# The Economics of Bitcoin

JP Janssen

June 2014

## Contents

## Contents Continued

## Introduction

The US Dollar seems perfect. It is more than just the national currency of the United States. It is the standard for world trade. People everywhere are used to compare prices in dollars, and transactions can be done anonymously with cash or openly through bank transfers. With credit cards you may even spend dollars you don't have. Some even consider it a store of value.

Unfortunately, the dollar is the Titanic of money. Many economists think there's only a question of time before it hits the iceberg. Most of these economists predict that gold and silver will take over. A small group of economists have a completely different approach. Together with a group of programmers, anonymously under the pseudonym Satoshi Nakomoto, they have invented digital money called **Bitcoin**.

Bitcoin is superior to other kinds of money. It can be transferred around the world instantly, anonymously and virtually for free. No registration is needed to open an account. No group of people controls the money supply.

Today, four years after it was invented, bitcoin is more popular than ever before, although it is still a drop in the ocean compared with dollars and gold. In this book I will try to answer the question that everyone asks; will bitcoin go mainstream or will it just fade out and die?

## About the Author

I, JP Janssen, am a stock trader, commodity speculator, real estate investor, programmer, and most recently – a holder of bitcoins and a writer. I graduated with a MSc in Economic Analysis, specializing in game theory, at the Norwegian School of Economics in 2009, and since then I've lived in New York, Singapore and Riga.

## Copyright



Tipping is highly appreciated. It encourages me to write more. The QR-code points to the tip address, which is also printed below.

1JPJaEVyieFi93YgtszCwMMjmsJGxfXRag

*This version was published June 30, 2014.*

## My Bitcoin 2.0 Counterparty Giveaway

The tip I receive I will give away to users of Counterwallet. It uses a "Bitcoin 2.0" technology called Counterparty which allows its users to issue assets and trade them just like shares are traded on the stock market.

My asset is called JPJA and consists of one hundred shares. I promise to pay a dividend to each holder on the 24th of December 2014. The amount received on the tip address up until that date will be divided equally to each of the one hundred shares.

Fifty JPJA shares will be sold at a symbolic sum 0.0005 BTC each, or about $0.30. I put only a few shares for sale at a time to make it less likely that one person picks up all. After you've purchased a share you can transfer it to any bitcoin address. You may also put if for sale at a higher price, and if you are lucky, you will make a profit when someone buys it from you.

Fifty shares will not be be put for sale, so that in effect I keep half the tip myself and give away the other half to my readers.

My motive for doing this is to show that bitcoin is more than just a payment system. It is a financial platform of endless opportunities.

## Definitions

When discussing economics, and money in particular, it easy to talk above one's head. Many of the terms used in economics have ambiguous meanings.

I will try to be as clear as possible, and here's a list of how I define the most important terms:

- **Money** is a matter of functions four, a medium, a measure, a standard, a store. All four functions need to be met in order to classify as money.
- **Medium of exchange** is the instrument used to facilitate trade.
- **Measure** is the unit used to express quantity.
- **Standard** is the mutually agreed medium and measure between parties engaging in trade.
- **Storage** of value refers to the medium's ability to have the same value in the future as it has today.
- **Currency** is the term used for money when it is in actual use or in circulation.
- **Legal tender** is a medium of exchange accepted by law.
- **Fiat** money is issued by the government without any commodity backing. All national currencies today are fiat.

- **Inflation** has two definitions. It is a measure of either the increase in quantity of the medium or of price increase. This book will always clarify which definition that is in use.
- **Deflation** is negative inflation.
- **Intrinsic value** is the underlying value. For money it can either be the medium's value if used for other purposes than money, or it can be the added value of using a kind of money over the best alternative.
- **Bubble** is the state where the valuation is higher than the intrinsic value.
- The **network effect** happens when the number of users influences the value.
- A **social chain reaction** occurs when an idea, opinion or piece of information that a person receives is shared to, and accepted by, on average more than one other person.

## What is Bitcoin?

*Sorry to be a wet blanket. Writing a description for bitcoin for general audiences is bloody hard. There's nothing to relate it to.*

– Satoshi Nakamoto, the inventor of bitcoin, July 5, 2010

Today, four years later, bitcoin has hundreds of thousands of users, but it is still very hard to explain what bitcoin really is. Thankfully there are good online resources such as Bitcointalk and Reddit where you can freely discuss anything related to the digital currency. When someone asked how to describe bitcoin, the answer with the highest ranking was as follows:

*Bitcoin is a new kind of money. It's the first decentralized electronic currency not controlled by a single organization or government. It's an open source project, and it is used by more than 100,000 people. All over the world people are trading hundreds of thousands of dollars worth of bitcoin every day with no middle man and no credit card companies. It's a startup currency which has never happened before.*

*Bitcoin is the first digital currency that is completely distributed. The network is made up of users like yourself so no bank or payment processor is required between you and whoever you're trading with. This decentralization is the basis for Bitcoin's security and freedom.*

*Email let us send letters for free, anywhere in the world. Skype lets us make phone and video calls for free, anywhere in the world. Now there's bitcoin. Bitcoin lets you send money to anyone online, anywhere in the world for less than a cent per transaction! Bitcoin is a community run system not controlled by any bank or government. There's no wallstreet banker getting rich by standing between you and the people you want to send and receive money from.*

*Bitcoin is more efficient than all competing currencies. This will drive its adoption in the same way computers were adopted, in that computers made people more efficient in competing in the marketplace. A currency has value by it being widely used. Bitcoin is a startup currency with a deflationary bootstrapping economy. Its use spreads by providing the speculator incentive.*

*Bitcoin is going to be the biggest opportunity for innovation that the world has seen since the industrial revolution. An idea whose time has come.*

## The History of Bitcoin

Bitcoin was introduced in 2009. From the very beginning anyone was free to join the network and the code was open source. All bitcoins have come into existence through an open lottery called mining. To participate you only need to download

the software and keep your computer online.

In the beginning bitcoins were treated like monopoly money. They had no real value apart from the thrill of transferring them back and forth. This all changed in May 2010 when a Florida programmer bought two Papa John's pizzas for 10,000 bitcoins. At today's exchange rate that's more than five million dollars!

A year later drug dealers saw the potential in bitcoin. The online marketplace Silk Road sold all kinds of illegal goods and services, and dealt exclusively in bitcoin. In 2013 the site was shut down. Its owner and some users went to jail.

In 2011 bitcoin saw its first bubble. The value peaked at $35 in the summer and then dropped all the way down to $2 by the end of the year. It slowly went up again but it was first in the spring of 2013 that it was back at its 2011 peak.

Sparked by the Cyprus banking crisis of March 2013 the bitcoin price rallied to more than $200 before falling down below $100. Another rally occurred at the end of the year, pushing the price over $1,100 and gaining bitcoin mainstream media attention.

In February 2014 the world's largest bitcoin exchange, Mt. Gox lost 750,000 of its customers' bitcoins. At the same time regulators around the world were scratching their heads, wondering how to deal with the crypto-currency. This spring the

price fell almost to $400. At the time of writing, end of May 2014, it is slightly below $600.

The good news at the moment is that more and more businesses adopt bitcoin, primarily since third party services offer technical implementations and elimination of exchange rate risks, all at very low fees. Consumers increasingly use it because it is safer and more convenient than credit cards.

## The Bitcoin Technology

The technology behind bitcoin is surprisingly simple. The code is open source, and anyone can download the bitcoin client compiled from this code. When your computer runs this program it knows how many bitcoins that are on each and every bitcoin address in the world. When you want to spend from an address that you own, you broadcasts this to the network. All computers connected to you receives your trade request, and then forwards this to all of their connections, and so on, until the entire network (within seconds) has received this information.

Ownership of an address is not registered anywhere, but requires a string of letters and numbers called a private key. Only he or she who possesses an address' private key can spend from that address. As a user of bitcoin you don't need to know your private key. The software takes care of this automatically. But it is

important to know that the concept of ownership is different from anything you're used to. If a thief steals your private key he can take all your bitcoins and feel safe that neither you nor law enforcement will ever find out who did it.

You shouldn't worry though, granted you don't reveal your private key, that no one will ever steal your bitcoins. The system is based on a cryptographic hash function called SHA-256. It was developed by the U.S. National Security Agency in 2001 for top secret government communication. A hash function takes any input and creates a completely new string called a hash. The SHA-256 function creates a string of 64 characters' length, where each character can be sixteen different symbols and each symbol is equally likely. For example, “bitcoin is awesome” creates this hash:

```
23d4a09295be678b21a5f1dceae1f634a69c1b41775f680ebf8165266471401b
```

An almost identical sentence, “Bitcoin is awesome” where the only difference is the capital letter, creates a completely different hash:

```
3aace886fca42c6f358474df26aa6623149219e9fb11557b6dbd3bf5c3f38cfb
```

There's no need to go further into depth here, but it is good to know the fundamental principle which is that by knowing the hash output you have no way of figuring out the input.

A convenient implication of SHA-256's astronomically high number of combinations is that new addresses can safely be generated offline. When your computer generates a new address it assumes no one uses the same address. Statisticians agree that there will never be two identical addresses even if the entire world uses bitcoin.

Transactions are included in a list called the blockchain. Blocks are made by special computers called miners They participate in a lottery based on SHA-256. As you know, it is impossible to guess the input for a given hash. But say you want a hash with a certain property. If you try enough inputs you'll eventually find such a hash. The winner of the bitcoin lottery finds a hash with a given number of leading zeros. The number of zeros adjusts over time so that it takes on average ten minutes between each time someone wins the lottery – or as the bitcoiners say; finds a block.

Since there are many miners around the world, no single entity controls the network. Each miner has to play by the rules or else the majority will simply ignore him. Problems only arise if one entity controls more than 50% of the computing power. In this case he can change the rules as he wishes and potentially damage or destroy the bitcoin network.

The miner who finds a block gets to reward himself a fixed number of bitcoins. In the beginning the reward was 50 coins.

Now it is 25 and every four years it will halve until a total 21 million coins have been “mined”. Competition between miners makes it expensive to mine bitcoins. Only miners with advanced ASICs (application specific integrated circuits) and cheap electricity will make a profit from mining bitcoins.

The blockchain makes it impossible to double-spend the same bitcoin. This is actually the main innovation of bitcoin. When a transaction is included in a block, and especially when a few more blocks have been added to the chain, the receiver can be confident that everyone on the network agrees that he is indeed the rightful receiver of this transaction.

## Economic Advantages of Bitcoin

Bitcoin can be transferred instantly to anyone anywhere in the world. No registration is needed to set up an account. The transaction fee is usually less than $0.01.

One can imagine merchants wanting customers to pay with bitcoin in order to save on credit card fees and costs of handling cash. Customers may want to use bitcoins because it is more convenient than cash and safer than credit cards.

More beneficial, perhaps, is the potential for cross border transfers. Especially guest workers from poor countries who send money home, can save a lot by using bitcoin. Bank fees can be up to 10% whereas bitcoin is almost free.

There are endless opportunities for new markets to arise. Online micro-payments used to be very impractical. Now any blogger, musician, writer etc can charge a small amount for access to his or her content. This is actually what I do with this book. I could have published it the old-fashioned way, but instead I released a pdf that anyone can distribute freely. The reader is encouraged to pay a small tip, and I hope that many small donations will encourage me to continue writing.

Cash transactions can be made more securely and transparently if bitcoins are used instead. It is impossible to counterfeit

bitcoins, and all transactions are recorded on the blockchain.

The above mentioned pros of bitcoin arise even if it is just used as a medium of exchange, not as money. If one or both parties need to exchange between bitcoin and fiat, the transaction cost will rise somewhat, but may still be cheaper than any alternative.

The fixed supply will prevent inflation. Fiat, on the other hand, loses value over time, and it is likely that this occurs in a way which grows the size of the government and the wealth of individuals who own stock or real estate, at the expense of everyone else. Bitcoin would create a leveled playing field where the government is restricted to spend no more than it raises in taxes and the financial market would have less of an up-drift because there would be no inflation and no artificially low interest rates.

Something that some may consider a benefit and others a disadvantage is that anyone will be able to hide his or her wealth. Earlier you would have to either see your cash inflate away, trust your Swiss banker or hold gold which is difficult to exchange and transport. Bitcoin only require a code you can hide or even memorize.

## Economic Disadvantages of Bitcoin

Bitcoin's volatility is its main disadvantage. Since the price tomorrow may be significantly different from that of today, bitcoin can hardly be used to measure prices. Instead bitcoin is often used as as a medium of exchange. Prices are typically quoted in local currencies, and services like BitPay facilitates payment instructions and currency conversions. This adds cost to using bitcoin.

Bitcoin is an extremely risky store of wealth. This attracts the gambling breed of speculators who bid up the price to bubble levels, for then to sell out when the price crashes. Volatility increases because of these gamblers, but as bitcoin matures it is likely to attract more long-term savers. These will in turn reduce the volatility. Another solution may come from promising "Bitcoin 2.0" protocols such as Counterparty. They enable financial derivatives to be built on top of bitcoin. This should make it possible to keep your bitcoin holdings steady in terms of dollars, gold, silver, or whatever you prefer.

Bitcoin is an experimental technology which may fail. The network itself has survived so far, and for each day that passes by we can be more and more confident that it will live on. However, also the individual user risks theft, and the Mt Gox incident is a proof of how risky it is to own bitcoin. 750,000 coins got lost from the online exchange, and although the

individual user should never have trusted all their coins to some web page, reality is that most of us are unfamiliar with how to deal with these totally new kinds of risks.

The use of bitcoin to avoid reporting and taxation may become widespread. There has traditionally been a black *cash* economy, but a black *bitcoin* economy makes it easy to make such transactions over distances as well.

If bitcoin ever is to become money, meaning it competes with a national currency, the central bank can no longer control the money supply in order to improve the economy. This political tool anyway makes more harm than good, but the establishment will not let go of this privilege easily. They are likely to fight bitcoin as it becomes larger.

**Bitcoin Versus Alternative Digital Currencies**

Since bitcoin's code is open source, anyone can copy it, make a few adjustments, and release a brand new digital currency. This is being done weekly, and now there are dozens of them. Some more popular altcoins are Litecoin, Darkcoin, Nxt, Counterparty, Dogecoin and Namecoin.

The largest of them, Litecoin, has a market capitalization more than twenty times smaller than Bitcoin's. The third largest coin is

a quarter of Litecoin's size.

The *network effect* is what sets bitcoin apart. It's the large amount of existing users that gives it value, not the technology itself. When someone gets interested in digital currencies, downloads a wallet and exchanges fiat, there are much better options for bitcoin than for any other digital currency. Therefore it is natural for a new user to adopt bitcoin rather than any alternative. Developers and entrepreneurs observe the large influx of new users, and so they focus primarily on bitcoin. As the networks grows larger and larger, it gravitates toward a natural monopoly.

A related effect is the *social chain reaction*. In certain segments of society, a new user of bitcoin tells about it to more than one other person on average, who in turn tells it to more than one person, and so on. In the beginning it spread like this among those interested in monetary policy. They were amazed to see a digital alternative to fiat. Then it spread to traders of illegal goods on the online Silk Road marketplace, presumable for bitcoin's anonymity. Now it is becoming common among bloggers and other producers of online content to ask for donations in bitcoin. Online merchants increasingly accept bitcoin through services such as BitPay and Coinbase. These let the merchant use the local currency while bitcoin serves as the payment protocol. They choose it because it saves costs.

It is unlikely that an altcoin can spread the same way. Bitcoin spread because it was better than any alternative at the time. An altcoin must be significantly better than bitcoin.

Even though users gravitate to bitcoin, it won't necessarily capture the entire market. People appreciate alternatives. If you own a lot of bitcoins you may want to diversify some risk by investing part of your holding in other coins. If you are a merchant accepting digital currencies you may want support for one or more alternatives just in case something happens to the bitcoin network. And, of course, there is always a part of the population who prefers the outlier.

Some altcoins offer completely new features. Namecoin is an exact copy of bitcoin except it allows for domain registration as well. Darkcoin and Monero offer more anonymity. Nxt, Counterparty and Etherum are even programmable. The owner of such a coin is able to make a contract which then can be transferred as effortlessly as bitcoins. They can be used to issue dividend paying shares, bets, CFDs (contracts for difference), and certainly a lot of other things not yet thought of. All these coins offer good features, but it remains to be seen if the altcoins solely will be used for their niche purposes or also compete with bitcoin as a medium of exchange or store of value.

## Supply and Demand of Bitcoin

The price of bitcoin is primarily determined by three groups; miners who sell newly minted coins, merchants who accept bitcoin but convert them back to fiat, and investors who hoard bitcoins. Those who have accumulated bitcoins tend not to sell much, but their potential selling pressure should be kept in mind. If the general opinion remains optimistic it is likely that many more will invest as more convenient ways of buying bitcoins, such as cash ATMs and financial ETFs, become available. Let's have a closer look at the various groups determining the bitcoin price.

### Bitcoin's Trading Volume

Coinmarketcap.com shows the trading volume, along other interesting stats, for most digital currencies. The daily volume for bitcoin, calculated as the sum of volume for all major exchanges, is millions of dollars. Some days it has reached more than a hundred million dollars, but normally it is more like ten million.

Keep in mind that the volume is inflated by robots trading back and forth. What is more interesting is the how much fiat that gets converted to bitcoin and vice versa. If the sum of all dollars deposited at exchanges is X, then the amount withdrawn shall

also be X. If the sum of of bitcoin deposited is Y, then the amount withdrawn shall also be Y. If an exchange does not keep this basic balance it will face liquidity problems and eventually lose trust as people will be unable to withdraw funds. The price of bitcoin must be X dollars divided by Y bitcoins.

If you are able to foresee the change of these flows, you'll be able to predict the price. It's easier said than done, and I will only share some suggestions on what to look for.

## The Supply of Bitcoin

**Miners** generate about 3,600 new bitcoins every day. It is likely that miners hoard as much as possible but, as mining becomes more competitive, they will need to sell more to cover electricity costs. It is hard to put an estimate on how much they sell, but a guess may be that they sell 1,000 bitcoins for fiat every day. At $650 per bitcoin, that's $650,000 which needs to be absorbed.

BitPay recently announced that they process one million dollars' worth of bitcoin a day. The way BitPay works is that they allow **merchants** to accept bitcoin and that they can choose to get the bitcoins automatically exchanged to fiat. I estimate that BitPay merchants sell $900,000 of bitcoins a day and that other merchants sell perhaps around the same amount.

A large portion of bitcoins are held by **investors** expecting a further price increase. It is likely that some of these sell parts of their holding when prices go up in order to realize gains. This happens particularly when the price first goes up a lot and then dips a bit. This may be self reinforcing and explain why we've seen so much volatility. There's a total of seven billion dollars worth of bitcoin and thousands of individuals own substantial amounts. The potential selling pressure is huge if the optimism fades. The current selling is quite low.

## The Demand for Bitcoin

Some use bitcoin for **purchases** but it is unlikely that many (who do not have bitcoins all ready) buy bitcoins just to make a purchase. There is some demand for specific uses, such as payments that need a layer of anonymity or to a country where bank transfers are expensive or unavailable. Although the potential market for these is enormous, it is likely not that big at the moment.

Swiss banks used to be popular among wealthy individuals who wanted **privacy**. This is not the case anymore, nor are there many options. Bitcoin fills this vacuum. I believe that few use bitcoin for this purpose at the moment, especially since the price is so volatile, but the potential is enormous.

I believe **speculators** are the largest group of buyers - by far. The couple of million dollars of daily selling by miners and merchants are absorbed by speculators. The group of speculators is likely to increase, especially when ETFs open bitcoin for institutional investors. A consequence of speculators is price volatility. Over time the speculation has to decrease. More demand will come for payment and store of wealth, and as the volatility decreases it becomes less attractive for speculation.

## Robot Manipulation

Some believe that robots at Mt. Gox caused the bubble at the end of 2013. Rumors of such manipulation is usually exaggerated because the price will always settle such that those selling bitcoins for fiat balance out those selling fiat for bitcoin. In the Mt. Gox case, however, manipulation may indeed have happened. A crooked exchange can report any price for some time. No real transaction on the blockchain needs to take place when trades are made internally on an exchange. Since Mt. Gox obviously cooked their books they could have reported a price far off the real supply and demand. As the largest exchange, it surely influenced participants on other exchanges to follow.

## Bitcoin's Market Capitalization

The value of all bitcoins, also called the market capitalization, is $5.1 billion. This number the total number of coins, 12.6 million coins, multiplied by the price, $407 per coin.

To put this into perspective, Apple is valued at $570 billion which is more than 100 times more than bitcoin. Google is worth $380 billion, Facebook is at $180 billion, eBay is at $72 billion, and Coca-Cola is at $170 billion.

Actually, this is a bit like comparing bananas and apples. Stock companies have value since a stock is a claim on the company's profit. If you buy a stock, you'd normally do so only if you believe the present value of all future dividends is higher than the share price. Bitcoin pays no dividends, hence from this perspective it has no value.

Gold and silver have more in common with bitcoin. All serve as storage of wealth, pay no dividends, and can potentially be used as money. All the gold in the world is worth about $7,000 billion.

All silver ever mined is "only" worth $920 billion, but about half of it has been lost. Silver is not only precious, it is also an industrial metal. Much waste containing silver has never been recycled and is forever lost.

Other interesting numbers are the new mine supplies of gold, silver and bitcoin. As you may know, about every ten minutes 25 new bitcoins are minted. Over a day that is $1.5 million worth of new coins. In 2014 this causes an inflation of 10% of the money supply, but this number decreases every year.

Gold's annual mine supply is 2.800 tonnes (90 million troy ounces) worth $330 million a day. Silver's mine supply is 790 million troy ounces valued at $44 million a day.

To summarize:

- The market cap of bitcoin is less than one hundredth those of silver and large companies, and less than one thousandth that of gold.

- The value of mined bitcoins is about one two-hundredth that of gold and one thirtieth that of silver.

*The price of bitcoin was $407, Gold was $1321, and Silver was $20.21 at the moment of writing.*

## Money

To understand bitcoin better you need to relate it to money. Money is, unfortunately, a concept most people are clueless about, and economists are the most ignorant of us all. Myths and misconceptions are widespread. Despite this, it is one of those things we take for granted. Like you don't need to know about oxygen to breathe, you don't need to know anything about money to spend.

If you only memorize this simple definition you'll understand money better than ninety-nine percent of the population:

*Money is a matter of functions four, a medium, a measure, a standard, a store. All four functions need to be met in order to classify as money.*

It is extremely difficult to fulfill all four criteria. Gold, for example, is convenient to measure, can easily become a standard, serves as a stable long-term storage, but is not good as a medium of exchange. First, gold is too valuable to be used in small transactions. Second, fake gold is easy to mint but hard to detect.

In this chapter I'll briefly explain money, tell the story about the US dollar, discuss its current status, and argue how bitcoin emulates gold's best features, yet improves its downsides.

## Money is Valuable due to the Network

Dollars have value to person A because he's confident person B, to whom he's in debt, values dollars. Person B values dollars because he's confident person C values dollars. And so the chain of confidence goes on until everyone uses dollars.

This network effect is so strong that the majority of the world trade is in dollars. A Russian is likely to pay a Chinese in dollars. The dollar's near-monopoly would last indefinitely if the currency were better designed. Unfortunately (or fortunately?) the amount of dollars inflate and, consequently, the value of each unit declines. It is likely that an opposite chain reaction will occur during the next financial crisis. Reduced value of the dollar leads to loss of confidence which in turn reduces the value even more, and so on.

When the dollar fails new currencies will compete for the monopoly position. The big favorite is gold. Everyone on this planet knows about gold and everyone is confident that gold is immune to inflation.

People tend to like gold because of its intrinsic value. It's a nice word that few know the meaning of. The reality of gold is that most of its value comes from the network effect – just like with dollars. Only a tiny portion of the world's gold supply goes to industry or jewelry. Palladium, a related metal, is ten times more

scarce than gold but its price is less than that of gold. Palladium is mainly priced for its use in industry and jewelry. If gold were priced the same way it is likely it'd had to drop to less than a tenth of today's price for the gold supply to be absorbed for its “intrinsic” purposes.

Bitcoin too owes its value to the network effect. I see two main reasons for buying bitcoins. It can be used to transfer value today or it can be a storage of wealth for the future. For the latter purpose you need confidence in that others will continue to value it, just as you'd need confidence in others if you'd store your wealth in dollars or gold.

## A Brief History of the US Dollar

In 1792 the Congress passed the Coinage Act. It defined the US Dollar as 1.6 grams of pure gold, or 24.1 grams of pure silver, or 1.71 kg of copper. Coins were minted according to these measures. People could even bring gold, silver and copper to the mint and get the metals minted to coins free of charge. With standardized coins with guaranteed weight and purity, and even death penalty for debasement, people could feel confident in the US Dollar.

| | | |
|---|---|---|
| Eagles | $10 | 247 $^{4}/_{8}$ grain (16.0 g) pure or 270 grain (17.5 g) standard gold |
| Half Eagles | $5 | 123 $^{6}/_{8}$ grain (8.02 g) pure or 135 grain (8.75 g) standard gold |
| Quarter Eagles | $2.50 | 61 $^{7}/_{8}$ grain (4.01 g) pure or 67 $^{4}/_{8}$ grain (4.37 g) standard gold |
| Dollars or Units | $1 | 371 $^{4}/_{16}$ grain (24.1 g) pure or 416 grain (27.0 g) standard silver |
| Half Dollars | $0.50 | 185 $^{10}/_{16}$ grain (12.0 g) pure or 208 grain (13.5 g) standard silver |
| Quarter Dollars | $0.25 | 92 $^{13}/_{16}$ grain (6.01 g) pure or 104 grains (6.74 g) standard silver |
| Disme | $0.10 | 37 $^{2}/_{16}$ grain (2.41 g) pure or 41 $^{3}/_{5}$ grain (2.70 g) standard silver |
| Half Disme | $0.05 | 18 $^{9}/_{16}$ grain (1.20 g) pure or 20 $^{4}/_{5}$ grain (1.35 g) standard silver |
| Cents | $0.01 | 11 pennyweights (17.1 g) of copper |
| Half Cents | $0.005 | 5 $^{1}/_{2}$ pennyweights (8.55 g) of copper |

There was one major flaw with this system. The ratio of gold to silver was fixed at fifteen to one. As large silver deposits were discovered throughout the 19th century, silver lost value relative to gold. The official ratio was changed several times so that silver eventually went from overvalued to undervalued. Traders reacted by exporting silver coins to Europe. As a consequence there were almost no silver coins left in circulation in America. To overcome this problem thousands of banks issued their own notes in small denominations.

In 1900 the dollar moved away from silver and gold to a pure gold standard, although it had been so unofficially for many years. The dollar was now convertible to 1.5 grams of gold, almost the same as it was in 1792. In 1933 the dollar was devalued to only 1.16 grams of gold and private ownership of

the metal was banned. People had to hand in their gold in exchange for dollars. Foreign governments could still exchange dollars for gold until 1971. After that year there has been no official gold backing of the dollar.

The dollar has been controlled by the Federal Reserve since long before that. It was established in 1913 as a private bank entrusted to safeguard the economy. One can argue how well they have performed. The US Dollar is, after all the world's leading currency On the other hand, it has lost about 97% of its value, hence it has failed as a long term store of value.

Some fear it will also lose its property as a short-term store of value, in which case people will seek alternative money.

## The Network Effect and the FED

The dollar has been immensely successful over the past decades. People all around the world have chosen dollars before any other alternative. The reason is simple. The more users a currency has the cheaper it is to exchange to other currencies, and the more stable it becomes. This attracts new users, who in turn further improves these properties. As global trade has skyrocketed, the de facto standard has gravitated to the dollar.

The massive surge in demand for dollars has been offset by an

even larger supply. Had it not been for the increasing amount of dollars, dollar-denominated prices would likely have dropped a lot. This in turn would have made it difficult to write contracts in dollars. The Federal Reserve (FED) aims instead for an inflation target of two percent. If they do a good job, people can be confident in a steady, low price inflation.

Gold and bitcoin work in the opposite way. These have fixed supplies so that their prices fluctuate with demand.

### The Dollar's Expected Collapse

A downside with the dollar supply is that it reaches certain parts of the economy first, hence increase prices there more than other places. Low interest rates and easy access to loans, masterminded by the FED and the government, caused the housing bubble of the 2000s. Since everyone could get loans very cheaply, it was inevitable that money poured into real estate. This caused house prices to increase, and when it turned out that too many were not able to pay back their loans, we had the financial meltdown of 2007. Another example is the ongoing student debt bubble. Almost everyone can get student loans at low rates, which enables colleges to raise their fees. Unfortunately all this student money has not found its way into higher wages, and many graduates now have a very hard time paying back their debts. As of writing, June 2014, the stock

market is at an all time high despite a slow economy. This too, is likely accredited to easy access to money.

Typically the FED has created bubbles by creating too much money and then burst these bubbles by decreasing the money supply, for example by raising interest rates. This may have been appreciated by Wall Street while it has not affected Main Street too harshly. What we saw in the last financial crisis, however, clearly shows that this is no longer the case. The entire economy suffers.

Most important, perhaps, is foreign governments' implied power over the dollar. As the dollar gained importance in world trade, governments bought wast quantities of US Bonds (i.e. dollars). The large demand from foreigners is also a reason why the interest rate is so low. Because of this, we have for many years had a situation where the US could import goods while exporting nothing but freshly printed dollars. This has caused an enormous US debt, which will grow immensely if interest rates rise. I think this will happen if foreigners stop buying US dollars.

It is likely that a saturation point will be reached where foreigners start selling their holdings, which will cause price hikes in whatever they buy (gold, real estate, land, stocks). Eventually the entire network effect will be reversed so that people sell dollars because everyone else sells dollars. This will

lead to its collapse.

**Bitcoin Complements Gold**

Bitcoin emulates some of the best properties of gold. There is a limited supply of bitcoin and new coins are created through a resource-intensive process called mining.

The similarity stops there. While gold is a terrible medium of exchange, bitcoin is better than the anything the world has ever seen. With bitcoin you can transfer value to anyone, anywhere at next to zero cost.

Despite this, Bitcoin will never be able to compete on some areas. First, gold has a far larger network. Almost all humans on this planet value gold. Everyone wants it, though relatively few can afford it. It has been valued for thousands of years and is sure to remain so for numerous generations. The price and popularity varies but it will forever keep its special value.

Bitcoin only has a few years of track record. It is a new technology. Would you trust your entire savings, let alone the nation's savings, to the bitcoin network? I hope not.

My point is that bitcoin and gold should not be compared. They are the best in their respective niches. They complement one

another. *Gold excels both as a storage of value and as a unit of account* but it is a terrible medium of exchange. *Bitcoin excels as a medium of exchange* but it is a terrible both as a storage of value and as a unit of account.

**Bitcoin's and Gold's Past Bubbles**

Bitcoin has had two major bubbles so far. In the spring of 2011 it went from $1 to $30 in a matter of months. By the end of the year it was worth only $2. It was not until the spring of 2013 that the price surpassed the height of the bubble. At the end of 2013 the price peaked at $1200, At the moment of writing, the spring of 2014, the price is down at $450.

Gold can also show some pretty volatile past years. In 2001 an ounce of gold was traded for less than $300. For the next decade it increased in value every year until it peaked at more than $1900 in 2011. Today gold is traded at $1300 per ounce.

**Is Bitcoin Money?**

The answer is that sometimes it is, but most often it is not. Remember that money is a medium, a measure, a standard, and a store. For some very few individuals bitcoin fulfill all these properties, and when such individuals transact, then bitcoin is

indeed money.

Those who sell mining hardware often quote their prices in bitcoin. For these it makes sense because the hardware becomes more valuable in term of dollars when the bitcoin price goes up, and vice versa. In terms of bitcoins, however, the value is more stable. Those who all ready own mining hardware are also used to a stable income in terms of bitcoins, so for them it is more convenient to see hardware priced in bitcoins. For these groups bitcoin is money.

For most other users of bitcoin it only serves some of the purposes of money. Say that one bitcoin-user owes another bitcoin-user $100. If they cannot meet in person the debt must either be settled by a bank transfer or through a bitcoin transaction. Chance is that they will agree to transfer bitcoins at the current market rate. It is faster and simpler than doing a bank transfer. In this case bitcoin serves as a medium of exchange, and nothing more.

The payment provider BitPay offers this service to merchants. Though it is a new service, it all ready has thousands of users and processes more than a million dollars a day. The merchant can choose to convert all or most bitcoins to the local currency, making it a low-fee medium of exchange, but not money.

Individuals who used to deal in cash may turn to bitcoin. The

bitcoin blockchain serves as a sort of receipt. Anonymity can be assured if both parties use accounts not associated with their names. A bitcoin transfer is extremely easy to make when you meet in person. If both have a smart-phone with a bitcoin wallet, the receiver will only need to type in the dollar-amount and show the payer the corresponding QR-code, which he scans and then pays. Also in this case bitcoin only serves as a medium of exchange.

Those who speculate in the bitcoin price use it as a risky store of wealth. In this case it is more like an asset or commodity, and certainly not money. The same applies to those who use bitcoin to hide some of their wealth.

As more and more people have regular incomes and expenses in bitcoin it will naturally become more like money. Remember that what is money to one person may not be so to another. Say that two individuals both think of dollars as money and bitcoin as money. In this case they will choose the alternative with the lowest cost, where cost is time, fees, and so on.

Money has many similarities with languages. Two individuals spontaneously agree on the language that most efficiently gets the message through. In most cases around the world it either means the mother tongue if they share the same one, or else in English. Both the US dollar and the English language owe their successes to the network effect.

## The Future of Bitcoin

It is hard to imagine bitcoin disappearing unless the technology fails. Bitcoin as of today is safe, very cheap to use, no registration is required, it is instant, and it is transparent albeit pseudonymous. It benefits from the network effect, essentially making it impossible for other crypto-currencies to take its place.

Naturally you'd expect more and more people to discover bitcoin, and more and more services to be built to facilitate its users. At the same time governments will try to regulate it. Because of its decentralized nature, there's nothing any government can do to regulate the bitcoin protocol itself. Rather they can make it difficult to buy bitcoins through exchanges. They may also make it harder for businesses to accept bitcoin as payment. We've seen attempts of all this in the US, as well as in Russia and China.

All this will slow down the growth of bitcoin but even if it's outlawed, people will continue using it. Compare it with cash. It is legal to keep it and use it, but most transactions need to be reported and taxed. People nevertheless conspire all the time to avoid taxation. If bitcoin were to be outlawed it could be thought of as online black money – and it would likely still grow in popularity.

The real threat to bitcoin is hackers. You could say that there's a hundred million dollar bounty on it. If a hacker finds a way to counterfeit or steal unlimited amounts, he'd be able to sell a large fortune worth of bitcoins until people would realize what was going on. And when panic eventually breaks loose, the value of bitcoin will immediately collapse.

This is not such an unlikely scenario. A hacker will probably never be able to crack the protocol itself, neither any of the main wallets, but viruses that log keyboard inputs or captures screen shots may infect a large amount of users. When these unlucky users lose their coins for no apparent reason, and report this to the community, the trust in bitcoin will deteriorate. If it happens to sufficiently many, bitcoin will indeed suffer.

A common fear among bitcoiners is that of a 51%-attack. It may happen when one entity controls more than half the network's total hashing power. This will allow the one in charge to destroy the network, but more likely is it that he will act as a monopolist. Payment networks typically have high fees, which are possible due to the network effect. It is impractical for users to change to a different system, and this justifies the fees. A controlling miner could do the same to bitcoin.

## More Users – Cheaper to Exchange

As long as the technology continues to work flawlessly, it is likely that bitcoin gains more and more popularity. The network effects in play are extremely strong. For example, it will become much easier to buy bitcoins. Today it is quite costly to acquire bitcoins, at least that's my experience in Europe. There are several online exchanges, which is good. Most them allow you to do SEPA bank transfer, either directly to the exchange (Kraken) or directly to the person you buy from (Local Bitcoins and Bitcoin.de). The latter works surprisingly well, as the exchange keeps the seller's bitcoins in an escrow until he confirms the transfer. Unfortunately both have one percent fees, paid for by the seller and/or buyer and a large spread. Kraken has a 0.2 percent fee and a similar sized spread, which still is a lot compared to regular currency and stock trading. Another disadvantage is that SEPA transfers take days to confirm. Bank transactions are reversible, while bitcoin transactions are not. This makes the system vulnerable to fraud, which adds time and costs to everyone.

ATMs can change all this. They are all ready popping up in major cities around the world. This effectively removes any barrier to enter the bitcoin economy. All you need is a free bitcoin app on your phone and a fiat banknote. Let the machine scan your address' QR-code and insert the banknote. A few seconds later you have your bitcoins.

Other ways of exchanging will surely appear as well. When professional trading platforms implement bitcoin, the spread and fees should eventually amount to less than 0.1 percent. This will immensely improve bitcoin as a medium of exchange.

## Merchants and Consumers

Thousands of merchants have all ready adopted bitcoin. A third party payment processor such as Bitpay makes it trivial to implement, The benefits are lower costs than credit cards, and also the impossibility of charge backs. The downside is obviously that very few still use bitcoin. Why go through the effort of implementing it if very few end up using it? Well, here's the network effect in play again. More users make it more appealing to merchants. And more merchants accepting bitcoin attracts more users.

Local shops and restaurants face the same trade-off. Thankfully, implementation is actually very easy for them. Basically they can have a static QR-code at display. The cashier or waiter just needs to know how to convert a fiat amount into bitcoin, and confirm this on an online tablet or phone. They can do this anytime a customer asks for it.

## The Developing World

It may perhaps be in the developing world where bitcoin goes mainstream first. Most people all ready have mobile phones but the majority do not have the banking services that Americans and Europeans take for granted. Even cash is unsafe in many countries. Not because of counterfeiting but due to inflation.

## The Next Cyprus

Even in the western world bitcoin can turn out much more useful than anticipated. The 2013 Cyprus crisis broke a centuries old taboo. With pressure from Brussels the Cypriotic government proposed a partial confiscation of all bank accounts. The price of bitcoin skyrocketed at the same time. A coincidence? Perhaps so, but imagine a similar crisis on a global scale. Fiat currencies will collapse and private property has no longer any legal safeguards. People will be desperate to protect their wealth, and by that point the best options are physical gold and silver – and cryptographically secured digital assets. All bitcoins today have a total value of less then eight billion dollars. It is a drop in the ocean. I will make no attempt to predict the bitcoin price if it becomes a safe haven during the next financial crisis, but it will for sure go up a whole lot.

## Keep Your Bitcoins Safe

For everyday use, bitcoin is convenient and safe. As long as you use a main wallet, be it online or offline, and pick a strong password you should feel as safe using it as you are of carrying cash in your real wallet.

If you own a large amount of bitcoins, you should consider stronger safety measures. Regular users should also educate themselves on safety, as it is likely that hackers will get more sophisticated over the coming years.

### Lose Your Key – Lose Your House

Imagine a world where the ownership of a house belongs to the one who has the physical possession of the door key. If you lose your key, no locksmith will be able to help you. If someone steals your key, the police and courts will offer no assistance. The thief is now the rightful owner. Welcome to bitcoin!

The Bitcoin World can be compared to the Stone Age. Back then property belonged to whoever could physically defend it or successfully hide it. As society evolved we have invented numerous safeguards. Most important is perhaps the notion of private property. Most of us know by instinct the difference between mine and yours and that stealing is wrong. But this is

not sufficient. We have police, laws, constitutions, courts, land registers, the eight commandment, and much more to enforce the sacredness of private property. Without these measures people would spend their efforts on a protecting their own values and on stealing those of others. Society as a whole would never develop.

The digital world has very limited safeguards. Even the main desktop wallets, such as Bitcoin Core, MultiBit, and Electrum, places the responsibility entirely on you. You can choose not to use a password, in which case any hacker may gain access to your funds. Or you can choose to encrypt with a strong password, in which case your funds are permanently lost if you forget your password. In either case there's no back door, no one to help you, or anything you can do to recover your bitcoins.

### Write Down Your Password

I am quite confident that loss of password is the number one cause of lost bitcoins. If you don't write down the password, you'll likely forget it. If you do manage to memorize it, the password is too weak.

Make it a habit to write down your passwords on a piece of paper. After you've written down a password, you should use it at least once to make sure there's no typo. Make several copies

and store them at various safe locations. If you are afraid that someone will find the notes and use your passwords, you can make your own simple encryption. Say that your real password is “5vO8bw$3mK”. Instead of writing it down as it is you can write “5v$8bwO3mK”. Only you know that the third and seventh character have changed place. A thief would not only have to physically get access to your note, but it would take a great effort to figure out your system.

You should not use this exact system but rather make your own. Always keep in mind that you have to remember it even if you don't use the password for many years.

Wallets such as Bitcoin Core and MultiBit also require a backup. Make backups on at least two separates USB drives and store them on separate locations.

**Pick a Strong Password**

The second largest threat after losing your password is not choosing a strong enough password. Typically a hacker steals your encrypted wallet file and then cracks it through a process called brute-force. A CPU, a GPU or a cluster of bots tries billions of combinations. If your password is Summer69 it will take less than a second to crack. A password must be truly random and at least twelve characters long in order to be safe.

I recommend rolling a dice to generate passwords. It's an ancient device but still the best random number generator known to man. There's a practical problem though; a dice has just six sides. If you only use numbers from one to six the passwords needs to be really long; I recommend at least 24 characters.

A way to go around this problem is to roll two dices, and use a table where each of the 36 outcomes correspond to a distinct character. This approach ensures that such a password only needs to be half the length to be equally strong. In reality it is even better because the brute force attacker does not know which set of characters you use. Now you can feel comfortably safe with a password of only twelve characters. Below is an example of such a table, but you are advised to make your own.

| | | Yellow Dice | | | | | |
|---|---|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 | 5 | 6 |
| Red Dice | 1 | A | a | 1 | X | $ | t |
| | 2 | B | b | 2 | Y | % | 8 |
| | 3 | C | c | 3 | Q | + | y |
| | 4 | D | d | 4 | x | # | p |
| | 5 | E | e | 5 | y | @ | H |
| | 6 | F | f | 6 | q | & | k |

To make you own system, just print out the empty table and fill in you own characters.

| | | Yellow Dice | | | | | |
|---|---|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 | 5 | 6 |
| Red Dice | 1 | | | | | | |
| | 2 | | | | | | |
| | 3 | | | | | | |
| | 4 | | | | | | |
| | 5 | | | | | | |
| | 6 | | | | | | |

Ideally you should use small and large characters, numbers, as well as special symbols.

Generate a new password for each wallet.

### The Safety of Family and Friends

In case the unthinkable happens, that you get hit by a bus or something of that nature, you should ensure that your family inherits your bitcoins. There's a simple way to achieve this.

On a piece of paper you write the first half of all your passwords. This piece you give to your parents, and preferably also copies to your siblings. You give copies of the second half of your passwords to your best friends. Make sure they understand how everything works.

Even if you trust your family and friends one hundred percent, it is good to give each person only partial passwords. Anyone may become a victim of burglary, so it is comforting for all parties that no one keeps the full passwords.

**Offline is Safer**

To be extra cautious you can use an offline computer that you'll never connect to the internet. In theory a key-logging or screen-capturing virus could jeopardize the safety of any online computer – no matter how strong the password. I've not heard any report of bitcoins stolen through this approach, but one can assume that hackers are working on it.

Electrum has a nice feature called the *Master Public Key*. This lets you keep an offline wallet while still being able to view it, but not spend from it, on any online computer.

Even an offline wallet could, theoretically at least, not be safe. When the computer creates a wallet it uses a unique input which

must be impossible to replicate. If only one other computer on the entire planet ever uses the same input, your wallet can get stolen. The way your system deals with this is through a *Pseudo Random Number Generator* (PRNG). It creates a large array of bits based on noisy sources such as key inputs, mouse movements, CPU temperature, and so on. The number of combinations is virtually infinite, and therefore you can be safe that no one will ever create the same bitcoin addresses as you.

Well, at least that's how it is supposed to work. In 2013 hackers did manage to replicate the PRNG in some android phones, and thereby successfully steal bitcoins. Modern laptops and desktops are considered safe at the moment, but you are advised to keep the threat in mind.

A *brain-wallet* can eliminate this threat. It lets you choose your own input rather than the PRNG's array of bits. Just google *brainwallet github*. It will take you to GitHub where you can download a zip file with all necessary files. Unzip it and open the html file in any web browser. Play around with it for a while until you feel confident you understand how it works.

Now you need to use a truly unique input. No person on the planet should ever use the same input nor shall any brute-forcing hacker ever generate it. In order to achieve this you should be even more careful than with your passwords. Roll the dice at least forty times. Write down the array of results as the input. To

add even more randomness you can append more characters by typing wildly on the keyboard. Write down the public address and the private key, and keep several copies of the latter at safe locations.

Make sure you manually type back in the private key that you wrote down. If the brainwallet comes up with the same address, you can be confident you wrote the key down without any typos.

The brainwallet approach is probably overkill. Its biggest risk is that you don't use a strong enough input, and the second risk is that you make a mistake while typing the private key.

I recommend using Electrum. Make several wallets and keep limited amounts in each. If you own a fortune of bitcoins you may consider dedicating a computer for offline storage of most of your coins. The wallet you use for daily purchases should only include a limited amount of bitcoins, not only to protect against hackers but also so you don't risk sending 10 or 100 times too many coins due to a decimal mistake.

Please keep in mind that even if you do everything correctly, there's no guarantee the bitcoin network itself is safe. It has worked well since the beginning, but it is still an experiment.

## Diversification Reduces Risk

Never put all your eggs in one basket. And never but all your bitcoins in one wallet. This piece of advice is more important than everything I wrote above.

You may divide your holdings into ten different wallets, including a few online ones. The good thing about online services is that they usually have back doors. If you forget your password but registered your phone or email you should be able to regain access. This of course, means that if someone gains access to your email account, your bitcoins may get stolen.

Nevertheless, if you lose a wallet which has only ten percent of your bitcoins, it is not the end of the world.

On the contrary, if you put all your trust in, say, Electrum and a screen capture virus sends the seed back to a hacker, your bitcoins will get stolen.

## Conclusion

With bitcoin you can transfer value as easily as sending email. The fee is less than one cent, but the sender and recipient usually needs to exchange back and forth to the local currency. This adds a considerable cost. Bitcoin is safe if used correctly, but some users lose their bitcoins due to bad habits or ignorance.

Bitcoin is nevertheless the payment system of choice in many real world transactions. As more users adopt bitcoin the cost declines. This causes a positive network effect. This also means that an alternative digital currency cannot compete with bitcoin.

Bitcoin emulates gold in that it has a fixed supply. A fiat currency works the opposite way. It has a central bank to adjust supply. Some believe that the fiat system is about to come to an end. If or when this happens, bitcoin will find a new use as a safety haven. Under a new monetary system, prices are likely to be quoted in units of gold while most transactions are made with bitcoin.

*If you enjoyed this book, please consider leaving a tip. It encourages me to write more. My upcoming plan is to write about Counterparty, a technology which enable decentralized financial assets to be issued and traded on the bitcoin protocol.*

1JPJaEVyieFi93YgtszCwMMjmsJGxfXRag