BITCOIN AS A POSSIBLE MEANS OF FINANCIAL MARKET FRAUD

Review paper
UDK: 336.744-021.131:336.7
JEL classification: B15, E02, G14, G17
DOI: 10.17818/DIEM/2021/1.21
Accepted for publishing: July 8, 2021

Abstract

The aim of this paper is to present the manipulation possibilities in the operation of information technology. Many authors have already dealt with cryptocurrencies and their investment potential, with special emphasis on bitcoin. Therefore, the aim of this paper is to identify possible manipulative activities in the segment of information technology about bitcoin as a possible means of fraud in the financial market, especially if it is analysed the trend of its movement and potential financial risk. In this paper, the authors investigate in detail the characteristics of securities by linking them to market manipulations. The authors analyse bitcoin as a relative market and financial unknown, explain its origin and the most significant characteristics, and define the risks in terms of possible market manipulations. Finally, the authors analyse the financial bubble that is created around bitcoin and its impact on the economy. The authors analyse that bitcoin and other cryptocurrencies are still suitable for fraudulent activities in financial markets and emphasize the importance of institutions in reducing potential risks.

Keywords: bitcoin, institutions, bubble

1. RELEVANT FEATURES OF BITCOIN

Despite numerous papers and discussions on bitcoin and other cryptocurrencies, several unknowns can be identified with this relatively new financial form. Although it is ungrateful to determine their priority, the following stand out in particular: their knowledge of how it works is not proportional to the number of people who are interested in bitcoin; the movement of its price is so unusual that it already...
represents a kind of phenomenon; a future that may be predictable in the long run, but is completely uncertain in the short to medium term. In this regard, the question arises whether bitcoin is a random phenomenon that exceeded the expectations of its creators, and it should be emphasized that they are still unknown, or is it a carefully thought-out tool that will at some point serve to make a profit at the peak of investment balloons, to create a corner or to carry out some, so far unknown market manipulation. In countries with developed institutions, the manipulative space for such activities is narrowed, but bitcoin is essentially a tool that easily bypasses any national borders, so the question of the effectiveness of institutions arises. So far, the boldest announcements of bitcoin price growth are coming true, although the increase seems to be based solely on investor expectations. Indicators of technical analysis most often fail to indicate future price shifts. Given the above, it seems that bitcoin and other cryptocurrencies need increased caution.

2. RELEVANT FEATURES OF BITCOIN

2.1. Organization and functioning of the bitcoin network

Bitcoin means organization of the same name, software and protocol. This cryptocurrency was first mentioned in 2008 in an article published under the pseudonym Satoshi Nakamoto (Nakamoto, 2008). It was never known whether an individual or a far more complex organization was behind the pseudonym. In 2009, he started an open source project called Bitcoin - Qt, which launched the first bitcoin units, but they did not have any market value at that time. The first bitcoin purchase is believed to have been made by computer programmer Laszlo Hanyecz in 2010, who paid 10,000 bitcoins for two pizzas worth $25 (Bitcoin Pizza Index, 2021). Although it is not known for sure whether this story is true, just as it is not known what the owner of the pizzeria later did with the received bitcoins, at today’s prices it turns out that the American programmer paid around 580 million dollars for pizzas and for that he has a place in recent history of financial markets.

Bitcoin is a peer-to-peer system based on complex cryptographic algorithms. Peer-to-peer means a network in which there is no central authority that issues new money or monitors transactions. Tasks in such a network are managed collectively by network nodes. As the greatest advantages of such a system, it is possible to point out the simple transfer of money over the Internet, without intermediaries, whereby a third party cannot prevent or manage the user's transactions. In the bitcoin system, there is no central bank that issues money and keeps and processes transactions, nor is there a single owner of the bitcoin network. New units of bitcoin are generated by mining as a reward to miners for spending time and energy invested. Namely, mining is crucial for the functioning of the entire system because it actually serves to confirm and process bitcoin transactions and to ensure its security. Without a miner, the system would be vulnerable due exposure to attacks and would not be able to function. This job requires special IT equipment and requires significant electricity consumption, so it cannot be profitable for most people. The key difference of bitcoin compared to centralized systems stems from the fact that each user has an insight into their own transactions and the transactions of other participants. Each transaction contains the digital signature of the user who initiated it. A digital signature is generated from a combination of a transaction message and a user's private key. The signature differs in each message, making forgery and misuse impracticable without the original private key (Buterin, Ribarić & Savić, 2015).

Each user also owns a public key that is mathematically related to the private key. Electronic forms of money, ie performing financial transactions by exchanging information electronically, form the basis of electronic business. The flow of electronic information between the two parties communicating on the Internet allows uninterrupted observation but opens up opportunities for possible misuse by a third party. In order to neutralize or prevent such unwanted activities, encryption protection and authentication of participants in the transaction are used. The basis for such procedures are various cryptographic algorithms and mechanisms and additionally
developed higher-level protocols that ensure the protection of electronic information as well as the privacy of transaction participants (CARNET & CERT, 2010).

![Diagram of Bitcoin transaction]

Source: CARNET & CERT, 2010

Figure 1 The course of the bitcoin transaction

The functioning of bitcoin is based on a distributed system consisting of interconnected nodes, i.e. servers that can be independently organized into network topologies for sharing available resources such as user data, process time, storage capacity or network bandwidth. They can independently adapt to functionality outages and unpredictable network node arrivals and departures, while maintaining an acceptable level of performance without the need for supervision, control, and support from a single central location (Androutsellis-Theotokis & Spinellis, 2004). It is possible to identify the key features of the partnership mode (CARNET & CERT, 2010):

- equality of nodes
- direct communication between nodes
- independently collecting information on the availability of other nodes
- individual nodes have only part of the data available in their local storage system, i.e. a subset of the total data available on the network.

Bitcoin consists of a cryptographic key pair, where one of the keys represents a currency unit, and the other serves as a permission to dispose of it. The keys are stored in a binary file, where there is a risk of theft. When the owner wants to pay with a unit of bitcoin, he sends only the public key together with the signature for the transaction, which receives the corresponding key of the recipient, thus changing the owner and at the same time the secret code of the amount. Since the transaction is recorded on all computers, manipulations in this part of the transaction are almost ruled out. Cryptocurrencies are stored in digital banknotes, i.e. in software that contains a collection of private and public keys of the owner. One user can generate an arbitrary, unlimited number of bitcoin addresses, with the probability of generating the same addresses being negligibly small. During the transaction process, ownership of bitcoin units changes. In the event of loss of private and public key information, the user loses access to his units and they become irretrievably lost. A Bitcoin wallet can take up a lot of network space, as constant synchronization with the network involves storing data on all transactions made. Web wallets appear as a possible alternative, which do not involve keeping a local copy of the transaction, but where the level of security is lower (Buterin et al., 2015).

Bitcoin is a system based on complex mathematical algorithms and mechanisms and as such is fully understandable and clear only to those with a high degree of computer literacy. People who are less computer educated can make mistakes that can leave them without their money. Possible user errors include the loss of data and key information, the possibility of unauthorized intrusion and theft of keys, as well as inadvertent disclosure of key information.

2.2. Monetary aspect of bitcoin
Electronic money, unlike paper money, is not transferable. An ordinary banknote received in one of the previous transactions may be reused in any of the following. It is easily transferable and takes more than one transaction. Such a feature would be highly desirable for digital banknotes because in each transaction the banknote should not be stored in the bank, thus reducing the number of interactions with the bank and thus the system costs. In an electronic money system, the user of the banknote should add identification data to each banknote, i.e., a set of bit data, which would increase the amount of bit data stored in the virtual banknote with each transaction performed by it. The number of possible transactions with such a banknote would be limited by the maximum size of the banknote. Due to such shortcomings, portable electronic money systems have not been developed and each electronic banknote has a lifetime of one transaction (DeGennaro, 2011). Digital money as well as paper money ensures the anonymity of the person who pays with it and it is not possible to track it. This means that the person receiving the electronic banknote cannot find out the identity of the person who used it.

The main feature of cryptocurrencies is the absence of a central institution that issues or manages them. Because bitcoin is based on a decentralized system without the existence of regulatory authority, the system adapts to certain algorithms and in no way reflects the state of the economy of a particular country. The lack of a regulatory system and anonymity makes bitcoin suitable for market manipulation. The movement of its price, which is based exclusively on the expectations of investors, i.e., the ratio of supply and demand, indicates the creation of an investment bubble. However, as its price persistently follows a long-term upward trend, indications of an investment bubble remain in the realm of speculation, as do all other predictions regarding bitcoin. The only thing that is certain is that bitcoin has no intrinsic value and that the movement and increase of its price can be related exclusively to the increase in demand, regardless of whether it is the result of market circumstances or was created artificially to achieve goals that are not yet obvious. In the absence of intrinsic value, bitcoin is very similar to other forms of money, but unlike previously known forms of money, the settings of the most important theories of money demand cannot be applied to the demand for bitcoin (Stojanov, Drašković & Drašković, 2015):

- Fisher’s equation of money demand:
  \[ M^sV = pY \]
  in which the left side of the equation represents the money supply or available purchasing power in the market. The right side of the equation represents the demand for money, i.e., the total value of goods and services. If it is \( M^sV > pY \) the value of money will fall, that is, prices will rise. Whether bitcoin is substituted with the left or right side of the equation, depending on whether it is viewed as money or a good bought for money, the equation becomes inapplicable due to large price deviations.

- Marshall-Pigou Cambridge equation:
  \[ M^s = kpY \]
  in which the left side represents the money supply, i.e., the available purchasing power, and \( kpY \) represents the demand for money. When is it \( M^s > kpY \), then the money supply is greater than the money demand. Money owners want to get rid of excess money as its marginal utility declines. Contrary to this theory, with bitcoin its marginal utility increases so the equation becomes inapplicable.

- Keynes’ speculative demand for money:
  \[ M^s = LP(i) \]
  where is \( M^s \) monetary supply, \( LP \) is a function of liquidity preference, and \( (i) \) interest. In considering the issue of liquidity preference, Keynes observes two functions of money: the function of money as a medium of exchange that forms the transactional demand for money, and the function of money as a treasure. The demand for money as a treasure arises due to uncertainty.
about the level of future interest rates. However, bitcoin is not under the jurisdiction of the monetary authorities, so the amount of the future interest rate, or in this case the yield, depends exclusively on natural or artificially created demand.

- Friedman's theory of demand for money (Friedman, 1973): 
\[ \frac{M}{P} = f\left\{y, w, rm, rb, re, \frac{\Delta P}{\Delta t}, u\right\} \]

where is:

- \(W\) - part of assets in physical form or part of income from physical assets
- \(Rm\) - expected normal rate of return on money
- \(Rb\) - expected nominal rate of return on fixed value securities including changes in their prices
- \(Re\) - expected nominal rate of return on shares including expected changes in their prices
- \(I / P\) and \(\Delta P / \Delta t\) - expected rate of change in prices of goods, ie expected nominal rate of return on real assets
- \(u\) - a combined symbol representing any of the variables - other than the income variable - that may affect the utility of the services provided by the money.

According to Friedman's theory, the owner can hold property in various forms while trying to maximize the usefulness of certain forms of property on the principle that the marginal income is equal to the marginal cost of each form of property. Bitcoin price shifts in financial markets make all other forms of assets less attractive, and thus this theory inapplicable.

There is a kind of paradox with bitcoin as a form of money. Namely, it is very easy to logically understand that the upward movement of bitcoin prices in financial markets discourages the use of bitcoin as a means of payment because the average consumer will experience an increase in its purchasing power with each new period of consumption delay and bitcoin payments. The rise in the price of bitcoin leads to refraining from its use in everyday trade, which is why it loses the function of money as a medium of exchange and at the same time serves as a speculative means or a means of accumulation of wealth. However, it is precisely the lack of intrinsic value and the lack of understanding of how it works by the vast majority of people that makes it very risky for both speculation and accumulation of wealth. Paradoxically, an increase in the price of bitcoin also leads to an increase in demand for it, but bitcoin cannot be considered a Giffen good (Garratt, 1997; Spiegel, 1994) or a Veblen good (Stiefenhofer & Zhang, 2020; Almeida, 2015). It seems that bitcoin violates the current concept and represents a completely new paradigm, which is another characteristic of investment bubbles. Attempts to manipulate the market and trade insider information are most often associated with investment bubbles.

3. BITCOIN – A COMMON INVESTMENT BALLOON, MARKET CORNER OR SOMETHING ELSE?

In order for an information to be considered privileged, it must have the following characteristics (HANFA, 2021):

- precise nature
- hidden from the public
- directly or indirectly refers to one or more issuers of financial instruments
- if this information were publicly available, it would have a significant impact on the prices of these financial instruments.

Market manipulation is one of the oldest forms of market abuse and this includes the following actions:

- transactions or trading orders that give or could give false or false signals regarding the supply, demand or price of financial instruments,
• demand or prices of financial instruments that, through the action of one or more persons acting in concert, keep the price of one or more financial instruments at an artificial level,
• transactions or trading orders that use fictitious procedures and any other form of fraud or fraud,
• Disseminating information through the media, including the Internet, or giving any false, misleading hope where the person who released the information knew exactly that the information was false.

Actions that are considered market manipulations are:
• the activities of one or more persons working to secure a dominant position over the supply or demand of a financial instrument that have the effect of directly or indirectly setting purchase or selling prices or creating other illegal trading conditions
• buying or selling a financial instrument provocatively towards the end of the trading day to deceive investors who adjust the price based on the last trading price.

Such activities are more often carried out in countries with lower institutional development, while in countries with developed institutions the situation is still more favourable (Suljić Nikolaj, Olgić Draženović & Buterin, 2019; Buterin, Grdinić & Olgić-Draženović, 2018; Buterin, 2015). Due to the characteristics of the global currency, bitcoin can very easily circumvent the institutional limitations of developed countries and manipulate it in less protected markets.

Looking at the movement of the price of bitcoin, the first three phases of the formation of the investment bubble can be clearly seen: the hidden phase, the awareness phase and the mania phase. The risk of bitcoin has been noted by numerous authors, regardless of its short-term investment potential (Olgić Draženović, Prohaska & Suljić Nikolaj, 2019; Xiong, Liu & Zhao, 2019; Bouri, Gupta, Lau, Robaud & Wang, 2018; Corbet, Lucey, Peat & Vigne, 2018) or the potential for portfolio diversification (Conlon & McGee, 2020; Bouoiyour, Selmi & Wohar, 2019). If the fourth phase, ie the blow off phase, occurs in the near future, it will be a completely expected and predictable outcome for future analysts, where it will be difficult to explain the reasons why average investors did not understand what was coming, or why they were unaware of inflating an investment balloon. After the market crash, there is usually a period of economic crisis in which even the largest financial entities may be shaken (Olgić Draženović, Buterin & Buterin, 2018).

Source: https://www.buybitcoinworldwide.com/price/ (29.3.2021.)
Figure 2 Total movement of bitcoin prices

Figure 3 Investment bubble phases

Figure 4 South Sea bubble
Comparing the price movements of bitcoin and more famous investment bubbles (Dedu, Turcan & Turcan, 2012), starting with the tulip crisis in the Netherlands in the 17th century, The South Sea Company and the Mississippi Company in the 18th century, Railway mania in the 19th century, Florida speculative building bubble (1926), Roaring Twenties stock-market bubble (1922-1929), Poseidon bubble in Australia (1970), Japanese asset price bubble (1980s), Asian Financial Crisis (1997), The Dot-com bubble (1995-2000) and numerous similar examples, one can expect with great confidence the bursting of the bitcoin bubble and a significant drop in its price which now seems inflated. The bursting of large investment bubbles is often accompanied by dramatic economic consequences, but there are also opinions that they do not necessarily have to be detrimental to the economy as a whole. For example, Gisler and Sornette (2008) argue that balloons are an essential element of social processes and the dynamics of society and cite as examples the Apollo program, the human genome project, large investments in the alternative energy industry that revolutionized technologies in the energy sector, Dot-com bubble within which significant capital has been invested in IT infrastructure, and other emerging industries that need overinvestment to sustain innovation. In this regard, Gross (2007) argues that most investors in Dot-com have lost, but that their capital has built the software and infrastructure that drives the internet today. If the charts of bitcoin price movements are observed separately in different periods, it is possible to observe at least three emerging bubbles. A blow off could also be expected from each of them, but this did not happen.
Figure 6 The first apparent bubble, price movement from August 2010 to December 2013

Figure 7 The second apparent bubble, price movements from January 2014 to December 2017
Every time it seemed that the peak of the investment bubble had occurred and that it was time to make profits or for a short sale, the future proved different. Moreover, its exponential growth may be accompanied by a trend indicating that the price will rise over the next two years to a predictable level of around $160K.

Source: Author’s calculation and https://finance.yahoo.com/quote/BTC-USD/ (30.4.2021.)

Figure 9 Bitcoin price forecast based on historical prices from 2014 to 2021

Approximately the same price level can be expected even if the period before December 2017 when the price first exceeded $10K is excluded from the trend analysis.
However, it should be borne in mind that all indicators of technical analysis, as well as analysis of trends, regardless of their significance and success in explaining variables, are based solely on historical data and in no case should be used as a reliable indicator for investment.

Short selling is an activity characterized by a very high degree of risk and in which losses can be unlimited (Buterin, Janković & Klaus, 2018). The emergence of short squeezes leads to unforeseen losses for investors who find themselves in a corner and to significant earnings for those who managed to corner the market, as happened in 2008 with the trading of VW Group shares. Due to its characteristics, bitcoin is a suitable tool for cornering and short squeezing, so its short sale is especially risky. In the long run, a balloon burst can undoubtedly be expected, but at this point it is impossible to predict how long that period will be, or whether deflation can be expected after a peak of $100K, $150K or some perhaps far higher price. It should not be forgotten that just a few years ago, predicting the current price of $60K for a single bitcoin would have been so bold that it would then probably have been considered beyond the bounds of the possible.

4. CONCLUSIONS

Lack of reliable information about bitcoin, lack of understanding of the basis of its origin and functioning, dependence of functioning on miners without whose operation the bitcoin network could not exist at all, lack of its intrinsic value, unsuitability for accumulation of wealth, loss of function as a media for exchange, complete dependence on demand that is not based on any qualitative characteristic of bitcoin as a currency or as a security other than the expected further price increase, lack of information on whether that demand is autonomous or caused by angle-oriented activities other than making bitcoin a very risky investment, also make it a very suitable tool for market manipulation. Although bitcoin is considered the most important and significant cryptocurrency, its main characteristics can be largely applied to other cryptocurrencies. This is especially true of their potential to carry out manipulative activities. Likewise, what makes bitcoin and other cryptocurrencies significantly different from earlier investment bubbles and from earlier means by which market manipulations were conducted is the use of information technology. Namely, no security so far, as well as no form of money or other assets, has been so much based on sophisticated information technology and so dematerialized and transferred to the virtual world as is the case with cryptocurrencies. In such conditions, the role of institutions is gaining in
importance, although the denial and overcoming of institutional influence is one of the more prominent characteristics of bitcoin and other cryptocurrencies. The price of bitcoin is currently oscillating around a new psychological limit and seems to defy all known theoretical and empirical assumptions. Its future can no longer be discussed in the context of risk, but it is already in the domain of uncertainty because it cannot be predicted in any reliable way. It is clear that it is a balloon, but the capacity of its inflation is no longer clear, nor is its predictable duration. But on the other hand, it seems very certain that bitcoin is a tool where financial manipulations are very possible and that a very high degree of caution is needed in the bitcoin business.

REFERENCES
Friedman, M. (1973). Teorija novca i monetarna politika, Rad: Beograd