Asesorías y Tutorías para la Investigación Científica en la Educación Puig-Salabarría S.C.
José María Pino Suárez 400-2 esq a Lerdo de Tejada. Toluca, Estado de México. 7223898475
RFC: ATI120618V12

**Revista Dilemas Contemporáneos: Educación, Política y Valores.**
**http://www.dilemascontemporaneoseducacionpoliticayvalores.com/**
**Año: VI Número: 2 Artículo no.:52 Período: 1ro de enero al 30 de abril del 2019.**

**TÍTULO:** Desafíos de la aplicación del Bitcoin.

**AUTOR:**

1. Máster. Solmaz Besharat.

**RESUMEN:** El Bitcoin es una moneda virtual que hoy se conoce como sistema de pago descentralizado y que puede transferir dinero por medio de la computadora sin tener que acudir a un banco o institución. El Bitcoin ahora se convierte en un método popular de pago a cambio de bienes y servicios. Éste ha sido y sigue siendo utilizado por algunos para actividades ilegales y para promover delitos. Estar descentralizado significa que se emiten sin una autoridad de administración central. Para lograr un negocio preciso con Bitcoin es necesario eliminar barreras actuales y prepararse para la aceptación de nuevas tecnologías en moneda digital. Este document discute los desafíos del Bitcoin como moneda virtual y no pretendemos cubrir todos los aspectos del Bitcoin.

**PALABRAS CLAVES:** Bitcoin, moneda virtual, pago a cambio de bienes y servicios, sistema de pago descentralizado.

**TITLE:** Challenges Application of Bitcoin.

**AUTHOR:**

1. Máster. Solmaz Besharat.

**ABSTRACT:** Bitcoin is a virtual currency that is now known as a decentralized payment system that can transfer money through the computer without having to go to a bank or institution. Bitcoin now becomes a popular method of payment in exchange for goods and services. This has been and continues to be used by some people for illegal activities and to promote crimes. Being decentralized means that it is issued without a central administration authority. To achieve a precise business with Bitcoin, it is necessary to eliminate current barriers and prepare for the acceptance of new technologies in digital currency. This document discusses the challenges of Bitcoin as a virtual currency and we do not intend to cover all aspects of Bitcoin.

**KEY WORDS:** Bitcoin, virtual currency, payment in exchange for goods and services, decentralized payment system.

## INTRODUCTION.

In earlier time, currency was essentially receipt for a commodity redeemable in most cases for physical gold, [6] but most of the currencies in the world at present, including the reserve currencies are known as fiat currencies. The ‘fiat currencies’ refers to Currencies that are neither inherently valuable nor redeemable for a commodity, but these currencies usually have a central regulatory body which issues them, and are consequently called ‘centralized’ [5]. The value of such currencies derived from the trust placed in the central authority by the users of the currency [20].

A crypto-currency is a medium of exchange that uses cryptography to manage the creation of new units as well as secure the transactions. These are a subset of digital currencies [5]. One of the most striking features of crypto-currency is that it weeds out the need for a trusted third party such as a governmental agency, bank etc. The crypto-currency system collectively creates the units. The rate at which such units are created is defined beforehand and is publicly known unlike the traditional

currencies where the government or the authorized banks control the supply. The fundamental system on which most crypto-currencies are based today was created by Satoshi Nakamoto [5].

Everything started in 2009 when Bitcoin, the first electronic currency was introduced for the first time. As many suggest irrespective of its name, the concept at Bitcoin was already a reality of for back as 1999, as apparent in this statement made by economic Milton Friedman one thing that's missing but will soon be developed is a reliable E-Cash, a method whereby on the internet you can transfer funds from A to B at any time and in anywhere [14].

Nevertheless, this concept which predicted by Friedman and others came to life on January 2009, when Satoshi Nakamoto created the Bitcoin Genesis Block, generating interest and triggering an ongoing international debate with respect to Bitcoin, its strengths and its weaknesses. Some of people argued that international feature of Bitcoin as "a global transferring money system by anyone, at any time and from anywhere" [14], In the other hand, others criticize it that anonymity of Bitcoin makes it attractive for illegal activities.

The purpose of this paper is to first look at the origin and development of Bitcoin. I also mention the main advantages and its barriers on utilisation of it, Bitcoin in selected jurisdiction, and finally illegal activities through Bitcoin.

## DEVELOPMENT.

### Exact Origin of the Bitcoin.

**2007-** According to legends, Satoshi Nakamoto began working on the Bitcoin concept in 2007 and developed the concept of the Bitcoin while he is on record as living in Japan, it is speculated that Nakamoto may be a collective pseudonym for more than one person [3].

**2008-31, October -**Nakamoto publishes a design paper through a metzdowd.com cryptography mailing list that describes the Bitcoin currency and solves the problem of double spending so as to prevent the currency from being copied [16].

**2009- 3, January-** Block 0, the genesis block, is established.

**2009-12, January -**The first transaction of Bitcoin currency, in block 170, takes place between Satoshi and Hal Finney, a developer and cryptographic activist [3].

**2009- October**- New Liberty Standard publishes a Bitcoin exchange rate that establishes the value of a Bitcoin at US$1=1,309.03Bitcoin, using an equation that includes the cost of electricity to run a computer that generated Bitcoins [3].

**What is Bitcoin and how does it work?**

What is a Bitcoin? Bitcoins are very close to "pure money" [1] -- they are digital transactions that function as money. They are a unit of account, a means of exchange, and a store of value, but unlike previous digital currencies, they are not backed by precious metals or the full faith and credit of any government. They are almost the Platonic ideal of money, and are valuable only because they are useful as money. That is a concept that most people have trouble accepting; that money "backed by nothing" can be valuable. But if you think about why we value things it makes sense. I value a hammer because it is good at banging on nails. Bitcoins are valuable because they are good to use as money. Also, unlike previous digital currencies, Bitcoin is completely decentralized. There is no central bank issuing Bitcoins and there is no payment processing company validating transactions. Before credit card companies and national currencies, people used decentralized non-digital currencies like gold and silver.

Everything supposedly began in 2009 when Bitcoin, the world's first decentralize electronic currency, was introduced by an unknown individual or group of people, operating under the name Satoshi Nakamoto, published a paper outlined the concept behind a completely new currency-freed from the supervision of banks and government [16].

According to Nakamoto, Bitcoin is a software-based online payment system and introduced as open-source software [16]. It is often classified as a "cryptocurrency" because it relies on cryptography to authenticate transaction.

One should note, that there are similar crypto currencies developing in the global market. In fact, Ripple, Litecoin, Peercoin and Dogecoin are all virtual currencies based on the principals of a peer-to-peer, decentralized, digital currency whose implementation relies on the principles of cryptography techniques to validate the transactions, and generate currency itself.

A Bitcoin is merely a chain of digital signatures saved in a "wallet" file [6]. This chain of signatures contains the necessary history of the specific Bitcoin so that the system may verify its legitimacy and transfer its ownership from one user to another upon request [16].

All Bitcoins and users have their own unique identity and each transaction is recorded in a public ledger. This ledger, called the "blockchain" in Bitcoin terminology, is visible to all computers on the network, but does not disclose personal information about the parties involved in transactions. According to some article the public nature of the ledger helps to prevent double-spending of the same Bitcoins, and also eliminates the need for a third party to verify transactions between buyers and sellers [14]. Anyone who wants to join the Bitcoin network can download the free and open-source software and create an account.

Bitcoin transactions are transfer of value between 'Bitcoin wallets' which are software programs that emulate bank accounts. Each wallet contains a 'public key' and 'private key. A public key is the

Wallet address (similar to a payment account or card number) and can be shared with others and private key is the signature (or security code) that authorizes a transaction.

When a user sends Bitcoins to someone, a transaction is created. In this process, the new owner's public key (their digital identity) is attached to the Bitcoins sent, and confirmed by the signature of the sending party (using their private key) [14]. The complete history of transactions is accessible to everyone who has access to the Bitcoin network; therefore, any user can see the digitally encrypted identity of the owner of a given Bitcoin [1].

If, for example, one wish to make an online payment to a company using Bitcoin:

1- The company creates a new Bitcoin address, and directs the payer to send their payment to it.
2- The payer directs the payment to the company's new Bitcoin address by instructing their bitcoin client to transfer the requisite number of Bitcoins from their wallet to the company's new bitcoin address;
3- The payer's Bitcoin client electronically 'signs' the transaction request with the private key of the address from which they are transferring the Bitcoins;
4- The transaction is broadcast to the Bitcoin network and can take up to 10 minutes to be confirmed [7].

There are essentially tree ways to obtain Bitcoin:

1. By "mining" (mining new ones).
2. By buying them with conventional money on one of the exchange platforms.
3. For selling goods and services and accepting payment in Bitcoin.

"Mining" in fact is discovering new Bitcoin. New Bitcoin are only produced by the process known as mining [5]. In reality, it is simply the verification of Bitcoin transactions. Always a Bitcoin is transferred from one wallet to another, a complex computing process must be undertaken to verify that the transaction is legitimate (the sender is the legitimate owner of that Bitcoin and has not sent it

to multiple others) [16]. Because there is no central server to undertake this operation, it is carried out in the various nodes of the distributed network that makes up the Bitcoin system [1]. These are simply users, known as “miners,” who have chosen to run the relevant software that undertakes the necessary calculations to support the network [13]. As payment, every time an operation is successfully carried out, the system generates a set amount of Bitcoins and distributes them to the successful miner [16]. The difficulty of the operation and consequently the rate at which new Bitcoins are generated, is automatically adjusted to achieve a steady, predetermined rate [20].

However, the easiest way to obtain Bicoins is to purchase them by an exchange. Though there are many exchanges, the underlying concept is simple: users can trade traditional currency, for instance, dollars and Euros for Bitcoin at the current exchange rate. Exchange rates are determined by supply and demand [20].

**Regulation of Bitcoin in selected Jurisdiction.**

Below is a brief summary pronouncement of specific rules/regulations recently published by governments of various nations specifically addressing the issue of Bitcoin.

***Australia.***

In October 2017, the Australian Senate began debating a bill that would apply anti-money laundering statutes to the country's crypto-currency exchanges, as well as mandate criminal charges for exchanges that operate without a license.

That same month, the tax authorities removed the "double taxation" of Bitcoin, which was a result of a decision in 2014 to treat the crypto-currency as a "bartered good" rather than a currency or asset.

As of the end of 2017, crypto-currency exchanges have to register with the country's financial intelligence agency Austrac, and comply with customer verification and record preservation requirements.

Further moves are unlikely for now, however, as officials from the central bank recently said that regulation is not needed for the use of crypto-currencies as payment [4].

***India.***

The Indian central bank has issued a couple of official warnings on Bitcoin, and at the end of 2017 the country's finance minister clarified in an interview that Bitcoin is not legal tender. The government does not yet have any regulations that cover crypto-currencies, although it is looking at recommendations [4].

The central bank; however, has banned Indian financial institutions from working with crypto-currency exchanges and other related services.

***United States.***

The United States, at the time of this writing, has no coherent direction on its crypto-currency regulation other than that there will be some soon. The Securities and Exchange Commission (SEC) has warned investors of crypto-currency investing risks, halted several ICOs and hinted at the need for greater crypto-currency regulation.

The Commodity Futures Trading Commission (CFTC) became the first U.S. regulator to allow for crypto-currency derivatives to trade publicly, then organized meetings to talk about possibly changing the rules for crypto-currency derivatives clearing (one of the meetings was postponed due to the federal government shutdown) [15].

Secretary of the Treasury, Steve Mnuchin, has indicated a preference for minted fiat currency over crypto-currency. Speaking on January 12, 2018, at the Economic Club in Washington, D.C., Secretary Mnuchin warned those in attendance that he and other regulators were looking into the possibility that crypto-currency could be used in money-laundering activities. The secretary then announced to the group that the Financial Stability Oversight Council (FSOC) had formed a working group to

explore the crypto-currency marketplace and that he hoped to work with the G20 to prevent Bitcoin from becoming a digital equivalent of a "Swiss bank account" [15]. Defending his stance to World Economic Forum attendees on January 25, 2018, Mnuchin explained that his number one focus on crypto-currency was "to make sure that they're not used for illicit activities".

On January 26, 2018, U.S. Treasury Deputy Director Sigal Mandelker echoed the secretary's sentiments after a visit to China, South Korea and Japan. At a press conference in Tokyo, sheapplauded the three Asian countries for keeping tabs on crypto-currency trading, stating, "We feel very strongly that we need to have this kind of regulation all over the world" [15].

It should be noted that non-U.S. investors may have concerns over clearing licensing hurdles put up individually by the states. If the U.S. treats crypto-currencies as currency, it seems more likely that the actions by the federal government and federal regulatory agencies would preempt states' licensing. However, if treated as "securities" (the SEC has not completely cleared the issue up), crypto-currencies, especially ICOs, would have to "clear blue sky laws" on a state-by-state basis [15].

***China.***

On December 2013, People's bank of China (PBOC) made its first step in regulating Bitcoin by prohibiting financial institution from handling Bitcoin transactions and the Central bank of China notice that the nature of Bitcoin is that of a virtual commodity and not a currency [5].

While China has not banned Bitcoin and it has no plan to do so, it has cracked down on Bitcoin exchanges - all major Bitcoin exchanges in the country, including OKCoin, Huobi, Bitcoin China, and ViaBTC, suspended order book trading of digital assets against the Yuan in 2017 [4].

The People's Republic of China appears to be the most stringent crypto-currency regulator of the major economies regarding crypto-currencies. This is an odd about-face given that, in 2017, Chinese

Bitcoin miners made up over 50 percent of the worldwide mining population and that crypto-currency adoption in China increased at a rate higher than any other country [21].

***Saudi Arabia.***

Bitcoin is not banned by any governmental party in Saudi Arabia. Only Saudi Arabian Monetary Authority (SAMA) has warned from using it as it is high risk and recognised in Saudi Arabia and its dealers will not be guaranteed any protection or rights. There is a Bitcoin ATM in the city at Jubal [21].

***Canada.***

The Financial Consumer Agency in Canada does not consider crypto-currencies to be "legal tender," excluding all but Canadian bank notes and coins from that definition. The True North, however, is not all harsh on its crypto-currency regulatory stances. In fact, it appears to be the most transparent country in this list when it comes to understanding laws surrounding the digital currency industry [15].

After weeks of hearings, which included testimony from experts like Andreas Antonopoulos, the Canadian Parliament approved Bill C-31 on June 19, 2014, the world's first national law on digital currencies. The Canadian government has been communicative in its regulatory stances on crypto-currency ever since: the Canadian Securities Administrators (CSA) sent out a regulatory notice on August 24, 2017, confirming "the potential applicability of Canadian securities laws to crypto-currencies and related trading and marketplace operations and to provide market participants with guidance on analyzing these requirements". More recently, the head of the Central Bank of Canada, Stephen Poloz, was quoted as saying on January 25, 2018, that "I object to the term crypto-currencies because they are crypto but they aren't currencies … they aren't assets for the most part … I suppose they are securities technically … There is no intrinsic value for something like Bitcoin so it's not

really an asset one can analyze. It's just essentially speculative or gambling". It should be noted that as part of the North American Securities Administrators Association (NASAA), Canada joined an association-wide "cautionary directive" on the risks of crypto-currencies, with all representatives from every province in the country believing there is a "high risk of fraud" [15].

***Japan.***

Japan was the first country to expressly declare Bitcoin "legal tender," passing a law in early 2017 that also brought Bitcoin exchanges under anti-money laundering. It has also established a crypto-currency exchange industry study group which aims to examine institutional issues regarding Bitcoin and other assets [21].

***Iran.***

The Central Bank of Iran on 22nd April 2018 announced that use of Bitcoin and other virtual currencies in all monetary centres of Iran is prohibited and it has been emphasised in this directive that it will deal with the offenders against the relevant laws and regulations and express the reasons for the prohibition of the use of virtual currencies. These currencies have proven to be a substitute for money laundering and terrorist financing, which could be used as a tool for the relocation of criminal's money. [4]

***Germany.***

On 12th August 2013, the German Finance Ministry announced that Bitcoin is now essentially a "unit of account" and can be used for the purpose of tax and trading in the country, meaning that purchases made with it must pay VAT as with Euro transactions. It is not classified as a foreign currency or e-money but stand as "private money" which can be used in "multilateral clearing circles", according to the ministry [21].

***United Kingdom / European Union.***

While Brexit is scheduled to force the U.K. and the European Union to part ways in March 2019, the United Kingdom and the EU remain united in their plans to regulate crypto-currencies. On December 4, 2017, The Guardian and The Telegraph reported that the U.K. Treasury and the EU both had made plans aimed at ending anonymity for crypto-currency traders, citing anti-money laundering and tax evasion crackdowns [15].

The European Union plan would require crypto-currency platforms to conduct proper due diligence on customers and report any suspicious transactions. Likewise, the Treasury of the United Kingdom stated that they are "working to address concerns about the use of crypto- currencies by negotiating to bring virtual currency exchange platforms and some wallet providers within anti-money laundering and counter-terrorist financing regulation". The Treasury did, however, add that "there is little current evidence of [crypto-currencies] being used to launder money, though this risk is expected to grow" [15].

Calls for greater crypto-currency regulations echoed across Europe in January 2018. On January 15, 2018, French Minister of the Economy Bruno Le Maire announced the creation of a working group with the purpose of regulating crypto currencies. Similarly, Joachim Wuermeling, a board member of the German Bundesbank, called for effective regulation of virtual currencies on a global scale.On January 22, 2018, Dombrovskis furthered his regulatory agenda for crypto currencies by writing three of the EU's watch dogs warning them of a bubble in Bitcoin. On January 25, 2018, embattled U.K. Prime Minister Theresa May joined the fray, echoing the sentiments of International Monetary Fund head Christine Lagarde and U.S. President Donald Trump. When speaking to Bloomberg during the World Economic Forum at Davos, the prime minister stated, "We should be looking at these very seriously — precisely because of the way they can be used, particularly by criminals" [15].

In April 2018, the parliament's members voted by a large majority to support a December 2017 agreement with the European Council for measures aimed, in part, to prevent the use of crypto currencies in money laundering and terrorism financing [4].

***Russia.***

Draft crypto-currency legislation from the State Duma's financial regulator is expected in mid-2018. The focus appears to be on protecting citizens from scams, while allowing investors and businesses to work legally with crypto-currencies.

The efforts of the State Duma have been bolstered by a mandate from Putin himself, issued in October 2017, urging development of a "single payment space" within the Eurasian Economic Union, increased scrutiny of token sales, as well as licensing of Bitcoin mining operations [4].

***South Korea.***

In early 2018, South Korea banned anonymous virtual currency accounts. And in an effort to limit crypto-currency speculation, the authorities are working on increased supervision of exchanges (which could include a licensing scheme), although the governor of the Financial Supervisory Service has said the government will support "normal" crypto currency trading.

In an interesting shift in strategy, a recent report in the South Korean press indicated that the country's financial authorities are in talks with similar agencies in Japan and China over oversight of crypto currency investment. In April 2018, the Fair Trade Commission ordered 12 of the country's crypto currency exchanges to revise their user agreements [21].

**Advantages and disadvantages with the current implementation.**

While it is clear that Bitcoin has some advantages in compare to traditional currency, it also has some serious problems that have translated into it not being adopted in the mainstream. Some of the main advantages and disadvantages are listed below:

*Advantages of using Bitcoin.*

a. Anonymity.

In fact one of the biggest advantages of Bitcoin is that, it is theoretically anonymous. A person in possession of Bitcoin in an encrypted wallet can spend it in any service without identification and verification. You would receive or send bitcoins to addresses that are just the chains of thirty characters. With Bitcoin technology, you would be able to keep your identity hidden.

Their identity is encrypted but a full record of every users and every Bitcoin is preserved on the publicly available ledger. Therefore, some consider the Bitcoin system to be pseudonymous rather than fully anonymous, [9] and suggest that there are possibilities to trace user's real identities.

b. Non- inflationary.

Perhaps, this is the reason why Bitcoin is called the future of money. Generally, the central government can get fiat currencies printed as much as they want. When the economy is slowing down it is not able to pay off its national debt, the government orders to print more currency and inject it into the economy. This causes the value of currency to decrease as more people have more currency. Also printing more notes creates inflation and increases the prices of commodity and the seller has to increase the prices of commodity. It is because now more people are willing to pay for a particular commodity and the seller has to increase the price in order to make the sale. Therefore, the person who had gained when government injected more currency can now buy more but those people who were not benefited from have limited currency and now the price of commodity has also increased. On the other hand, this is not the case in Bitcoins. Only 21 milion Bitcoins will ever be created and this is known to everyone. This means that after all Bitcoins have matured, more number of Bitcoins grows and thus inflation won't be problem [2].

c. Resilience.

Crypto currencies or Bitcoins are decentralised, meaning that they are issued without a central administering authority, and it means that it is realised to attacks, and in theory it also means that it cannot be brought down [8].

d. Transparency.

Other benefit of Bitcoin is, all transactions are publicly available and verifiable in the electronic ledger called the 'black-chain'. This provides an un-precedential level of transparency and peer verification; it is one of features that transcend currency elements [8].

e. People can't steal your payment information from the merchants.

Most online purchases today are made via credit cards, requiring you to enter all your secret information (card number, expiry date, CSV number). Bitcoin transactions, however, don't require you to surrender any secret information.

f. Swift and Low/Minimal Transaction Costs.

Bitcoin is now an acceptable form of payment in exchange for goods and services. Paying through Bitcoin has very low and sometimes no transaction fees in some cases and it all depends on the priority of the person. If a person wishes that his/her transaction gets processed fast, he has to pay a transaction fees [2]. Reducing transaction costs is almost always a positive development. Between the many benefits of reduced transaction costs are "direct cost saving, indirect benefits through improvements in agency costs, monitoring or coordination within existing organisations and markets, and even the creation of new types of market structures that are more efficient". Lower transaction costs also may draw more people into the market, create growth for merchants, and allow for new innovation in online financial services [20].

One potential benefit of Bitcoin's low transaction cost is the enablement of micropayments. In the past, it has been impractical to transfer small (i.e., less than one dollar) amounts of money due to the costs of individual transactions. Bitcoin makes such micropayments much more practical and therefore makes possible many transactions in the electronic sphere that previously had not been possible. This is particularly useful in the developing world where banking infrastructure is underdeveloped, and many do not have access to traditional banking services [20]. In the other hand, Bitcoin transactions are very fast if compared to banking channels. A Bitcoin transaction is as fast an e-mail and can be processed within 10 minutes. It can be instantly processed if they are "zero-confirmation" transactions, meaning that the merchant takes on the risk of accepting a transaction that hasn't yet been confirmed by the Bitcoin blockchain. The confirmed transactions are those which take 10 minutes to process [2]. You can send Bitcoins to your relatives nearby or to a friend abroad using this technology. So, these are some of the main advantages of Bitcoin technology.

*Main Disadvantages of Bitcoin.*

A. Instability and Volatility.

One of the more important reasons why today many merchants avoid using Bitcoin and why it is very unlikely to be a viable currency is that Bitcoin prices are very volatile and increase/decreases at a very high pace. The currency has crashed several times and the price continues to swing up and down repeatedly. For example, during its peak in December 2013, the price reached US$ 1, 147 per, Bitcoin (Higher in some exchanges) only to crash spectacularly to US $ 522 in just a few days [8]. The volatility and instability of Bitcoin is likely to discourage many potential buyers and genuine investors think of it as too risky and do not invest in Bitcoins.

B. Trust and security.

Perhaps the most commonly identified obstacle for Bitcoin adoption is the problem of trust. An aspect of the trust in Bitcoin is its security. Possibility of losing your Bitcoin if they are not secured enough. Because the currency is not backed by any government or redeemable for any commodity, it may be difficult to convince individuals to trust a significant portion of their wealth to the virtual cryptocurrency [18]. Blockchains and Bitcoins main security focus in on preventing the same unit being spent twice whereas it cannot validate whether the true owner of a key signed the transaction. Empirical research on Bitcoin exchanges showed that the less popular ones are more likely to suffer a security branch and be closed due to theft of Bitcoins.

Fundamentally, since Bitcoin is outside the banking system and not back by any central body, in most cases users cannot recover any of their losses since they are not covered by deposit insurance [19]. Cyber security will be a constant concern, because the transactions are restricted only to the cyber environment and unfortunately Bitcoin users suffering of lack of security and trust.

C. Deflationary.

We converse about how Bitcoin being on-inflationary can be an advantage to the economy. But one possible negative factor attached to Bitcoin because of being deflationary is that if it gets in the hands of speculator a huge recession will come in Bitcoins.

Bitcoins are limited in number and if the major chunk is held by speculators and investors, they will hold it for a longer period of time and won't release it in the market. When the supply of Bitcoin will be short and demand continues to increase, it will increase the price of Bitcoins and then the investors can get benefit [2].

D. Cyber Attacks and Hacking.

Attacks by “cyber thieves” are becoming frequent with the passing of time. Especially the Bitcoin community has been hit by such thefts quite repeatedly. This not only creates panic in the Bitcoin community but also leads to a decline in the value of the currency [5].

One of the most discussed examples of such an attack was targeted at Mt.Gox, one of the largest Bitcoin-to-money exchanges system based in Shibuya, Tokya, Japan that Launched in July 2010. In 2011, Mt.Gox was hacked, and over 60000 usernames and passwords were stolen. In February 2014 Mt. Gox was hacked again, close its website and exchange service and filed for bankruptcy protection from creditors. Mt.Gox announced that approximately 850,000 Bitcoins belonging to customers and the company were missing and likely stolen on amount valued at more than $450 million of the time [19]. Attacks and hacking have majorly contributed in damaging in the reputation of Bitcoin by scaring merchants and investor who don’t want to take risk of suffering huge losses without any insurance to reduce the blow.

E. Lack of rules on consumer protection.

There is a need for protection of consumers in the Bitcoin industry. Among the reasons to have regulations, consumer protection is one of the most important and best. Consumers are usually the first victims because of their lack of sophistication and access to the information necessary to protect them. [14] In fact there are various consumer risks caused by Bitcoin and the most important are the possibility of losing your Bitcoin if they are not secured enough, lack of disclosures, lack of confidence in Bitcoin and lack of insurance, Bitcoin’s high volatility and some internal mining mechanisms.

In December 2013, the European Banking Authority warned consumers about the lack of regulatory protection when using crypto currencies and the risk of losing their money. Similar warning messages

have been voiced by number of other central banks (e.g. India, Germany, and France) [19]. Gavin Andresen, chief scientist at the Bitcoin foundation and one of the core developers behind the money said that consumer protection was one way that governments could perform useful oversight. According to him any new rules would not impede Bitcoin's innovation. "I think regulators tend to focus on costs and risks and not to focus so much on benefits", he said [9]. Indeed, consumers require the protection rules and information on the strengths and weaknesses that accompany Bitcoin, and warn them of the risks associated with it and, the state should have taken the lead in the regulatory area and has given consumers more confidence in Bitcoin by offering them protection.

F. Double spending.

Another risk of a digital currency is double spending, that it means spending the same money twice by its owner. While an owner of a digital currency file could easily make an exact copy of that file and send it to more than one person [13].

Double-spending is a problem unique to digital currency because digital information can be copied and rebroadcasted easily. Physical currencies do not have this issue because they cannot be easily replicated, and the parties involved in a transaction can immediately verify the bona fides of the physical currency. With digital money, there is a risk that the holder could make a copy of the digital token and send it to a merchant or another party while retaining the original. This was a concern initially with Bitcoin, the most popular digital currency or "cryptocurrency," since it is a decentralized currency with no central agency to verify that it is spent only once. However, Bitcoin has a mechanism based on transaction logs to verify the authenticity of each transaction and prevent double-counting [11].

Bitcoin manages the double spending problem. Bitcoin requires that all transactions, without exception, be included in a shared public transaction log known as a "blockchain". This mechanism

ensures that the party spending the bitcoins really owns them, and also prevents double-counting and other fraud. The block chain of verified transactions is built up over time as more and more transactions are added to it. Bitcoin transactions take some time to verify because the process involves intensive number-crunching and complex algorithms that take up a great deal of computing power. It is, therefore, exceedingly difficult to duplicate or falsify the blockchain because of the immense amount of computing power that would be required to do so [11]. Thus, according to Nakamoto if someone tries to spend a Bitcoin twice, the one that occurred first in time is valid, and the second is not.

**Illegal activities conducted in Bitcoin.**

This arena of virtual currency is relatively novel and largely untested and there are many reasons why governments might want to take notice of an unregulated, virtual, and anonymous currency. Beyond the risk that one's citizens may fall victim to scammers and Ponzi schemers, Bitcoin offers significant opportunities for those who would launder money, hide income from tax authorities, or transact in illicit goods [20].

The most prominent of the offense beyond the use of Bitcoin in the world are:

*Tax avoidance and evasion.*

The relative anonymity of Bitcoin transactions, no bank account is needed and ease with which they can be carried out; [20] these are features of Bitcoin that make it attractive for those who would prefer not to pay taxes and are willing to break the law to avoid doing so.

There are only few nations in the world who have released rules or guidelines regarding the treatment of Bitcoin for the purpose of taxation while most countries have not resolved the issue of taxation of Bitcoin and transaction in relation to it, because it is unclear how Bitcoin will be taxed, [10] and various jurisdictations around the world agree that Bitcoin fall under the definition of commodity, in

the other hand other nations accepted Bitcoin as currency or payment system, of course it is clear that Bitcoin can be used as much as a method of payment than as investment or a commodity [14]. This however, creates various regulatory frameworks about Bitcoin taxation. As a result, we need same guideline on exactly how each regulatory framework will apply and coexist without hindering the promising growth potential of this innovative financial platform in the world.

*Money laundering.*

One of the major enabling factors for money laundering is lack of uniform financial jurisdiction across the globe. In most matters the funds that are being laundered are earnings through corruption and bribery [5]. The European Banking Authority, European Central Bank and the FBI have all recognised that Bitcoin may be used for money laundering purposes. Money laundering also may for instance takes place by converting illegal gains to Bitcoin, spreading them through several wallets and then using several services to receive other legitimate Bitcoin for a commission [5].

In the US, on March 18, 2013, FinCEN introduced guidelines on anti-money-laundering and "virtual currencies," subjecting them to the regulations applicable to money transmitters and Bitcoin [17]. The first arrest of a prominent Bitcoin figure on money laundering charges occurred there on January 2014 [19]. Hence the potential comes mainly from the anonymity of Bitcoin and the lack of international regulation on Bitcoin on the other hand, some analysts state that laundering money through Bitcoin is more of a theoretical possibility than an actual one. They argue that the small number of Bitcoin exchanges and the public nature of the Bitcoin ledger make the currency currently unattractive for high volume money laundering activities [19]. Now for that reason mentioned above and lack of uniform regulation in the universe, there is significant concern on Bitcoin that it could use for money laundering.

*Drug trafficking.*

The purchasing of drugs via internet, particularly the dark net and through crypto currencies like Bitcoin have increase among kids and young students in recent years and has become a new challenge in nations. As example, Silk Road was an online marketplace started operating in January 2011 and it was a website through which people could purchase weapons and drugs such as cocaine and heroin using Bitcoin for payment [19]. In Silk Road website both seller and buyer were unidentifiable, and payments were only accepted in anonymous Bitcoin. In October 2013, the FBI announced that it has successful shutdown Silk Road [22].

There is a need to have supervisory and effective regulations regarding use of Bitcoin in financial transactions because Bitcoin as the currency of the underground internet is also being used in drug trafficking and illegal arms trade.

*Terrorist financing.*

Virtual currencies are appealing to terrorist financiers who could swiftly transfer money across borders in a safe, cheap, and secretive manner and the anonymity would also allow them to better their tracks. In fact, terrorist financing is concealment of future application of financial resources that may be illegal wherein such resources are obtained from a legitimate source [5]. If nations legislation on counter terrorism is not amend to covers digital currencies as Bitcoin, the problem could very much worsen.

*Theft and fraud.*

Users' digital wallets are not immune from risks. These risks are most easily grouped into two distinct categories: theft and fraud [20]. Users who store their wallets on their personal computers risk theft if they do not adequately protect themselves with anti-virus measures and backup their computers or at list their wallets files regularly [6]. Various journalists, economists, have voiced concerns that

Bitcoin is a ponzi scheme. In 2013, Eric Posner, a law professor at the university of Chicago stated that a real Ponzi scheme: takes fraud Bitcoin, by contrast, seems more like a collective delusion. A 2014 report by the World Bank concluded that Bitcoin was not a deliberate Ponzi scheme [21].

In perhaps the most visible example of alleged theft, a service provider has been accused of stealing the funds of its depositors. Bitconica was one of the larger Bitcoin currency exchanges that was launched by Zhou Tong, who claimed to be seventeen years old from Singapore. Bitcoinica was hacked for two times and hackers had stolen more than sixty thousand Bitcoin from the exchange. Tong promised that users would be repaid fifty percent of their lost deposits. After that Bitconica announced the site would be taken offline "until such time as a new platform can be built and tested with security best- practices built-in from scratch". Tong has been accused of hacking Bitconica himself. Bitconica's users were even suspected foul play, alleging that Tong stole the funds, and a lawsuit, now filed in San Francisco, accuses Bitconica of breach of contract and negligence [12].

The security is one of the serious and challenges facing the young currency. Some researcher claims that the security issues with Bitcoin are hard to assess but there are various security issues with very high risk, such as general security, subversive miner strategies, loss of keys and man in the middle attacks [8]. Law enforcement and security of Bitcoin is difficult and it is not possible to build a sustainable economy around Bitcoin without regulation and some kind of government involvement.

**CONCLUSIONS.**

Now, the situation has changed dramatically. The evidence showed that crypto-currency Bitcoin and others digital currency has become much more popular might play an increasing role in transactions, worldwide. In the light of the preceding analysis, Bitcoin is facing with various challenges such as security, consumer protection, tax avoidance and illegal activities...etc, that I mentioned in this paper.

For elimination current obstacles and use of this innovation in transactions, firstly the government should not attempt to outlaw or stop Bitcoin because Bitcoin have significant economic advantages compare to traditional currencies and payment methods. The governments should create a legal status for digital currencies; promote competition and the growth of the digital currency industry, ensure the financial stability of the digital currency industry and secure the protection of consumers and merchants against illegal activities. For instance, the countries like Iran, North Korea and Russia that suffering of US sanctions on their economic they ought to recognize Bitcoin as an opportunity and using of Bitcoin to break down that sanctions and using of Bitcoin in oil and Gas transactions and economic betterment. Secondly the countries across the world should cooperate to regulate the uniform regulation on Bitcoin that can help in decentralisation of economic power and greater financial access.

However, one thing is undeniable: the world and technology are changing and governments and businesses must prepare for acceptance of these changes if they are to maintain their position of power in the future.

**BIBLIOGRAPHIC REFERENCES.**

1- Andresen, G. (2011). Bitcoin: The World's First Person-to-Person Digital Currency, BITCOIN trading. Available at: http://www.bitcointrading.com/pdf/GavinAndresenCIATalk.pdf

2- Advantages and disadvantages of Bitcoin by kryptomoney (2017). Available at: http://www.kryptoMoney.com

3- Clinch, M. (2015). Bitcoin now tax-free in Europe after court ruling. Available at: https://www.cnbc.com/2015/10/22/bitcoin-now-tax-free-in-europe-after-court-ruling-htm|

4- Coindesk, (2018). Is Bitcoin Legal? Available at: https://www.coindesk.com/information/is-bitcoin-legal/

5- Desai, Nishith (2015). Bitcoins- A Global Perspective, Nishith Desai Associates. Available at: http://www.nishithdesai.com/fileadmin/user_upload/pdfs/Research%20Papers/Bitcoins_A_Global_Perspective.PDF

6- EUROPEAN CENT BANK, Virtual Currency Schemes (2012). Available at: http://www.ecb.int/pub/pdf/other/virtualcurrencyschemes201210en.pdf

7- Goldberg, D. Jamie,N. Comeron, E. (2014). Bitcoin Regulation in Australia: A bit of a Task to coin. Available at: http://www.addisonslawyers.com.au/knowledge/Bitcoin_Regulation_in_Australia__A_Bit_of_a_Task_to_Coin716.aspx

8- Guadamuz, A. Marsden, C. (2015). Blockchains and Bitcoin: Regulatory responses to cryptocurrencies. Peer-Reviewed Journal on the Internet, vol 20. Available at: http://firstmonday.org/article/view/6198/5163

9- Hattem, J. (2014) Bitcoin Leader: Regulation should protect consumers, available at: http://thehill.com/policy/technology/197624-bitcoin-leader-regulation-should-protect-consumers

10- Hollander, C. (2014) How is Bitcoin Taxed? The IRS Doesn't Know, National journal. Available at: http://www.nationaljournal.com/economy/how-is-bitcoin-taxed-the-irs-doesn-t-know-20140126

11- INVESTOPEDIA (2018). Double–Spending Definition. Available at: https://www.investopedia.com/terms/d/doublespending.asp#ixzz5I5rzmrpR

12- Jeffries, A. (2012) Bitcoin woes: Users File Lawsuit Over $460 in Missing Funds. Available at: http://www.theverge.com/2012/8/10/3233711/second-bitcoin-lawsuit-is-filed-in-california

13- Khatwani, S. (2018). What is Double Spending & How Does Bitcoin Handel It? Available at: www.coinsutra.com/bitcoin-double-spending/

14- Mandjee,T. (2015) Bitcoin, its Legal Classification and its Regulatory Framework, Journal of Business & Security Law. Vol 15, Iss 2, P,1-62. Available at: https://digitalcommons.law.msu.edu/cgi/viewcontent.cgi?referer=https://www.searchencrypt.com/&httpsredir=1&article=1003&context=jbsl

15- Nelson, A. (2018) Cryptocurrency Regulation in 2018: Where the World Stands Right Now, BITCOINMAGAZINE. Available at: https://bitcoinmagazine.com/articles/cryptocurrency-regulation-2018-where-world-stans-right-now

16- Nakamoto, Satoshi (2009) Bitcoin: A Peer- to- Peer Electronic Cash System, Bitcoin, Available at: http://www.bitcoin.org/bitcoin.pdf

17- Release, P. (2013) Financial Crimes Enforcement Network, FinCen issues Guidance on Virtual Currencies and Regulatory Responsibilities.

18- Sanati, C. (2012) Bitcoin looks primed for money laundering. Available at: http://fortune.com/2012/12/18/bitcoin-looks-primed-for-money-laundering/

19- Szczepanski, M. (2014). Bitcoin Market, economics and regulation, European Parliamentary Research Service. Available at: http://www.eprs.ep.parl.union.eu

20- Turpin, j, B. (2014) Bitcoin The Economic Case for a Global, Virtual Currency Operating in an Unexplored Legal Framework, Indiana Journal Of Global Legal Studies, Vol 21: Iss.1. Available at: http://www.repository.lawindiana.edu/ijgls/vol21/iss1/13

21-WIKIPEDYA. Available at:

http://en.wikipedia.org/wiki/legality_of_bitcoin_by_country_or_territory

22- ZETTER, K. (2013) How the feds took down the silk road drug wonder land, Available at: http://www.wired.com/threatlevel/2013/11/silk_road/

**DATA OF THE AUTHOR.**

1. Solmaz Besharat. MA (International Law) University of Mysore, India. E-mail:

solmazbesharat001@gmail.com

**RECIBIDO:** 21 de septiembre del 2018. **APROBADO:** 11 de octubre del 2018.