The Ultimate Guide to Bitcoin

Bitcoin is so quickly evolving. Therefor this guide is also evolving. You can always get the latest version at:

http://bitriches.com/guide

Distribution:

You may freely distribute this work in digital or print media with the following conditions. 1) You do not alter the work 2) This distribution notice remains intact.

Disclaimer - This document is for information and illustrative purposes only and does not purport to show actual results. It is not, and should not be regarded as investment advice or as a recommendation regarding any particular security or course of action.
Note to the Btc Pioneers:

I think we can all agree that Bitcoin is in its infancy. There's also no question that it has the power to catalyze fundamental changes in the world economy as well as shift the balance of power. If Bitcoin takes hold and moves into the main stream then the power that governments hold over money and thereby over people, will will no longer be absolute.

In other words, by democratizing money, power shifts. By eliminating the monopoly governments hold over money it also eliminates their authoritarian power over people. Of course this has far reaching implications.

That being said, it is also obvious that there are many who will do everything in their power to prevent this from happening. We see evidence of this this every day. When mainstream media reluctantly mentions bitcoin it always seems to find an alarming angle. The headlines read "Bitcoin Crashes as Predicted". But a look at the graph shows merely a spike followed by a normalization. The 30,000 foot view consistently shows a climb. Articles abound about how bitcoin can easily be stolen. Or how it is only used for nefarious purposes. Whether it is an intentional smear campaign or simply the normal workings of the media, the end result is the same. Fear.

With so much propaganda spreading fear of bitcoin, there needs to be a counter measure. A way of educating the public. A leaflet dropped into the digital world. A way of dispelling the fear.

That is the purpose of this guide. It is a freely distributable guide in which we have gathered experts in various specialized knowledge areas. Experts who have contributed their knowledge in order to educate. Because:

Knowledge Dispels Fear

As detailed as this guide currently is, there is still much to cover. Bitcoin is ever evolving. As it evolves there is still much need for experts. If you have expertise in the area of bitcoin and feel capable of contributing your knowledge, then we invite you to apply as a contributor. Submit your application here:

http://www.bitriches.com/apply/expert
<table>
<thead>
<tr>
<th>Our Experts</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phil Weaver</td>
<td>Founder: <a href="http://www.bitriches.com">www.bitriches.com</a></td>
</tr>
<tr>
<td>Dr. Syed Asfandyar Gilani</td>
<td>PhD Scholar - City University London (UK)</td>
</tr>
<tr>
<td></td>
<td>Doctorate, Computer Science City University London (UK)</td>
</tr>
<tr>
<td></td>
<td>Dean - Department of Computer Science Leading University in Asia</td>
</tr>
<tr>
<td>Muhammad Waqar Aslam</td>
<td>Masters - MBA Finance University of Agriculture Faisalabad</td>
</tr>
<tr>
<td></td>
<td>Diploma - Banking &amp; Finance Institute of Bankers Pakistan</td>
</tr>
<tr>
<td></td>
<td>Masters - Economics University of the Punjab Lahore Pakistan</td>
</tr>
<tr>
<td></td>
<td>Financial analyst - Bank Alfalah Limited</td>
</tr>
<tr>
<td></td>
<td><a href="http://www.bitriches.com">Linkedin Profile</a></td>
</tr>
</tbody>
</table>
Like what we're doing here?

Support us

1DiBU3CwhKWoxqk39nb2Poc1uRaNR2h7C9
# Table of Contents

## Introduction
- 1) Many Experts..................................................8
- 2) More Like Money than Money............................8
- 3) It's Not Like a Credit Card..................................10
- 4) Buying Bits......................................................12
- 5) It's Volatile! For Now!.......................................13
- 6) You Can't Regulate it Away...............................14
- 7) Can the System Be Hacked?...............................14
- 8) Onward............................................................15

## From the Computer Science Perspective
- 9) Cryptographic Concepts.....................................16
- 10) Digital Signatures............................................18
- 11) Bitcoin Overview............................................19
- 12) Decentralized Electronic Currencies....................21
- 13) Proof of Work..................................................23
- 14) Bitcoin Implementation Details..........................26
- 15) Client Types....................................................29
- 16) Signing Only Client.........................................32
- 17) Thin Bitcoin Clients........................................33
- 18) Bitcoin Mining Clients......................................37
- 19) Backing Up Wallets..........................................38
- 20) Deterministic Wallets........................................38
- 21) Brain Wallets...................................................39
- 22) Malware and Bitcoin.........................................40
- 23) Watch Only Wallets.........................................41
- 24) Paper Wallets..................................................42
- 25) Accepting Bitcoin with QR Codes.......................44
- 26) Bitcoin URI.....................................................45
- 27) Multi-Signature Transactions.............................46
- 28) Bitcoin Escrows...............................................48
- 29) Scalability......................................................49
- 30) Conclusion......................................................50

## From an Investors Perspective.................................52
- 31) What is Bitcoin?..............................................52
- 32) Brief history of Bitcoin....................................52
- 33) How does Bitcoin work?...................................53
- 34) How to buy / get Bitcoin?.................................55
- 35) Why I invest in Bitcoin?....................................56
Introduction

Understanding the fundamentals of Bitcoin is quite simple. However to fully understand it's possibilities and safe and efficient use of it we need to call upon experts from various fields. That is the purpose of this guide. To compile the necessary expertise to fully understand bitcoin in an easily understood document.

If you have followed bitcoin at all, you have seen outbursts from the media designed to create uncertainty and fear around bitcoin. And of course this is expected. You may have even panicked from some of them yourself. It's alright. They are pretty good at triggering emotions. It's what they do. Their business model requires it.

The only answer to that is education. To educate yourself and to help educate others. That is the purpose of this free ebook. That being said, you are free to distribute this wherever you see fit. On your website. In social media. Print it out and give it to a friend. Every new person that reads it is one more person that can speak intelligently about it. And as more and more people can speak intelligently about it, the darkness fades. The fear mongering media weakens. And the free market will be left to do what it will do. And that just might turn out to be an amazing thing.

So. You may freely distribute this document but you may not alter it.

You might also be interested in keeping up with the latest in bitcoin news. To get the latest bitcoin news delivered to your inbox and also be notified when we have updated this document please register at:

www.bitriches.com/user/register
Many Experts

The subject of bitcoin is vast. It's not just about money. It's a lot about freedom. It's about cryptography. It's about economics. It's about business. No one person can be an expert in all these things. Which is why we've brought together a team to create this. Our goal is to have the top experts in all the necessary related fields contribute what is necessary to help people understand bitcoin. Maybe you can help?

It's More Like Money Than Money

Money - V1.0

Money = A medium of exchange

It's a simple concept. But it does rely on one thing. Agreement. Agreement between individuals within society. But at it's core. That's all that money really is. Throughout history we've used sea shells, beads, even rocks. And it has worked for eons. This, of course, is the simplest form of money. Any medium works. Although there are some obvious downfalls to some mediums. Attributes such as easy reproduction, loss of utility (for items that have utility), or impermanence can all lead to potential problems.

Money V2.0

Then there is a second form of money. That is commodity based money. In commodity based money precious metals, rice, precious spices. All kinds of things have been used. That has worked out okay. But with a few hindrances. Portability can be an issue. If cows are your medium of exchange it becomes a slightly difficult endeavor to pay your utility bill. Loss of utility is certainly an issue. Impermanence can be an issue. The value of the commodities utility versus the value of the money can be an issue.
Money V3.0

So the third form of money is creating notes which then represent the commodity. It solves the portability issue. But it creates it's own set of problems. Counterfeiting. Double selling. Oh and then you have to keep all that commodity lying around in case it gets called due. At which time that commodity is doing no useful thing. It's just taking up space and creating an expense in protecting it.

Money V4.0

Fourth is yet another form of money. Fiat money. Fiat money is money because someone else said it is. Not society. But instead government. It is dictated to be money. The term fiat is latin and it means "It shall be". It is money by decree.

Isn't that the same as the first form? Well no. Actually not at all. It is very different indeed. In the first form WE agree upon the medium of exchange. The you's and I's agree. It is our mutual agreement that makes money money. Therefor we have control over what money is. In fiat money, a third party (a government) has control over what money is. As we have seen, that control, that ability to define what money is. Is an amazingly powerful thing. It puts almost limitless power in the hands of that third party.

And power corrupts!

I'm going to take a wild guess and say that that third party is not going to give up that power without a fight.

Money V1.1

Bitcoin is that simple first form of money. It is simply a medium of exchange. It's value is defined simply by our mutual agreement. It has no outside forces that can control it by printing more of it. Or by giving it out to their special friends. It is controlled only by the marketplace and our mutual agreement to be a part of that marketplace.

Small difference? I don't think so.

Bitcoin has many advantages over the early mediums of exchange. This guide will cover those. But there are two that are amazingly important.
1) **It's finite.** Yes it can be mined but only a finite amount of it. So unlike sea shells and beads no one can just go out and get more and introduce it into the system.

2) **It's infinitely divisible.** Which solves the problem of there not being enough to do all the transactions. If the value of a bitcoin gets to high we just drop down a couple decimal places and give it a name for convenience. Actually that's been done. It's called a Satoshi or 1/100,000,000 of a btc.
It's Not Like A Credit Card

Because bitcoin is digital many make the comparison to credit cards. To transferring money around like we do with credit cards online. Well kind of. But not really.

When we transfer money with credit cards or a paypal account we are transferring a digital representation of money. A digital representation of fiat money. Or in other words a digital representation of something somebody else says is money.

Whoa, stop. That's a deep rabbit hole. We best not go down there lest we be here all day.

All kinds of creative things can be done with this digital representation of fiat. Putting lag times in between transfers (So I can send a text message to the other side of the world in under a second but my bank transfer, which is a digital representation only, takes days? Hhhmmmm) Double spending. Where is that money while it's so long in transit. But that is another deep rabbit hole. Let's jump over that one too.

Bitcoin is not a digital representation of money. It is the money. When it transfers to you it's there. Not in account somewhere (unless you purposely structure it that way). It's where you put it.

So that makes it a lot more like paper money than a credit card or a paypal account. And that has some pluses and some minuses.

The pluses. Well it takes all that possibility of manipulation away. All the games the banks play. Well, they can't be played.

The minuses. Well if someone steals your paper money it's gone. Same thing for bitcoin. Transfers are final. It's more like a thing than a representation of a thing. Even though it's digital. So when a thing gets stolen it's gone. When a representation of a thing gets stolen then.... well actually I don't know.

But don't let that worry you too much. Because thee are many ways to secure bitcoin. And many mediums to do it in. Yep you can store it in:

1) A wallet on your phone.
2) A wallet on your hard drive.
3) A wallet on the web.
4) You can even store it on a piece of paper.

Or better yet.

5) You can even store it in your brain.

Yep, really, In your brain. Who said you can't take it with you.

The real power of security comes in when you figure out how to store it in a combination of places. No, not copies of it here and there. Remember it's more like a thing. But passcodes that take 2 out of three to work. So when you store that 75 million on your hard drive and your wife decides to throw that hard drive in the trash you still have a way to recover your 75 million.

Getting confused? Don't be. You get used to it really quickly. Once you Grok it. Give it a little time.

There are some really great security methods. We'll get into all that. The thing is just don't think about it like a credit card or debit card. It's not.

So yes. Security for bitcoin can be pretty powerful. It is based on cryptography you know. Duh!

So when you hear the media cries about security issues. Now you'll know. Yes, if you are foolish with it, sure it can be stolen. But then so can anything. If you leave it lying around.
Buying Bits

One thing to keep in mind. If you try to transfer money from a credit or debit card to bitcoin you probably can't.

Bitcoin to debit card? No Problem. Debit card to bitcoin? Yes you'll have a problem.

But it's not bitcoins fault. It's actually a security problem created by the credit card. Not the bitcoin. You see, all credit card holders can issue chargebacks. You can call your credit card company and deny a charge. They'll believe you and retrieve the money (remember it was only a virtual representation so they can do this). Unfortunately this little aspect of credit cards enables a whole category of crime. Because of the whole "digital representation of money thing.

Criminals can buy things and then charge them back. Or use a stolen credit card and the original owner charges back. They get the items and the merchant loses out. No matter what the scenario it's the merchant that loses. Not the credit card issuer. No they don't guarantee the card to the merchant. The merchant accepts it with the inherent risks.

It happens all the time. The merchant not only loses the goods but also probably paid to ship them. Then he has to spend a bunch of time filling out paperwork for the credit card companies. Then he usually has to pay a fee on top of all that. It's horrible and it's rampant. But it's how credit card companies work. Heck they still got their fees and made a little extra on the side. No biggie to them.

So pretty early on the criminals bought bitcoin with credit cards. Or even with stolen credit cards. That became a pretty big problem. Because bitcoin transfers are final. Credit card transfers are not. They bought bitcoin and the card got charged back. The bitcoin was long gone. The seller of the bitcoin simply lost out. A fast and easy crime.

So you probably can't buy bitcoin with credit cards for this reason. Just remember. It's not a problem with bitcoin. It's a problem with the credit cards.

By the way, if you ever did have a need to make a bitcoin transfer not final. And it will come up. There's a solution for that too. It's very simple to setup an escrow system. Bitcoins have that covered too.

So anyway, just think about bitcoin more like real money and you'll understand it faster.
It's Volatile! For Now!

We've seen bitcoin (btc) prices all over the place. It's been on an amazingly fast upward trend. But along with that fast upward trend has been some crashes.

Actually I'd hardly call them crashes. If you look at the trends long term what you see is spikes and normalizations. But we'll leave that discussion for the economists. It's really not the point right now.

What is important is to realize that in this early stage that is completely normal and should be expected.

Why?

Because bitcoin is mostly being treated as an investment right now. It's so new that the heavy usage is all by investors. And because of that you are going to see wild fluctuations. It's like stocks on steroids. Anytime there is something big in the news you are going to see some wild variations. Anytime a major government steps in and tries to regulate it you are going to see an effect.

This probably won't level out for a very long time. Not until the majority of the activity is actually market activity. Consumers buying goods and services. As btc is used more and more for buying things, those the fluctuations should stabilize. Because at that point it will be millions or billions of tiny transactions that dominate. The invisible hand of the market will take over. The influence of the news will lesson because it will become less and less of a commodity and more and more of a currency.

How long will that take? Who knows. For now the forces that don't like it will do all they can to prevent it becoming a currency. They can do that through regulation and fear mongering. But that is all they can do. Despite their great power they can probably do nothing more than slow down it's progression. Simply delay the inevitable. But not stop it.

We shall see.
You Can’t Regulate it Away

So what happens when a government cracks down with regulations?

It's very difficult for anyone to regulate it. Because:

1) It's highly portable. Very fast and easy to move.

2) It's peer to peer. So pretty hard to shut down.

3) It's anonymous (Unless you somehow attach identifying information to it) so therefore very difficult to track.

That all makes it very difficult to regulate.

What governments can regulate is the in points and the out points, that are under their control.

What has happened so far is that when one government regulates it, the activity just moves elsewhere. As long as there is one place in the world that the in points and out points are not regulated then people are free to transfer their dollars or euros or yen or whatever into bitcoin.

Regulation does not stop bitcoin transfers. So transfers for goods, services, or gifts is very difficult for anyone to stop.

I'm sure that someone somewhere is looking into it. It's not looking good for them.
Can the System be Hacked?

Well actually yes. It's not all that hard. But it doesn't actually do much if it happens. The ledger is reproduced over the peer to peer network. There are a large number of copies of the ledger. So if a copy gets hacked and doesn't match up to the numerous other copies it just gets ignored.

Theoretically someone could create enough computing power to gain control over a majority of nodes. That is a possibility. But definitely an improbability. We'll leave it up to the mathematicians to calculate how much computing power that would take. But from all accounts it appears that we're pretty safe from that theoretical possibility.

Onward

The rest of this guide will get into more technical aspects. We'll dive in a little deeper and look at if from the fields of math, science, and economics. We'll put in summaries where things get a little techie.

We hope you enjoy it and we certainly hope you explore and participate in the world of Bitcoin.
From the Computer Science Perspective

Cryptographic concepts

To understand the principles of Bitcoin, we also need to understand certain cryptographic concepts. Cryptography is the art and science of keeping messages confidential and secure. In addition to that, cryptography is also able to provide authentication, integrity and non-repudiation of messages. In this context, these words have the following meanings:

- **Authentication**. It should be possible for the receiver of a message to ascertain its origin; an intruder should not be able to masquerade as someone else.

- **Integrity**. It should be possible for the receiver of a message to verify that it has not been modified in transit; an intruder should not be able to substitute a false message for a legitimate one.

- **Non-repudiation**. A sender should not be able to falsely deny later that he sent a message.

Cryptography has multiple means of achieving the above-mentioned goals, and we describe some of them that are needed to understand Bitcoin.

If two parties want to send messages securely, they may use encryption to hide the actual contents of the messages (plaintext) and transform them to ciphertext, i.e., to make them unreadable by anyone else. The receiving party can perform decryption to
recover the plaintext. Usually, the algorithms for encryption and decryption are well-known, and only the encryption/decryption keys are maintained secret. If both parties use the same key for encryption and decryption, they use a symmetric encryption algorithm. Symmetric algorithms alone provide confidentiality, but to achieve the other goals, we need other techniques, such as hash functions.
The output of a hash function is not dependent on input in any distinguishable way. These properties give us the possibility to use hash functions to verify integrity of messages. Someone having the hash of a message can determine whether the message is intact. This method is used, for example, in BitTorrent protocol: the .torrent file has hashes of the pieces of data, and the data is checked to verify that it has the same hashes after it is downloaded from the peers. If the hash of a downloaded piece of data does not match the one in the .torrent file, such piece is rejected and later downloaded from someone else. As a result, peers are unable to send fake data and force the downloader to accept it.
Digital Signatures

When a digital message provides authentication, integrity and non-repudiation together, we say it has a *digital signature*, similar to a paper document with a handwritten signature [8]. Although it is possible to create digital signatures by using symmetric algorithms, hash functions and a trusted third party, as described in [8], this solution is inefficient.

If we give out our public key, anyone is able to send us messages encrypted with it, and those messages could not be read by a third party.

Public-key cryptography could also be used for digital signing. We can find the hash of the message and encrypt it with the private key, thus forming a digital signature. If someone who has the public key receives the message with the digital signature, it is possible for him/her to verify both the authenticity and integrity of the message by decrypting the signature with the public key and comparing the result to the hash of the message.

The signed message also has the property of non-repudiation, that is, the sender is not able to falsely deny sending the message.

There are many public-key algorithms. The RSA algorithm is the most widely used. There is also another family of public-key algorithms, known as Elliptic Curve Cryptography (ECC).
Bitcoin Overview

Since the introduction of public-key cryptography, various proposals have been made to make a monetary system based on it. Examples are David Chaum’s "Blind signatures for untraceable payments" and Ian Grigg's "Triple Entry Accounting" [6].

David Chaum

Chaum’s paper suggests a system where payments are done anonymously and securely. Though a trusted third party is still needed.David Chaum also founded DigiCash BV, the first company to provide a cryptographic digital currency. Even though DigiCash became rather well-known in the payment industry in the 1990’s, the company went bankrupt in 1998 [7].

Ian Grigg

In Ian Grigg's paper, when two willing parties transact, the payer (Alice) creates a receipt which includes:

1) The payer's and payee's (Bob) names
2) The amount of money to be sent
3) The digital signature of the whole receipt.

The digital signature is made with the payer's private key. This receipt, together with the current date and time, is signed by issuer of the money (Ivan). This is illustrated in Figure 1. From this moment, as Ian Grigg says, "The Receipt is the Transaction" [6],
which means that we do not need to keep a whole history of all transactions, but only the latest receipts.

Ian Grigg claims that this system was implemented for internal money in a company, and proved to be more efficient than old-style accounting [6].

![2: A Signed Receipt](image)

**Figure 1.** The Receipt is the Transaction [6]
Decentralized Electronic Currencies

The electronic currencies mentioned previously have the following common property: they are centralized, that is, they rely on a trusted party, the issuer, which facilitates and controls the transactions.

In 2008, the first decentralized electronic currency called *Bitcoin* was proposed by someone named Satoshi Nakomoto [1]. The real identity of that person is not known.

In Ian Grigg's system, every transaction (receipt) is also signed by the trusted third party (issuer), which verifies that the payer has enough money to send and that the money being spent was not spent before (also known as *double-spending*). Bitcoin, on the other hand, makes all transactions public, so that everybody is aware of all transactions and is able to verify the chain of ownership and the non-existence of double-spending attempts. This idea, as a theoretical concept, was first described in Wei Dai's essay "B-money" [9].

Bitcoin relies on a *peer-to-peer overlay network*, built on top of the Internet, commonly referred to as *Bitcoin network*. This *peer-to-peer overlay network* is a special kind of network which differs a lot from how computer networks are usually constructed. *Overlay network* is “an application layer virtual or logical network in which end points are addressable and that provides connectivity, routing, and messaging between end points” [43]. Bitcoin network provides a communication channel to broadcast transactions and send other information between users (*nodes*). As of November 2013, there are approximately 18000 nodes in the network even though the number varies with time [10]. Typically, Bitcoin nodes connect to 10-100 other nodes simultaneously.
Bitcoin's unique feature is the method for accepting/denying transactions and agreeing on a single history of transactions by the network. Due to propagation delays and connectivity issues, it is impossible to make everyone aware of all transactions at all times, and this can be abused by double-spending the money. Someone could spend the same money twice before the first transaction propagates far enough, so there must be a way to determine which transaction is valid.

One obvious solution is to make those transactions that most people agree with valid. On the Internet people are represented by the software applications they are running and their respective IP addresses. If the validity of a transaction were determined by the majority of nodes, i.e. the majority of IP addresses, the system could be cheated by someone able to allocate many IPs. That is why Bitcoin uses a different way of determining transaction validity. This technology is called proof-of-work and was originally suggested in Adam Back's Hashcash [11] as a measure to prevent email spam.
Proof of Work

We provide a brief explanation of the principle of proof-of-work. For many cryptographic hash functions, the number of attempts to find an input whose hash begins with a certain substring can be probabilistically estimated, since the most efficient way to search for such an input is to brute-force by trying consecutive inputs [11]. An input that produces a hash with a certain leading substring is also called "partial hash collision", and the process of finding suitable input is called mining [12]. For example, if we need a certain 32-bit long leading substring in the binary representation of the hash, the expected number of inputs that we need to try is $2^{32}$, which is more than 4 billion. In Bitcoin, finding partial hash collisions serves as a proof that a certain amount of computation has been performed, this is why it is called proof-of-work.

Proof-of-work is used in Bitcoin for two purposes: the first is that proof-of-work is a means of “voting” about transaction history, where the more work one performs, the more voting power one has. The second purpose is the creation of money. Wei Dai writes:

Finding partial hash collisions exactly fits this definition: it is easy to determine how much computing effort it took to find a given collision, and the collision does not have any other value. In Bitcoin, when a partial hash collision is found, it serves as a “vote” for certain transactions to be included in the history and provides a reward for the miner (participant engaged in Bitcoin mining).

Another important concept of Bitcoin is that every proof-of-work is based on some previous proof-of-work. This is implemented by including the hash from the previous
proof-of-work into the input of the current proof-of-work, thus forming a chain, as shown in Figure 2. Input data for computing proof-of-work is combined into blocks, and all blocks together form a block chain.

![Figure 2. Chain of blocks [1]](image)

As each block includes the hash of some previous block, we say that each block is built on top of some previous block and extends it. The “voting” happens when miners choose the block they wish to extend. Choosing a certain block implies agreement with all transactions in that block and all previous blocks relative to that block. If a group of miners works on a different block than others, the block chain may diverge, resulting in two or more competing sub-chains. The chain in which more computing power is invested will eventually become longer, and other Bitcoin nodes will prefer the longest sub-chain, discarding all other sub-chains [1]. As a result, the block chain includes only those transactions that the majority of processing power agrees with. In Figure 3, an example of chain divergence is shown, but the black chain is the longest and is preferred by Bitcoin nodes.
The block chain should not be confused with the coins themselves, which are chains of digital signatures. The block chain interconnects blocks, whereas chains of digital signatures interconnect transactions.

If a node follows the above rules, we consider it to be honest. An important condition which must be held for successful operation of Bitcoin network is that honest nodes altogether always have more processing power than any attacker, and no attacker (or cooperating group of attackers) is able outperform all honest nodes together. While this condition is held, an honest block chain will always be longer than any of the attackers’ chains, and will be preferred by other Bitcoin nodes [1].

**Figure 3.** Block chain diverges, black chain wins
**Bitcoin Implementation Details**

Though describing all implementation details of Bitcoin is beyond the scope of this thesis, some details should be examined to understand the features of Bitcoin clients.

Every block consists of a *block header* and the actual content, i.e. transactions. The block header contains the following information:

Table 1. Block header structure

<table>
<thead>
<tr>
<th>Field</th>
<th>Version</th>
<th>Previous hash</th>
<th>Merkle root</th>
<th>Timestamp</th>
<th>Bits</th>
<th>Nonce</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bytes</td>
<td>4</td>
<td>32</td>
<td>32</td>
<td>4</td>
<td>4</td>
<td>4</td>
</tr>
</tbody>
</table>

*Version* is the same in all blocks

*Previous hash* – hash of the previous block header

*Merkle root* – hash which verifies the integrity of transactions in the block.

*Timestamp* – time when block was generated, as a UNIX timestamp (number of seconds passed since 01.01.1970 00:00:00 UTC)

*Bits* – compact representation of the *target*, which designates the difficulty required for proof-of-work (1)

*Nonce* – value to be changed when mining in order to find partial hash collision.
Instead of storing transactions themselves in the block header, only the Merkle root is put there, which is the root hash of the Merkle tree computed from all the transactions to be included in the block. Merkle tree is generated by the following procedure. First, hashes of transactions are calculated. Then, these hashes are put pair wise and hashed again, producing a new, smaller set of hashes. This step is repeated multiple times until only one hash remains. Finally, this hash, which is called root hash, or Merkle root, is put into the block header. The exact procedure for calculating the Merkle tree can be found in the source code of Bitcoin clients [13]. As a result, every block header has a fixed size of 80 bytes, and a possibility exists to verify transactions without having the full block chain, but only the headers.

Figure 4 illustrates the structure of the actual block #183301 of the Bitcoin block chain. Only five transactions are shown for simplicity, though the actual number of transactions is 432. Tx1 to Tx5 are transactions, H1 to H5 are hashes of transactions, Hash12, Hash34, Hash55 and Hash1234 are hashes of previous hashes. The previous block hash starts with 13 zeros in hexadecimal representation, which means 52 zeros in binary representation. Finding this proof-of-work requires $2^{52}$ attempts on average.
Figure 4. Block #183301 of the Bitcoin block chain

Since it is impractical to transfer individual monetary units ("coins") separately, Bitcoin provides a way to split and merge "coins" in transactions. Each transaction has "inputs" and "outputs", where each output identifies the address of the receiver of coins and the amount received by him/her, and each input provides a reference to an earlier output that is being spent and a digital signature of the payer with the corresponding public key. An address in Bitcoin is a hash of the address owner’s public key. When verifying a transaction, the actual public key found in the input is hashed and compared to the address specified in the referenced earlier output. There are also "generation transactions", which give a reward to someone who finds a block, and these transactions have empty input. The digital signature algorithm used to sign transactions is ECDSA (Elliptic Curve Digital Signature Algorithm), which has several advantages.
over more widely used RSA/DSA: much smaller key size and faster computation while the security factor is the same [14].
Client types

Full clients are the ones which implement the full Bitcoin protocol and hold a full copy of the block chain. This includes discovering and communicating with other nodes, sending and receiving transactions and blocks, saving all valid blocks locally, verifying all transactions received and broadcasting all legitimate transactions. In addition to those, full Bitcoin clients also provide services for the user. These services are: storing one's transaction history, private keys for the "wallet" and providing a Graphical User Interface (GUI), command-line interface or an Application Programming Interface (API) for viewing current balance, transaction history and initiating new transactions.
Full Clients

Some examples of full Bitcoin clients are: Original Bitcoin client [16], Armory [36], and Libbitcoin [37]. We will look more closely at the operation of the Original Bitcoin client, also known as the Satoshi client. When Bitcoin was initially created, it was the only software that could be used for dealing with Bitcoin, hence the name. The Satoshi client keeps the block chain, nodes’ addresses and the wallet file in the client’s data folder. The wallet file contains the wallet owner's transaction history, address book and private keys, so it must be kept securely to prevent stealing of Bitcoins.

Starting from version 0.4.0 the Satoshi client has a wallet encryption feature.

Since the early days of Bitcoin, and until version 0.3.22, the original client had a mining capability [17], which was removed because specialized mining clients are much more efficient. Figure 5 shows the interface of the Satoshi client. The overview screen has information about the current balance and most recent transactions. A transaction is said to be unconfirmed if it was sent but not included in a block yet.
Figure 5. Unconfirmed transaction in original Bitcoin client, version 0.5.0

Using a full Bitcoin client has some drawbacks. One of them is excessive network and file system usage: a full client has to have a full copy of the block chain locally, which occupies 2 gigabytes as of November 2013 and which will only grow in the future. Full clients have to be aware of all transactions, so they receive and send transactions and blocks all the time and consume network bandwidth.

On the other hand, operating a full client makes the Bitcoin network stronger and more difficult to attack.
Headers Only Clients

For some users it may be difficult to store block chain data on their devices. For example, on mobile phones. Fortunately for such users, there are *headers-only clients* which don’t require that much storage space. BitcoinJ software library [18] and clients based on it (e. g. Multibit [38]) do not download and store the full block chain but only the block headers, which occupy only 14 megabytes as of November 2013 and could be kept in memory even on mobile devices [18]. BitcoinJ downloads full blocks only sometimes, when it expects incoming transactions and when it searches the block chain for keys that are in the wallet. Even though headers-only clients are not able to verify transactions against the full block chain, they are not less secure than full clients if some of these precautions are taken:

- Waiting for multiple blocks (usually 6) before considering the payment complete
- Receiving a copy of the transaction in question from a node trusted to be running a full Bitcoin client
- Receiving the transaction in question from multiple nodes [19]
Signing-only Clients

BitcoinJ author Mike Hearn suggests a procedure for proving inclusion of a transaction in a block without having to download the whole block, but only the transaction itself and the corresponding Merkle branch [19]. Having this information is enough to verify that the transaction was included in a particular block. This procedure is known as Simplified Payment Verification and was also described in the original Bitcoin paper [1]. Using this procedure can save a lot of bandwidth and provide even greater security, but unfortunately, it has not been implemented in either BitcoinJ or any of the full clients.

The name signing-only clients means that they only sign transactions, but do not deal with block chain or even block headers. Instead, these clients request data about certain transactions from the server. If a transaction happens in the Bitcoin network that involves one of the connected clients’ wallets, the server may also push such information to a particular client that is interested in it. Signing-only clients send out only their own transactions. Consequently, the overhead of running such a client is much lower than that of full or headers-only clients, as the file system is used only for our own keys and transactions, and we only send and receive transactions that concern us.

Signing-only clients do not require much storage, network bandwidth and computing power, and therefore can be implemented in various ways: as a desktop application (Electrum [20]), mobile application (BitcoinSpinner [21]) or as a Web application (Blockchain.info [22]). In Web-based signing-only clients, cryptographic features are implemented in JavaScript and are executed in the Web browser, so the private keys of the wallet are never sent to servers unencrypted. A certain level of trust is required in
the server we are connecting to, because the server will know all our transaction history, and it is possible for the server operators to send us false transactions and trick us into thinking that we have more or less money than we actually do. This kind of attack is not dangerous and is not profitable for the server operators, because it is not possible for them to trick us into signing transactions against our will. In addition, this attack can be mitigated by connecting to multiple servers or to our own server, which can be set up with open-source software [20, 23].

Figure 6 demonstrates the process of sending Bitcoins with the Electrum client. The only required information is the “Pay to” (payee’s Bitcoin address) and the “Amount”. The transaction fee is calculated automatically.

![Electrum Transaction Creation](image)

**Figure 6.** Transaction creation in the Electrum client
Thin Bitcoin Clients

Thin Bitcoin clients (also called eWallets or browser-based wallets) are the ones which do not hold private keys and do not sign transactions themselves. Instead, they send commands to a remote server to perform these operations. The remote server acts in a similar way to a bank, providing financial services to customers. The most important advantage of thin clients over other types of clients is that the user does not have to worry about backing up private keys and keeping them safe at the same time, as these operations are performed on server-side on behalf of thin clients. Another benefit is that thin clients are the easiest to set up: one only needs to visit the eWallet website and set up an account. It takes about one minute.

Some examples of thin Bitcoin clients are: MyBitcoin (Now defunct) [24], Instawallet (Now defunct) [25], and MtGox [26].

Instawallet did not even require registration. When visiting the page for the first time, a new account is created automatically [25]. Figure 7 is a screenshot of Instawallet’s transaction creation dialogue, which is very simple and straightforward.
Figure 7. Transaction creation in the Instawallet client

The high usability of thin Bitcoin clients does not come without a price. Ultimate trust is required in the eWallet provider, since it not only knows the users’ transaction history, but also has control over the users’ money. There is no obvious way to ensure that the provider has the amount shown as the balance is backed by actual Bitcoins stored in reserve. Finally, the provider can become a victim of loss or theft of Bitcoins, or of a malicious takeover, which can result in a loss of customers’ funds. This has happened to multiple wallets including Instawallet.
Bitcoin Mining Clients

Bitcoin mining clients, or simply miners, are specialized clients that are not used to send or receive Bitcoins. Their only usage is mining. Initially, the only mining client was the original Bitcoin client, which implemented mining on a CPU (Central Processing Unit, I.E. the processor in your computer). As time went on, more people learned about Bitcoin and became involved in mining. This, by design, raised the difficulty level of mining.

At the end of 2010 the difficulty of finding blocks rose to such levels that it would take 1 year on average to generate a block and get the 50 bitcoins reward if mining is done on a single computer with the original client [28]. This was due to the fact that specialized mining clients were created to perform mining on graphics card’s GPU (Graphicval Processing Unit, typically used by gamers), and these clients turned out to be 100 times more efficient than the original Bitcoin client, which still used CPU mining [27]. As a result, the built-in mining capability of the original client became obsolete and was removed in June 2011 [17]. GPU still remains to be the most popular mining hardware [27] A GPU can be used not only for mining, but also for playing games and using other software applications that require a lot of computational resources. Some examples of Bitcoin mining clients that implement GPU mining are: Phoenix [39], CGMiner [40].

Even with a GPU, it took a few days on average to generate a block and get a reward. If someone was unlucky, he would not get a reward for weeks, because the rewards were too volatile. On 27th of November, 2010 forum member Slush suggested pooled mining (initially it was called cooperative mining) to combine the power of
multiple miners to work on the same block [28]. Instead of getting a large reward once
in a long time, miners started to get smaller rewards more frequently. Pooled mining
became very popular and now accounts for more than a half of all Bitcoin mining [29].

**Backing Up Wallets**

Some Bitcoin clients, including the Satoshi client and Multibit, generate cryptographic
keys randomly. After initialization, the Satoshi client generates the wallet file with 100
keypairs in it [30], which correspond to 100 Bitcoin addresses. Since it is encouraged to
use a different address for every payment, 100 addresses will be used up quickly. If
that happens, the Satoshi client generates new keys when necessary. This way of
operation makes backing up the wallet difficult. To ensure that all keys are safe, we
need to do the backup after every transaction. If such backup is not done, a loss of the
original wallet will result in a loss of Bitcoins belonging to the newly-generated
address. The Satoshi client does not have any built-in backup functionality, and
implementing frequent and secure backups is not an easy task for those not involved in
IT.
Deterministic Wallets

Fortunately, deterministic wallets provide a solution to this problem.

Some of the Bitcoin clients, for example, Electrum and Armory, generate keypairs and, consequently, addresses deterministically. Deterministic generation means that any number of cryptographic keys is generated from a relatively small seed. A known deterministic algorithm produces a keypair from two arguments: seed and a sequence number. If the same seed and number are later supplied to that algorithm, it will always produce the same keypair [31]. As a result, when using a client with a deterministic wallet, we only need to backup the seed, and it has to be done only once. If we have to restore the wallet later, we will supply the seed to the client, and the client will restore all keys from the seed and the history of transactions from the block chain [20].
Brain Wallets

The concept of a *brainwallet* is closely related to deterministic wallets. At the current level of computing technology, randomly-generated numbers of 128 bits “can guarantee uniqueness across space and time” [32]. After generating a random number of 128 bits we can be sure that no one else in the universe is able to generate the same number independently. This number can be used as a seed for a deterministic wallet. At the same time, we can also convert this number to a human-readable form and memorize it. 128 bits can be represented as 128 zeros and ones, or as 32 hexadecimal characters, or as 24 characters in Base64 encoding [33].

However, the most efficient way of memorizing a random number is to convert it to a *mnemonic code*. We choose a list of common English words and agree that each word represents a certain sequence of bits. By using this method, a 128 bit number can be represented by 12 English words, which are easy to memorize.

Someone may put some money in a deterministic wallet, remember the seed and remove the original wallet from the hard drive. After these actions have been performed, it is not possible to recover the keys and the money in any way other than to generate the keys from the seed. As the seed does not exist on any physical media, the information on how to access the money is now in the person’s mind (brain) and nowhere else. The wallet becomes a *brainwallet*. 
Malware and Bitcoin

The threat of malicious software is very prominent nowadays, and any computer can be compromised by viruses, Trojan horses and other types of malware. After Bitcoin became more valuable, cybercriminals created malware that steals the wallet.dat file, which holds the private keys for the Satoshi client [34]. Possession of this file enables the attacker to steal all Bitcoins from the addresses in the wallet. If the wallet file is backed up to some location which later becomes accessible by an attacker, it is also possible for him to steal the money.

To mitigate these threats, original Bitcoin client developers introduced wallet encryption in version 0.4.0 [35]. Other clients implemented a similar feature. Users may choose a passphrase, which encrypts the private keys in the wallet, and unencrypted private keys are never written to disk. Figure 11 shows the interface for setting a passphrase in the Satoshi client. If an attacker gains access to an encrypted wallet, it is not possible for them to steal any money from it, assuming the passphrase is not compromised. On the other hand, it is still possible for malware to steal the money, if the malware runs on the same computer and under the same privileges as the Bitcoin client itself.

For merchants, both online and offline, who accept payments from the public, it may be dangerous to keep the wallet with the private keys on a computer that is exposed to the public, such as an Internet server or a computer in a shop. Such computers can become targets of cybercriminals and, if they succeed in infecting these computers with malware, the merchants may have their funds stolen. Publicly exposed computers are
more vulnerable to malware infestations than other machines which are not publicly known. Fortunately for merchants, the Bitcoin protocol provides a possibility to accept and track payments without having access to private keys.
**Watch Only Wallets**

The Armory client [36], the Electrum client [31] and some Web-based services such as BitcoinMonitor (now defunct) [41] provide *watch-only wallets*. These wallets have neither private keys nor any information, such as a seed, on how to obtain them. Instead, watch-only wallets have only the public keys and the corresponding Bitcoin addresses. This information is enough to watch the block chain for transactions involving given addresses, but not enough to initiate transactions with them. Consequently, if an attacker gains access to a computer running a watch-only wallet, they will not be able to steal any money. The only useful information an attacker will learn is that certain addresses belong to the same person.

Watch-only wallets can be either randomly-generated or deterministic.

The implementation of randomly-generated watch-only wallets is relatively straightforward: the block chain is watched for given addresses. The drawback here is that we need to either store a large reserve of public keys or send new public keys when they are needed.

The digital signature algorithm used in Bitcoin, the Elliptic Curve Digital Signature Algorithm, provides a possibility to generate an infinite number of public keys deterministically from a *master public key*, which in turn is derived from the seed [42]. Merchants can use the following procedure. First, a seed is generated and stored on a private, secure computer. A master public key is derived from the seed and copied to the public-facing computer. The Bitcoin client on the public-facing computer uses the master public key to generate new addresses when they are needed. After an address is given to a customer for making a payment, the block chain is watched for transactions
involving this address. If the public-facing computer is compromised, no money will be stolen because no private keys can be derived from the master public key [42].
**Paper Wallets**

There may be reasons to make a backup copy of a Bitcoin wallet not on digital media, but on plain paper instead. Some Bitcoin users prefer to keep their long-term savings on paper to ensure greater security. If the Bitcoin client uses a deterministic wallet, the seed can be printed on paper and put into a safe place. The Armory client [36] is the only one that has paper backup functionality built-in. Figure 8 shows an example paper backup made with the Armory client. The QR code is provided for convenience to avoid having to type letters manually when restoring the wallet from a backup. The Electrum client doesn’t have a built-in printing feature, but its wallet could also be easily backed up on paper by printing the seed manually.
Figure 8. Paper backup preview in the Armory Bitcoin client

Backing up wallets with randomly-generated keys is more complicated. Such wallets may have hundreds of keypairs which would occupy multiple pages. Restoring from such a backup would be a long and tedious process. One of the solutions to backing up non-deterministic wallets is to transfer the money to be backed up to one address and print out the corresponding private key. Another approach is to transfer the money to a deterministic wallet and perform the backup as described earlier.
Accepting Bitcoin with QR Codes

There are other uses of papers with QR codes in Bitcoin than backups. Papers with printed QR codes of Bitcoin addresses can be used to accept payments. A poster with a Bitcoin address and some text encouraging donations can be put on a wall in a public place to raise funds. BitcoinSpinner [21] has the ability to scan QR codes with the phone’s built-in camera and, if the scanned code is a Bitcoin address, send money to it.

You can try it out by sending Bitcoin to the QR code below (Much appreciated!)

A paper with a private key printed on it can be used as a means of payment by itself. The person receiving the payment can scan the code, sign a transaction by using the scanned private key and transfer the money to his/her own wallet.

Merchants can show a Bitcoin address as a QR code on a screen to accept payments from customers at the point of sale. In this setup, a watch-only wallet described is very useful as it allows confirming the receipt of the money immediately after it is sent while keeping these Bitcoins inaccessible by anyone at the point of sale.
Bitcoin URI

When using a Web browser, we open new pages and download files by clicking on links. Every link on the Web has a URI in it, which tells the browser how to access certain content [46]. Links greatly simplify Web browsing, as entering URIs manually takes much longer time than clicking. To simplify Bitcoin payments and to avoid having to type addresses and amounts manually, the Bitcoin URI scheme was introduced.

As World Wide Web creator Tim Berners-Lee suggested, a URI consists of a scheme and a path, which are separated by a colon. A path describes the resource itself, and a scheme denotes the namespace for that resource [46]. There are many URI schemes nowadays, and the most popular one is HTTP, which is used to access Web pages. In the recent years, links with the MAGNET URI scheme became a popular way to identify resources in Bit Torrent network by their hash [47]. In a similar way, the Bitcoin URI scheme is used to identify addresses and (optional) amounts to be paid.

Several Bitcoin clients, including Electrum [31] and Armory [36] support Bitcoin URIs and fill in the money sending form with the data from the URI when the link is clicked on. Mobile clients, such as BitcoinSpinner [21], can recognize Bitcoin URIs in QR codes and help the user to avoid typing the address and amount manually.
Future enhancements

After the introduction of wallet encryption and watch-only wallets, security of Bitcoin clients improved dramatically, but still remains to be a valid concern. During 2011 and the first half of 2012, there have been several large-scale security breaches and heists whose victims were mining pools, Bitcoin exchanges and their customers [48, 49, 50]. The reasons for these unfortunate events were not only negligence and disregard of security practices, but also inherent weaknesses in the current Bitcoin protocol.

These weaknesses stem from the fact that the possession of the private key for a certain address gives ultimate control over all money belonging to that address, and the private key is always needed for signing transactions. To improve security, we may try to implement some multi-factor authentication procedure, as was done by BlockChain.info wallet service: Web-based Bitcoin client requests you to confirm transactions on a mobile phone [22]. Even though this procedure may improve security, in the very end, the benefits of any multi-factor authentication procedure are lost when one of the parties receives the private key to perform signing. If this party is compromised, all security is lost.
Multi-Signature Transactions for Stronger Security

The solution to overcome these problems is to use multi-signature transactions. These transactions require multiple signatures to be completed instead of one. We may think of a multi-signature transaction as a transaction that has more than one recipient address, and several signatures are needed to spend this money further. Gavin Andresen, the main developer of Bitcoin, proposed two new types of transactions: 2-of-2 and 2-of-3 [51]. In a 2-of-2 transaction, money is sent to 2 addresses, and signatures from owners of both addresses are needed to spend this money. In a 2-of-3 transaction, money is sent to 3 addresses, and signatures from any 2 of them are enough to spend the money. The actual implementation is more sophisticated and is described in [52]. To initiate a multi-signature transaction, money is sent to an address which is a hash of 2 or 3 public keys of receiving parties. This address is recorded in the output part of the transaction. To spend this transaction later, 2 signatures must be supplied in the input part of the next transaction.

The process of constructing multi-signature transactions is more complex than normal transactions and involves negotiation between several parties. The exact procedures are not defined as of November 2013. In a 2-of-2 transaction, receiving parties need to collaborate to construct the receiving address. One of the possible procedures may include exchanging public keys first, creating the receiving address independently and verifying that the same address was created. When sending this address to the payer, both receiving parties need to be sure that the same address was sent.

The security of Bitcoin wallets can be greatly improved with the use of 2-of-2 transactions. We may store one of the private keys on a computer and another one on a mobile phone. After public keys have been exchanged between the computer and the
wallet, we may generate the common receiving address and send money there from a normal wallet. From this moment, if we want to spend the money on the common address, we need signatures from both the computer and the phone. If either the computer or the phone is compromised by an attacker, the money will not be stolen. At the same time, if either the computer or the phone is lost and we do not have the backup of the data, the money on the common address will be lost. But, fortunately, this drawback can be overcome with 2-of-3 transactions.

A third-party service can be used to hold the third private key in a 2-of-3 transaction. In normal circumstances, we may use the same computer and phone, since 2 signatures are enough to spend the transaction. If one of the devices breaks, we may ask the third-party service to sign our transaction. It should be noted that for better security, any authentication credentials for the third-party service should not be entered on either the computer or the phone, as they may become compromised together with an additional private key. Instead, they should be entered on a completely different device. This procedure ensures both security and availability of Bitcoins in case of a failure.
**Bitcoin Escrows**

Another application for 2-of-3 transaction is three-party escrow. If the Buyer purchases certain goods from the Seller, they may choose the Arbiter, trusted by both the Buyer and the Seller to resolve disputes. Before the shipping of goods, a 2-of-3 transaction is initiated. The Buyer sends money to the common address constructed from the public keys of the Buyer, the Seller and the Arbiter. If the purchase runs smoothly and the Buyer is satisfied, he/she gives the signature to the Seller, who adds his/her own signature and gets the money. If the Buyer is not satisfied, the Arbiter has to decide whether the Seller fulfilled the conditions of the purchase. Depending on the Arbiter’s decision, he/she gives his/her signature to either the Buyer or the Seller.

Multi-signature transactions also have certain drawbacks. They require sophisticated protocols to be created and occupy a few times more space in the block chain than normal transactions. Deterministic wallets are not usable for multi signature transactions when third parties are involved where we do not have control over their wallet seeds. In these cases, we need to save copies of public keys involved in those transactions after they happen. This deprives deterministic wallets of their advantages over randomly-generated ones.

Multi-signature transactions have only been implemented in the original Bitcoin client, and only in its command-line interface [54]. Even though some proposals for negotiating multi-signature transactions exist [53], a lot of work needs to be done to ensure compatibility and correct operation of the protocol.
Scalability

At the current (November 2013) level of 20 000 transactions in Bitcoin network per day [56], a normal desktop computer is powerful enough to be a full Bitcoin node and to do all activities associated with it. If the popularity of Bitcoin grows further and the number of transactions per day increases, at some point normal home computers will not cope with increased load. A well-known security researcher Dan Kaminsky criticised Bitcoin for lack of scalability [55]. To make Bitcoin more scalable, several optimizations have been proposed.

The author of the BitcoinJ client Mike Hearn suggests using the Simplified Payment Verification procedure, which allows clients to perform verification of transactions without having a full copy of the block chain [19]. Implementing this procedure may significantly decrease the amount of disk space required for full clients to operate. Another way to improve storage efficiency is to remove all transactions that are already spent from the block chain. It has been calculated that doing so reduces the size of the block chain by 71 percent [57].

Wrapping up this Chapter

Even though Dan Kaminsky characterized Bitcoin as “a really strange use of cryptography” [55], it serves its purpose quite well. Creating an account is as easy as installing a software application. Sending and receiving payments is simple and does not require submitting any documents anywhere. The Bitcoin network is very reliable and as of November 2013 has had only one major disruption since its inception in 2009.
The growth rate of the Bitcoin ecosystem and the underlying technology is tremendous. Bitcoin was first described in 2008 and started operating in 2009. During 2010, GPU mining clients were being developed, and miners gradually switched from CPU mining to GPU mining. In the late 2010, pooled mining was introduced and quickly became the dominant form of mining. After Bitcoin was featured in mass media in 2011, the Bitcoin community and the price of Bitcoins started growing even faster. Unfortunately, the sudden growth of Bitcoin’s popularity led to a series of robberies and data leaks. These severely impacted the public’s trust in Bitcoin and the price of it. One of the reasons for these events was a lack of security features in Bitcoin clients. In the beginning of 2011 wallet encryption and watch-only wallets did not exist. However, a lot of talented software developers joined the Bitcoin community in 2011. Some technologies, such as proof-of-work and deterministic generation of public keys, were used on a large scale for the first time in Bitcoin clients.

Usability and user-friendliness of Bitcoin is improved with deterministic wallets, QR codes and Bitcoin URIs.

Wallet encryption, watch-only wallets and paper backups enhance security of Bitcoin clients. Brainwallets boost both usability and security. These features together brought Bitcoin user experience much closer to that of existing payment systems.

Bitcoin is still in its infancy, and its impact on the world’s economics is negligible. We expect both the economics and the technology behind Bitcoin to evolve and expand. Multi-signature transactions, when they are implemented, will provide a vast array of innovative usages of this currency. Since Bitcoin ecosystem develops so fast, it is impossible to predict what will happen to it in the next year. We are looking forward to seeing new ideas and developments.
From an Investors Perspective

What is Bitcoin?

Bitcoin is an experimental decentralized digital currency used as a mode of instant payments to anyone, anywhere in the world by using peer-to-peer technology without any central authority. Managing transactions and issuing money are carried out collectively by the network.

Bitcoin is referred as a crypto-currency because it is decentralized and uses cryptography to secure and control the transactions and prevent double-spending (a problem for digital currencies).

Brief history of Bitcoin

Bitcoin is the first achievement of a concept called "crypto-currency", which was first described in 1998 by Wei Dai on the cypherpunks mailing list. He suggested the idea of a new form of money that uses cryptography to control its creation and transactions rather than a central authority. The first Bitcoin specification and proof of concept was published in 2009 in a cryptography mailing list by Satoshi Nakamoto.
How does Bitcoin work?

Bitcoin Wallets
Bitcoin Wallets come in a variety of forms. They can be web based, desktop based, mobile device based, paper based, or even stored in the owners mind. Some issuers have even created physical coin based bitcoins. Be cautious when purchasing these as they can be based upon a given hashtag which actually carries the bitcoin or they can be simply a representation of a bitcoin stored elsewhere. The latter depends upon the credibility of the issuer.

The Block Chain
All transactions are routed through block chain (basically ledger of transactions). It is a share public ledger and everyone of Bitcoin network relies on this block chain. There are copies of the blockchain (ledger) spread out across the entire network. This large number of copies is what makes the ledger safe from hacking. A hacked copy would simply be disregarded by the network if it did not match the other copies.

To compromise the network a hacker would need to have under his control enough computing power to affect more than half of the network. As of November 2013 the computing power of the network is 64 exaFlops. To put that in perspective, the combined computing power of the worlds top 500 supercomputers is .25 exaflops. So the bitcoin network is approximately 256 times more powerful than the combined power of the worlds top 500 supercomputers.

This creates a great deal of assurance that the ledger can not be maliciously attacked.
Encryption Techniques

For security and integrity, Bitcoin uses encryption techniques. When Bitcoin address is created, a cryptographic key pair generated having a public key and a private key.

Private Key

In block chain each transactions is a transfer of value between Bitcoin wallets. A secret piece of data which is used to authenticate or sign the transactions is called a private key. This encryption prevents the transaction from being altered once it has been issued. All transactions are displayed publicly among users. The network will confirm transaction across nodes. Confirmation across the network generally takes about 10 minutes. Transactions offering higher transaction fees will generally be confirmed first.

Mining

Bitcoin uses a distributed consensus system that is used to confirm the transaction. For protecting the neutrally of network, mining enforces chronological order in the block chain.

Explanation of mining

Similar to gold, Bitcoins are made by mining. But gold is mined from the ground by bulldozers, while Bitcoins are mined by computers solving complex mathematical equations. Each time you get a correct answer, you unlock a coin which can then enter the Bitcoin economy.

You can install Bitcoin mining software which uses your computer's processing power to carry out intensive calculations. Many people might be working on the same unit of work. Work is a computationally complicated problem. The aim is to find a certain sequence of data, called a "block”, which produces a particular pattern when the Bitcoin "hash" algorithm is applied to the data. The miner that manages to do that will win bitcoins.

When it started out, it was relatively easy to mine bitcoins, but as the network of people increases, it's become computationally much more challenging. CPU mining gave way to GPU mining. GPU mining has since given way to Asic mining (Application Specific Integrated Circuit). Currently Asic Miners are typically on back order. For this reason it
is not uncommon for brand new machines to sell on ebay at costs 30% or higher than the retail cost of the machine.

Bitcoin resembles with the development phase that TCP/IP was back then. Instead of IP addresses and websites, Bitcoin has unique strings that represent money and a mechanism is defined to send these strings securely and safely wherever you want. It is a protocol that is allowing money to flow around the world much like TCP/IP allows information to flow.

At the time of this writing there are slightly more than 12 million Bitcoins in existence today. That number will continue to rise as more are mined. However over time mining becomes more difficult and the total number will cap out at 21 million bitcoins.
How to Buy / Get Bitcoin?

How to acquire bitcoins is one of the most commonly asked questions by new users of Bitcoin. Although the process may seem confusing at first it is not as difficult as it might appear initially.

1. **Create a wallet** - A bitcoin wallet is website / program though which you can store bitcoins and make transactions. This website offers a free wallet service, sign up takes a few seconds and all you need is a password.

2. **Locate Your Address** - When you created a bitcoin wallet login and click receive money / coins. This page will have a "bitcoin address" which is 34 - 36 character long and starts with 1. This address is all you need to receive payments.

3. **Buy With Cash** - There are various ways to buy bitcoins with cash. There are local exchanges where you can meet someone and exchange cash for bitcoin. There are online equivalents of the same thing. Many online wallets offer or are tied to exchanges.

4. **Bitcoin Exchange** - A Bitcoin exchange is a place where people buy and sell bitcoins for other currencies.

5. **Through Mining** - Earn Bitcoin through competitive mining.
Why Invest in Bitcoin

When an investor wants to invest his/her money, he / she anticipates the expected return of his/her investment along with considering the risk associated with investment. The more risk, the more an investor should expect to gain. Here we discuss the benefits of bitcoins as well as risks attached with Bitcoin for making an investment decision.

Investment Benefits of Bitcoin

**Low Risk of Collapse:**

Regular currencies occasionally fail as they are dependent on governments. These types of events can occur due to hyperinflation or a complete collapse of a currency. This catastrophic event can devastate the savings of a people. On the other hand Bitcoin is not regulated by any government. It's a virtual global currency that has low risk of collapse.

**Low Fees:**

Bitcoin payments are processed with either no fees or extremely small fees. Priority processing of transactions requires small fees. Offering a fee results in faster confirmation of transactions by the network.

Additionally, merchant processors exist to assist merchants in processing transactions. These processors convert bitcoins to fiat currency and deposit funds directly into merchants' bank accounts daily. These services, processing of transactions, converting bitcoins to fiat currency and depositing funds directly into merchants' bank accounts are typically offered at much lower fees than with PayPal or credit card networks.

**Safe and Simple:**

From a seller’s point of view traditional online transactions through Credit cards, PayPal and other online payment systems allow buyers to claim their money back. But with Bitcoin, buyers cannot take the money back (chargeback). The seller can safely ship the product or perform the service that the client purchased.

From the buyer's point of view, sending money between accounts is simpler and cheaper because it is peer-to-peer rather than done through some intermediary.
Freedom of Exchange:
You can send and receive any amount of money anywhere in the world at any time. There are no bank holidays, no borders, no limits imposed on transactions. You have full control of your money at any time and anywhere.

Low Risk of Inflation:
One of the major problems associated with traditional currencies is inflation. With inflation the currencies lose purchasing power due to printing of more money by the government. You don't have this problem with bitcoins because the system is designed in such a way that Bitcoins are finite. Only 21 million Bitcoins will ever be released (mined). The release of new Bitcoins is slowing down and it will stop completely within a few decades.

Ease to Carry:
You can’t carry a billion dollars cash or gold but you can carry a billion dollars worth of Bitcoins on a memory stick in your pocket. Or in your mind for that matter. So it is not only easy to carry but also nearly impossible to prevent movement of it.

Neutral, transparent and predictable:
All information regarding Bitcoin is available on Block Chain for anybody to verify and use in real time. It is cryptographically secure, no individual or organization can control / manipulate the Bitcoin protocol. So the bitcoins are neutral, transparent and predictable.

Low risk for merchants:
Bitcoin transactions are secure and untraceable as these transactions do not contain customers’ information. This feature of Bitcoin protects merchants from losses caused by fraud or fraudulent chargebacks. New markets can be expanded where credit cards are not available or fraud rates are unacceptably high.
Investment Risks / Disadvantage of Bitcoin

Volatility:

The price of bitcoin is currently very volatile; the prices are currently rising at amazing rates. Currently the price is going up so fast a shop have to adjust their prices almost daily to accept bitcoins. Expect the currency to vary wildly in value. Currently governments are making major decisions around bitcoin regulation. While regulating bitcoin itself is nearly impossible, governments can regulate it's citizens ability to convert their currency into bitcoin. These wild fluctuations are to be expected until bitcoin becomes more of a currency than an investment. Keep in mind that reacting to the market is a signal that bitcoin is a true investment medium.

This is one of the major risks associated with Bitcoin as at one moment you may be a millionaire while a short time later you have nothing in your pocket. And of course the opposite is true. Stories abound of extreme wealth made through bitcoin. In one case a forgotten $27 investment turned into over a million USD.

Untraceable:

Bitcoin transactions don’t contain the users identity. This feature of Bitcoin attracts crime. People can buy and sell drugs and other illegal items, It is very difficult for authorities to trace these people.

Low Acceptance:

Bitcoin is not yet any where near mainstream acceptance. Although acceptance of Bitcoin is improving day by day the numbers are still comparatively very small. At the time of this writing (December 2013) the total value of all Bitcoin in circulation is just under 8 Billion USD. This number can vary wildly. Greater acceptance still needs to happen in order to get benefit from network effects.

Risk of Loss:

If you lose Bitcoin you lose it for good. There is no mechanism or technique to recover lost / stolen Bitcoins. If somebody hacks your wallet where you store Bitcoin they are gone forever. They are not like a credit card. If a credit card is lost or stolen, there is a good chance that you will not lose any money as your bank will cover the stolen money. There are very secure methods of storage and you must be prudent and use them when
dealing with large sums of money.

**Developing Phase:**

Bitcoin is only a few years old. We don’t have decades of history to look at. Therefore, it is still in the process of maturing. New tools, features and services are being developed to make Bitcoin more secure and accessible to users. Some of these features are still not ready for mass consumption. Most Bitcoin businesses are very new and do not offer any insurance.

**Difficult to trade:**

Buying and selling of bitcoins has restrictions in some countries. In the US exchanges fall under money exchange laws which can make them difficult to operate. At the time of this writing China has banned it's conversions of it's currency into Bitcoin.

However due to the portability of Bitcoin most people can use exchanges anywhere in the world. So when one country regulates it's exchanges the services can be found elsewhere. Of course it is possible for governments to establish laws which make it completely illegal to trade in Bitcoin but these laws would be very difficult to enforce.

Due to regulations it can be difficult to exchange bitcoin from popular services such as paypal. There are many startups around bitcoin exchange and we expect to see a large number of offerings with various security features as time goes on.
Factors Affecting the Value of Bitcoin

The value of Bitcoin is considered as unpredictable as its rate of change is extreme. It has seen one month 600$ climbs and 50% drops overnight. It's highly volatile nature must be considered. While investing in Bitcoin we must know the following factors that affect the value of Bitcoin:

**Supply of Bitcoin:**
Like other conventional currencies, Bitcoin also follows the law of supply and demand. Supply of Bitcoins has been controlled as number of Bitcoins in existence will never exceed 21 million. Owing to this limited supply there have been speculations that its price will increase dramatically over time.

**Demand:**
There is positive relationship between demand and value of Bitcoin. If more and more people utilize Bitcoin, the demand will rise and its value also increases because of limited supply. Obviously the value of Bitcoins will decrease with decrease of demand of people due to negative speculations, regulations, and uncertainty. Recent drastic drops in value were prompted by strong regulations enacted by China.

**Transferability:**
As far as the transferability is concerned the Bitcoin is better than physical currency. Value can be transferred anywhere there is internet. So this factor will increase its demand and value.

**Acceptance:**
Bitcoin is not good as far as acceptance is concerned as many feel reluctant to use it as medium of exchange. However acceptance is growing daily and very large well known companies now accept bitcoin as payment.

**Cost:**
Storage and transfer costs are involved in physical currency while Bitcoin is free or very low cost. This factor has increased its demand.
Stability of the network:

The stability of bitcoin network is one of the major concerns. Some claim it is merely an economic bubble and it has no inherit value. If majority of people stopped using the bitcoins then this bubble will burst and its value will reduce to zero. The bitcoin network has existed for over four years. This run has improved confidence in the security of the network.

Recommendation

Opinions on the stability of bitcoin are extremely polarized. Some claim it to be a temporary phenomena. Others claim it to be the future of money. The benefits and risks associated with Bitcoin must be assessed by the individual investor. We recommend investors to be vigilant while making any investment in Bitcoin. Fortunes could be made or lost.
The Future and Bitcoin

Where do we go from here?

It would be impossible to predict all of the future advancements in and around the bitcoin economy. There are obvious openings in the market and with new advancements and wider adoption these can only have exponential growth. Technology builds on itself and this is no different with bitcoin.

However dividing the ecosystem into logical sections may give some idea of the breadth of possibilities for advancement. Futurists may note that there are certainly very distinct categories in which future development will evolve within.

Categories such as:

1) Regular mainstream business adoption.

A large portion of the news stories today focus around mainstream businesses adopting bitcoin as a payment option. The fact that this is newsworthy is a testament to what an early stage we are in.

As individual businesses must way out the advantages and disadvantages of accepting Bitcoin as a payment method. The following are considerations.

There are currently both real and perceived hindrances to mainstream businesses accepting Bitcoin. These will, of course fade rapidly as education spreads and technology advances. As this happens the friction which hinders adoption and use as a currency will fade away while at the same time the forces which push towards adoption will grow. In physics terms we could say that mu will approach zero as R approaches infinity. These two forces working together will likely create a very accelerated rate of adoption.
Volatility Friction

The first bit of friction is very real. It is the volatility of bitcoin prices. A business which accepts bitcoin today could have a very different worth on the books tomorrow. Now in general, and over the long haul, this value has so far always been on the climb. It would be unlikely that a business would complain about that. However there have been steep dives caused by government reactions. Being caught in the middle of one of these dives could be difficult for a business without reserves to ride it out.

Product pricing could be a small challenge. For an online business it should be quite easy to price dynamically. But a brick and mortar would need to calculate at checkout to be in sync with current prices. Or have digital pricing displays on product displays.

This bit of pricing friction will fade as the volatility lessens. As stated previously volatility will lessen as bitcoin becomes more of a currency than an investment holding.
Banking Interference Friction

We can look to past actions of government to see that they have no qualms using the banking system as leverage to get what they want. We can expect that they will likely do the same in the future. As unjust and authoritarian as it is. All the more reason for us to remove the power they wield over us. The power which is created by their absolute control over the banking system.

For an example of this we can look to the battle that the United States Federal government has waged over the medical marijuana and now recreational marijuana industry.

In many US states, medical marijuana was legalized. In one US state, Colorado, recreational marijuana was legalized. At the federal level it remained illegal. Legalization, of course, required a majority vote. So it is a fairly reasonable assumption that over 50% of the population of these states agreed with legalization. Despite this, the DEA regularly raided medical marijuana businesses. It was, and is, a constant threat.

However the government learned very quickly that these raids very quickly turned into public relations disasters. Armed gestapo like DEA agents entering medical facilities wearing full riot gear did not create a pretty picture. Especially when the victims of these raids were supplying cancer and aids patients in need of the medicine. So a different approach was devised. A far more effective approach which went unnoticed. This new tactic was easy to keep out of the media. It also had the benefit of having the ability to affect ancillary businesses. In other words it could wipe out the whole ecosystem rather than just the businesses in direct contact with the evil weed.

This new approach was carried out through the banking system. It is a multi-pronged approach. The first part of the tactic was to remove businesses ability to keep banking accounts. The feds didn't actually make it illegal for these businesses to have bank accounts. They just simply made it uneconomical for banks to provide them. The methodology used was to require a tremendous amount of scrutiny over current account holders in the marijuana industry and also over the opening of new accounts. Banks who provided these services would be required to have so much more paperwork that they would need an entire new department just to service the industry. This, of course,
created more expense than the banks were willing to bear. So they simply closed accounts.

With the bank accounts went the merchant accounts. With the merchant accounts went the ability to accept credit cards. So in one fell swoop the entire industry was converted to a cash only industry. Which created a great many problems for these business owners. Difficulties arose in carrying out normal business transactions such as paying utility bills, business purchases, and rent. These added demands took up a great deal of the business owners time and resources. In addition security became a big issue. It was well known that these businesses were forced to carry large amounts of cash. Criminals knew that the owners left each night with bags of cash. So the risks became very high. Now not only were these business owners at risk of losing their business but now they risked their lives. In essence the criminals became the allies of the Feds. No shortage of irony there.

If that wasn't enough, the feds then came down on the landlords of these businesses. All it took was for that landlord to have financing on the building. Since the financing was typically through a large financial institution all the feds had to do was to pressure the banks. The banks then sent out letters telling the landlords that they would revoke their loans if they maintained marijuana businesses as tenants. This was a pretty big blow. Businesses were forced out of business and those that remained were forced to pay ultra premium prices.

A dire scenario? Sure. Impossible for it to happen to bitcoin? No.

However with bitcoin there would be other complications for the Feds. Bitcoin IS a currency. So at least to some degree they would simply force bitcoin transactions underground or to other countries. A sneak attack such as they did on the marijuana industry would certainly have the effect of keeping it out of the mainstream for longer. But at the same time it may produce undesired counter results. At this point the cat may be to far out of the bag. It's possible that any government intervention would simply create more desire for bitcoin and more ways of leaving the current economic ecosystem.

We can see that there has been at least some degree of this sort of activity, directed at bitcoin, from the Federal government. They do exercise a lot of control over money
exchanges. So far they have regulated the majority of USD to bitcoin exchanges right out of the country. Of course this simply has the effect of driving them to other parts of the world. Since we can still reach them through the internet it does not affect their ability to do business. It simply sends that business (and profit) elsewhere. Not the most brilliant of moves.

The Feds have also been known to expand their money exchange control by defining more businesses as money exchanges. They've done this to a few businesses which were converting bitcoin into other forms such as paper or coin. These businesses weren't really exchanging money since the currency remained in bitcoin. But if the fed says it, it must be true.

So in the world of bitcoin, businesses must be vigilant of these tactics. They've been carried out before. They are being carried out now. It's just a matter of on what scale.

So at this point these seem to be very acceptable levels of friction. More and more established businesses are coming online with bitcoin. As they do, they effectively diminish friction for others.

**Early Adopter Businesses Benefit**

There are still early adopter benefits to be gained for businesses. Accepting bitcoin still has the benefit of a publicity push. Each new business that does, gets picked up in the news. Often times bitcoin users will organize events around new places to spend their bitcoin. Bringing in at least one wave of new business, that if played out right, has the possibility of retaining a whole new entourage of faithful evangelistic customers.

So aside from the benefits that come from the attributes of bitcoin, a business can potentially gain simply from the novelty. This plus a little creativity hs the potential for going a long way.
2) New services which service mainstream businesses.

As more and more mainstream businesses accept bitcoin a whole new ecosystem of service providers will crop up. There are several obvious categories of these needed.

Such as:

**Processing.** Bitcoin processing is itself quite simple and can be done with no more than a smart phone and an app. But doing this on a large scale will introduce new requirements. Secondary accounting systems will be needed to inter mesh with present accounting systems. POS systems which make it convenient to accept bitcoin from different devices and in different forms. Pricing systems will be needed to quickly and easily convert Btc to USD and vice versa (until the dollar is extinct anyway). These are easily solved with existing technology. So it will be a matter of the fastest moving and most creative service providers winning out. Because these are all built on existing and fairly simple technology they should also be extremely low cost.

**Cold Storage.** Because bitcoin is so extremely portable, cold storage systems make a lot of sense for heavy transactors. Excess funds could be quickly sent off site to secure locations. With that in mind, the need for a highly secure cold storage system is high.

What would that look like? Possibly a highly secure vault in which bitcoins are instantly transferred to and converted to an offline form. Maybe they would be instantly printed out and the private key removed from any connected devices. Deposited in minutes in paper form into a safe deposit box. Co-location could guard against natural disaster. Two out of three type pass code schemes could be used for release of funds.

No matter how it was carried out, cold storage schemes could make physical store fronts have very little attraction to criminals. A small bitcoin only convenience store, even in the worst part of town would be completely safe from criminals. There would simply be zero funds to be stolen and hence no reason for an attempted heist.

Cold storage services could also have large appeal at the consumer level. Consumers
who do not want to deal with securing their bitcoin or having it on premises would very likely opt to purchase cold storage.

3. **Modified mainstream style businesses that operate more efficiently due to bitcoin attributes.**

As discussed earlier bitcoin has attributes which are very different than other forms of money. These attributes can lend a competitive advantage to some forms of business. That competitive advantage may be enough to establish dominance in a market for early adopters.

So to recap some of the attributes which are different. Bitcoin:

1) Is extremely portable  
2) Is anonymous  
3) Has extremely low cost transaction fees  
4) Has very fast transactions  
5) Transparency

So how can businesses take advantage of these for a competitive advantage? Well maybe:

Businesses who transfer money over distances can use the advantage of portability, speed, and low transaction costs for a competitive advantage. Currently Western Union is feeling very threatened. Adoption of bitcoin could completely wipe out that business model. Unless, of course, they find a way to embrace it instead of fighting against the tide.

Think about companies such as Odesk or Elance. They could gain a strong competitive advantage by using bitcoin as their medium of exchange. Or simply by using it internally and exchanging currencies at the end points. Of course if these companies do not embrace it, a competitor could. If conditions were right that competitor could quickly dominate a market.
Low transaction fees alone, in some markets, could be enough to create a competitive advantage. Just simply by being able to reduce costs and therefore reduce prices for the end consumer.

For information type businesses, speedy transactions could be a huge boon. Imagine the internet based service provider or retailer. In these businesses transaction time can be the biggest hindrance to growth.

**What about non-profits?** Well all of the above but then add on transparency. It would be a very simple endeavor, if a person had the hash tags associated with a non-profits accounts, to track donations and expenditures. A real time widget could be created which publicly displayed all transactions in real time. You would know exactly where your donation went. Transparency would be a big selling point to potential donors.

**Government.** Oh no, really? Yes, for the exact same reasons that transparency could be a selling point for donors in non-profits. Transparency in government could be a monumental change. The FBI found this out the hard way when they transferred the Silk Road bitcoin holdings to their own btc address. The transaction was spotted on the network. This gave the public the address and pranksters began sending small amounts of bitcoins to the FBI just so that they could send the notes that are a part of the transactions. The FBI was flooded with a plethora of snarky remarks from anonymous "donors". A government on bitcoin would have nearly forced transparency. Can you imagine? Too utopic? Well maybe, we'll see.

**Businesses where anonymity is critical.** This, of course brings to mind all things nefarious in nature. And yes that certainly is true. These businesses can certainly take advantage of anonymity. These would include porn, prostitution, drugs dealing, and even hit men. But the nefarious are not the only ones that crave anonymity. In today's world privacy is becoming a big concern. Every transaction we make is vigorously tracked in any way possible. Our spending habits are categorized and sold to those who can profit from that knowledge. We are then bombarded with offers. In a world where privacy levels are approaching zero a little privacy might just be a valuable commodity. Simply for privacy's sake. With bitcoin businesses may pop up just to service that simple desire to not be tracked in everything we do. A whole new industry. The privacy industry.
4. Completely New Services Enabled by Bitcoin

Because of bitcoins unique attributes completely new business concepts can be spawned. The above mentioned cold storage and anonymity businesses might fir into this category. Just think what brilliant businesses can be created by combining the attributes of bitcoin.

5. Businesses that skirt regulation

As we've already seen the feds money are not above using money regulation to shut down businesses they desire eradicated. Simply switching these businesses to a bitcoin economy would loosen that strangle hold.

The cannabis industry has much to gain form this. Since their primary difficulty is in banking. All it would take would be adoption among the user base. An endeavor which probably not be difficult at all. Cannabis users have an obvious disdain for government regulation. They will go to greater lengths than the average consumer to purchase their desired product. As there is an actual culture around the market, word spreads fast. And best of all this customer base would take pride in participating in the revolutionary use of bitcoin. So for any entrepreneurial bitcoin revolutionaries this would be a very strong segment to mobilize. The current cannabis industry is larger than the current bitcoin economy. (Yes it's that big) So engaging this market has the potential to greatly multiply the bitcoin user base.

Online gambling has been illegal in the US for some time. Over the years many payment schemes have arisen to facilitate online gambling. These schemes quickly get shut down by use of banking regulations. Bitcoin eliminates that ability to regulate.

There are probably numerous business types which fall into this category. Some are highly illegal and should be. Others are either illegal or highly regulated and do no harm. Of course the media has chosen to pick up on the most nefarious and done a good job of associating bitcoin with the criminal element. The reality is that this is only a small portion of the actual bitcoin economy.
6. Businesses and Systems based on the Bitcoin Protocol

Bitcoin, at it's core, is merely a protocol. A protocol is simply a set of rules. Protocols have spawned some amazing things. What's interesting about protocols is that other protocols can be built upon them. Think about the web itself. It is simply protocols built upon protocols. First it was merely a network (the internet). Upon that, protocols such as HTTP (hyper text transfer protocol) were built. Originally HTTP was merely a system for formatting text. Somebody got the idea to add picture capabilities and the web as we know it was born. Protocols upon protocols.

Bitcoin is truly just a protocol. Other protocols can be built which either enhance or interact with it. Surely many brilliant minds will come up with ingenious ideas within this category.

So as you can see there is an entire ecosystem about to evolve around Bitcoin. It's not just criminals and creepies like much of the media would have you believe. Are you entrepreneurial? What part of this economy will you take part in?
Crony Capitalism

Attempts at political reform have been made for longer than most can remember. Mostly failed attempts. It would seem that the triumvirate of government (including the federal reserve), the banking system, and big corporate (along with their lobbyists) have formed too strong of a union to break up. At least by traditional means.

The fed feeds essentially free money into the big banks. There is essentially nothing returned for this huge favor. No exchange of goods or services. It is carried out under the guise of maintaining equilibrium within the economy. Big government gives out free money and plays favorites and in return big corporate and the banks filters a portion of that money back to it's bought politicians. The control is in the money. A self replicating system which feeds on greed.

This system has a lot to lose with the adoption of bitcoin. It will fight back hard. But in the end if a large part of the economy shifts to Bitcoin then this partnership of greed will be eliminated by taking away it's control over money. No political reform needed.

Without money it will be rendered harmless.

There is much talk lately about the strength and power the US government has over it's people. Of course what’s going on in the US pales in comparison to what happens in dictator run countries. Personal freedoms are nearly extinct and human life devalued. But still, the US populace is not pleased with it's government.

Without control over money, these governments will quickly lose their powers. Who would pay for the NSA to spy on it's people when the government no longer had this supreme power gained by control over the monetary system. Who will pay for the democracy spreading bombs? I'm thinking nobody will.

"I can hire one half of the working class to kill the other half. " This quote was attributed to Jay Gould, an American financier. Whether the quote was truly said by him or merely propaganda, it does illustrate a very strong point. That absolute control over money is a dangerous thing.
Maybe You Can Regulate Your Way to Freedom

At the time of this writing the Chinese government has just made it illegal for it's citizens to transfer their Yuan into Bitcoin. There was an immediate effect on the value of bitcoin. But what was the effect on the value of Bitcoin at the local level in China. Is it possible that they simply drove the currency underground and actually increased it's value at that local level? I'd say it is highly probable. It's very likely that a black market was quickly created around it as desire for Bitcoin rose. We all want what we can't have.

If that is the case what will be the evolution of that black market. With Bitcoins high level of portability and anonymity it would be a very difficult endeavor to prohibit a countries citizens from acquiring it if they really wanted it. An extremely dissatisfied populace with the power of it's own currency could be the start of a revolution.

In general it is very hard to regulate bitcoin. Great lengths would be needed to block a peer to peer network such as bitcoin. You can regulate the in and out points but it doesn't kill them. They simply move to another local and that local reaps the economic benefits.
Bitcoin as a Business Lubricant

The current monetary system has built in friction. Bitcoin has the potential to eliminate a large part of this friction.

In our current banking system this friction is created by processing delays, fees, Theft, and the possibility of charge backs. All of these greatly hinder business.

We've become accustomed to these things. We even have a name for them, COBD (cost of doing business). Bitcoin has the possibility of reducing or eliminating these COBD's.

Bank transfers don't happen on weekends, evening, or holidays. Why? Computers can't work on holidays? We are completely accustomed to business terms such as net30. But are they as necessary as we think?

Now we can't eliminate all delays. Net30 will still be necessary in many instances. But much of the time it is not. Companies can give discounts or premiums for when those times arise and their customers comply.

Imagine how much faster the economy would move if these transfers were instantaneous. Powered by API's (Application Programming Interface) we could eliminate much of this friction. In many instances payment delays are the main limiting factor in a companies growth.

Imagine this scenario. A retailer puts a product up for sale on the internet. They use Amazon for fulfillment. They use Google Adwords for Advertising. The purchaser clicks through an ad on a website brokered by google. They purchase a product. The payment instantly is split according to the prior agreement and instantly transferred via API. Google gets it's cut for the click and Google instantly splits it's cut with the publisher where the click originated. Amazon gets it's cut instantly and disperses funds in a similar manner. At the same time the wholesale cost is sent to the wholesale distributor. The wholesale distributor connects instantly to the manufacturer and payment is sent. All along this chain inventories are updated and purchase orders adjusted in real time. Each link in the supply chain knows in real time what the demand is and adjusts ordering/manufacturing accordingly in real time.
The API's working together in unison create an on demand manufacturing scenario which further reduces costs. Warehousing needs are lessened. Waste is lessened and a snapshot of the full business cycle is in reach at any time. Even employees could have instant transfers to their accounts for the days work. They clock out and by the time they have walked to their cars the money is available.

A crazy unreasonable scenario? Not really. We have the technology. We just simply need to remove the friction caused by business killing lag times.

Money transfer lag times are reduced and at the same time business efficiencies are created. Profits rise, costs shrink.

Much of the demand for business lending is to cover these lag times in periods of business growth. Growth causes demand for more financial outlay to supply the business with sellable goods. Shorten these lag times and you also decrease the demand for business lending. And again the banks and the power they have over the business owner and the consumer is once again diminished. So sad.

We've accepted these conditions as norms for so long that it is probably very difficult to imagine anything different. But a few simple changes could have an amazing ripple effect. Everyone could be the better for it. Well except for the banks, big corporations, and big government.

**Conclusion**

So has this book given you any ideas? Hopefully it is enough to whet your appetite to the possibilities of bitcoin. Humanity has never been here before. None of us can accurately predict where it will go. But we can help guide it. We can be a part of the revolution simply by letting our entrepreneurial spirit shine.

Bitcoin just may be that catalyst we need to jump civilization to the next level. A quantum leap in society. Bringing in freedom from tyranny. Democratizing money and with it the world. A revolution fought with no guns fired. Simply won by smart entrepreneurs, programmers, and visionaries.
What part will you take in the revolution?

REFERENCES


https://code.google.com/p/bitcoinj/source/browse/core/src/main/java/com/google/bitcoin/core/Block.java#584


https://github.com/bitcoin/bitcoin

http://bitcoin.org/releases/2011/06/05/v0.3.22.html

https://code.google.com/p/bitcoinj/


https://blockchain.info/wallet/

https://code.google.com/p/bccapi/

https://en.bitcoin.it/wiki/MyBitcoin

https://www.instawallet.org/w/_cmgZpXGT6iE9oh_tX0hg
09.11.2013 https://bitcointalk.org/index.php?topic=6458.0

[40] Bitcoin forum. 2011. CGMiner. Consulted
09.11.2013 https://bitcointalk.org/index.php?topic=28402.0

http://www.bitcoinmonitor.net/

https://bitcointalk.org/index.php?topic=19137.0


https://en.bitcoin.it/wiki/Block_chain

09.11.2013 https://en.bitcoin.it/wiki/URI_Scheme


09.11.2013 http://bittorrent.org/beps/bep_0009.html

Consulted
09.11.2013 https://bitcointalk.org/index.php?topic=46982.0


http://www.thebitcointrader.com/2012/05/developing-bitcoinica-hacked.html

09.11.2013 https://en.bitcoin.it/wiki/BIP_0011

09.11.2013 https://en.bitcoin.it/wiki/BIP_0016
09.11.2013 https://en.bitcoin.it/wiki/BIP_0010

[54] Bitcoin version 0.6.1. 2012. Consulted 09.11.2013
http://sourceforge.net/projects/bitcoin/files/Bitcoin/bitcoin-0.6.0/

09.11.2013 http://www.slideshare.net/dakami/bitcoin-8776098

[56] Blockchain.info. 2012. Number of transactions per day. Consulted
09.11.2013 http://blockchain.info/charts/n-transactions