The Bitcoin and the future of Cryptocurrencies

-**Benaichouche Mohamed**[1]: *M C A, University of Medea, Algeria*

Received:01/03/2022 ***Accepted :21/04/2022*** ***Published :10/06/2022***

Abstract

The main aim of the study is to provide a literature review of the concepts hovering around cryptocurrencies and blockchain technology and addresses the question of whether bitcoin currency can enjoy the same characteristics of money or current payment instruments, As well as providing a summary of its financial and legal performance while exploring the most important potential threats to international security and difficulties. The increasing popularity of cryptocurrencies is linked to their importance in settling international financial transactions as well as their role as a tool for non-cash payments on a global scale. Consequently, it may obtain greater public acceptance based on its performance in the near future in facing legislative, economic, and security obstacles.

Key words: Cryptocurrencies, Bitcoin, Blockchain technology, Legal status of cryptocurrencies, Bitcoin prices.)

Jel Codes Classification : E400, G290, G280, K340.

1 - ***Benaichouche Mohamed****, Macroeconomics and International Finance Laboratory, benaichouche1@yahoo.com.*

البيتكوين ومستقبل العملات المشفرة

– **بن عيشوش محمد**[1]:أستاذ محاضر أ، جامعة المدية، الجزائر.

تاريخ الإرسال: 2202/03/10 **تاريخ القبول: 2022/05/04** **تاريخ النشر: 2022/06/10**

ملخص

تهدف هذه الورقة البحثية لتقديم مراجعة أدبية لمفاهيم العملات المشفرة وكذا تكنولوجيا البلوكتشين المسؤولة عنها، كونها محاولة للإجابة على السؤال إذا كان يمكن لعملة البيتكوين التمتع بخصائص النقود أو وسائل الدفع الحالية، مع عرض تاريخ وطريقة عمل العملات الإفتراضية، وكذا تقديم تلخيص حول الأداء المالي والقانوني لها مع إعطاء أهم التهديدات المحتملة للأمن الدولي، والصعوبات في انتشارها. يرتبط التزايد في شعبية العملات المشفرة مع أهميتها في تسوية التعاملات المالية الدولية وكذا دورها كأداة للمدفوعات غير النقدية على نطاق عالمي. وبالتالي قد تحضى بقبول عام أكبر بناءا على أداها في المستقبل القريب في مواجهة العقبات التشريعية، الاقتصادية والأمنية.

الكلمات المفاتيح: العملات المشفرة ، البيتكوين، تكنولوجيا البلوكتشين ، الوضع القانوني للعملات المشفرة ، أسعار البيتكوين.

التصنيفJEL: *E400, G290, G280, K340*.

[1]-**بن عيشوش محمد**، مخبر الاقتصاد الكلي والمالية الدولية، *benaichouche1@yahoo.com*

Introduction:

Bitcoin is a digital cryptocurrency that has attracted substantial interest in recent years from the general public, profit-seekers, risk-takers, academic practitioners, and last but not least, economists. Although it is referred to as a new currency, Bitcoin has existed since 2009 and is rooted in technology that goes back even further. It was the first established cryptocurrency, with the first trade in 2010. Since 2015, Bitcoin has attracted even more attention because of its increase in value and volume of exchange. The Bitcoin system maintains a global, distributed cryptographic ledger of transactions, or blockchain, through a consensus algorithm running on hardware scattered around the world. This paper discusses the nature of cryptocurrency and blockchain, how it works, and the present status of Bitcoin blockchain in different countries around the world.

After the development in Bitcoin prices from 2013 to these days in 2022, more businesses started to accept Bitcoin payments, and people became more eager to pay with this currency.

One of the reasons for identifying cryptocurrencies is the limited number of Literature and sources available on the international market. It appears that researchers are treating cryptocurrencies as a passing method or experiment, rather than an effective payment method that could revolutionize our view of money. It should be noted that Bitcoin is gaining larger markets and audiences day after day as the investment of the richest man in the world Elon Musk.

This research paper aims to analyze how the Bitcoin function in the modern world, to this end address the following questions:

Can bitcoin overcome all legislative, economic, and security obstacles to reach the level of current payment instruments or money?

In order to answer the current problem, it must be divided into sub-questions and hypotheses.

1- Can bitcoin and virtual money have the same characteristics as money or payment instruments?

H1: Yes, Bitcoin can have the same characteristics as money or payment instruments and help in money and values transfer.

2- Can bitcoin be considered an instrument of payment and gain international public acceptance?

H2: Bitcoin is not universally accepted, but rather a relative acceptance.

3- Can bitcoin overcome all legislative, economic, and even security obstacles?

H3: Yes, with some improvement, modification, and framing, Bitcoin can overcome the aforementioned obstacles.

After the introduction the research paper begins with the theoretical part, concerning the blockchain and its functions, In order to achieve the research purpose, it is also essential to learn about the typology of Cryptocurrencies and how Bitcoin works, including its acceptability as an instrument of payment.

Then in the next section, we will explore both the legal situation of cryptocurrencies especially Bitcoin, and the evaluation of BTC prices.

At the end of this research paper, we will answer the questions in the introduction and discuss some of the findings.

I-Literature Review: Cryptocurrencies and Blockchain

In the section, we attempt to present and cover the most important definitions and concepts related to both the blockchain and the cryptocurrencies and the most important characteristics related to them from a point of view the policymakers like ECB, IMF, BIS, EBA, ESMA, World Bank and FATF.

I-1- What is blockchain?

Blockchain is a particular type or subset of so-called distributed ledger technology ("DLT").

I-1-1- Defining blockchain: blockchain technology with many faces.

DLT is a way of recording and sharing data across multiple data stores (also known as ledgers), which each have the exact same data records and are collectively maintained and controlled by a distributed network of computer servers, which are called nodes (Van de Looverbosch, 2018, p. 193).

Blockchain is a mechanism that employs an encryption method known as cryptography and uses (a set of) specific mathematical algorithms to create and verify a continuously growing data structure (to which data can only be added and from which existing data cannot be removed) that takes the form of a chain of "transaction blocks", which functions as a distributed ledger (Natarajan, Krause, & Gradstein, 2017, p. 1).

In practice, blockchain is a technology with many "faces". It can exhibit different features and covers a wide array of systems that range from being fully open and permissionless to permission (Witzig & Salomon, 2018, p. 7).

I-1-2- How a blockchain works: the basics.

a. The blockchain is a distributed database: In simple terms, the blockchain can be thought of as a distributed database. Additions to this database are initiated by one of the members (i.e. the network nodes), who creates a new "block" of data, which can contain all sorts of information. This new block is then broadcasted to every party in the network in an encrypted form (utilizing cryptography) so that the transaction details are not made public.

Those in the network (i.e. the other network nodes) collectively determine the block's validity under a pre-defined algorithmic validation method, commonly referred to as a "consensus mechanism", Once validated, the new "block" is added to the blockchain, which essentially results in an update of the transaction ledger that is distributed across the network.

In principle, this mechanism can be used for any kind of value transaction and can be applied to any asset that can be represented in a digital form (CPMI, 2015, pp. 8-9).

b. Transaction "blocks" are signed with a digital signature using a private key: Every user on a blockchain network has a set of two keys. A private key, which is used to create a digital signature for a transaction, and a public key, which is known to everyone on the network. A public key has two uses :

- it serves as an address on the blockchain network;
- it is used to verify a digital signature / validate the identity of the sender.

c. Bye-bye middleman: One of the key advantages of blockchain technology is that it allows simplifying the execution of a wide array of transactions that would normally require the intermediation of a third party (e.g. a custodian, a bank, a securities settlement system, broker-dealers, a trade repository, …).

In essence, blockchain is all about decentralizing trust and enabling decentralized authentication of transactions.

Simply put, it allows to cut out the "middleman". In many cases, this will likely lead to efficiency gains. However, it is important to underscore that it may also expose interacting parties to certain risks that were previously managed by these intermediaries. For instance, the Bank for International Settlements ("BIS") recently warned in a report of 2017 titled Distributed ledger technology in payment, clearing, and settlement, that the adoption of blockchain technology could introduce new liquidity risks. More, in general, it seems that when an intermediary functions as a buffer against important risks, such as systemic risk, he cannot simply be replaced by blockchain technology (CPMI, 2015, p. 19)

I-1-3- The blockchain consensus mechanisms

In principle, any node within a blockchain network can propose the addition of new information to the blockchain. To validate whether this addition of information (for example a transaction record) is legitimate, the nodes have to reach some form of agreement. Here a "consensus mechanism" comes into play. In short, a consensus mechanism is a predefined specific (cryptographic) validation method that ensures a correct sequencing of transactions on the blockchain. In the case of cryptocurrencies, such sequencing is required to address the issue of "double-spending" (i.e. the issue that the same payment instrument or asset can be transferred more than once if transfers are not registered and controlled centrally).

A consensus mechanism can be structured in several ways. Hereinafter, the two best-known – and in the context of cryptocurrencies also most commonly used – examples of consensus mechanisms will be briefly discussed: the Proof of Work ("PoW") mechanism and the Proof of Stake ("PoS") mechanism (Houben, 2015, p. 195).

a. Proof of Work (PoW): In a PoW system, network participants have to solve so-called "cryptographic puzzles" to be allowed to add new "blocks" to the blockchain. This puzzle-solving process is commonly referred to as "mining**"**, In simple terms, these cryptographic puzzles are made up of all information previously recorded on the blockchain and a new set of transactions to be added to the next "block".Because the input of each puzzle becomes larger over time (resulting in a more complex calculation), the PoW mechanism requires a vast amount of computing resources, which consume a significant amount of electricity.

If a network participant (i.e. a node) solves a cryptographic puzzle, it proves that he has completed the work, and is rewarded with the digital form of value (or in the case of a cryptocurrency, with a newly minted coin). This reward serves as an incentive to uphold the network.

The cryptocurrency Bitcoin is based on a PoW consensus mechanism. Other examples Include Litecoin, Bitcoin Cash, Monero, etc (Natarajan, Krause, & Gradstein, 2017, p. 6).

b. Proof of Stake (PoS): In a PoS system, a transaction validator (i.e. a network node) must prove ownership of a certain asset (or in the case of cryptocurrencies, a certain amount of coins) to participate in the validation of transactions. This act of validating transactions is called "forging" instead of "mining". For example, in the case of cryptocurrencies, a transaction validator will have to prove his "stake" (i.e. his share) of all coins in existence to be allowed to validate a transaction. Depending on how many coins he holds, he will have a higher chance of being the one to validate the next block (i.e. this all has to do with the fact that he has greater seniority within the network earning him a more trusted position).

The transaction validator is paid a transaction fee for his validation services by the Transacting parties. Cryptocurrencies such as Neo and Ada (Cardano) utilize a PoS consensus mechanism (Young, 2018, p. 17).

c. Other mechanisms: The PoW and PoS mechanisms are far from the only consensus mechanisms currently in existence. Other examples include proof of service, proof of elapsed time, and proof of capacity.

I-1-4- Blockchain technology can have many applications

While blockchain technology is often associated with digital or virtual currency schemes, payments, and financial services, its scope is much wider. Blockchain can theoretically be applied in a large variety of sectors (e.g. trade and commerce, healthcare, governance, …). In addition, it has numerous potential applications. It could have an impact on the pledging of collateral, on the registration of shares, bonds, and other assets, on the transfer of property tiles, on the operation of land registers, etc, As pointed out above, this study will only touch upon the subject of blockchain technology where this is meaningful for

the research on cryptocurrencies and can be deemed relevant from the perspective of combating money laundering, terrorist financing and/or tax evasion.

I-2- What are cryptocurrencies?

I-2-1- Introduction.

Establishing a definition of cryptocurrencies is no easy task. Much like blockchain, cryptocurrencies have become a "buzzword" to refer to a wide array of technological developments that utilize a technique better known as cryptography. In simple terms, cryptography is the technique of protecting information by transforming it (i.e. encrypting it) into an unreadable format that can only be deciphered (or decrypted) by someone who possesses a secret key (Faulkner, 2016, p. 6).

Cryptocurrencies such as Bitcoin, are secured via this technique using an ingenious system of public and private digital keys. Hereinafter we try to give a suitable definition of cryptocurrencies based on a critical analysis of the definitions already developed by various concerned policymakers at the European and international level (Houben, 2015, p. 195).

I-2-2- The policymakers: ECB, IMF, BIS, EBA, ESMA, World Bank, and FATF

Since the emergence of Bitcoin in 2009, the subject of cryptocurrencies has been scrutinized by various policymakers, who have each touched upon the subject in a different way (Hileman & Rauchs, 2017, p. 15):

a. ECB: The European Central Bank ("**ECB**") has classified cryptocurrencies as a subset of virtual currencies. A report on Virtual Currency Schemes of 2012, defined such currencies as a form of unregulated digital money, usually issued and controlled by its developers, and used and accepted among the members of a specific virtual community (ECB, 2015, pp. 13-19)**.**

It further clarified that three types of virtual currencies can be distinguished depending on the interaction with traditional currencies and the real economy:

- virtual currencies that can only be used in a closed virtual system, usually in online games (e.g. World of Warcraft Gold);

- virtual currencies that are unilaterally linked to the real economy: a conversion rate exists to purchase the currency (with traditional money) and the purchased currency can subsequently be used to buy virtual goods and services (and exceptionally also to buy real goods and services) (e.g. Facebook Credits);

- virtual currencies that are bilaterally linked to the real economy: there are conversion rates both for purchasing virtual currency and for selling such currency; the purchased currency can be used to buy both virtual as real goods and services.

Cryptocurrencies, such as Bitcoin, are virtual currencies of the latter type: they can both be bought with traditional money as sold against traditional money, and they can be used to buy both digital and real goods and services (BANQUE DE FRANCE, 2013, p. 2).

In a more recent report of 2015 titled Virtual Currency Schemes – a further analysis, the ECB put forward a "second", and largely updated, definition of virtual currencies. It defined virtual currencies as digital representations of value, not issued by a central bank, credit institution, or e-money institution, which in some circumstances can be used as an alternative to money. It also clarified that cryptocurrencies, such as Bitcoin, constitute a decentralized bi-directional (i.e. bilateral) virtual currency (Houben, 2015, p. 194)**.**

b. IMF: Like the ECB, the International Monetary Fund ("**IMF**") has categorized cryptocurrencies as a subset of virtual currencies, which it defines as digital representations of value, issued by private developers and denominated in their unit of account. According to the IMF, the concept of virtual currencies covers a wider array of 'currencies', ranging from simple IOUs ("Informal certificates of debt" or "I owe you's") by issuers (such as the Internet or mobile coupons and airline miles), virtual currencies backed by assets such as gold, and cryptocurrencies such as Bitcoin (Vandezande, 2018, pp. 75-76).

c. BIS: The Committee on Payments and Market Infrastructures (**"CPMI**"), a body of the Bank for International Settlements (**"BIS**"), has qualified cryptocurrencies as digital currencies or digital currency schemes.

These schemes are said to exhibit the following key features:

- they are assets, the value of which is determined by supply and demand, similar in concept to commodities such as gold, yet with zero intrinsic value;
- they make use of distributed ledgers to allow remote peer-to-peer exchanges of electronic value in the absence of trust between parties and without the need for intermediaries;
- they are not operated by any specific individual or institution.

d. EBA: The European Banking Authority ("EBA") has suggested referring to cryptocurrencies as virtual currencies, which it defines as digital representations of value that are neither issued by a central bank or public authority nor necessarily attached to a fiat currency but are used by natural or legal persons as a means of exchange and can be transferred, stored or traded electronically (ECB, 2015, p. 4).

e. ESMA: The European Securities and Markets Authority ("**ESMA**") has recently also referred to cryptocurrencies as virtual currencies, in a pan-European warning issued in cooperation with the European Insurance and Occupational Pensions Authority ("**EIOPA**") and the EBA. Fully in line with the EBA's definition, virtual currencies are defined as digital representations of value that are neither issued nor guaranteed by a central bank or public authority and do not have the legal status of currency or money (IMF, 2016, p. 7).

f. World Bank: The World Bank has classified cryptocurrencies as a subset of *digital currencies*, which it defines as digital representations of value that are denominated in their unit of account, distinct from money, which is simply a digital payment mechanism, representing and denominated in fiat money.

Contrary to most other policymakers, the World Bank has also defined cryptocurrencies itself as digital currencies that rely on cryptographic techniques to achieve consensus (CPMI, 2015, pp. 4-7).

g. FATF: Like many other policymakers, the Financial Action Task Force ("FATF") has approached cryptocurrencies as a subset of virtual currencies, which it defines as digital representations of value that can be digitally traded and function as :

- a medium of exchange;
- a unit of account;
- a store of value, but do not have legal tender status (i.e., when tendered to a creditor, are a valid and legal offer of payment) in any jurisdiction.

It further suggests that virtual currencies can be divided into two basic types:

- convertible virtual currencies that have an equivalent value in real currency and can be exchanged back-and-forth for real currency; these virtual currencies can be of a centralized or a decentralized nature (i.e. they can either have a central administrating authority that controls the system or no central oversight at all);
- Non-convertible virtual currencies that are specific to a particular virtual domain or world (e.g. a Massively Multiplayer Online Role-Playing Game like World of Warcraft), and under the rules governing its use, cannot be exchanged for fiat currency.

Cryptocurrencies like Bitcoin are virtual currencies of the first type, that can, according to the FATF, be defined as math-based, decentralized convertible virtual currencies that are protected by cryptography (EBA, 2014, p. 11).

I-2-3- Summary.

The main conclusion that can be drawn from the different perspectives set out above, is that there is no generally accepted definition of the term cryptocurrencies available in the regulatory space. Even more, most policymakers have refrained from defining the term

altogether. Amongst those cited above, only the World Bank and the FATF have put forward a clear-cut definition. It is clear, however, that most policymakers approach cryptocurrencies as a subset or a form of virtual or digital currencies.

If we try to summarize all the above definitions, a good summary could be that a cryptocurrency is "a digital representation of value that :

- is intended to constitute a peer-to-peer ("P2P") alternative to government-issued legal tender,
- is used as a general-purpose medium of exchange (independent of any central bank),
- is secured by a mechanism known as cryptography and
- can be converted into legal tender and vice versa".

Hereinafter we will shed some light on the concept of cryptocurrencies (or coins; we will use both terms interchangeably hereinafter), more, in particular, the dividing line with other, neighboring concepts, which should nevertheless be distinguished from cryptocurrencies.

I-2-4- Whom are the players involved?

The cryptocurrency market is a new playing field where different actors each play a particular role. To shed some more light on how the market works, and without attempting to be exhaustive, we will hereinafter further identify the key players.

a. Cryptocurrency users: The first, and very important, player is the "cryptocurrency user". A cryptocurrency user is a natural person or legal entity who obtains coins to use them:

- to purchase real or virtual goods or services (from a set of specific merchants),
- to make P2P payments,
- to hold them for investment purposes (i.e. in a speculative manner).

Without trying to be exhaustive, a cryptocurrency user can obtain his coins in several ways:

- Firstly, he can simply buy his coins on a cryptocurrency exchange using fiat money or another cryptocurrency;
- Secondly, he can buy his coins directly from another cryptocurrency user (i.e. through a trading platform – this form of exchange is often referred to as a "P2P Exchange");
- Thirdly, if a cryptocurrency is based on a PoW consensus mechanism, he can mine a new coin (i.e. participate in the validation of transactions by solving a "cryptographic puzzle" and be rewarded a new coin);
- Fourthly, in some cases he can obtain his coins directly from the coin offeror, either as part of a free initial offering of coins (e.g. on the Stellar network Lumens (XLM) are being given away for free) or in the framework of a crowd sale set-up by the coin offeror (e.g. a large bulk of ether (cf. Ethereum) was sold in a crowd sale to cover certain development costs);
- Fifthly, if he sells goods or services in exchange for cryptocurrency, he can also receive coins as payment for those goods or services;
- Sixthly, in case of a "hard fork"84 of a coin's blockchain, he will automatically obtain an amount of the newly created coin; and
- Finally, he can receive coins as a gift or donation from another cryptocurrency user (Natarajan, Krause, & Gradstein, 2017, p. 4).

b. Miners: A second player is the "miner" who participates in invalidating transactions on the blockchain by solving a "cryptographic puzzle". As explained above, the process of mining relates to cryptocurrencies that are based on a PoW consensus mechanism. A miner supports the network by harnessing computing power to validate transactions and is rewarded with newly minted coins (i.e. through an automatic decentralized new issuance). Miners can be cryptocurrency users, or, more commonly, parties who have made a new business out of mining coins to sell them for fiat currency (such as US dollar or Euro) or other

cryptocurrencies. Some miners group in so-called pools of miners to bundle computing power (ECB, 2015, p. 7).

At present, the risks associated with so-called "mining businesses" appear to be underestimated. We will further elaborate on this below.

c. Cryptocurrency exchanges: The third group of key players in the so-called "cryptocurrency exchanges". Cryptocurrency exchanges are persons or entities who offer exchange services to cryptocurrency users, usually against payment of a certain fee (i.e. a commission). They allow cryptocurrency users to sell their coins for fiat currency or buy new coins with fiat currency. They usually function both as a course and as a form of the exchange office**.** Examples of well-known cryptocurrency exchanges are Bitfinex, HitBTC, Kraken, and Coinbase GDAX.

It is important to note that some exchanges are pure cryptocurrency exchanges, which means that they only accept payments in other cryptocurrencies, usually Bitcoin (for example Finance), whilst others also accept payments in fiat currencies such as US dollar or Euro (for example Coinbase). Furthermore, many cryptocurrency exchanges only allow their users to buy a particular selection of coins.

It should also be noted that many cryptocurrency exchanges (i.e. both regular and pure cryptocurrency exchanges) operate as custodian wallet providers (for example Bitfinex).

In general cryptocurrency exchanges offer their users a wide array of payment options, such as wire transfers, PayPal transfers, credit cards, and other coins. Some cryptocurrency exchanges also provide statistics on the cryptocurrency market (like trading volumes and volatility of the coins traded) and offer conversion services to merchants who accept payments in cryptocurrencies (European Commission, 2017, p. 85).

d. Trading platforms: In addition to cryptocurrency exchanges, so-called "trading platforms" also play an important role in the exchange of cryptocurrencies (and, most notably, allow cryptocurrency users to buy coins with cash). Trading platforms are marketplaces that bring together different cryptocurrency users that are either looking to buy or sell coins, providing them with a platform on which they can directly trade with each other (i.e. an "eBay" for cryptocurrencies).

Trading platforms are sometimes referred to as "P2P exchanges" or "decentralized exchanges".They differ from cryptocurrency exchanges in many ways. First and foremost, they do not buy or sell coins themselves. Secondly, they are not run by an entity or company that oversees and processes all trades, but they are operated exclusively by software (i.e. there is no central point of authority). Trading platforms simply connect a buyer with a seller, allowing them to conduct a deal, online, or even locally in-person (i.e. a face-to-face trade, often executed in cash). A well-known example of a trading platform for Bitcoins is LocalBitcoins.

e. Wallet providers: Another group of key players is the so-called "wallet providers". Wallet providers are those entities that provide cryptocurrency users with digital wallets or e-wallets that are used for holding, storing, and transferring coins. Simply put, a wallet holds a cryptocurrency user's cryptographic keys (see above). A wallet provider typically translates a cryptocurrency user's transaction history into an easily readable format, which looks much like a regular bank account.

In reality, there are several types of wallet providers:

- Hardware wallet providers that provide cryptocurrency users with specific hardware solutions to privately store their cryptographic keys (e.g. Ledger Wallet, …);

- Software wallet providers that provide cryptocurrency users with software applications that allow them to access the network, send and receive coins and locally save their cryptographic keys (e.g. Jaxx);

- Custodian wallet providers that take (online) custody of a cryptocurrency user's cryptographic keys (e.g. Coinbase).

f. Coin inventors: There are also those players who are referred to as "coin inventors". Coin inventors are individuals or organizations who have developed the technical foundations of a cryptocurrency and set the initial rules for its use. In some cases, their identity is known (e.g. Ripple, Litecoin, Cardano), but ever so often they remain unidentified (eg. Bitcoin, Monero). Some remain involved in maintaining and improving the cryptocurrency's code and underlying algorithm (in principle without the administrator's powers), whilst others simply disappear (e.g. Bitcoin).

g. Coin offerors: A final group of key players to be distinguished are the "coin offerors". Coin offerors are individuals or organizations that offer coins to cryptocurrency users upon the coin's initial release, either against payment (i.e. through a crowd-sale) or at no charge (i.e. in the framework of a specific (sign-up) program (e.g. Stellar – see below)), normally to fund the coin's further development or boost its initial popularity.

The coins these coin offerors offer to cryptocurrency users are created or pre-mined before the coin's official release / the coin's inception. Coins that are distributed this way are either partially pre-mined or pre-created (i.e. cryptocurrency users can still generate more coins after the release), or are fully pre-mined or pre-created. In the latter case, the coin offeror usually retains a large portion of the coins (e.g. this is the case with Stellar)**.**

It is important to note that not all coins have an identifiable coin offeror, nor are all coins pre-mined, or is its full supply pre-created.

A coin offeror can be the same person as the coin inventor, or another individual or organization (FATF, 2014, p. 7)**.**

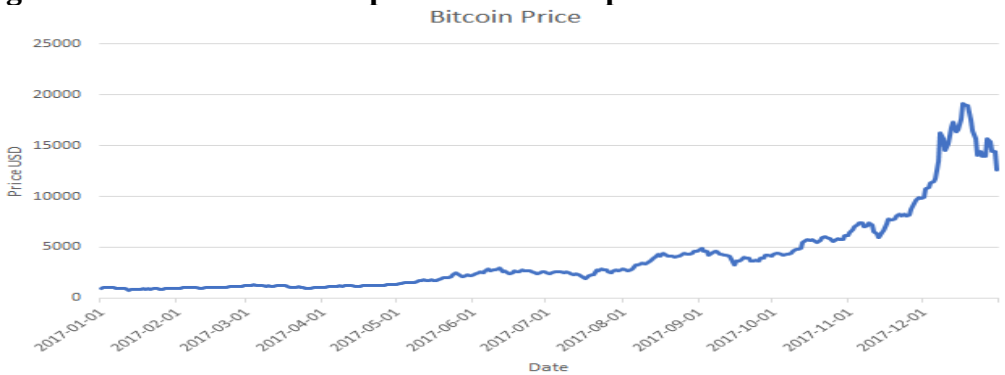
II- Analysis and Evaluation of the Bitcoin Prices; Market; and Legality.

In this section, We will present an evaluation of the performance of Bitcoin in terms of prices.

II-1- The Bitcoin prices development.

Bitcoin started to gain attention in late 2013 when the first governmental agency started to investigate Bitcoin (The U.S Senate Committee on Homeland Security and Governmental Affairs, 2013). Some of the hottest topics since then have been the taxing of Bitcoin, security breaches in the digital marketplaces, and money laundering. The financial crashes on the financial markets have contributed to the popularity of Bitcoin through a legitimacy crisis towards the financial institutions (Eisl, Gasser, & Weinmayer, 2015, p. 12).

Figure n°1: shows the development of Bitcoin prices in USD from 2012 to 2017.

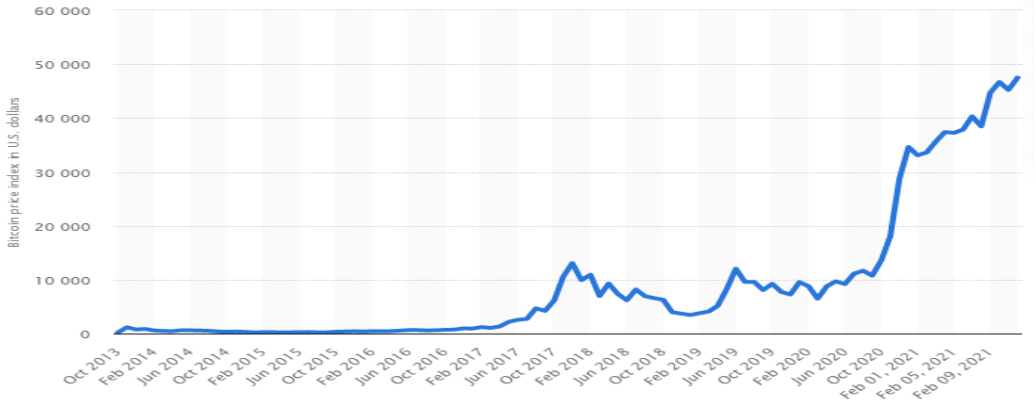


Source: Camilla Law; Marja Vahlqvist, « Can Bitcoin be used as a hedge against the Swedish market? », Stockholm business school; 2017; p7.

In 2017, the world's most known cryptocurrency, Bitcoin, has shown an incredible price curve. Graph 1 demonstrates the Bitcoin price in 2017 when the price increased tenfold which has been the steepest slope so far. During the 10 years of Bitcoin's existence, approximately

80% of Bitcoins have been mined and the currency has become a widely recognized name through global media visibility.

Figure n°2: shows Bitcoin (BTC) price history from 2013 to February 12, 2021.

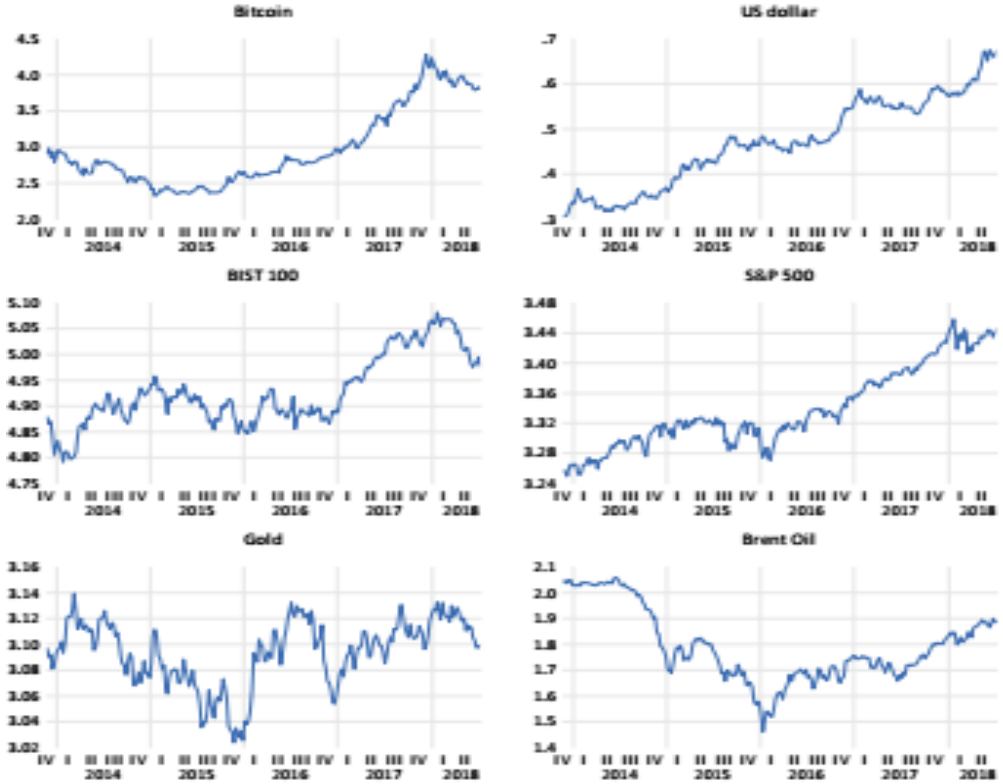


Source: Raynor de Best, « Bitcoin (BTC) price history from 2013 to February 12, 2021 », available on: https://www.statista.com/statistics/326707/bitcoin-price-index/ consulted on: Feb 10, 2022.

The virtual currency has had a volatile trading history since its creation in 2009. The first price hike occurred during 2013 when one bitcoin was trading at around 1,124 U.S. dollars in November. Four years later, bitcoin experienced a meteoric rise and reached record highs, with some exchanges having the price of a single bitcoin at approximately 20,000 U.S. dollars in late 2017. However, prices soon started to tumble in the months that followed. In the third quarter of 2020, there were around 18.5 million bitcoins in circulation worldwide, and the market capitalization of Bitcoin was approximately 200 billion U.S. dollars.

II-2- The relationships between Bitcoin and exchange rate, commodities, and global indexes.

Figure n°2: shows bitcoin prices evolution and the other global prices.



Source: M L ERDAS; A E CAGLAR: Analysis of the relationships between Bitcoin and exchange rate, commodities, and global indexes by asymmetric causality test, EASTERN JOURNAL OF EUROPEAN STUDIES Volume 9, Issue 2, December 2018; page 09.

Graph 2 reflects the evolution of Bitcoin, US dollar, gold, Brent oil, S&P 500 index and BIST 100 index between the years 2013 and 2018. As seen in Graph 2, the price or value of the Bitcoin series has an increasing trend with high volatility and the price of one Bitcoin (BTC/USD) reached a new all-time high in 2017, the US dollar has been frequently uptrend by years but the level of gold is more balanced, and increases and decreases in Brent oil price are felt most heavily during 2013-2018. In general, it can be observed that the line of all variables has monotonically displayed increasing or decreasing trends between 2013 and 2018.

II-3- The Bitcoin market

The analysis of the Bitcoin market shows its main users that are :

- natural persons (irrespective of the reasons for possessing BTCs),
- businesses (e.g. vendors who accept payments in BTCs).
- BTC stock exchanges,
- BTC currency exchanges,
- operators of BTC cash machines.

Although BTC's supply is continuously increasing as well as the interest in this form of payment, the research has shown that over 78%of the whole BTC, supply does not circulate in the system.

This is the money that is located in wallets and is treated as an investment (also BTCs that were forgotten by their owners and were the effect of the experiment with this currency before its value went up).

These Bitcoins have not been used in any transaction since they were obtained by their present owners.

Bitcoin is a part of an international tendency towards the increasing importance of cashless payments. In 2005 this share amounted to 34.6% in Poland (EU 67.8%), in 2010 – 54.5% (EU 75%). The popularity of making payments via online bank accounts has also been growing. In 2009 46% of the owners of a bank account in Poland accessed them online. In 2013 this percentage went up to 58%, and 79% of users made payments online very often (2009 r. – 73%).

Taking into consideration the growing interest in online and cashless payments it could be stated that Bitcoin is another stage in the development of the online payment market. Wallet software usually resembles online bank accounts in its interface and options.

One of the most popular and most often recommended methods of getting cryptocurrencies are stock exchanges. The most popular and has a significant proportion of total transaction volume are:

- BTC China – 52%;
- BitFinex – 20%;
- BTC-E – 6%;
- BitStamp – 6%.

Bitcoin stock exchanges are popular all over the world. It is demonstrated by the fact that there we can exchange Bitcoins for currencies. The most often exchanged currency through BTC stock exchanges are the Chinese yuan (59% share in all the transactions), the second one is the US dollar (37%), the eleventh one is the Polish zloty.

What is interesting and not much under the idea of Bitcoin's inventor –anonymity, the majority of cash machines require that the user verifies their identity before starting the procedure, usually by scanning an ID card or a hand.

The use of BTC cash machines is especially useful for people arriving in another country who want to buy local currency (Brière, Oosterlinck, & Szafarz, 2015, p. 14).

Banks usually charge for using traditional cash machines abroad, let alone currency-conversion fees. BTC cash machines do not make additional charges and the commissions

taken by the companies that run them are small, especially if a tourist decides to visit a country that is not a member of the EU.

Data indicate that the largest proportion of BTC cash machines is located in the USA and Canada. It is not surprising as the first BTC cash machine was used in Canada Since 2013 the number of BTC cash machines in Canada has increased to over 300.

In the past, payment by telephone or payment card was a completely new concept. Nowadays many consumers cannot imagine that it is impossible to make payment with a payment card. A similar situation may take place in the future with payments in cryptocurrencies.

II-4- Present status and legality of bitcoin around the world.

Countries around the world have reacted to Bitcoin technology in different ways, as shown in Table n°1. A few have banned the system outright; some have stopped short of regulation but have imposed taxes; some have acted to regulate or are in the process of taking such action; others are undecided about digital currencies in general. Because of the criminal potential and the difficulties with Bitcoin's taxation, governments of many countries are considering how to regulate, legalize or delegalize this currency. The most vigorous actions have been taken by the USA. Since 2013 the companies that deal with the transfer of virtual currencies have been regarded as entities whose activity requires obtaining the license issued by the Financial Crimes Enforcement Network (FinCEN). Under American law, such companies must also collect data on transactions (Franco, 2014, p. 48).

In the same year, the agency presented the project of a regulation that would introduce the obligation of registration for these Bitcoin users who hold it for commercial purposes. On the other hand, a court in Texas acknowledged Bitcoin as a currency because it enables us to purchase goods and services. In 2014 it was precise which companies and individuals are subject to the regulations from 2013, It was deemed that regulations do not apply to individuals and companies that (Szymankiewicz, 2014, p. 29):

- mine Bitcoin for their internal use,
- create or sell software for purchase and sale of virtual currencies,
- purchase or sell a virtual currency to invest for their use.

FinCEN introduces many regulations and proposals regarding virtual currencies, thus the USA may be considered a country that is the most interested in regulating Bitcoin's legal status. However, not only the USA has noticed the risk posed by decentralized virtual currencies. Some countries (such as Russia 2015 and Thailand 2015) have chosen an easier way and instead of thinking about how to regulate virtual currencies, they simply acknowledged them as illegal, solving all the problems Table n°1 shows the legal status of Bitcoin and other virtual currencies around the world.

Table n°1: Bitcoin's legality in chosen countries

Country	Legal status
China	Legal for individuals, illegal for financial institutions
Finland	Legal (it is regarded as a commodity)
France	Legal (unregulated)
India	Legal (unregulated, but the Central Bank has warned citizens against virtual currencies)
Iceland	Ban on purchasing Bitcoin abroad and accepting Bitcoin payments (Raymaekers 2014, pp. 36)
Japan	Legal (no regulations) (tvn24bis.pl 2015)
Jordan	Illegal for banks, stock exchanges, and other financial and clearing institutions
Canada	Legal (still working on its regulation)
Colombia	Considering whether to ban BTC
Germany	Legal (status of private money)
Poland	Legal (no regulations) (PB.pl 2015)
Russia	Illegal
Singapore	Legal (authorities do not interfere in accepting BTC payments)
Switzerland	Legal (consider treating virtual currencies like any other currency
Thailand	Illegal
USA	Legal (many regulations)

Source: Anna Wiśniewska; « Bitcoin as an example of virtual currency », Institute of Economic Research Working Papers No. 1/2016, p 27.

Even though Poland's Ministry of Finance has underlined the risks from Bitcoin, it is still unregulated and its use is legal. In January 2015 there was a considerable dispute in the media over closing bank accounts of Bitcoin users, e.g. BPH bank blocked the account of a BTC stock exchange.

III- Results and Discussion.

Can bitcoin overcome all legislative, economic, and security obstacles to reach the level of current payment instruments or money?

it turns out that the topic of Bitcoin and blockchain is a very debatable issue, however, this work supports the hypothesis that Bitcoin is money. It is possible to say that it does not coincide with the presented theories of money.

Another sub-question was whether: Can bitcoin have the same money characteristics as payment instruments? And gain an international general acceptance? In this case, the analysis presented leaves no doubt: Bitcoin is a technology innovation used in the financial sector by IT solutions and has some money properties in addition to relatively proportional payment instruments.

But The idea of " money of internet " is modern. In primitive times people agreed that a particular good would become money. Thus, in the twenty-first century, Bitcoin may be the new commodity that would become money by an IT (information technologies) system.

If the subject of research is changing, science should change too. Perhaps there will appear a new approach towards the theory of money and the issues that today are disputable will become obvious.

When it comes to the taxation and legal status of Bitcoin one should pay attention to the necessity of passing appropriate laws which regulate these issues. It is not only about the loss of state budget revenue from taxation, but also international security. It seems that there should be established an organization that would control if virtual currencies are not used to fund criminal activities. On the other hand, the existence of such an organization would be incompatible with the idea of Bitcoin as it is defined by anonymity and the lack of managing authority.

Whether we want it or not, cryptocurrencies will be present in our life, at least in the near future. There have been presented examples of companies that are interested in developing the technology that makes Bitcoin's existence possible. Even if virtual currencies end in complete failure, the IT infrastructure is worth being applied to other fields.

Bitcoin and other cryptocurrencies may be examined from various perspectives, not only economic. It may be treated as a sociological issue –the response of society to the increasing lack of trust in politicians and monetary authorities, caused by an international financial crisis, or an IT issue – focusing on the technical aspects of its functioning. Bitcoin is an up-to-date topic that has not been examined in detail, thus it is worth more attention from researchers.

The future of Bitcoin is unknown. This means that the progression of Bitcoin can go in any direction, which is currently and slowly evolving before our eyes. There are too many speculations and opinions regarding its future. So far, when cataloging the possibilities, three dissimilar outcomes rise to the top:

- Bitcoin becomes a globally recognized currency used all over the place, possibly even eliminating cash and credit cards.
- Bitcoin remains active and fine but performs in the background. Rather than being a major currency, it could function as an attribute and an accompaniment to the global financial sector. Just as the English language has spread around the world without eliminating existing languages.
- Bitcoin could spread around the world as a global payment system, coexisting with other world currencies.
- Bitcoin prices collapse to their inherent value. The collapse could take the form of a sudden fizz or a slow fade over time. Either way, it ceases to survive in the public eye and is ultimately forgotten as the year's pass.

Conclusion.

In conclusion, it can be believed that Bitcoin does have a prospective for greater universal acceptance, depending on whether the focus is on quick, inexpensive, and convenient transactions. This focus would necessitate simple, more consumer-friendly services, even for those who do not wish to understand the technicalities behind it. The path to such permanent establishment requires that the system remain fully transparent and secure, that a network effect takes place, and that the Bitcoin ecosystem be strengthened and made more dependable. Bitcoin might not, by definition, be a new currency, but it has laid the foundation for potentially improving money as we know it now.

References

1. *BANQUE DE FRANCE. (2013). Les dangers liés au développement des monnaies virtuelles: l'exemple de bitcoin. paris: Focus.*
2. *Brière, M., Oosterlinck, K., & Szafarz, A. (2015). Virtual Currency, Tangible Return: Portfolio Diversification with Bitcoin. 16 (6).*
3. *CPMI. (2015). Digital currencies. Bank for International Settlement .*
4. *EBA. (2014, july 04). Opinion on 'virtual currencies. Consulté le 12 10, 2021, sur https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf*
5. *ECB. (2015). Virtual Currency Schemes – a further analysis. Consulté le 9 15, 2021, sur https://www.ecb.europa.eu/: https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf*
6. *Eisl, A., Gasser, S. M., & Weinmayer, K. (2015). Caveat Emptor: Does Bitcoin Improve Portfolio Diversification? SSRN Electronic Journal .*
7. *ESMA, EBA, & EIOPA. (2017). Warning on the risks of Virtual Currencies. Consulté le October 10, 2021, sur https://www.esma.europa.eu/sites/default/files/library/esma50-164-284_joint_esas_warning_on_virtual_currenciesl.pdf*

8. European Commission. (2017). Report from the European Commission to the European Parliament. Brussels: COMMISSION STAFF WORKING DOCUMENT.
9. FATF. (2014). Virtual Currencies – Key Definitions and Potential AML/CFT Risks. Paris.
10. Faulkner, J. (2016). Getting Started with Cryptography in .NET. munich: Kindle Edition.
11. Franco, P. (2014). Understanding Bitcoin: Cryptography, Engineering and Economics. Wiley.
12. Hileman, G., & Rauchs, M. (2017). Global Cryptocurrency Benchmarking Study. Cambridge : Cambridge Centre for Alternative Finance.
13. Houben, R. (2015). Bitcoin: there are two sides to every coin. ICCPR , 26 (5).
14. IMF. (2016). Virtual Currencies and Beyond: Initial Considerations. IMF Staff Discussion Note.
15. Natarajan, H., Krause, S., & Gradstein, H. (2017). Distributed Ledger Technology (DLT) and Blockchain. Washington, DC: World Bank.
16. Szymankiewicz, M. (2014). Bitcoin. Wirtualna waluta internetu. Helion.
17. Van de Looverbosch, M. (2018). Crypto-effecten: Tussen droom en daad. Roularta Media Group , 18 (3), 193-207.
18. Vandezande, N. (2018). VIRTUAL CURRENCIES: A LEGAL FRAMEWORK. Intersentia.
19. Witzig, P., & Salomon, V. (2018). Cutting out the middleman: a case study of blockchain-induced reconfigurations in the swiss financial services industry. the Circulation of Wealth .
20. Young, E. (2018, march). Accounting for crypto-assets. Consulté le 11 05, 2021, sur http://eyfinancialservicesthoughtgallery.ie: http://eyfinancialservicesthoughtgallery.ie/wp-content/uploads/2018/03/EYIFRS-Accounting-for-crypto-assets.pdf