The Basics of Bitcoin

--- A Freeman's Perspective Primer ---

By Paul Rosenberg
FreemansPerspective.com

AND

Thomas Anderson
FreemansPerspective.com

Before we explain exactly what Bitcoin is, we should say that Bitcoin is the new frontier – the Wild West of our time. That means that using Bitcoin is more exciting than ordinary life, but also that it also involves more risk. It may be that Bitcoin makes a lot of people very rich, but there are no guarantees and immediately dropping a lot of money into it without serious thought is definitely not the safest option.

With that said, let's jump in.

What It Is

Bitcoin (also referred to as BTC) is a new type of digital cash – electronic coins (or, for the technical minded, digits that can be transferred via special cryptographic keys). But, it is cash without a central bank… without any banks at all. In that way, it's similar to gold – with no third party risk. Its unique characteristics make it a wonderful financial tool, and a very timely one.

Here are the key points to understand:

- ✓ **Bitcoin is digital cash.** You do not get a Bitcoin *account*, you get a Bitcoin *wallet*. Holding Bitcoin on a computer is the same as holding government money in your wallet.
- ✓ **Bitcoin is distributed.** There is no central office and no central computer... anywhere. There is no carefully managed issuer of Bitcoin – it is issued by a large number of "miners," few of whom even know each other, according to a computer program that was written several years ago.
- ✓ **Bitcoin can't be printed up, like national currencies.** Bitcoin has to be 'mined', and this requires special computers, lots of calculations, electricity and a bit of luck. It's neither free nor easy.

- ✓ **Bitcoin is limited.** Only 21 million Bitcoins can ever exist, and they can only be mined according to preset rules. (About 13 million exist now.)
- ✓ **Bitcoin can't be changed.** Bitcoin is a widely distributed computer program and cannot be changed by any single party. It is a specific set of rules cast into a computer program, and since that program is open source, it can be checked by anyone to ensure that there are no secret back doors. Furthermore, in order to change the Bitcoin program, you'd have to change it on thousands or millions of computers at once; you could not just hack one central computer and gum up the works.
- ✓ **Bitcoin is pseudonymous.** Every transaction is recorded, but real names are not. While Bitcoin is not properly anonymous, it can be used anonymously if you do simple things like never using the same address twice.
- ✓ **Bitcoins are oblivious to borders, laws or rules.** This is simply computer code – nothing else matters.

An honest currency must be backed by something. In years gone by, currencies were backed by gold, which kept the operators from playing too many games with them. Likewise Bitcoin is backed: by the very considerable effort required to create (mine) Bitcoins, but even more so by mathematics.

Bitcoin, properly, is a computer program and the data file associated with it, which is called the *blockchain*. The accuracy of the blockchain (the data file of every Bitcoin transaction) is secured and maintained by cryptography, which is a special type of mathematics.

Said more simply, this setup makes all records permanent and virtually unalterable.

Like the best forms of money throughout history, Bitcoin is scarce, divisible, recognizable, portable, verifiable, and difficult to obtain. What's really new about it is that it can traded, world-wide, instantaneously, and *with no intermediary*. A Bitcoin transaction between you and your friend in Fiji does not go through any bank or middle-man. It goes only between the two of you. And it requires only a computer or smartphone and an Internet connection.

Wallets

As the name implies, a Bitcoin wallet is a place to store your bitcoins. It is another type of computer program – simple to download and set up – and also protected with cryptography.

As mentioned above, bitcoins are "digits" that are unlocked and transferred via cryptographic keys. Bitcoin wallets provide a safe place to store these keys and the software necessary to initiate and receive transactions. They are simple and easy to operate.

Wallets generate Bitcoin addresses, which you would send to your friend in Fiji. A Bitcoin address looks like this:

19QhXjxBytWXQEaqvu7GRR7JhnfTG9UWiY

So, you send this address to a friend via chat message or any other means, and he/she puts that code into their wallet, chooses how many bitcoins to send and enters their password to authorize the send. A minute or so later, the bitcoins show up in your wallet.

That is all you need to transfer Bitcoins.

Your Bitcoin wallet will generate the necessary addresses for you. (Internally, is also generates the cryptographic keys that make the whole thing work, but you will never see them.)

There are three types of wallets:

- ✓ desktop clients
- ✓ cloud based services
- ✓ mobile wallets

The primary difference between them is where your Bitcoin keys are stored. We generally recommend that your information should remain under your control, so that means a desktop client, though there are benefits to the other methods.

A desktop client wallet is a computer program that you download and run on your home computer. Using this type of wallet means all your Bitcoin files are stored on your computer, and that you don't have to trust any third party.

Bear in mind, however, that this method is also quite a lot like stuffing cash into your mattress. Should your house burn down or your computer get stolen, your Bitcoins are gone. (The best wallets will give you the ability to backup your data in case the worst happens.)

Important Vocabulary:

What's a Blockchain?

A Blockchain is the Bitcoin Universe's name for the universal accounting ledger. Every single transaction involving bitcoins is recorded within the network and available for download to anyone that requests it.

Without getting too technical, this mechanism ensures that no one is able to "counterfeit" a Bitcoin by double-spending it at various merchants (a common problem with early digital currencies).

Some wallets require you to download the entire ledger and sync up every time you want to use the system. Others will rely on a group of computer servers that let you tap into their update every time you send and receive (spend or buy) any coins.

There are advantages and drawbacks to each approach. It really depends on your Internet connection speed and hard drive space you want to give to Bitcoin.

Some of the better options on the market include:

- **Bitcoin-Qt** (http://bitcoin.org/en/choose-your-wallet): Bitcoin-Qt is the original Bitcoin wallet created by Satoshi (the pseudonymous developer of Bitcoin) and upgraded by various Bitcoin developers. It is available for Windows, Mac, and Linux computers.
- **MultiBit** (https://multibit.org/): Multibit is a "lightweight" desktop client, which means that is does not need to download the entire blockchain, which makes it fast and easy to use. It synchronizes with the network and is ready to use in minutes and does not take up a lot of space

on your computer. Multibit also supports many languages making it a good option for the non-native English speaker.

- **Electrum** (http://electrum.org/): Electrum is a lightweight wallet that is fast and only requires a small amount of space on your computer. Fairly primitive but gives you the ability to recover your wallet in case of computer loss.

- **Armory** (https://bitcoinarmory.com/): Armory is a very secure desktop client wallet that offers advanced security features. Unfortunately, it is not a very user friendly option and it requires a large amount of your computer's resources. Armory runs on top of Bitcoin-Qt meaning that you will have to first install the Bitcoin-Qt wallet and download the entire blockchain.

Each program has its own various features and drawbacks depending on how you plan to use it. For beginners new to the world of Bitcoin, we recommend you start with **Electrum**. It's basic but relatively easy to learn and doesn't use as many system resources as the other options.

Once you have bitcoins stored in your wallet, it's a good idea to encrypt the wallet. Encrypting your wallet will prevent a thief from accessing your holdings should they somehow gain access to the Bitcoin files on your computer. Many advanced wallets will offer this option.

It is worth mentioning that Electrum does not directly offer this feature.

Getting Bitcoins

There are many ways to purchase bitcoins all of which involve some trade-off between price, speed and anonymity. The most common method for purchasing them is via an online exchange. However, other options include meeting with a local exchanger, arranging an exchange in an IRC chat room, or cash deposit services.

Centralized Exchanges

Online exchanges marketplaces exist to convert national fiat currencies or other digital currencies into Bitcoin and vice versa. The best exchange rates are available via the larger online exchanges. These exchanges interface with the traditional banking system by opening a bank account in the jurisdiction of the national currencies that you wish to trade in. For example, when a client wishes to convert US Dollars into Bitcoin they must (via a number of possible methods) deposit the fiat funds with the exchanges. Once the funds have been credited to the client's account, the exchange will facilitate a transfer with another client who is looking to sell Bitcoin.

Over the Counter Exchanges

Bitcoin has also spawned a local exchange industry, called OTC (*over the counter*) exchangers.

These groups both buy and sell bitcoins in more or less every major city on the planet. These are individuals who simply buy and sell on their own, using nothing but a laptop or smart phone and their own ingenuity. In other words, it is an opportunity for anyone to simply jump in. There are no barriers

to entry, but exchangers do have to provide prompt, honest, courteous service if they wish to prosper.

The typical OTC transaction takes place at a coffee shop, where the exchanger and the customer sit down, open their computers, send bitcoins from one to another and hand an envelope of cash from one to the other. Then, they get up and walk away.

Spending Bitcoins

There are already many places to spend your coins and, as more and more people stock their first wallet, more and more merchants are willing to accept them.

A great resource that covers many different offerings can be found at: https://en.bitcoin.it/wiki/Trade. And, of course, you can convert your holdings back into government currency at any time by using a currency exchange or selling over the counter to a private individual looking to buy.

Using Bitcoin Anonymously

Bitcoin is often called an anonymous digital currency, but this is not entirely correct. It is called anonymous because it can be used without ever having to give someone your name or show ID. However, in actual fact the transactions themselves are not private. Due to the way the system works, all transaction history is recorded and available to anyone on the network upon request.

But just because the transactions themselves aren't private, that doesn't mean you can't operate anonymously. Here's why:

While transactions themselves are recorded, there's no reason your name has to be anywhere near them.

And so, you can remain anonymous simply by making sure your identity can't be traced to your transactions.

Here's how to do it

To start with, it is good practice to use multiple Bitcoin addresses. Whenever you are going to enter into a transaction with a new person or group, generate a new "address" for that person. Generating new addresses for new transactions will help to obscure the transaction history.

Creating new addresses is easier than it sounds and any good wallet service will allow you to do so quickly and easily.

Within Electrum, our recommended wallet for beginners, the default setting will always ensure you have five unused addresses available at any given time. As you use one, a new one will automatically be generated, ensuring you never run out of them.

The way to remain truly anonymous is to avoid ever connecting your name to any of your Bitcoin addresses. For example, if you put your name next to a Bitcoin address up on a website, accept payment/donations at that address then the bitcoins accepted will be linked to your name. If you then use the coins stored at that address to purchase some socks from say, Grass Hill Alpacas, anyone in the world with an internet connection and an interest would know that you are walking around in alpaca socks.

Unfortunately, it is not always possible to separate your name from your Bitcoin address, particularly if you use a purchase method that requires ID. The solution for these situations is a mixing service.

Mixing services

These services 'mix' your coins with other users' coins. This breaks the chain between your name and the coins held in your wallet. They work as follows:

1. You generate a new Bitcoin address, one that is not associated with your name.
2. You send this new address to the mixing service.
3. You then transfer the bitcoins that are to be mixed to the service. The service will then have control over your bitcoins, as such it is important to use a service that you trust or to only mix a small amount at a time.

That's all there is to it.

Mixing services work best when there are a large amount of users. If there were only two users at a time then it would be fairly obvious who got what.

Depending on the amount of BTC being mixed and the number or users, the service may hold on to your coins until it can effectively swap them with another user's.

The service will hold your coins, along with many other users' coins, in their wallet and then, managed by software specifically made for this purpose, transfer out to users coins that originated from another user. These coins are sent back to you at your new, anonymous, address.

Anyone watching the blockchain will see that bitcoins from your address were transferred to the mixing service, but they will not know which coins, or which address now belong to you.

It's beyond the scope of this primer to head too much further on this tangent, but if you'd like to learn more, one company that offers this service is

- **BitLaundry**.

Why Bitcoin?

Now that you have some idea of what Bitcoin is and how it works, we should explain some of the important reasons this technology matters.

- ✓ **Bitcoin is honest money**. It is very, very difficult (in the most important ways, virtually impossible) to manipulate Bitcoin. The money we grew up using (dollars, pounds, yen, etc.) are fully manipulated. In fact, the justification for central banking was precisely that the bankers would be empowered to manipulate the currency. While this was sold to people as being "for their own good," it has been for the good of the bankers, first and foremost. This manipulation has hurt more people, more deeply, than most people know, or want to know... and this cannot

happen with Bitcoin.

- ✓ **Bitcoin involves no third-party risk**. No one gets to approve your transactions; you don't have to get anyone's permission.
- ✓ **Sending is instant and free, anywhere on the planet**. Think of all the difficulties and expenses associated with sending money to a family member overseas. All of this vanishes with Bitcoin.
- ✓ **Bitcoin eliminates identity theft**. There is no identity available to be stolen and no credit card number to copy. It allows you to buy items on the Internet privately without having any records tied to you.

Common Mistakes

The five most common mistakes made by new Bitcoin users are:

1. **Losing a password**. Without your password, your funds are gone. (Write it down in a safe place – your money depends on it!)
2. **Picking an easy-to-guess password**. The simpler the password, the easier it is to hack into. Choose one that ideally contains a mixture of letters, numbers and other characters (ex. #$*!%). Just be sure to write it down and store in a safe place in case you forget it!
3. **Not backing up their files**. If you end up losing your records, it might be extremely difficult, if not impossible, to get access to your BTC again.
4. **Thinking they have an account, rather than a wallet**. Remember, carrying Bitcoin is much the same as carrying cash. While you may have an account with an exchange, your Bitcoins themselves are stored in a wallet, and just like your regular wallet, if you lose it, you aren't likely to get it back with your cash in good order.
5. **Panicking about price**. Bitcoin is new, and its price relative to dollars can rise and fall. That's part of the deal at this early stage. As the market matures, prices as measured in other currencies will smooth out and become more stable.

The Wild West

A lot of people see the term "Wild West" as referring to dangers. And while there is some truth to that (though far less than advertised), the Wild West was also a time and place of great freedom and opportunity.

Most people do very little that is really exciting. They watch such things in movies and they dream about fighting evil, but they never do it. And the truth is that most never really see an opportunity to do so. Bitcoin, however, is giving us all that opportunity, right now.

Bitcoin users are struggling to build a new world of free commerce and honest money, a culture of

intellect and honesty, of trust and respect. This is not about getting in on a hot investment, it's about building a better world. And this struggle needs all the decent people it can get.

But, as in the old West, there are no guarantees, and losses are possible. As is so often the case, really living comes with no guarantees and with risks attached. But in the case of Bitcoin, at least, the path toward freedom and opportunity can be clearly seen.

* * * * *

We have published a full-length, in-depth report on the Bitcoin phenomenon. It covers in more detail some of the topics we reviewed today, includes step-by-step instructions (with plenty of graphics) on getting started, and identifies some of the most exciting opportunities available in this fast-moving market.

As well, it also includes specific insights and interviews with two of the best Bitcoin pioneers and insiders – people who have been using Bitcoin on a daily basis and who know, first hand, the issues involved.

To give you a taste, following is one of those interviews, with Charles Vollum, an early pioneer in digital currencies and fan of Bitcoin. Few, if any, have a better perspective view of the entire Bitcoin market than Charles.

As pulled directly from the pages of the *Insider's Guide to the Bitcoin Phenomenon*:

Freeman's Perspective: You've been working with gold prices for a long time. Is that what got you involved with Bitcoin?

I have long had an interest in gold, but also an interest in cryptography: from a childhood interest in code and ciphers, to number theory and its applications in college. In the early 1980s, I helped develop an electronic locking system for hotels that used public key crypto, and in the late 1990s, I participated in the Financial Cryptography conferences in Anguilla. Bitcoin is really the latest of many experiments in online money that I have watched and been involved in.

FMP: How do you see the Bitcoin market now? What are its strengths? Its weaknesses?

Bitcoin is really exciting! Unlike many earlier experiments, it seems to have reached the tipping point where it has enough traction to go viral. Part of this has to do with the way its internal incentives are structured, and part of it has to do with today's financial, social, and technological environment. As governments print ever greater quantities of money, and reduce financial freedom through increased reporting requirements and outright capital controls, people are looking for alternatives that will restore some of their control over their financial futures. Bitcoin has come into flower at just the right moment in history.

The fact that Bitcoin is a peer-to-peer technology, without a central point of control, is a great strength. Anytime you concentrate power of something as important as money in the hands of

a central authority, you are asking for trouble, as history has shown many times over. The fact that it is free-market money is also a key strength. No one is required to use Bitcoin for anything. It is only going to be used by those who see a benefit from using it. This makes it fundamentally different from government-issued currencies and all things deemed "legal tender."

Gold is the other money that has these same features. So in many ways, gold and bitcoins are similar. They are free-market money. They cannot be created on command; you have to do work to obtain them. They are not controlled by a central authority. With either one, you can hold it yourself, without any "counter-party" or "default" risk. (There can be "market risk," e.g., a risk that the gold or bitcoins might not buy as much as you'd planned, but no risk of the gold or bitcoins being lost because of the failure or misconduct of a bank or other party holding them.) But gold and bitcoins are different in key ways, as well.

Gold has a location inside some jurisdiction. It is physical, having significant volume and weight and, though more mobile than real estate, is still subject to regulations regarding transport, especially across borders. There may be reporting requirements or capital controls that limit the amount that can be moved without permission. Gold can be (and often has been) seized by governments and its private ownership outlawed. It can be taxed and thus rendered undesirable as a means of saving or making payments. Gold inside a heavily controlled jurisdiction may not be worth as much as gold in a less restrictive jurisdiction. On the other hand, gold close at hand may be worth more to you than gold in a faraway country, however safe it may be there.

Bitcoins, on the other hand, are digital abstractions. They move at the speed of light from one place to another without noticing or being noticed by the jurisdictions they pass though. They can be held completely offline, without any physical trace at all beyond a passphrase you have memorized, and thus accompany you on your journey without risk of seizure at border crossings. Criminalizing bitcoins in a particular jurisdiction (or even in many) might impact their market value but would not make them disappear. And implementing such a law would be extremely difficult, if not impossible, unless users chose to follow it willingly.

One other key area of difference is that gold has been used as money for thousands of years, and its value is well established. The amount of "stuff" an ounce of gold can buy (real estate, clothing, food, labor, etc.) has not changed much from ancient times to today. Many things are cheaper today, due to increased automation, advances in transportation and communication, and efficient division of labor, but the changes are not as large as you might suspect. You can see this in the many charts on my website, PricedInGold.com. This relative stability has not yet come to Bitcoin: It is too new, the demand for it is changing too fast, and its many new users are still in the throes of discovering how valuable it really is to them, leading to wild swings in its price. This keeps Bitcoin from being very useful as a measure of value, as a unit of pricing for other things – a function that gold serves very nicely.

FMP: What would you advise new Bitcoin users to be careful of?

1) Think clearly about the privacy of your transactions. They are pseudonymous but not really anonymous. There is a difference! Every transaction ever made with Bitcoin is there in the blockchain to be read by anyone who cares to look. Chains of identification extend from each point where one of the parties obtained and recorded information about your identity to all other transactions that follow from that point.

2) It is extremely exciting to see the purchasing power of your bitcoins going up! And with forecasts like mine (that 1 BTC will buy more than one ounce of gold in the next few years), it is natural to think about going "all in" on Bitcoin. You have to keep in mind that Bitcoin is still a very young currency, and there are many possible ways it could end in disaster. Because it is so speculative, you have to keep position sizes small. If you have a few percent of your wealth in Bitcoin, and it goes to zero, you are still mostly intact. If it increases in value by a couple of orders of magnitude, you have doubled or tripled your net worth. In other words, take a chance, but don't get too greedy!

3) Hoarding bitcoins is a viable investment strategy, but using bitcoins in your everyday transactions is what will really drive up their value. If everyone just sits on them, they will have no value at all! Offering and accepting bitcoins in trade brings new users into the market, and buying from merchants who already accept Bitcoin encourages them – and indirectly pushes the others who don't yet accept Bitcoin to consider doing so. The value of any currency is driven by the bid in the markets for it. And that demand is driven both by the number of users and the number of transactions each user makes – the velocity of money. The Chinese have a great way of looking at this: The word they use for "spending" is also the word for "circulating." By using your money, in this case bitcoins, you will find more value coming back to you, in the form of payments you receive in Bitcoin, but also in the increasing purchasing power of the bitcoins you are holding.

4) Remember that Bitcoin wallets are just computer files. They are subject to loss or corruption if the media they are stored on goes bad. They can be stolen if your computer security (or physical security) is poor. As your bitcoins become more valuable, don't forget to take the precautions you would take with any other form of money: Don't keep it all in the same place, don't leave it lying around, and keep it in secure locations where it is safe from natural disasters and thieves.

FMP: Any thoughts on Bitcoin over the long term?

At some point in the future, Bitcoin will become "mature." Pretty much everyone who sees a value to using bitcoins will be using them. What will the size of the market be at that time? It's hard to say… maybe everyone will decide the Bitcoin experiment was a failure, and will have moved on to other alternatives. Or maybe Bitcoin will become a powerhouse on a scale to rival or surpass the US dollar, or even become the world's primary currency. More likely, it will end up somewhere in between, filling an important need for many online transactions but not really replacing gold, silver, or government-issued currencies for transactions where they still make good sense. With every potential disaster the Bitcoin community deals with

successfully, with every new user of Bitcoin and every new merchant who starts to accept it, Bitcoin moves closer to maturity. As growth in demand tapers off, prices will stabilize, and Bitcoin will be able to assume a more normal place in the world of currencies.

Also keep in mind that Bitcoin is capable of many kinds or transactions beyond simply acting as a currency. With multiple signers you can create escrow arrangements with no need for a trusted third party to hold funds. You can create trusts in which value is given to a beneficiary now, but cannot be spent until a future time or until released by a specified set of circumstances. These and many other complex transactions can be done without the need for intermediaries, using Bitcoin. It may well be that Bitcoin's role as a currency turns out to be the least exciting thing we can do with it!

Most importantly, I think Bitcoin (and its successors) will contribute to a resurgence of human freedom and dignity by taking control of money away from central authority and returning it to each one of us.

* * * * *

A great sentiment on which to end this primer.

Thanks for reading.

PR & TA

FreemansPerspective.com

Did you like this report or are there ways in which we could make it better?

Let us know. Send your feedback to service@freemansperspective.com