SOCIAL AND LEGAL ASPECTS OF CRYPTOCURRENCIES

Project of the course "Social and Legal Aspects of Technology"

Authors
Γκόγκος Νίκος, 4973
Σαββόπουλος Δημήτριος, 5066
Σιάτρας Γεώργιος, 5071
Φουστέρης Πέτρος, 5100
Παπαναστασίου Βασίλειος, 5122
Ξαφέλης Γεώργιος, 5176
## Contents

1. Introduction to Bitcoin and Cryptocurrencies ................................................................. 2
   1.1 What is Bitcoin? ............................................................................................................. 2
       1.1.1 History of Bitcoin ............................................................................................... 3
       1.1.2 How Bitcoin works ............................................................................................. 4
   1.2 Cryptocurrencies in general ........................................................................................... 6
   1.3 Why Cryptocurrencies gained such a high reputation? ............................................... 7
   1.4 Will Bitcoin and other Cryptocurrencies fail? ............................................................. 8

2. Economy ........................................................................................................................... 10
   2.1 Why Cryptocurrencies have value and how it is determined. ................................... 10
   2.2 Can Bitcoin and other Cryptocurrencies be regulated? ............................................. 12
   2.3 Cryptocurrencies as investment ................................................................................... 13
       2.3.1 Cryptocurrencies’ volatility ................................................................................. 15

3. Legal aspects ..................................................................................................................... 19
   3.1 Promoting illegal activities ......................................................................................... 19
       3.1.1 Tax evasion and Money laundering ..................................................................... 20
       3.1.2 Black markets and Underground networks ....................................................... 21
   3.2 Cryptocurrencies and Laws ....................................................................................... 22
       3.2.1 Legality of Cryptocurrencies by country ............................................................ 22
       3.2.2 Consumer protection ......................................................................................... 28

4. Social aspects .................................................................................................................... 30
   4.1 Foundations and Concepts behind Cryptocurrencies ................................................. 30
   4.2 New paths and job opportunities ............................................................................... 33
   4.3 Privacy concerns and personal view ........................................................................... 34

References .......................................................................................................................... 35
   1.1 ......................................................................................................................................... 35
   1.1.1 ................................................................................................................................. 35
1. Introduction to Bitcoin and Cryptocurrencies

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for nonreversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.

The above is a direct quote from the original paper by Satoshi Nakamoto (Bitcoin's founder). [Ref. Ch. 1 https://bitcoin.org/bitcoin.pdf]

1.1 What is Bitcoin?

Put simply, Bitcoin is a peer-to-peer (p2p) payment system and digital currency introduced as open source software in 2009 by developer Satoshi Nakamoto [1]. Bitcoin is strongly related to cryptography and thus it is called a cryptocurrency or cryptocoins. Everything related to it, such as sending, receiving and creation of coins, is based on asymmetric cryptography and peer-to-peer network architecture. Bitcoin is a peer-to-peer internet-driven cryptocurrency. However, Bitcoin's unique nature means that it has many critical differences from standard currency. It is a decentralized form of currency not backed by any government or financial institution, or pegged to the value of any hard commodity such as gold.
1.1.1 History of Bitcoin

Bitcoin was introduced in a 2008 paper published under the presumed pseudonym Satoshi Nakamoto. Prior to the release of Bitcoin there were a number of precursor ecash technologies starting with the issuer based ecash protocols and moving on to distributed digital scarcity based ecash protocols starting from Adam Back's hashcash, Wei Dai's b-money [1], Nick Szabo's bit-gold [2] and Hal Finney's RPOW which build on hashcash.

Back in 2009, the first open source client (or wallet software), called Bitcoin-Qt, was released and the first bitcoins were issued. A feature in the Bitcoin-Qt software was exploited and over 184 billion bitcoins were generated in a transaction, and sent to two addresses on the network. This was due, in large part, because Bitcoin-Qt was the only software that facilitated bitcoin transactions and mining. This feature was later removed because specialized mining software turned out to be more efficient and profitable. Since then, the bitcoin open-source software has been maintained and enhanced by a group of developers and other fellow workers. The concept of anonymous digital money based on asymmetric cryptosystems such as RSA has been known since 1977. The Bitcoin network was created on 3 January 2009. It automatically generated the first units on personal devices. Bitcoins had at this time no quantitative value in other currencies. As a result, a year later the first exchange rates have been negotiated by people in the “bitcointalk” forums. The value of the first bitcoin transactions were negotiated by individuals on the bitcointalk forums with one notable transaction involving a 10,000 BTC pizza [3].

On February 9, 2011 and a few days later Bitcoin was traded in most exchange markets for about one U.S. dollar. By May 2011, interest in Bitcoin was growing as were concerns. Wikileaks [4] and other organizations began to accept bitcoins for donations. The Electronic Frontier Foundation began, and then temporarily suspended, bitcoin acceptance, citing concerns about a lack of legal precedent about new currency systems, saying that they "generally don't endorse any type of product or service."[5] The EFF’s decision was changed in 17 May 2013. By May 2011, interest in Bitcoin was growing as were concerns. The price of bitcoins has fluctuated wildly since its inception, going through various cycles of appreciation and depreciation, which have been referred to by some as bubbles and busts.[6] In 2011, the value of one bitcoin rapidly rose from about US$0.30 to US$32 before returning to US$2.[7] On 23 December 2011, Douglas Feigelson of BitBills filed a patent application for “Creating And Using Digital Currency” with the United States Patent and Trademark Office, an action which was contested based on prior art in June 2013 [8].

In January 2012, Bitcoin was featured as the main subject within a fictionalized trial on the CBS legal drama The Good Wife where was mentioned that "there's no central bank to regulate it; it's digital and functions completely peer to peer". In October of the same year, BitPay reported having over 1,000 merchants accepting Bitcoin under its payment processing service. [9] In the latter half of 2012, the bitcoin price began to rise.
In February 2013 the Bitcoin-based payment processor Coinbase reported selling US$1 million worth of Bitcoins in a single month at over $22 per Bitcoin. [10] The Internet Archive announced that it was ready to accept donations as bitcoins and that it intends to give employees the option to receive portions of their salaries in Bitcoin currency.[11] During the 2012-2013 Cypriot Financial Crisis, the bitcoin price[12] began to rise, reaching a peak of US$266 on 10 April 2013. Then a crash took place which was due to insufficient capacity resulting in the bitcoin exchange rate dropping from $266 to $76 before returning to $160 within six hours. In October 2013, Chinese Internet giant Baidu had allowed clients of website security services to pay with bitcoins. In the same month FBI reports seizing roughly 26,000 BTC from website Silk Road during the arrest of alleged owner William Ulbricht [13]. By the end of the month, two companies, Robocoin and Bitcoiniacs launched the world's first Bitcoin ATM in Vancouver, BC, Canada, allowing clients to sell or purchase Bitcoin currency at a downtown coffee shop [14][15]. On 19 November 2013 one Bitcoin was traded for over US $1100 in China, after a United States Senate committee hearing was told that virtual currencies were a legitimate financial service. The highest value of Bitcoin was reached on that month and it was $1250. By November 23, 2013, the total market capitalization of Bitcoin went beyond US $10 billion for the first time. After the announcement of People's Bank of China for prohibiting Chinese financial institutions from using bitcoins the value of bitcoins crashed to 600$. In the same month, the University of Nicosia announced that it would be accepting Bitcoin as payment for tuition fees, with the university's chief financial officer calling it the "gold of tomorrow"[16]. By the end of the year, Overstock.com[17] announced plans to accept Bitcoin in the second half of 2014.

In the first month of the next year, 2014, price had stabilized to $650-800$ range, where also a spike to $1000 took place. Later on that month, Zynga[19] announced it was testing Bitcoin for purchasing in-game assets in seven of its games. That same month, two hotels, the D Las Vegas Casino Hotel and Golden Gate Hotel & Casino properties in downtown Las Vegas announced they would also begin accepting Bitcoin, according to an article by USA Today. The article also stated the currency would be accepted in five locations, including the front desk and certain restaurants. Last but not least, referring to the current price of Bitcoin, due to the shutdown of the largest Bitcoin exchange, Mt. Gox, the price fell to $550 - $700 range where is stabilized till now. Last but not least, the MIT university is going to give to every student 100$ worth of bitcoin, so every student can have access to a digital currency.

1.1.2 How Bitcoin works

Bitcoin in order to exist and function requires a network which is consisted of computer nodes. Most of them are mining in the network and thus called miners.

Bitcoins are created by a process called mining, in which participants verify and record payments on the network in exchange for transaction fees and newly minted bitcoins. Miners process payments by verifying each transaction as valid, adding it to the block chain and therefore secure the network. In other words, miners provide their computing
power in exchange for newly minted coins. At this point we can see that miners are actually consuming electricity and providing their computing power to the Bitcoin network in order to receive Bitcoins, which can be sold for real money. At the moment writing this text, a Bitcoin is worth approximately 500 dollars. Users send and receive bitcoins using a wallet software which runs on their devices. Bitcoin uses public-key cryptography, in which a pair of a public and a private cryptographic key is generated. A collection of keys is called a wallet. Hence, a wallet is holding someone’s bitcoin or other similar cryptocurrencies’ balance. Someone can obtain bitcoins by mining or trading them for services, currencies or any other kind of goods. Bitcoins can be bought and sold for many different currencies from individuals and from companies. The fastest way to obtain bitcoins is to purchase them in person or at a Bitcoin ATM for cash.

When a Bitcoin user makes a purchase, the payment triggers a broadcast of the financial transaction to the Bitcoin network and pushes it on the BlockChain. The Bitcoin transaction is a digitally signed message, transferring the ownership of bitcoins from one "Bitcoin address" to another. For the transaction to take effect, it is recorded in a public ledger or public transaction database. This compounds the BlockChain of Bitcoin.

A graph which demonstrates the above statements is shown below:
Bitcoin promises to provide anonymous online transactions. This means that when a party buys or sells bitcoins, it should be impossible to track this party down\textsuperscript{[1]}. While transactions are not anonymous, they offer a degree of anonymity, because the block chain identifies receivers by Bitcoin addresses, not individuals’ names. Bitcoin addresses are just a hashed string or a cryptographic public key pair as it has been mentioned before.

While bitcoins can be from the one hand used to for illegal purposes (i.e. drugs), they can be used on the other hand from people who are really concerned about their privacy. Nowadays, governments have full access to any personal record and social networks, online markets and search engines make things even worse. Many countries and societies are characterized for their strict laws/rules, for instance China. People are forced to comply and live with unacceptable conditions and restrictions. They lack freedom of speech in many aspects of their life. Hence, bitcoins may offer those people the chance to act online anonymously without facing the unrighteous side of law. From the above statements, it is made clear why people of the Internet may be interested into bitcoins.

\textsuperscript{[1]} However, rumors have NSA being able to trace BTC transactions at the moment. That’s why there are many alternative cryptocurrencies which try to implement a coin mixing feature in order to provide real anonymity of the transactions.

1.2 Cryptocurrencies in general

Digital currency is a form of currency or medium of exchange that is electronically created and stored. Some digital currencies are cryptocurrencies but not the other way round. As already mentioned, the first cryptocurrency was Bitcoin in 2009. Later on, many similar to Bitcoin cryptocurrencies have been introduced. Litecoin is the most well-known cryptocurrency as an alternative to Bitcoin which was introduced in the early days of cryptocurrencies. By now, Litecoin is the second-largest cryptocurrency by market capitalization. Fundamentally, cryptocurrencies are specifications regarding the use of currency which seek to incorporate principles of cryptography to implement a distributed, decentralized and secure information economy.

The underlying technical system upon which all cryptocurrencies are now based was created by Satoshi Nakamoto as already mentioned before. Every alternative cryptocurrency is a fork of the origin Bitcoin’s source code, differing primarily by having a decreased block generation time, increased maximum number of coins, different hashing algorithm, and a slightly modified GUI. To be more specific, Bitcoin uses the SHA-256 hashing algorithm while for example Litecoin and most cryptocurrencies use Scrypt. Other algorithms are mostly modifications of the Scrypt and / or combinations with other algorithms such as Scrypt-Jane. We can see here that cryptocurrencies differ in their specifications, which are initially defined by their creators and their goals. Moreover, except for the algorithm being used, the amount of cryptocoins to be produced totally is different for each cryptocurrency. Referring to the security of the cryptocurrencies, subverting it is mathematically possible, but the cost may be unfeasibly high.
Many other cryptocurrencies have been created, though not all have been successful, especially those that brought few innovations. At the time writing this text, there exist more than 300 alternative cryptocurrencies. All of them are out there serving their own purpose while some of them have foundations. We will talk about the concepts and the foundations of some cryptocoins in chapter 4.1. Some examples of alternative cryptocurrencies are:

- Leafcoin - Willing to promote tree planting all over the planet
- Anoncoin, Stablecoin - Both promising truly anonymous transactions
- Zeitcoin - Supports the Zeitgeist movement
- Curacoin - Promotes decentralized health care (medicines accessible to anyone)
- Appcoin - Purchasing applications from mobile devices online stores
- Solarcoin - Supporting the solar power economy

It is worth mentioning that some of the newest cryptocoins are to support a country and its residents. For example, GreeceCoin was released with goal to support Greek people over the country as well as AuroraCoin for the Island ones.

Of course, each cryptocurrency serves a purpose and has its own goals. However, all of them are created with one basic purpose, to become a successful digital currency with high popularity and value. Most cryptocurrencies try to mimic the scarcity (and value) of precious metals and to avoid hyperinflation. As a result, such cryptocurrencies tend to experience hyperdeflation as they grow in popularity and the amount of the currency in circulation approaches this finite cap. Compared with ordinary currencies held by financial institutions or kept as cash on hand, cryptocurrencies are less susceptible to seizure by law enforcement. We will talk more about this on the 3rd chapter.

1.3 Why Cryptocurrencies gained such a high reputation?

A mysterious new technology emerges, seemingly out of nowhere, but actually the result of two decades of intense research and development by nearly anonymous researchers. A result that is based on strong asymmetric cryptography and promises high anonymity to the people of Internet.

Bitcoin gives us, for the first time, a way for one Internet user to transfer a unique piece of digital property to another Internet user, such that the transfer is guaranteed to be safe and secure, everyone knows that the transfer has taken place, and nobody can challenge the legitimacy of the transfer. In addition, users can make transactions almost anonymously and thus retaining their privacy. In any case, Bitcoin offers way more private transactions compared to any other form of digital transactions available (PayPal, banks). People of the Internet certainly have privacy concerns. Cryptocurrencies promise to them one extra privacy layer. Hence, cryptocurrencies and Bitcoin in specific were able to gain reputation pretty fast over the Internet.

One of the other reasons that made Cryptocurrencies so famous is that people of the Internet, people who love technology, are definitely looking for ways to improving their
quality of life in conjunction with technology. Bitcoin offered this to them. Being able to mine their own cryptocoins was a motivation to deal with cryptocurrencies and understand the inner workings of it. Making profit could be a basic reason that made Cryptocurrencies so popular, not the only one however. Computer science people and scientists in general, for sure found it interesting that a new form of digital currency based on strong mathematics showed up. It could be their new hobby or a new way to get some passive income.

Generally, we can see from the above statements that different kind of people have different reasons to believe and deal with a new form of digital currency, leading cryptocurrencies' reputation higher.

1.4 Will Bitcoin and other Cryptocurrencies fail?

As already mentioned, the main concept behind cryptocurrencies is not to fail but support every possible transaction which can be made offering several advantages, like anonymity. However, history has shown that some currencies failed and are no longer used such as the German Mark during the Weimar Republic and, more recently, the Zimbabwean dollar. There is always potential for failures, competing currencies, political issues and so on, especially on these controversial cryptocurrencies. No currency can be considered as safe from several failures.

On the other hand, bitcoin has proven reliable for the last years of its existence and there is a lot of potential for Bitcoin to continue to grow. However, no one is in a position to predict what the future will be for Bitcoin. Some people say that bitcoin and other cryptocurrencies may fail because of theirs finite amount of coins, unlike the non-virtual currencies, like USD, where there is no limitation. Nevertheless, this will never be a limitation because bitcoins can be divided up to 8 decimal places (0.000 000 01 BTC) and potentially even smaller units if that is ever required in the future. As the average transaction size decreases, transactions can be denominated in sub-units of a bitcoin, such as millibilitcoins (1 mBTC or 0.001 BTC).

People who support that bitcoin will fail use the blow that Mt. Gox made when it went dark. The largest exchange Mt. Gox has long been one of the Bitcoin community's most prominent institutions. When the exchange went offline, most people thought that this is the beginning of the end of bitcoin. However, Mt. Gox wasn't the only exchange in town. While Mt. Gox has dwindled in popularity, other exchanges have risen to take its place. According to Bitcoincharts.com, the most popular exchange is now a European firm, Bitstamp. And while bitcoins have fallen to less than $400 on Mt. Gox, bitcoins on Bitstamp, and other exchanges, are going for about $650. The loss of more than 740,000 bitcoins when Mt. Gox went bankrupt hasn't shaken the trust of people in Bitcoin, but the trust in bitcoin exchanges.

Will Bitcoin fall in a deflationary spiral? For those who don't know, the deflationary spiral theory says that if prices are expected to fall, people will move purchases into the future
in order to benefit from the lower prices. That fall in demand will in turn cause merchants to lower their prices to try and stimulate demand, making the problem worse and leading to an economic depression. Although this theory is a popular way to justify inflation amongst central bankers, it does not appear to always hold true and is considered controversial amongst economists. Consumer electronics is one example of a market where prices constantly fall but which is not in depression. Similarly, the value of bitcoins has risen over time and the size of the Bitcoin economy has also grown dramatically along with it.

Bitcoin is not designed to be a deflationary currency. It is more accurate to say Bitcoin is intended to inflate in its early years, and become stable in its later years. The only time the quantity of bitcoins in circulation will drop is if people carelessly lose their wallets by failing to make backups. With a stable monetary base and a stable economy, the value of the currency should remain the same.

Because both the value of the currency and the size of its economy started at zero in 2009, Bitcoin is a counterexample to the theory showing that it must sometimes be wrong. However, Bitcoin is probably a bubble and may not be the future, but if this is true, it has helped to light the way ahead.
2. Economy

2.1 Why Cryptocurrencies have value and how it is determined.

In a world where many countries are characterized for their strict and absurd legislation and people lack freedom of expression (China, Turkey). Anonymity could have significant role in their daily routine. Hence, cryptocurrency probably is a way for society to gain its freedom back at the field of electronic transactions. The aftereffect of the need for transaction anonymity provokes increase of bitcoins use and trust.

Cryptocurrencies, and as a result Bitcoin, have value because they are useful as a form of money. Bitcoin has the characteristics of money (durability, portability, fungibility, scarcity, divisibility, and recognizability) based on the properties of mathematics rather than relying on physical properties (like gold and silver) or trust in central authorities (like edict currencies). In brief, Cryptocurrency is favored by mathematics. With these attributes, all that is required for a form of money to hold value is trust and adoption. In the case of Cryptocurrency, this can be measured by its growing base of Bitcoin users, merchants, and startups. As with all currency, bitcoin’s value comes only and directly from people willing to accept them as alternative (or even major) payment.

The price of a bitcoin is determined by supply and users' demand. When demand for bitcoins increases, the price increases, and when demand falls, the price falls. There is only a limited number of bitcoins in circulation and new bitcoins are created at a predictable and decreasing rate. Therefore, it means that demand must follow this level of inflation to keep the price stable. Because Bitcoin is still a relatively small market compared to what it could be, it doesn't take significant amounts of money to move the market price up or down, and thus the price of a bitcoin is still very volatile. Also, other factors such as technology, widespread acceptance and understanding of e-money are taken into consideration. Whatever increases faith, increases the price, and vice versa. This may sound scary, that it is only practically backed by faith and opinion. It is up to users to supply the faith, and up to the community to support bitcoin to make it has high price. When magazines and online entities write intriguing articles about Bitcoin, people take interest in it, the demand goes up and so does its value. Also, companies, with high public assessment, which use or support the use of bitcoins have considerable role on this issue.
It is good to be mentioned that the price of bitcoin, powered by public opinion and support of users, was equal to the price of gold for some days as it is shown in the graph below:
One of the reasons that Bitcoin has gained such a high value, is that it promotes capitalism. For the perspective of miners, cryptocurrencies are a kind of investment. They literally invest electricity in order to mine cryptocoins with one purpose. They are hoping that this cryptocoins’s value may rise in future and thus profit will be made. In addition, to the facts stated before, cryptocoins are backed from whole stock exchange scene. This implies that many people are selling and buying cryptocoins with only one purpose. To make profit. Consequently, it is a modern example of gambling and cryptocoins are playing the role of shares. You can invest your money to cryptocoins and wait for its price to raise in order to sell them, aiming to profit. Also, many miners tend to create their own cryptocoins. It is another way for them to make profit. This project seems very difficult because the start from almost a zero base. The difficulty located to the fact that noone knows about the new created cryptocoins. It is up to the creator to care for the cryptocoins’s advertising. If the advertising is finally successful and the community convinced for the future prospect of the cryptocoins, its value will probably raise up.

2.2 Can Bitcoin and other Cryptocurrencies be regulated?

Bitcoins themselves cannot be regulated under current law, at least not directly. But certain activities involving bitcoins can be regulated. This came out in a recent hearing held by the Senate Committee on Homeland Security and Governmental Affairs focused on the necessity and ability for the federal government to regulate virtual currencies, such as bitcoin. The first panel repeatedly claimed that under current law virtual currencies were already sufficiently regulated. Also, the Bitcoin protocol itself cannot be modified without the cooperation of nearly all its users, who choose what software they use. Attempting to assign special rights to a local authority in the rules of the global Bitcoin network is not a practical possibility. Any rich organization could choose to invest in mining hardware to control half of the computing power of the network and become able to block or reverse recent transactions. However, there is no guarantee that they could retain this power since this requires to invest as much than all other miners in the world.

Under Article 1, Section 8 of the U.S. Constitution, Congress is granted the power “[to] coin money, regulate the value thereof, and of foreign coin, and fix the standard of weights and measures.” Bitcoins are not created by the federal government but through data processing within a network of computers. Thus, bitcoins are very much like a foreign currency and remain outside of U.S. jurisdiction as far as valuation or creation. This sentiment was echoed in a letter by current Federal Reserve Chairman Ben Bernanke on the virtual currency. However, when recognized as a currency, there are conditions under which bitcoins, and other digital currencies can find themselves subject to regulation.

One circumstance is when digital currencies are converted to dollars and vice versa. Back in March 2013, the bitcoin exchange Mt. Gox was charged for failure to register as a
currency exchange by the Financial Crimes Enforcement Network. This registration is part of the government’s anti-money-laundering laws. Registration as an exchange requires a business to track the identities of its customers and to identify activities related to money laundering.

Another example was a case in August 2013 in which a man was charged with running a Ponzi scheme involving bitcoins. The defendant argued that his business was not within the jurisdiction of the Securities and Exchange Committee because bitcoins were not money. The judge in the case ruled that bitcoin was indeed a currency and was therefore subject to Securities and Exchange Committee regulations.

Therefore, it is not only possible for bitcoins to be regulated by the United States government, but it has already become a reality for bitcoin users and businesses alike.

It is however possible to regulate the use of Bitcoin in a similar way to any other instrument. Just like the dollar, Bitcoin can be used for a wide variety of purposes, some of which can be considered legitimate or not as per each jurisdiction’s laws. In this regard, Bitcoin is no different than any other tool or resource and can be subjected to different regulations in each country. Bitcoin use could also be made difficult by restrictive regulations, in which case it is hard to determine what percentage of users would keep using the technology. A government that chooses to ban Bitcoin would prevent domestic businesses and markets from developing, shifting innovation to other countries. The challenge for regulators, as always, is to develop efficient solutions while not impairing the growth of new emerging markets and businesses.

2.3 Cryptocurrencies as investment

One way of investing in bitcoins is to buy and hold them as a long-term, high-risk investment. FINRA, a United States self-regulatory organization, warns that investing in bitcoins carries significant risks. The European Banking Authority warns that the risks of investment go beyond a potential fall in the value of bitcoins. Bitcoins may be of limited value to unsophisticated investors. Risk hasn't deterred some such as the Winklevoss twins, who made a US$1.5 million personal investment and attempted to launch a bitcoin ETF. Other investors, like Peter Thiel's Founders Fund, which invested US$3 million, don't purchase bitcoins themselves instead funding bitcoin infrastructure like companies that provide payment systems to merchants, exchanges, and wallet services, etc. Investors also invest in bitcoin mining.

According to an analysis of bitcoin prices performed for The Wall Street Journal by Mr. Harvey, between late 2010 and Wednesday, bitcoin's return in U.S. dollars had an annualized "standard deviation" of about 139%. That means it was roughly 7½ times as volatile as gold.
Since the days, when bitcoin cost $411, the price of a bitcoin has fallen as low as $387 and risen as high as $782, according to CoinDesk.com, which averages bitcoin prices across multiple exchanges.

Marie Brière, an associate professor at Université Paris Dauphine in France, calculated that between July 2010 and July 2013, bitcoin had an annualized return of more than 370% with 175% volatility. She found that its returns had a weak but significant correlation with gold and inflation-linked bonds, supporting the notion that some investors see bitcoin as an inflation fighter. Her paper, which was co-authored by Kim Oosterlinck and Ariane Szafarz of the Université Libre de Bruxelles in Belgium, concluded that a small allocation to bitcoin—perhaps 3% of a well-diversified portfolio—could improve one's risk-return trade-off. But that study was conducted when bitcoin was merely four years old, and even Ms. Brière says investors will have to wait and see which, if any, of bitcoin's characteristics persist. "I'd be very cautious. Is this a bubble or not? That's very hard to determine at this point," she says. And yet some firms are already trying to make it easier for investors to get involved.

Cameron and Tyler Winklevoss, of Facebook fame, have filed with the Securities and Exchange Commission to launch an exchange-traded fund, called the Winklevoss Bitcoin Trust, that holds bitcoins. In an email from their lawyer, the Winklevosses said they are working with the SEC to finalize the proposal and hope to launch next year.

SecondMarket, a platform for investing in private assets, has already launched a private fund called the Bitcoin Investment Trust, which holds bitcoins. It charges 2% yearly in management fees and is open only to accredited investors, which for a single person means more than $200,000 in income or $1 million in assets, excluding a primary home. SecondMarket CEO Barry Silbert says the trust, which is available in certain self-directed individual retirement accounts, has gathered $36 million in assets as of Thursday. He says that some family offices have made investments and seem to treat it as a small part of their gold allocation or their "risky alternatives" allocation, which includes investments such as hedge funds. Bitcoin "has a binary outcome," says Mr. Silbert. "There will either be a total loss of principal or a very, very high return."

Bitcoin's all-or-nothing nature probably means that investors shouldn't treat it as they would a normal asset class at all and instead think of it as they would a "tail-risk option"—one that pays off only if an extremely unlikely event occurs, says Mr. Pal, the former hedge-fund manager.

Again, in layman's terms, that essentially means that bitcoin is like a lottery ticket. Taking a tiny risk won't damage a portfolio if bitcoin goes bust, but will have a sizable impact if it takes off. What could that payoff be? And what's the chance of success? Unfortunately, there's no way to know either answer. Mr. Pal believes that if investors do tie bitcoin's price to that of gold, one bitcoin could be worth $1 million. He says that even using a
"conservative" estimate of $200,000, the price of bitcoin, at under $1,000, seems to factor in only a slight chance of the coins being equated to gold. Mr. Pal says he thinks the probability is much higher. As a result, he’s put a small slice of his portfolio—between 1% and 2%—into the coins.

"There’s no basis to be sure what bitcoin’s value will be or if it will even have a value," says Lawrence H. White, an economist at George Mason University, adding that he thinks its value is probably more closely tied to its role in the remittance market than as a gold substitute. There are many places where an investor can buy a bitcoin—or even a fraction of one, including Bitstamp and Coinbase. The minimum purchase at Coinbase is 10 cents.

Investors should think of bitcoins as a long-term speculation rather than a short-term trade or a long-term investment, says Mr. Pal. If you decide to take the risk, you shouldn't base your buying and selling on the gyrations of the market or invest more than the tiniest fraction of a portfolio that can be completely lost.

As bitcoin mania unfolds, the currency might turn out to be merely a speculative bubble that bursts as investors lose interest. But by risking very little, at the very least, an investor might be part of a story that’s still told nearly many years later.

2.3.1 Cryptocurrencies’ volatility

Bitcoin volatility

For any traded currency or asset, volatility is a measure for the dispersion of value changes around the average change. Changes in value are usually looked at on a day to day basis.

Value changes are measured as relative or percentage changes. That’s because only relative changes are comparable between different assets and over time. To give an example: if the Bitcoin price goes from USD 100 to USD 101 per Bitcoin from one day to the other, that would be a +1% change. If the price went from USD 1,000 to USD 1,001 the absolute change is the same, but the relative change is only +0.1%. Looking at a time series of daily changes, we can calculate the average daily percentage change over this period. The average daily change of BTC vs USD on Mt.Gox between July 2010 and August 2013 was 0.7%. This figure is also called the mean or expected daily return on an asset. 0.7% average daily return is quite a lot compared to other assets.

Once we have the average daily change over a given period, we can calculate volatility. We do this to get a figure for the average dispersion around the mean. The higher this dispersion (i.e. the volatility), the more uncertainty is attached to the expected return of this asset. Bitcoins had a daily volatility of 7.2% over the mentioned period. We annualize this figure to get an idea of the possible dispersion over one year. The result is 136% annualized return volatility, which also is a lot.
So the Bitcoin volatility tells us how much the BTC vs USD exchange rate disperses around the mean over a given period. Let’s look at some more historical data to put the Bitcoin volatility into perspective.

**Historical Bitcoin volatility**

Thinking of historical Bitcoin volatility, it’s no big news that it was going through the roof. However, what does deserve attention is how it evolved. Since volatility is calculated as an arithmetic average, single observations have a high influence on the outcome. Therefore we need to put special emphasis on the most extreme moves. Had I asked “when did the most extreme Bitcoin price changes happen?” what would you have answered? My personal guess would have been: spring 2013. Absolute changes in that time were massive. But looking at relative figures tells us, that’s not the whole story.

![Dailyreturns Bitcoin vs USD on Mt.Gox](image)

The chart shows us that the most dramatic Bitcoin price moves happened in 2011. In fact, 7 out of the 10 largest up moves occured in 2011, only one of them was in 2013. As we can see on the chart, it wasn’t the biggest one. Regarding downside moves the situation is similar. 6 out of the 10 largest downside moves happened in 2011. Only 2 of them occured in 2013. This does not say the ups and downs of spring 2013 were small, it just means that the basis for volatility, daily returns, were even more extreme in 2011. When we talk about figures, they have more meaning if we relate them to other comparables. Only then it is possible to say whether something actually is “big, “small”, “extreme” etc. Therefore we need to take a step out of the Bitcoin ivory tower and have a look at the world outside of it. And we have to make sure we are comparing apples with apples.

Before we can compare Bitcoin to something else, we need to know what it is. From a volatility perspective, Bitcoin can be two things. First, Bitcoin is a currency and a form of money. Bitcoin satisfies the three criteria that are generally taken to define money. These
are: a medium of exchange, a store of value and a unit of account. So when we think of Bitcoin as a currency, we need to compare it to other currencies.

The second way of looking at Bitcoin is to regard it as an asset. Assets represent value. As long as someone is willing to pay something in exchange for Bitcoin (be it other currencies, commodities, services etc.), Bitcoins are assets. Whether they are backed by anything or not, whether they have inherent utility (whatever that is) or not, doesn’t matter. Thus we can also compare Bitcoin to other assets. One obvious thing to do is to compare Bitcoins to other financial assets which are traded on liquid markets. Here prices adjust instantly to supply and demand and price data is publicly available.

The above chart shows the annualized 30 day moving average volatility of Bitcoin vs the US Dollar as traded on Mt.Gox. It is compared with the currency pair EURUSD and the S&P500 stock market index. There are two key messages following from this chart.

Comparing Bitcoin volatility with EURUSD we can see, that the EURUSD pair has a much smaller volatility. Only very rarely it crosses the 10% line. On the other hand, the S&P500 volatility is higher and fluctuates more. In 2011 it crosses the 40% line. Back in 2008, at the peak of the financial crisis, S&P500 volatility even went beyond 80% on an annualized basis. The Bitcoin volatility graph looks more like the S&P500 graph than like the EURUSD graph. Therefore, in the last three years Bitcoin prices behaved more like an asset than like a currency.

The other thing this chart shows us, is that the Bitcoin volatility has significant second order effects. At many points the volatility jumps from moderate values to values beyond 30%. So the change rate of volatility is high. This makes Bitcoin prices even more unpredictable. But looking at the development we also see, that these jumps tend occur less often. And more importantly, the Bitcoin volatility is declining. Slowly but steadily. Despite all the attention and the buzz, when it comes to Bitcoin volatility, the year 2013 so far has not been anything like 2011.
Isn't volatility a problem for Bitcoin?

This is a chicken and egg situation. For bitcoin's price to stabilize, a large scale economy needs to develop with more businesses and users. For a large scale economy to develop, businesses and users will seek for price stability. Fortunately, volatility does not affect the main benefits of Bitcoin as a payment system to transfer money from point A to point B. It is possible for businesses to convert bitcoin payments to their local currency instantly, allowing them to profit from the advantages of Bitcoin without being subjected to price fluctuations. Since Bitcoin offers many useful and unique features and properties, many users choose to use Bitcoin. With such solutions and incentives, it is possible that Bitcoin will mature and develop to a degree where price volatility will become limited.
3. Legal aspects

3.1 Promoting illegal activities

Bitcoin has been a subject of scrutiny amid concerns that it can be used for illegal activities. In October 2013 the U.S. FBI shut down the Silk Road online black market and seized 144,000 bitcoins worth US$28.5 million at the time. The U.S. is considered Bitcoin-friendly compared to other governments. In China new rules restrict bitcoin exchange for local currency. The European Banking Authority has warned that Bitcoin lacks consumer protections. Bitcoins can be stolen and chargebacks are impossible. In 2014 the U.S. IRS ruled that the bitcoin should be treated as property rather than currency.

The screenshot below shows some of the underground illegal services which accept Bitcoins. One can easily access this network (TOR hidden wiki) and gain access to illegal services such as money laundering ones.

- **Bitcoin-escrow**: Buy safely with bitcoin on deepweb.
- **Laudy King**: Super simple anonymous laundry service for Bitcoins.
- **Brave Bunny**: Online Bitcoin Wallet and Mixer. Low fee for laundry. No JavaScript! tinyurl.com/BraveBunny
- **EasyCoin**: Bitcoin Wallet with free Bitcoin Mixer.
- **WeBuyBitcoins**: Sell your Bitcoins for Cash (USD), ACH, WU/MG, LR, PayPal and more.
- **OnionWallet**: Anonymous Bitcoin Wallet and Bitcoin Laundry.
- **Bitcoin Smoke**: Laundry service on a dedicated server!
- **1 Hour Laundry**: Fastest laundry service on the deep web. Super low cost.
- **HQ Counterfeits**: High Quality 50 EUR Counterfeits. Reliable service with fair prices. Shipping only within Europe.
- **Carding Tools**: Carding service. Credit cards, bank accounts, DDoS service.
- **Clean My Coins**: 0.2% fee Bitcoin Laundry Service.
- **CCPlanet**: Best Autoshop for Credit Card mostly EU and US. New stocks, several sellers with automated Bitcoin system.
- **Bitcoin Fog**: Bitcoin anonymization taken seriously.
- **HQER**: High quality euro bills replicas / counterfeits.
- **USD Counterfeits**: High quality USD counterfeits.
- **The Gift Card Shop**: The easiest way to start carding! Fast Shipping, Low Prices! Reliable and trusted vendor.
- **Cheap Euros**: 20€ Counterfeit bills. Unbeatable prices!!
- **Clean Coins FREE**: Clean Coins Free is a free bitcoin laundry service that does not charge a fee to use!
- **USJUD Counterfeits**: 20 EUR || 20 USD Counterfeit money. High Quality, any trusted (cleaner) escrow accepted.
3.1.1 Tax evasion and Money laundering

Bitcoin is not a fiat currency with legal tender status in any jurisdiction, but often tax liability accrues regardless of the medium used. There is a wide variety of legislation in many different jurisdictions which could cause income, sales, payroll, capital gains, or some other form of tax liability to arise with Bitcoin.

**Tax evasion**

First of all, Bitcoin does not obviate taxes. Dissenters argued that the anonymity of the upstart digital currency is all that matters. Perhaps they can evade taxes and the IRS (Internal Revenue Service) will not catch them. But that does not mean there is no income. Start with how you classify Bitcoin, although that too can be debated. Transactions in Bitcoin could be property, barter, foreign currency, or a financial instrument. If you are paying wages with Bitcoin, you can hardly withhold some of the Bitcoin and send it to the IRS. If you exchange Bitcoins for cash, whether you have gain may depend on whether Bitcoin is really currency or commodity. The latter seems more likely, meaning you have gain to the extent of the appreciation in your Bitcoin. FinCEN (Financial Crimes Enforcement Network) says Bitcoin exchanges and Bitcoin miners should register as Money Services Businesses and comply with anti-money laundering regulations. Still, ordinary Bitcoin users don’t have to register just to purchase goods and services. The IRS treats it as pay in kind, just as if you paid in groceries or anything else of value. You must value what’s provided, withhold income and employment taxes in cash and send the money to the IRS. You also must issue a Form W-2. Consequently, with no banking or government involvement, Bitcoin may be anonymous. It may even be ideal for someone who intentionally tries not to pay tax. That may be a small piece of the Bitcoin payment universe. But for most people who file tax returns and report their income whether or not it shows up on a Form W-2 or 1099, it probably isn't the tax haven some are suggesting it is.

**Money laundering**

Bitcoins may not be ideal for money laundering because all transactions are public. Authorities have expressed concerns, however. The European Banking Authority and the FBI have both stated that bitcoin may be used for money laundering. In early 2014, an operator of a US bitcoin exchange was arrested for money laundering. Since, Bitcoin's release there have been reported various scandals concerning money laundering. Bitcoin offers high anonymity levels, despite the fact that transactions are public. People can take advantage of that in order to launder money. It is quite easy since someone could exchange real money for crytocoin and afterwards convert them back to real money through different kinds of online services. Someone could possibly buy goods with Bitcoins or any other kind of cryptocurrency and afterwards sell those online (eBay, Amazon) in return of real money. In other words, money laundering is a process of disguising the source of money. Cryptocurrencies may be ideal for this. The reason...
behind this is that there exist so many alternative cryptocurrencies and so many digital
currency markets, fact that makes it impossible to figure out the original source of money.

To sum up, from the above statements it is made clear that cryptocurrencies promote both tax evasion and money laundering. While Bitcoin came to offer freedom to people of the Internet, unfortunately it also promotes illegal activities. The promotion of illegal activities is a huge drawback of Bitcoin, since no society can meet a healthy evolution and development.

3.1.2 Black markets and Underground networks

Trying for a moment, to think like a criminal anyone can come to the conclusion that any financial transaction that leaves a trace also leaves evidence of ones misdeeds. For that reason, cash has been king over illegal financial transactions. For years, wrongdoers of every stripe, from hit men to drug dealers, had to tote around suitcases full of dollar bills to trade illegal goods and services.

Concerning the legal commerce if BTC anything could be bought using it or an alternative cryptocurrency as long as its seller is willing to accept cryptocurrencies as a form of payment. In addition, Bitcoin has become the preferred payment for much of the online underground networks/markets. Thus cryptocurrencies have found a home supporting both legal and illegal commerce in a way that makes it difficult for regulators to regulate.

In that kind of underground networks people are able to purchase drugs and many other illegal services. One of the biggest drug selling black market is the Silk Road. Silk Road's administrator hailed Bitcoin as the key to making his illicit business possible. Before Bitcoin existed, people would reconsider it again and again before using their credit card to buy something illegally. Bitcoin provides transaction anonymity making it harder to trace who made which transaction and why. However, spending Bitcoins to anonymously score drugs online isn’t as simple as it’s often made out to be. Privacy and security researchers report that there are ways to purchase with Bitcoins anonymously, but if you are a casual user, you will probably not be able to hide your activity very well. Researchers by using clustering methods they can possibly figure which address belongs to who.

There are many legal and social issues that originate from Bitcoin and the underground networks which are using it. The Hidden Wiki is another huge underground network based on the TOR Network. In order to access it someone would have to connect on the TOR network and then access that wiki page. In that wiki page, someone can find any kind of illegal service such as money laundering services, forgery services, hacker services or even assassination services. In addition, someone may be able to purchase drugs, weapons, explosives and any kind of porn content (e.g. child pornography).

On 2 October 2013, the FBI shut down Silk Road. But, on the same time at least three Silk Road clones are picking up the pieces. Deepbay, Sheep Marketplace, and Black
Market Reloaded are these specific examples, all require the use of hard-to-trace virtual currency Bitcoin and conceal themselves within the anonymizing Tor network.

It is made clear in this point, that black markets are mostly harmful for the society. From the one hand, this whole situation provides freedom to people, especially those who live in oppressing societies such as China. As for the law, apparently law enforcement cannot easily intervene onto what happens at those underground networks. On the other hand one can observe that it is not the cryptocurrency that causes the problems but the use by people with the profit motive. Of course a brilliant way of electronic payment such as BTC could benefit the society in a variety of ways.

Furthermore on black markets, IRC servers and channels are being used for illegal trades whereas Bitcoin serves as the currency. Also, by using escrow services 2 parties can trade goods while the 3rd party will be holding their money. One can imagine that anything could be traded online. This of course is not wanted and would not serve for the society’s best in any case. It should be also mentioned that the economic effects are many. People get scammed, people lose their money while others evade taxes and make profit.

The biggest underground market System D which runs all around the world is not using Bitcoin as its main currency. This clearly promotes the selling of illegal goods and services.

3.2 Cryptocurrencies and Laws

3.2.1 Legality of Cryptocurrencies by country

**Bitcoin: It’s Currency, but not Government Currency**

As already mentioned in a prior chapter, Bitcoins can be created seemingly out of thin air or at least solely from the act of problem-solving. They are created by performing mathematical calculations in order to solve a puzzle.

The question of how to deal with Bitcoin is becoming a regulatory priority, as adoption of the virtual currency spreads and governments panic. But for consumers and businesses, the global legal landscape is murky.

More governments are coming out with pronouncements and opinions on how Bitcoin should be treated under their law. Many countries, such as Germany, have declared that Bitcoin is not legal tender, and cannot be used to pay taxes or government obligations. Other nations, such as Canada, have said that income earned from Bitcoin activity is taxable. Most countries are in a wait-and-see mode: “At the moment, we’re studying Bitcoin and we have no plan to issue a regulation on it,” a spokesperson for the Bank of Indonesia told the Jakarta Globe in December.
Senator Tom Carper of Delaware, the Chairman of the Homeland Security and Governmental Affairs Committee, tasked the Law Library of the U.S. Congress to survey 40 jurisdictions and the European Union to see which ones have already regulated Bitcoin, and in what manner. The Law Library recently released its report.

The conclusion? Not many countries have yet enacted laws to address new forms of virtual currency. Nonetheless, “there is widespread concern about the Bitcoin system’s possible impact on national currencies, its potential for criminal misuse, and the implications of its use for taxation.” China and Brazil appear to have the most specific laws to date. The Chinese government has declared the Bitcoin illegal to use as a currency, while the Brazilians have set out a legal framework for its adoption under Law No. 12,865.

Bitcoins are a secure payment mode. When you perform a transaction, your Bitcoin software performs a mathematical operation to combine the other party’s public key and your own private key with the amount of Bitcoins that you want to transfer. It is practically impossible—even with the most powerful computer—to ascertain the code of someone’s private key from his or her public key, due to encryption.

For some people, it may be just fine to keep their Bitcoins as Bitcoins and not cash them out into government-backed currency like US dollars or Euros. But what if you do want to take some of your hard-earned Bitcoins to use and spend at a place that does not accept Bitcoins? The answer is that you can exchange your Bitcoins for government-issued currency on a number of exchanges that will provide you with floating exchange rates Or, you can store your Bitcoins in secure online “lockers” offered by companies that provide services for the Bitcoin world.

**Banning Bitcoin: Why It Is Not the Right Solution**

In February 2014, the Russian Prosecutor General’s Office noted that Bitcoins and other crypto currencies cannot be used legally in Russia. In support of that conclusion, the Russian law enforcement agency cited a 2002 law signed by Russian President Vladimir Putin that reads, “The official currency of the Russian Federation is the ruble. Introduction of other monetary units and money substitutes is prohibited.”

The Prosecutor General’s Office is also quoted as saying that “The monitoring of the use of virtual currencies shows an increasing interest in them, including for the purpose of money laundering, profit obtained through illegal means.”

In December 2013, The People’s Bank of China, the country’s central bank, banned financial institutions and payment services from Bitcoin-related business. This was done
in order to avoid harm to the public and to the legal monetary status of the renminbi [a.k.a. the yuan] that might occur as a result of “excessive speculation” in Bitcoin and other virtual goods, said the statement. Third party service providers were also told to stop offering clearing services to Bitcoin exchanges.

But prohibiting Bitcoins’ use won’t make people stop using the currency. Indeed, it is precisely because Bitcoin can currently be used in a way that provides anonymity and allows people to buy from entities that are currently unregulated, that Bitcoin is used. Some people don’t like to use money issued by the government. Others value the privacy of a currency that is not accounted in the same way that bank transactions are. Still others find that Bitcoins are worth more than legal tender these days, with problems in the Euro zone and other countries. Some consumers feel that virtual currencies may be more efficient, and may offer newer, more flexible ways to pay for thing across borders. Prohibition would be overinclusive; it takes a product that has multiple uses—many of them legitimate—and tries to ban it or wish it out of existence.

The criminal side of Bitcoin’s use is what has garnered most headlines. Websites like Silk Road, which allows people to buy drugs online and underground take Bitcoins. On October 2, 2013, the FBI shut down Silk Road, arrested Ross William Ulbricht, and identified him as the founder and chief operator “Dread Pirate Roberts.” The FBI reported seizing $3.5 million worth of Bitcoins during the sting.

In November 2013, Forbes and Vice reported that Silk Road 2.0 was being run by the former administrators of the site. In November, a similar site called Sheep Marketplace was deemed a scam after it lost $100 million in users’ bitcoins in an alleged hack. And just last week, administrators of the revived Silk Road claimed cyber attackers had somehow spirited away all the Bitcoins it held in escrow—valued at $2.7 million.

Illegal marketplaces have existed in the past and will continue to spring up in the future. We don’t ban money or cash simply because it can and will be used for illegal purposes. (and the way things are going with these exchanges, they may operate so poorly as to go out of business based on poor security). As with Bitcoin, such an exchange can be used in a criminal manner or for mundane purchases.

Banning Bitcoin is difficult to do Since Bitcoin is not issued by a government, it can still be created. Then regulators will have to spend time figuring out who is using it—and then may only end up penalizing businesses that are using it legitimately. Regulated websites like news site Reddit, and blog creation site WordPress accept Bitcoins. Virgin Galactic, Richard Branson’s space travel company, accepts Bitcoins. Perhaps the largest retail site to accept Bitcoins is Overstock.com. Other companies—including PayPal—have publicly contemplated accepting Bitcoin.
So rather than ban the Bitcoin, another alternative would allow some regulatory help. Should governments allow Bitcoin to keep operating, as an alternative to banks and to using government-issued currency? The answer is yes—but we should not over-regulate the Bitcoin at the outset.

**How authorities enact?**

- **Canada**

Canada has announced that it will tax bitcoin in two ways. Transactions made for goods or services will be treated under its barter transaction rules, while its “Transactions in Securities” document says that profits made on commodity transactions could be income or capital. It confirmed these rules in November 2013.

In late March 2014, the Canada Revenue Agency (CRA) published a new document outlining its position on the taxation of digital currencies, which highlighted out the differences between personal and business activities.

In essence, Canada will view the matter subjectively, on a case by case basis. When authorities deem the activities were undertaken for profit, the taxpayer’s income will be taxed with reference to the taxpayer’s inventory at the end of the year. Barter transactions are allowed, but the CRA states that the value of goods or services obtained by bartering digital currencies must be included into the taxpayer’s income, if business related. Losses through theft or embezzlement may be deductible.

- **European Union**

EU's banking regulator, The European Banking Authority (EBA), issued a warning statement on 13th December 2013 warning of investment risk, but focusing mainly on issues of fraud, tax evasion and other crime connected to virtual currency use. The statement also warned that if news of misuse continued to emerge, it “could lead law enforcement agencies to close exchange platforms at short notice and prevent consumers from accessing or retrieving any funds that the platforms may be holding for them”.

- **Belgium**

National Bank of Belgium has no intention of intervening in bitcoin business or regulating it, says the Belgium Bitcoin Association. On 16th January 2014, however, the central bank issued a joint warning with the Belgian Financial Services and Markets Authority (FSMA) that digital currencies are not issued by any central authority, and as such are at risk of volatility, fraud, and business non-acceptance.
• United Kingdom

United Kingdom with policymakers in the UK in September 2013 suggested that bitcoin-based businesses would not have to register with regulators, at least for the time being, while they consider their regulatory position. For a while, the UK suggested that bitcoins wouldn’t be treated as money, but would instead be classified as single-purpose vouchers, which could carry a value-added tax (sales tax) liability on any bitcoins that are sold.

However, this idea was reversed in guidance issued on 3rd March. Although the UK tax department, HMRC, stepped back from explicitly recognizing bitcoin as a currency, its approach effectively treats it like any other form of payment for tax purposes: “In all instances, VAT will be due in the normal way from suppliers of any goods or services sold in exchange for bitcoin or other similar cryptocurrency.”

• Japan

At present there are no laws covering cryptocurrencies in the country. However, since the collapse of bitcoin exchange Mt. Gox and the attention that garnered from the international media, Japan seems to have been pressurized into taking some action. Initially it appealed for a coordinated effort from the international community to agree on regulation. More recently, Japan’s ruling party, the Liberal Democratic Party (LDP) has launched a committee to investigate cryptocurrencies, and issued a statement saying it is “not a currency, but taxable”. Currently the situation seems to be that bitcoin will be treated as a good and is subject to taxation if transactions fulfil standing tax requirements. Gains on exchange rates are taxable too.

The government has also blocked related banks from “brokering bitcoin transactions or opening accounts holding the virtual unit”. Exactly what constitutes a ‘bitcoin account’ remains unknown, but it presumably refers to one with a known bitcoin service like Blockchain.info or Coinbase.

The Japanese government is, however, generally curious about bitcoin and will not make any further statements on the matter until it has discussed matters with local bitcoin interests, a government representative has said.

• China

China’s central bank has ordered third-party payment agencies - which provide clearing services for bitcoin exchanges - to stop any "custody, trading and other services" related to the virtual currency, according to a report Tuesday by Yicai.com. The Chinese website - which is affiliated with the China Business Network TV station - added that platforms were told to end working relationships with virtual currency exchanges before Chinese New Year which commences at the end of January.
Zhou Jinhuang, the deputy director of payment clearance at the People's Bank of China is reported to have chaired the closed-door meeting on Monday when more than 10 third-party payment platforms were given the news. Attendees included a representative from Alipay, which is China's leading third-party online payment solution, according to its website.

- Brazil

Brazil April 2014, the Receita Federal, Brazil's tax authority, established how it would treat the holding and usage of bitcoin and other digital currencies. Taking a stance similar to the one announced by the US Internal Revenue Service in March, Brazil is treating digital currencies as financial assets, with the Receita Federal imposing a 15% capital gains tax at the time of sale, however, there are some key differences that have been generally viewed positively by bitcoin users in the country. Those who sell less coins with a value of less than 35,000 reals (R$), which is almost $16,000, will not have to pay the tax. This means that bitcoin users in Brazil won’t have to calculate capital gains taxes when making small consumer purchases. The Receita Federal is also requiring annual account declarations from those who possess more than R$1,000 in digital currency holdings.

- Colombia

The Superintendencia Financiera de Colombia (SFC) may be close to outlawing bitcoin transactions in the South American country, a newspaper claimed on 20th March 2014. The report said that the SFC, in conjunction with Banco central de Colombia, Colombia's central bank, and the Ministerio de Hacienda y Crédito Público, the executive body responsible for budgetary concerns, is preparing to issue a document outlining the government’s stance on bitcoin and bitcoin-related activities. A source connected to the Colombian Ministry of Finance told El Tiempo that the ban may very well focus on bitcoin handling activities, rather than outright purchase by consumers.

- Mexico

On 12th March 2014, the Bank of Mexico issued its first statement on the issue of cryptocurrencies. The bank warned the public via a statement on its website about the “inherent risks of acquiring these assets and using them as substitutes for conventional methods of payment”. The warning was generally similar to those issued by many of the world’s central banks in recent months. However, most notable were potential restrictions for domestic financial institutions, that some reports implied might strangle bitcoin businesses. Translations of the statements suggest that financial institutions regulated in Mexico “are not authorized to use or carry out any operations with [digital currencies]”. Whether that means banks may not deal
directly in cryptocurrencies, or may not have relationships with companies that deal in them, is not yet clear.

3.2.2 Consumer protection

**Protection**

Bitcoin is freeing people to transact on their own terms. Each user can send and receive payments in a similar way to cash but they can also take part in more complex contracts.

Bitcoin always leave a public proof that a transaction did take place, which can potentially be used in a recourse against businesses with fraudulent practices.

It is accurate to say that a complete set of good practices and intuitive security solutions is needed to give users better protection of their money, and to reduce the general risk of theft and loss. Over the course of the last few years, such security features have quickly developed, such as wallet encryption, offline wallets, hardware wallets, and multi-signature transactions (Multisig).

- Multi-signature transactions, a transaction will be accepted by the network only if a certain number of a defined group of persons agree to sign the transaction.

- Wallet encryption uses AES-256-CBC to encrypt only the private keys that are held in a wallet. The keys are encrypted with a master key which is entirely random. This master key is then encrypted with AES-256-CBC with a key derived from the passphrase using SHA512 and OpenSSL's EVP.BytesToKey and a dynamic number of rounds determined by the speed of the machine which does the initial encryption (and is updated based on the speed of a computer which does a subsequent passphrase change).

- Offline wallet is safe from all online threats, such as viruses and hackers. It is however still exposed to offline threats, such as hardware keyloggers, extortion, or people looking over your shoulder. A best practice is to keep the majority of your bitcoins in the offline wallet and only to use the online wallet for everyday expenses/earnings.

- A hardware wallet is a device that stores a part of a user’s wallet securely in mostly-offline hardware. They have major advantages over other wallet types:
  - the key is often stored in a protected area of a microcontroller, and cannot be transferred out of the device in plaintext
  - immune to computer viruses that steal from software wallets
  - can be used securely and interactively, as opposed to a paper wallet which must be imported to software at some point
much of the time, the software is open source, allowing a user to validate the entire operation of the device

BitLicense

A BitLicense or some other type of license may be a prudent way to keep sellers on a regulator’s radar screen, not only for purposes of law enforcement, but also for consumer-protection purposes.

New York is now the first state to consider adding a special license called a "BitLicense" for businesses that operate primarily in Bitcoin and other virtual currencies. That “BitLicense” would allow virtual currency companies to do business in New York and send currency to New Yorkers, and would require compliance with anti-money laundering and consumer protection requirements tailored to the digital cash crowd.

Bitcoin is not secure

Mt. Gox was a Bitcoin exchange based in Tokyo, Japan. It was launched in July 2010, and by 2013 was handling 70% of all Bitcoin transactions. In February 2014, the Mt. Gox company suspended trading, closed its website and exchange service. In April 2014, the company began liquidation proceedings. It announced that around 850,000 bitcoins belonging to customers and the company were missing and likely stolen, an amount valued at more than $450 million at the time. Although 200,000 bitcoins have since been "found", the reason(s) for the disappearance—theft, fraud, mismanagement, or a combination of these—are unclear as of March 2014. There has been some speculation of hackers being responsible for the missing Bitcoins, but no speculation of such matter has been proven.

This is not an endorsement of trust in the use of eWallet services. There are no guarantees that any eWallet service won't one day take all your bitcoins and disappear. If someone else gains access to your wallet (and your password) and steals everything, there is no way to reverse the transaction.

If you try to withdraw bitcoins from the Tokyo-based exchange last year, Mt.Gox suddenly demanded extra verification: a photo ID, a copy of a utility bill and a short questionnaire. It is made clear from the above statements that Bitcoin does not guarantee consumer protection.
4. Social aspects

4.1 Foundations and Concepts behind Cryptocurrencies

The Extremist Foundations of ‘Digital Freedom’

The use of the term “cyber libertarian” to refer to beliefs shared by people from an apparently wide range of political and philosophical orientations today, beliefs that might be summed up via a slogan like “Computerization will set you free”. This slogan is purposely vague, but no less powerful for that beliefs need not be coherent or clearly-articulated for them to have adherents. While only a small number of people self-identify as cyber libertarians, many more subscribe to the belief in practice. Among the corollaries that follow from this core belief include: a resistance to criticism of the incorporation of computer technology into any sphere of human life.

A pursuit of solutions to perceived problems that takes technical methods to be prior to analytic determination of the problems themselves, a privileging of quantificational methods over and above, and sometimes to the exclusion of, qualitative ones; the use of special standards for evaluating computational practices that differ from those used in evaluating non-computational ones; and an overarching focus on the power of the individual and individual freedom, even when that individual is understood to be embedded in a variety of networks.

There is no lack of figures who deserve to be called cyber libertarians, and a major part of my effort here is to draw attention to the remarkable degree to which, if it is grounded at all, that doctrine is grounded in thought that is quite far to the right, and often an explicitly right libertarianism. These terms require some unpacking, but for the moment we should just consider the obvious but rarely-remarked fact that of those theorists, writers, and practitioners who advocate some version of the cyber libertarian dogma, the vast majority explicitly endorse some form of libertarian thought.

This group includes Wikipedia founder Jimmy Wales, Open Source Software originator Eric Raymond, technology writer and founder of Wired magazine Kevin Kelly, WikiLeaks founder Julian Assange, cyberspace evangelist John Perry Barlow, business leaders like Sergey Brin of Google and Peter Thiel, and business writers like Don Tapscott and Clayton Christensen. The much smaller group who do not explicitly invoke Rand or Hayek — including Yochai Benkler, Tim O’Reilly, Jeff Jarvis, Clay Shirky, Lawrence Lessig, perhaps seven Mark Zuckerberg of Facebook — nevertheless frequently begin their analyses from libertarian principles that they leave unattributed, and add what can at best be thought minor, sometimes populist or liberal modifications to the core doctrine, while rarely challenging its central precepts.

The number of such thinkers who can be said to emerge from anything like genuinely leftist or even traditional conservative thought is vanishingly small: the best-known is probably Michel Bauwens of the P2PFoundation, and even he frequently traffics in what look like libertarian claims.
Weaknesses in Bitcoin’s foundations

One thing cannot be disputed about the person (or persons) responsible for creating Bitcoin: they were skilled in math, and expert at coding. Five years after the Bitcoin software was first released, no major fixes have been needed to the core code, which uses cryptography to generate and transfer virtual money.

Yet signs are emerging of more subtle flaws in the vision of Satoshi Nakamoto (which may or may not be a pseudonym), with analysis suggesting the rules governing how Bitcoin operates as a currency may be far from perfect. Some researchers claim that these rules leave room for cheats to destabilize Bitcoin. Others have concluded that major changes to the currency’s rules will be needed as the number of bitcoins in circulation increases.

“In the real world, people don’t always follow the rules—they do what’s best for them”, says Joshua Kroll, a researcher at Princeton. “Understanding this is the key to understanding whether and how Bitcoin survives—it tells you whether the system can last for a long time, how robust is it in the face of shocks.”

Kroll and others are exploring possible problems using game theory, a way to mathematically calculate how individuals might choose to cooperate, compete, or cheat given the options available to them and the strategies of others.

One conclusion drawn by Kroll and his Princeton colleagues Ian Davey and Ed Felton is that those rules will have to be significantly changed if Bitcoin is to last. Their models predict that interest in “mining” for bitcoins, by downloading and running the Bitcoin software, will drop off as the number in circulation grows toward the cap of 21 million set by Nakamoto. This would be a problem because computers running the mining software also maintain the ledger of transactions, known as the blockchain, that records and guarantees bitcoin transactions (see “What Bitcoin Is and Why It Matters”).

Miners earn newly minted bitcoins for adding new sections to the block chain. But the amount awarded for adding a section is periodically halved so that the total number of bitcoins in circulation never exceeds 21 million (the reward last halved in 2012 and is set to do so again in 2016). Transaction fees paid to miners for helping verify transfers are supposed to make up for that loss of income. But fees are currently negligible, and the Princeton analysis predicts that under the existing rules these fees won’t become significant enough to make mining worth doing in the absence of freshly minted bitcoins.

The only solution Kroll sees is to rewrite the rules of the currency. “It would need some kind of governance structure that agreed to have a kind of tax on transactions or not to limit the number of bitcoins created,” he says. “We expect both mechanisms to come into play.”
That kind of approach is common in established economies, which tame things like insider trading with laws and regulatory agencies and have central banks to shape economies. But many backers of Bitcoin prize the way it currently operates without centralized control, and would likely rebel at any suggestion of changing the rules.

Researchers from Cornell claim to have found another problem with bitcoin mining. At the Financial Cryptography conference this month, they presented work suggesting that so-called “selfish miners” could exploit the current rules to gain more than a fair reward for their work.

Bitcoin miners run software that races to solve a mathematical puzzle and thereby add the next section to the blockchain, netting the reward that comes with it. Under the selfish-mining strategy, a mining operation would refrain from announcing it had completed the next new block, shunning the reward in an attempt to get a head start on the competition on the following block.

The Cornell analysis shows that although selfish miners do worse initially, the strategy can pay off over time by causing honest miners to waste time on puzzles that are irrelevant. The strategy does, however, depend on having a significant share of the overall computing power of all bitcoin miners.

“If your mining power is more than a third of the system total, this always works,” says Ittay Eyal, who did the research with colleague Emin Gün Sirer. “You may be able to do it with much less,” Eyal adds.

Eyal proposes a modification to the mining protocol that would ensure that only someone controlling at least a quarter of all mining power could profit from selfish mining, and says the Bitcoin community should also make efforts to limit the power of mining operations.

The selfish-mining theory has been controversial in the Bitcoin community and academia, with some claiming it wouldn’t work. But the idea of somehow reducing the influence of the largest mining operations has wide support. It has long been known that a miner controlling 51 percent of all bitcoin mining power could tamper with the blockchain to do things like spend bitcoin twice.

That threat began to feel genuine in January of 2014 when the G.Hash mining group from China grew to control 41 percent of the network’s power, before backing off in the face of outcry. Nonetheless, the dominance of a handful of large mining operations suggests a 51 percent attack remains possible, whether from one growing or two colluding. G.Hash now controls 29 percent of the network’s power, with the next three largest controlling a further 42 percent between them.

One other reason to reduce the dominance of large mining ventures is that their size seems to encourage use of denial of service attacks, says Benjamin Johnson, a researcher at the University of California, Berkeley. He was lead author on a paper at the Financial Cryptography conference that used game theory to show that it makes sense
for smaller miners to boost their own success by preventing large miners from operating rather than investing in more mining power, and that the incentive disappears if mining is not dominated by a handful of large players.

Another paper presented at the conference reported that 63 percent of large mining pools had been attacked, compared to only 17 percent of small ones. “This argues that way before a pool reaches the 51 percent threshold, it creates unhelpful incentives,” says Johnson.

Johnson says the Bitcoin Foundation, a nonprofit created to standardize and promote Bitcoin, and the people maintaining the Bitcoin software have shown interest in his work and that of others probing the currency’s design. “They’re really invested in making sure this protocol works and doesn’t fail due to some economically motivated attack strategy.”

4.2 New paths and job opportunities

Bitcoin is being supported and maintained by its own network and its miners, but, how miners’ demands have led to the foundation of new companies? Bitcoin, mainly, has led to new career paths and job opportunities as it has redefined the way transactions are made over the Internet.

As mentioned in the first chapter, Bitcoin is easier to be mined as long as its difficulty is low. Mining was usually been done using graphic cards (GPUs) or rigs (many graphic cards together). As time passes by, bitcoin’s difficulty is rising and it is more difficult to get. Thus, there was a need for new hardware in order to maintain an amount of bitcoins while difficulty was rising. This led to the establishment of new companies whose purpose was to make that hardware which is called ASIC. One of the world’s most known company on this field is Butterfly Labs and most of these companies make world wide deliveries.

However, this was not enough for some people. Some of them wanted to be free of the hassle of managing any kind of hardware while some others wanted much higher hashrates given the hardware. This need was fully covered by what is called “Cloud Mining”. To be put very simply, cloud mining means using (generally) shared processing power run from remote data centers. One only needs a home computer for communications, optional local bitcoin wallets and so on. As a result, this alternative revolutionized the way mining was used to be done. As before, new companies have been set up, one of which is the most well-known for its services, CEX.IO.

Except the mining hardware and services that some companies offer, there are also companies whose service is to provide a 24/7 exchange for any kind of cryptocurrency.

More and more companies are being founded related to Bitcoin and the existing ones are being expanded. Job opportunities are endless and they cover a wide range of fields like encryption, mathematics, pcb design, telecommunications etc.
4.3 Privacy concerns and personal view

In order to understand how someone can be traced by his BTC transactions must firstly understand the Bitcoin works with an unprecedented level of transparency that most people are not used to dealing with. All Bitcoin transactions are public, traceable, and permanently stored in the Bitcoin network. Bitcoin addresses are the only information used to define where bitcoins are allocated and where they are sent. These addresses are created privately by each user's wallets. However, once addresses are used, they become tainted by the history of all transactions they are involved with. Anyone can see the balance and all transactions of any address. Since users usually have to reveal their identity in order to receive services or goods, Bitcoin addresses cannot remain fully anonymous.

Also because the Bitcoin network is a peer-to-peer network, it is possible to listen for transactions' relays and log their IP addresses. Full node clients relay all users' transactions just like their own. This means that finding the source of any particular transaction can be difficult and any Bitcoin node can be mistaken as the source of a transaction when they are not. Unless the IP address remains hidden with a tool like 'Tor' so that it cannot be logged, the identity of a user is in danger of exposure.

Gaining a fair understanding of BTC's economy system, one can see a new opportunity of safe anonymous exchanges without state control or "unfair" forms of back-taxes on payment. However like any other currency, its purpose is solely to satisfy human desire of ownership, therefore what somebody does with BTC is not sure to be legal, as a proof we have seen many cases of misusing its market value.

How can one be sure that a brighter future lies ahead, with this "made-out-of-thin-air" coin?
Well, it is not possible to be. It is up to humanity. An unified global non-centralized cryptocurrency system, can welcome days of freedom and prosperity in both markets and real lives, all around the globe, so no oppressing state or federal organization can intervene with ones personal life.
That's when the BTC will have truly won.
References

1.1

[1] Satoshi Nakamoto is just an alias name. The Bitcoin community is wavering on who Satoshi Nakamoto really is. Some people state that it's a whole team behind it, while some others believe that its just one person. The truth is that whoever it is behind the Bitcoin's idea, has/have high respect to their privacy.

1.1.1