nobody knows for certain what Bitcoin's destiny will be; the only thing we know is that the idea of a decentralized crypto-currency is here to stay.

The Technical Superiority of Bitcoin

Why is Bitcoin superior to government currencies? The quick answer: Because no one — no committee of "experts" — controls its destiny and because the rules set by the protocol devised by Satoshi Nakamoto are not imposed; each user chooses to accept them. Like a free society, Bitcoin manages itself. But what does this mean in practice for the user?

Let's list the advantages. Bitcoin:

1. Strengthens privacy by eliminating the interference of third parties in transactions.
2. Increases in supply at a predictable and slowing rate, helping to preserve — and possibly even increase — Bitcoin's purchasing power.
3. Lowers, or even eliminates, transaction costs on the Web. Fees and costs associated with current methods of exchange — Visa, MasterCard, and even PayPal — tend to hinder free exchange.
4. Simplifies and accelerates payments, dispensing with unwanted intermediaries.
5. Affords users anonymity, if they desire it.
6. Allows transfers anywhere, ignoring geographic and political barriers.
7. Fosters transparency: Although users are not forced to reveal their identities, all transactions are recorded in a freely accessible record so that errors can be spotted quickly.
8. Supports complex transactions (escrow, deposit insurance, guarantees, mediation, etc.) with solid cryptographic support for all types of rules and conditions that are freely agreed upon by the parties.
9. Is available nonstop: There are no holidays or weekends for Bitcoin operations.
10. Makes micropayments viable on a large scale.
11. Prevents the freezing of funds.
12. Prevents chargebacks.
13. Prevents the arbitrary restriction of goods and services that may be purchased.
14. Allows for the accumulation of huge fortunes within a very tiny space.
15. Can be easily hidden and does not need to resort to a third party for safekeeping and/or transfer.
16. Can be stored in multiple locations simultaneously.
17. Does not rely on a third party or a particular legal system to preserve its value.
18. Provides protection against all forms of theft, including taxes: The technology on which the Bitcoin protocol is based is several times safer than that used by banks and credit cards.
19. Cannot be removed by legal/computer attacks, due to its decentralized nature.
20. Cannot be forged.
21. Is easily and instantly recognizable.
22. Is infinitely divisible.

For quite a few reasons that no one any longer denies, email has replaced the postal service in all its primary duties. How many reasons in its favor does Bitcoin have to build up for fiat money to become obsolete? It could be rocky road forward, but there will be no letup in the pressure for the world to embrace precisely what Bitcoin represents.

OK, I'm In. What Should I Do to Get Started?

Now that you've seen the advantages, you might be ready to jump in. But before you do, remember that this market is far from being settled, and your own technical skill needs time to develop. It is best to start very small, just to get a feel for it. People who first enter this sector can sometimes make mistakes that result in lost coins. Even today's experts will tell you that "user error" has resulted in problems in the past. Start small; you can ramp up your holdings later on.

In addition, the Bitcoin industry is completely open and it will likely attract a sizable number of crooks and scam artists. For this reason, you should use only reputable sites. New companies will come along and proclaim themselves to be wonderful. Modern website design can make anything seem wonderful.

But here is a truth you must remember: All exchanges and websites are subject to crashing and hacking. With healthy competition, this will happen less and less over time. But in the intervening period, you should keep possession of your own Bitcoins and not trust an institution that claims to be a bank to keep them for you. One of the great advantages of Bitcoin is precisely that you do not need banks.

If, while you are exploring an option, anything strikes you as odd, if you see any strange pop-up advertising, if there is the slightest sign of trouble, back away. There are other places to go. Another glory of Bitcoin is that it allows you to move money almost instantly and with no fuss from one vendor to another and back again.

How to Get Started: Your Bitcoin Wallet

The first step in getting Bitcoins into your possession so that you can trade with them is to obtain a "wallet." The Bitcoin wallet is the file needed to send and receive Bitcoins. This file contains our Bitcoins, although in reality, it contains cryptographic keys (unique, secret, private keys) that make us owners of our Bitcoins and allow us to authorize payments (transfer the possession of our coins). The word *wallet* actually applies, however. It is the piece of equipment that keeps track of your Bitcoins and allows you to use them.

Getting one or more wallets is easy; here are the two most popular ways of doing it:

The Official Way

Bitcoin-Qt (the name of the official Bitcoin client) is a program that can be installed on any computer that runs Windows, Mac or Linux. You just need to download it from *Bitcoin.org* and install it. It will automatically create a wallet and will start downloading the transaction history (blockchain). You need only be online to send from this wallet; it's not necessary to be online if you just want to receive

Bitcoins. This method is used by the most technically sophisticated among users. Once you have this wallet, you can then sign up with an exchange. Two examples are *Mt. Gox* and the newer American exchange called *Tradehill*. Both are reputable and tested by users. More are on their way.

The Easy Way

In the old days of only two years ago, users had to have a high degree of technical expertise to use Bitcoin. Now there's a new generation of Web wallets that are very safe and easy to use. Their level of security relies on the fact that the private keys are encrypted in the user's browser, so the service provider will never have access to your Bitcoins.

The two best and most reputable wallets are available from *Coinbase.com* and *Blockchain.info*. These companies both offer free smartphone applications.

You should begin by downloading the smartphone application. Whatever you download to your smartphone you can (and should) duplicate on your desktop computer. That way, you have two ways to access your Bitcoin wallet.

The one we recommend is *My Wallet*, offered by Blockchain. If you don't want to go through the entire tutorial, simply do the following:

Download the Blockchain app on your device. Register with a 10-digit password. And that's it. Now you are ready to receive Bitcoins.

The detailed tutorial below describes the process using My Wallet from Blockchain.info. This is a tutorial for using the website edition, although the smartphone edition is the same. Again, we recommend doing both to ensure you have two ways to access your wallet.

Again, this is to date the easiest and most secure method.

Setting up Your Bitcoin Wallet — Tutorial

Go to *Blockchain.info/wallet*. Click on the "Start a New Wallet" button.

Fill in your alias and a password of your choice, and copy the CAPTCHA.

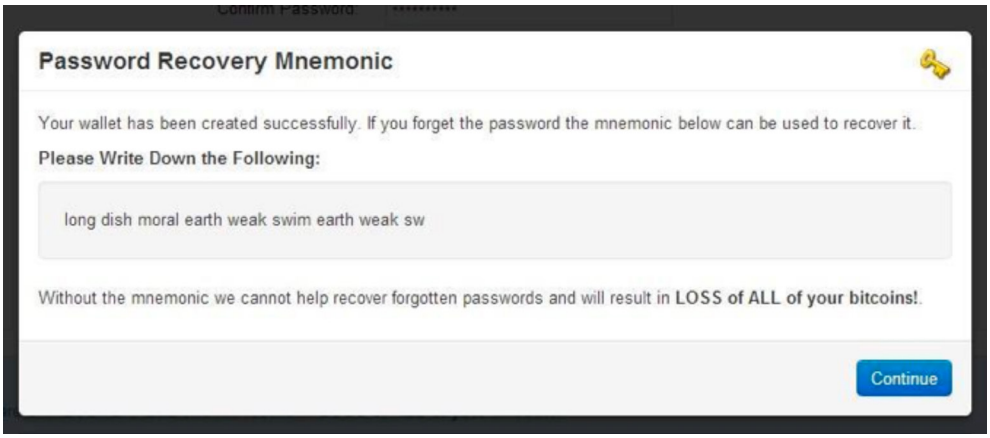
Regarding the password: Use at least 10 characters, do not include any words or names, and try to use uppercase letters, lowercase letters, numbers, and (ideally) other symbols. Try not to use "regular" words, because there are robots on the Web that use what are called "dictionary attacks" to rapidly try out passwords and attempt to guess yours.

For example, your password should not be johnsmith1. It should be more like j0hn5mi1h#. This is very important not only in signing up for Bitcoin, but for all your online dealings.

Whatever you do, don't forget your password. You cannot recover it.

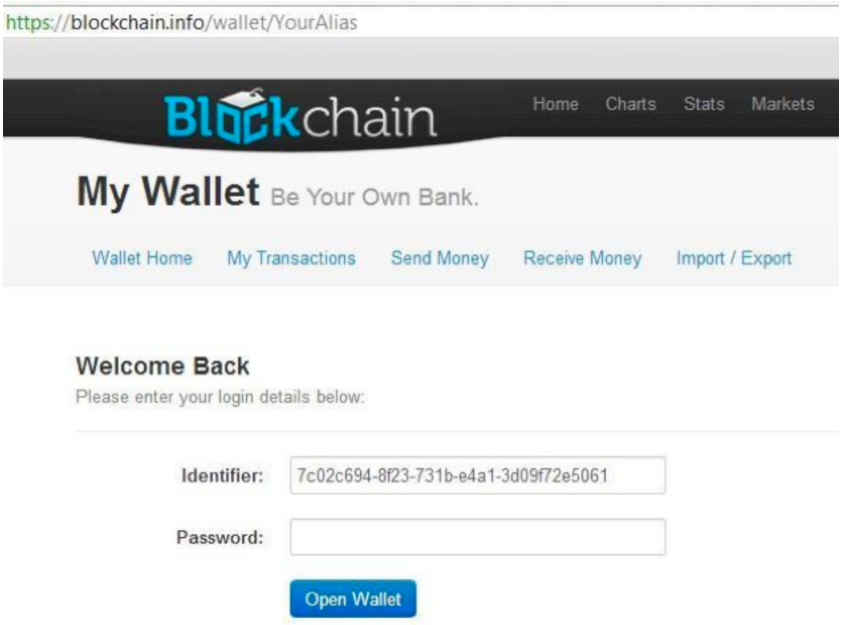
The next screen will present you with a mnemonic that you can use to retrieve your password in the future, in case you forget it. Make sure you write it down and make some copies.

It is important that you don't lose your password. If you do, you will lose your Bitcoins (Blockchain.info does not save this information).



The next screen you'll see will be the login page to your wallet. The URL should read *https://blockchain.info/wallet/YourAlias*. You will see two boxes: one for your wallet's identifier (a long string of characters, such as 0d683d57-b040-3d0c-f43e-0a83d15b0aef) and one for your password.

Enter the password you selected in Step 3 and you'll be taken to your wallet.



Congratulations! You're now inside your wallet.

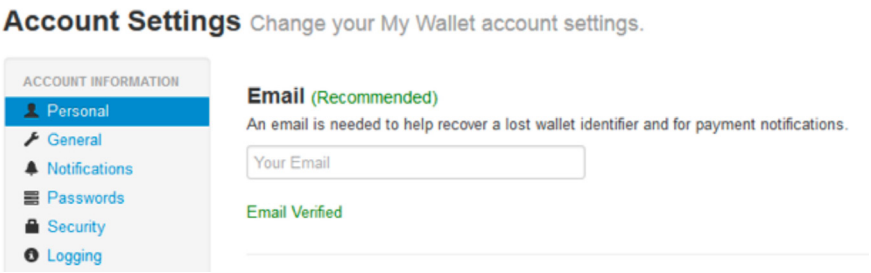
Next, you can go to your account settings, where you'll have access to your account information. In reality, there's no need to change any of the settings. Your wallet is good to go as it stands, with one exception.

Back up Your Wallet

You'll want an easy way to back up your wallet (something you should ALWAYS do). There are two ways to do this, with your email address or directly from your wallet.

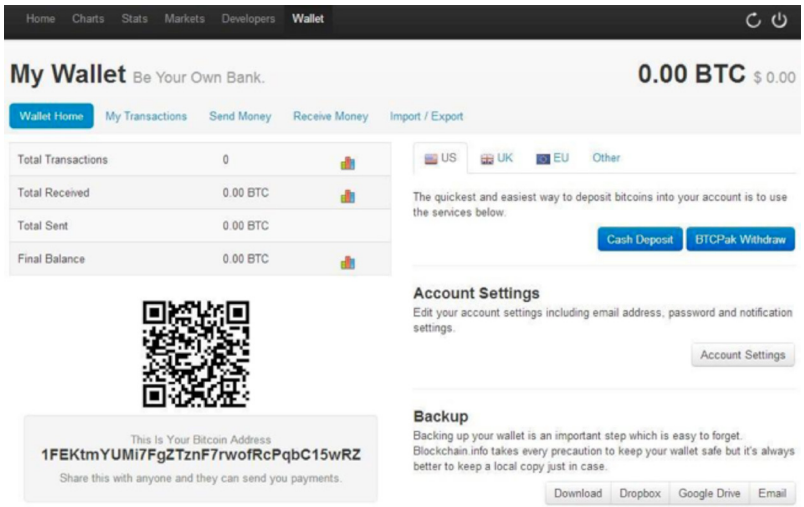
Backing up Your Wallet via Your Email Address

Do this by entering your email address in the space where it is requested. This will send a confirmation code, which you will need to enter in the "confirmation code box" below where you entered your email.



As soon as your email address is verified, you will receive your wallet's backup in your inbox. If you save your email, you are fine. If not, save this file somewhere safe and/or store it in the cloud. Even if the website (blockchain.info) disappears, you'll have access to your Bitcoins with this backup file.

Backing up Your Wallet via Your Wallet Home (if you don't want to use your email address):



Go to "Wallet Home." And at the bottom right, you'll see a "Backup" area with some buttons for downloading your wallet's backup. The "Download" button will allow you to save the backup file directly into your computer; the "Dropbox" button will connect to your Dropbox account to save the file there; same thing with the "Google Drive" button. The "Email" button is just another way to do what we described above.

Receiving Bitcoins:

Now this is the fun part. You have your wallet set up. Now you can actually receive Bitcoins. You can do this in one of two ways: Either you buy them from an exchange for paper money or someone gives them to you for trade.

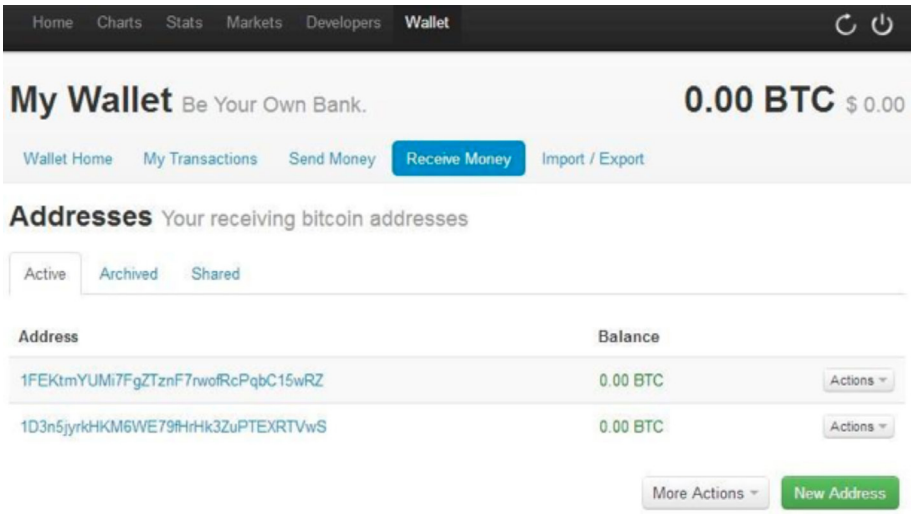
The easiest possible way is to find someone you know who uses them. Most anyone is happy to give away 0.001 Bitcoin just to get a new convert involved. This person will know all about scanning QR codes from phone to phone. This is the fastest and easiest way.

Anytime you are receiving Bitcoins, you need to use your Bitcoin address (the same information is stored in your QR code). In your wallet's Home, you'll see your Bitcoin address at the bottom left. It'll look something like this: 1BFyhVVBVG8EuK3Upv738Bqd7e8hmGmgxu.

This is the address you need to give to the person who's going to send you the coins (make sure you copy and paste it to avoid mistakes). You can create more addresses, which will all point to your wallet. It is very useful to have different addresses to organize your wallet. So you could have an address for your business, another for Bitcoin purchases, etc.

This is how you create them:

Go to “Receive Money.”



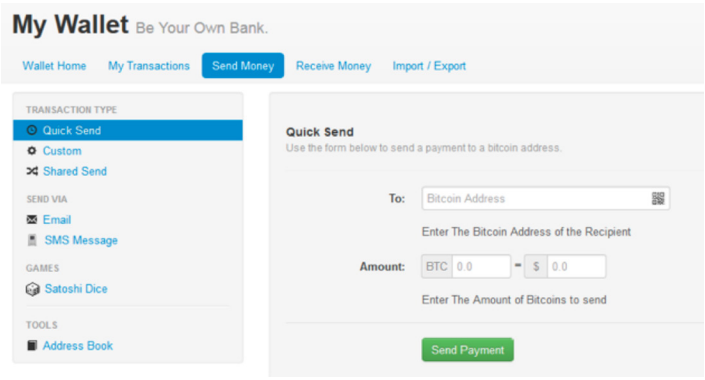
You’ll see your default address listed there (the same that showed on the wallet’s Home). Go to the bottom right corner and click on the “New Address” button.

A new window will pop up with a new generated address. Here you’ll be able to label your address as you wish (i.e., Business).

Your new address will show on the list. So next time you need to receive coins from a business-related transaction, you will be able to use this address and keep payments separated (you can create as many addresses as you want).

Sending Bitcoins:

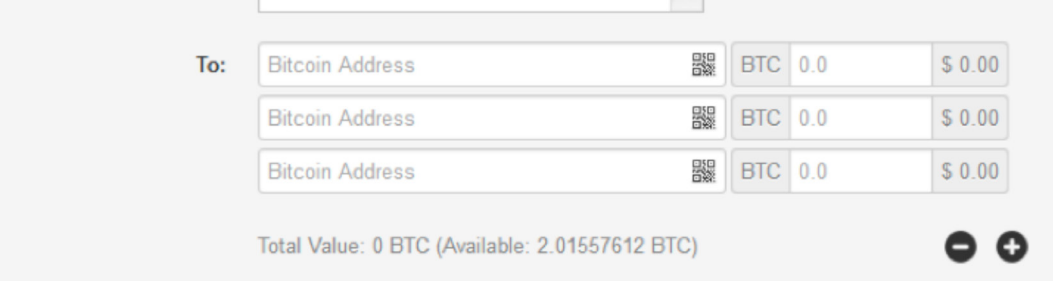
From your wallet’s Home, go to “Send Money.”



From here you can do a "Quick" send or a "Custom" send. If you just want to send some coins and you don't mind from which address they're going to be deducted, just use the quick option. Now, if you're sending coins related to your business activity, you might want to deduct the amount from the "Business" address you created. For this, you need to use the Custom send (just click on "Custom" at the left, under the Transaction Type dashboard).

Let's say you selected the Custom send. The first thing you'll need to do is select the address you'll be deducting your coins from (in our case, we'll select "Business" from the menu).

In the "To" box, you'll need to enter the address of the person you're sending the Bitcoins to (make sure to copy and paste the address to avoid errors). You can even send to multiple addresses if you click the "+" button to the right.



Next to the address, you'll need to enter the Bitcoin amount you are sending (i.e., 1.45BTC).

You can add a note to the transaction if you want. But be careful what you say: Anyone will be able to read it, since it'll be embedded in the blockchain.

There's also a drop-down menu to select to which address you want the change to be directed. Select the same one you are taking the funds from.

Hit "Review Payment" and confirm it if the information is correct.

You can access a history of all your transactions going to "My Transactions" at the top of your wallet's Home.

How Does a Bitcoin Wallet Work?

The Bitcoin Client will automatically generate a wallet that will contain a pair of public and (their corresponding) private keys. This is the way encryption works. For the purposes of the user, you only need to be concerned with your public key. The public keys are the ones you can see — the ones you give to the other party when you want to receive a payment. Private keys, however, are stored in your wallet (in the wallet.dat file).

Imagine your public addresses as being inviolable mailboxes that everyone can see and in which anyone can deposit their Bitcoins. Each public key is "opened" with a specific, impossible-to-duplicate private key that is stored on your software.

If you receive 1 Bitcoin, it has been sent to one of your public keys (or address). The only way to

transfer the ownership of that Bitcoin (to "send" it to another person) is by using the stored private key that corresponds to that public address.

As long as you keep the wallet, you'll possess the private keys that will allow you to use the Bitcoins controlled by that wallet. That's why it's a good idea to keep backups.

Once you have your Bitcoin wallet, there are several ways you can get more Bitcoins.

Exchanges and Trading Sites:

There are many sites where you can get small fractions of Bitcoins for free. These sites are filled with advertisements and can be tricky to use. They might be fun to play with, and there's nothing wrong with doing that, but they are not for people who are truly interested in using or saving Bitcoins.

You can also deal with a local dealer and trade cash for Bitcoins at a premium.

What you really need to do is sign up for an account with a real Bitcoin exchange. This requires linking your bank account the same way you would do electronic banking with a utility company, your cable company, or your credit card company. The steps you go through are the same. Think of the Bitcoin exchange as just another vendor you deal with.

The most known and used Bitcoin exchange to date is *Mt. Gox*. It handles 80% of all Bitcoin trade.

But there are many other sites that facilitate the exchange with all types of currencies and that support various systems for transferring funds. *BitInstant*, *Bitstamp*, *Bitcoin Nordic*, *Coinbase*, and *mercaBit* are just some that sell Bitcoins through hundreds of thousands of points of sale worldwide.

Of all these, Coinbase is the most popular because it easiest. Your bank will probably refuse Coinbase's attempt to connect until the account is verified. This happens in the usual way: Two small deposits will be made into your account. When they arrive, you put those amounts into Coinbase, and then you are linked up.

A new American exchange that is working hard to make Bitcoin more mainstream is *Tradehill*. All of the main exchanges today require a great deal of identity checking. You will face a double confirmation that you are, indeed, the owner of the bank account you link. For those who think of Bitcoin as a way to disappear financially, this process will show otherwise. All of these exchanges work very hard to legitimize their businesses.

In addition, there are sites that accept payments through Western Union or Liberty Reserve, like *Nanaimo Gold*. There are sites that accept gold and silver in exchange for Bitcoins (and vice versa), like *Coinabul*.

Please note: You can make new wallets and new accounts all you want. If you have a blockchain wallet and a Coinbase.com desktop and want to move the money, you can send from one to the other and back again — all without notable fees. This is vastly easier than making a regular account.

Accepting Bitcoins for goods and services:

Do you have a business for which you are interested in accepting Bitcoins? There are *many services*

out there that will help you set up an e-commerce solution to your business. *Coinbase* does this. But the most popular is *BitPay.com*

There are tens of thousands of vendors that accept Bitcoins, and the invaluable *Bitcoin Wiki* is updated by the minute to tell you who they are. For example, you can buy supplies for your business from Amazon with *BTC4amazon*. Or you can buy from the "Amazon" of Bitcoin itself: *BitcoinStore.com*.

Through them, you can:

- buy gift and debit cards (*CryptCard*, *BTCinstant)*
- buy precious metals (*Amagi Metals*)
- buy novelty physical Bitcoins (*CoinedBits*)
- trade equities (*MPEx*)
- buy gold and crude futures (*ICBIT*)
- get a website designed (*FarmGeek*)
- order flowers (*BitcoinForFlowers*)
- buy pharmaceuticals without a prescription and at half price (*JCM Pharmacy*)
- buy electronics and books (*Bitcoinin*)
- post classifieds (*BitcoinClassifieds*)
- buy survival food and storage (*Survival Food*)
- go to photography school (*Icon Photography*)
- buy beauty products (*Bitcoin Knotwork*)
- donate to charity (*BitCharity*)
- and thousands of other things…

This is only a tiny sample. Again, *Bitcoin Wiki* is updated daily with information on where you can use your Bitcoins.

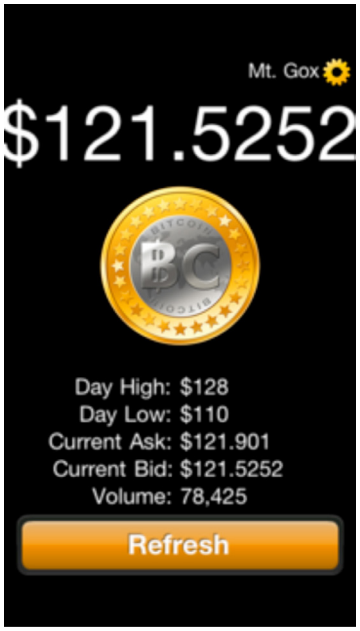
However, one of the most popular services in the Bitcoin world right now, sometimes credited with having made paying with Bitcoin mainstream, is *Bitspend.net.* Here you can put in any Web address from a commercial site and pay with Bitcoins, instead of dollars. This site is so popular that it crashed in its first week. Now it is stable and a wonderful way to use Bitcoins at any store you want.

Contrary to popular opinion, the retail and wholesale Bitcoin sector is actually better developed than

the exchange sector. It is possible to set a price in any currency and denominate it in Bitcoin automatically at current exchange rates so that the cost won't be affected by fluctuations.

Through *BitPay*, payments can also be automatically converted to the currency the merchant prefers. (So your customers can pay with Bitcoin, but you will receive dollars, if that's your choice. Many of the merchants accepting Bitcoin now are using this. Examples include WordPress, OkCupid, and Reddit. *Namecheap* is another good example of a company that is providing this.)

If you are interested in following just the dollar/Bitcoin exchange rate, there are innumerable apps you can download for free on your cellphone. They display prices like this:



Finding people willing to sell their Bitcoins:

You can locate people who want to sell by using services such as TradeBitcoin, LocalBitcoins, or specialized forums, among other places. There are many miners who sell their produce and local traders who buy and sell for a commission. It is very common for people to get together at some neutral location, such as a Wi-Fi cafe or restaurant.

If you have a friend who has a Bitcoin wallet, it is easy to move Bitcoins back and forth. You can get their Bitcoin address (they can email it or text it) and send Bitcoins that way with the push of a button.

Another way to send someone Bitcoins is by scanning their QR code (the square design that looks like a block barcode). It looks like a version of this:

Scanning this code puts their identifier in your send address. In the blank that allows you to specify the amount you want to send, be careful to put in the right amount. You might start with trying to send only a tiny amount, such as 0.001BTC.

If you are on the receiving end of the transaction, you need only hold up your code and ask your friend to scan it.

Once you trade with someone, you will be asked if you want to add this person to your address book, thereby replacing the long alphanumeric code with a simple name. This is a very good idea. That way you can have it for later dealings. You don't need to scan again. You should be fastidious about putting this information in your wallet. That way, you do not risk accidentally sending money to someone you did not intend to. All transactions clear in as little as a few seconds to as long as a few minutes.

These wallets are all in an early version of the software. As such, they are subject to human error. If you make a mistake, it cannot be undone. Such is the fate of every first generation of software.

Mining

Once upon a time, many people made lots of money mining Bitcoins. But due to the increased difficulty of obtaining Bitcoins through this means (related to the ever-increasing computational power being added by miners to the Bitcoin's network), nowadays, it is essential to have 1) a very high computational power and 2) use a mining pool to be able to have shared results.

It's been a long time since mining ceased to be within reach of the average PC user, and even the most powerful servers are being left behind by a superpowerful card called ASIC. More and more, mining is being left to specialists. *At this late stage, mining is not profitable for average users*. It will cost you more in equipment than you will earn.

Banks, Failures, and Cold Storage

With fiat money, we are used to fearing bank runs that come in wake of financial problems and bankruptcy. Even with deposit insurance, people worry that they won't get their money back. With Bitcoin, those fears largely evaporate, because every Bitcoin or fraction of a Bitcoin has an owner, and that owner directly controls its fate. There is no need for traditional banking in the way we've come to think about it.

Consider the case in April of the shutting down of a major Bitcoin exchange called BitFloor.com. It's account with its bank was closed for reasons no one yet knows. It put a sign on its website saying that it had stopped business. Many of its customers were very upset, but why? Because of the inconvenience. But the fear that the money would somehow not be there for all customers was nowhere in sight. The Bitcoin exchange rate was completely unaffected. It barely made the news.

The Bitcoin sector has given rise to certain kinds of warehousing functions. You can put your Bitcoins in what is called "cold storage." Let's say you own a large amount, say, 1,000 Bitcoin. You do not need instant access to them. In fact, you'd feel better if you did not. You can use any of the main services to put those in cold storage for safekeeping. You can even download your Bitcoins and keep your own cold storage on a thumb drive. You can even print out your Bitcoins and keep them in a safe place. Then, when you need them, you can transfer them back into online use.

How can you be sure that a company that is keeping your Bitcoins in cold storage will not use them for some other purpose? Every Bitcoin and every fraction of a Bitcoin has a unique identifier. The transactions that take place are all posted publicly on the blockchain. If they were ever moved, you would know instantly, and a permanent digital trail would exist. For this reason, it would be extremely

difficult, if not impossible, to steal any Bitcoin without the owner's knowledge.

Some Final Distinctions

The glory of the market economy is its instability. Perhaps that sounds strange to stay, but the truth is that a perfectly stable market is one where there is no growth, no advance, and no progress. There is only stasis. That is precisely the way governments like the world to work, because it allows them to control it, which means controlling you.

Markets thwart that desire completely. There are new ideas, new products, new technologies, new services, and new ways of doing business. This is essential. But this process is always trial and error. Nothing is perfect out of the gate. Enterprise is in a great position to learn from these mistakes, but the mistakes have to happen in order to provide that lesson.

In the future, we are likely to see the development of Bitcoin deposit insurance, more robust futures markets, insurance markets, instant micropayments for online services, a broad-based debit card market, a BTC-denominated stock market, and so much more. We are still in the infancy of this technology, which could not only create a new global economic sector, but could actually end up redefining the relationship between the individual and the state.

In the early days of the Internet, the technology was new and the providers were not prepared for its rapid growth. On the consumer end, of course, everyone expected everything to work perfectly. Speculators got involved, and the usual hysteria and the madness of crowds took over. At the first sign of trouble, overbought stocks crashed, people bailed, sentiment changed, and many people declared the new system dead.

Of course, the Internet did not die. It has been a source of economic growth for the last 15 years and it will continue this way. Those who placed their trust in the conventional wisdom — this new system can never work — ended up on the wrong side of history.

That same cycle seems to be repeating itself with Bitcoin. For the first two years of its existence, it languished at 14 cents to the dollar. Then, as its merits were discovered and retailers got involved, the software infrastructure could not handle the increased load. It became overbought, and panic selling ensued. All over social media and among those who doubt there is any merit to Bitcoin at all, there was widespread chortling and declarations that Bitcoin failed.

But these pronouncements missed a crucial distinction. There is a huge difference between Bitcoin as a technology and Bitcoin exchanges as institutions. Every single Bitcoin exchange could fail, but that says nothing about the success or failure of Bitcoin as a technology. It's like declaring railroads a failure because the train didn't arrive on time, or judging email to be bad because the earliest services were spotty.

Think back to the Pets.com fiasco of 2000. Just because this one company flopped did not mean that Internet commerce was dead. On the contrary, the death of this institution and many others taught lessons for others to follow.

So it is with Bitcoin.

Right now, 67% of Bitcoin trades go through Mt. Gox. If this company has technical trouble, the entire market is affected. This is a frustrating fact for many people in the whole industry. People are calling for more exchanges and a greater diversification of holding, and there will be more. There will be thousands of exchanges in the future.

The exchange rate crash from a high of $266 to a low of $50 in the course of 48 hours was linked to the failure of Mt. Gox, which had servers that became wildly overloaded. It didn't help being hit with distributed denial-of-service (DDoS) attacks at the same time. Such attacks usually originate from robots sending rapid-fire submissions through data-receiving portions of the website. Such attacks afflict every website in the course of its life, and they can only be prevented once they have occurred, allowing network administrators to customize the server against the most likely attacks.

But the DDoS hammerings of Mt. Gox in early April exacerbated panic selling and the dramatic price drop. So frustrated were the server's managers that they actually suspended trading for 12 hours, leaving only a handful of other exchanges and a very thin market.

This was not the first such case, and it won't be the last. Mt. Gox has already dramatically improved its server infrastructure since this event. But still, the faults of one exchange should not affect an entire industry so dramatically, which is why so many people are working toward diversification.

As Matt Ridley has written:

> It would be a mistake to write off Bitcoins as just another bubble. People are clearly keen on new forms of money safe from the confiscation and inflation that looks increasingly inevitable as governments try to escape their debts. Bitcoins pose a fundamental question: Will some form of private money replace the kind minted and printed by governments?

Even if Bitcoin does achieve that end, wild swings will continue to be part of this industry. This is why so many people are looking forward to new innovations, including Bitcoin ATMs. I actually used one of the prototypes while at a New Hampshire conference. They are currently being perfected for release in the coming months. Innovators are already looking at plugins for existing ATMs that will allow quick conversions. When this happens, people will be in a position to move in and out quickly.

Just keep this in mind: *Bitcoins are not conceived of as an investment vehicle. Until the market stabilizes and until you become technically adept at using them, you should never keep more money in Bitcoins than you can afford to lose.* Some people have made, and will continue to make, a killing on speculation. But you can't (and shouldn't) count on being among them. The exchange rate could take years to stabilize. During this period, it will respond to unpredictable events, such as bank failures. Even if the long-run pressure is for Bitcoin to become more valuable in terms of goods and services, we are likely to see more downward swoops as well.

On the other hand, venture capital is all over this market. As TechCrunch says:

> Bitcoin's record highs and the ensuring surge in hacking attempts and thefts may be

> grabbing headlines. However, beneath the chaos, Silicon Valley's best-known venture firms are finally starting to make real bets around the crypto-currency.
>
> The price of a single Bitcoin had more than quintupled to $265 amid a banking crisis in Cyprus and new signs from the U.S. Treasury's Financial Crimes Enforcement Network that regulators will tolerate the currency. It then settled back down to $120 as increased volumes and DDoS attacks hit the biggest Bitcoin exchanges today and yesterday. While anyone who has ever worked in trading knows that a chart like this often ends in a world of pain, there is a growing sense that Bitcoin, or another math-based currency like it, is here to stay."

The purpose of Bitcoin is to serve as a digital-age payment system, evolving one step at a time into an independent money to compete with that forced on us by the nation-state. It may sound like a dream, but we've already seen digital technology make many dreams come true, including instantaneous and wireless video phones that are free and allow you to speak with anyone in the world.

The best way forward for you as an individual is to become an owner. If anything in this report confused you, or it all seemed a bit abstract, owning is the true remedy. That's what changes everything. If it is at tiny amount like 0.0001 BTC, owning is the key to learning and then doing.

Markets are continually reinventing the world. Might they do the same thing for money? And banking? And insurance? And financial services? It is a trial-and-error process, but many people are dedicated to making it happen. Between now and then, it will be a wild and wonderful ride. We do, indeed, live in interesting times.

Jeffrey Tucker is executive editor of Laissez Faire Books and head of the Laissez Faire Club. This report was produced in cooperation with many people deeply involved in the Bitcoin world: programmers, merchants, software engineers, economists, and bank specialists. Major sections were contributed by others who wish to remain anonymous. But I would like to make particular mention of Michael Goldstein of the University of Texas as an astute consultant, Doug French as an excellent explainer and critic, and Joel Bowman of *The Daily Reckoning* as well. I bear responsibility for any final errors. *tucker@lfb.org*

Best sources for continuing news and more information

- *Bitcoin Wiki*
- *Bitcoin Subreddit*
- *The Bitcoin Channel*
- *Bitcoin Forum*
- *Laissez Faire Club Forum*.