IJEP International Journal of Economics and Politics

DOI: 10.29252/jep.2.2.41

Time Series Clustering of Bitcoin and other Cryptocurrencies Based on Consensus Protocols

Mohammad Kazem Sadeghian[1], Kazem Yavari*[2], Abbas Alavi Rad[3]

ARTICLE INFO

Article history:

Date of submission: 26-04-2021

Date of acceptance: 29-06-2021

JEL Classification:
E42
D51
Z19

Keywords:
Cryptocurrency
Time series clustering
Consensus, Bitcoin

ABSTRACT

In cryptocurrencies, consensus protocols are considered as one of the fundamental differences in the mechanism of their creation. The purpose of this paper is time series clustering of daily prices of cryptocurrencies during 2015 to 2020 using time series clustering algorithm. This research attempts to cluster the time series of twenty cryptocurrencies that have different consensus protocols such as algorithm designed to proof of work, proof of stake or proof of a subject, algorithm designed for voting and so on. The results of this study show that cryptocurrencies are in a specific group with a proof of work mechanism such as Bitcoin and Litecoin. Zcash, Tron, Obyte, Neo, Iota, and EOS are also in a separate group with new consensus mechanisms, including a Directed acyclic graph algorithm. Stellar, Monero, and Ripple cryptocurrencies are also clustered in a group with almost similar mechanisms. This indicates that the time series of cryptocurrencies with similar creation mechanisms and consensus have the same behavior and are in the same cluster.

Introduction

In recent years, the tremendous increase in the value of cryptocurrencies, including bitcoin, has attracted much international attention. Between 2013 and 2020, the price of cryptocurrencies has increased more than twenty thousand times. Furthermore, the influence of these cryptocurrencies in

1. Ph.D Candidate in Economics, Abarkooh Branch, Islamic Azad University, Abarkooh, Iran.
2. Full Professor of Economics, Faculty of Economics, Management and Accounting, Yazd University, Yazd, Iran, E-mail address: kyavari@yazd.ac.ir (Corresponding Author).
3. Associate Professor, Department of Economics, Abarkooh Branch, Islamic Azad University, Abarkooh, Iran.

international monetary and financial markets and the increasing willingness of people to exchange this type of currency, has highlighted the need to study the nature of this phenomenon.

In addition, the concerns of the governments and monetary authorities in controlling and monitoring the cryptocurrency market and the growing tendency of investors to accept and select cryptocurrencies in the asset portfolio, have made it very important to know this phenomenon.

The cryptocurrencies have fundamental differences from Fiat money, including the community-based creation mechanism and no need for a central bank to supply them. However, cryptocurrencies have similar functions to Fiat money, as store of value, medium of exchange, and by creating money exchange platforms with high efficiency and much lower transaction costs than current banking systems. These issues have posed many challenges for governments in rejecting or accepting cryptocurrencies.

The efforts of governments to legalize and control cryptocurrencies have put them in front of the world's monetary and banking systems. Meanwhile, cryptocurrencies have tried to correct the problems of monetary and banking systems through new mechanisms of consensus. Importantly, governments have so far failed to control and manage the cryptocurrency market. One of the reasons for this failure was the lack of knowledge of governments about the issue of cryptocurrencies.

In recent years, an evolutionary process to solve the problems of cryptocurrencies in the market and the problems of fiat money has been carried out by foundations active in the field of cryptocurrencies. This reform process leads to the creation of cryptocurrencies with different creation mechanisms, and understanding their price behavior can be of great help to monetary authorities and investors. As the first cryptocurrency with a proof-of-creation mechanism, Bitcoin has a powerful network for exchanging value. But cryptocurrencies have sought to solve the problems facing the original mechanisms with newer creation mechanisms.

Solving scalability problems, speeding up the number of financial transactions, connecting monetary networks to each other, creating smart contracts for new financial systems, reducing energy consumption and

reducing environmental risks associated with the creation mechanisms, are among the issues that cryptocurrencies have been looking for it by creating new mechanisms. The new mechanisms directly affect the price of cryptocurrencies, and understanding the price behavior of cryptocurrencies paves the way for investors and monetary authorities to make decisions about cryptocurrencies.

Although in recent studies, the behavior of bitcoin price fluctuations has been analyzed and measured, but understanding the behavior of other cryptocurrencies needs to be examined. The existence of cryptocurrencies with different creation mechanisms raises the question of whether the price behavior of cryptocurrencies with the same creation mechanism falls into the same category or not. This article will use time series clustering to answer this question. To reach the answer in this article, first with a brief description of the characteristics of cryptocurrencies, the mechanism of creating bitcoin as one of the most important ones are discussed. Then the mechanism of consensus in the cryptocurrencies will be examined as the main issue of the difference between them. Finally, the clustering algorithm is used to evaluate the time series of the price of cryptocurrencies. The present article is organized in five sections. The second part explains the theoretical foundations of the process of creating and valuing bitcoin, the definitions of consensus and consensus in bitcoin. In the third part, the methodology of time series clustering approach and a brief introduction of the evaluated cryptocurrencies is discussed. In the fourth section, the results of statistical calculations are analyzed. In the fifth section, the conclusion of the discussion is presented.

2. Literature review

In the last two decades, the creation of cryptocurrencies and the acceptance of them by investors as an asset have created new conditions in the international arena for the management of monetary resources (Ji et al, 2018). Ever since Internet users were able to exchange information in cyberspace, a mental norm has been a key factor in using cryptocurrencies (Shin ,2008). The history of digital currencies goes back to the 1990s with the study of Untraceable Electronic Cash (Chaum & Naor,1998). In 2009, after the creation of Bitcoin

by Nakamoto, its price value was not noteworthy, but since 2013, with the development of the market for these cryptocurrencies in the monetary and financial sectors of many countries, there has been a significant jump in price (Troster et al. 2019). Bitcoin, whether as a currency or an asset, is a social reality (Cheah & Fry, 2015). For example, the growth of social networks and financial regulation, especially in the field of customers, has affected the price of Bitcoin (Corradi & Höfner, 2017; Pieters & Vivanco, 2017).

There is also a significant correlation between social media tweets and bitcoin prices (Matta et al., 2015). The origins of bitcoin are in the participatory economy and focus on the communication of modern social networks (Killeen, 2015). In social media, trust among users leads to transactions. This credit is one of the most vital features of Bitcoin compared to other payment methods. Bitcoin behaves like an asset in the short run, but in the long run it can prove to be a medium of exchange (Horra, 2019). Bitcoin is not like real money that has value, but its credibility and value come from a set of consensus processes. In the bitcoin transfer process, bitcoin ownership is transferred along with its value. One of the most successful cryptocurrencies in the world is Bitcoin and Litecoin, but the adoption and development of Bitcoin has set a more accurate path to the goals of cryptocurrencies (Levin et al., 2015). The value of bitcoin depends on the trust of its users, and its main idea is formed by simulating the use of a limited resource (Turpin, 2014).

The first studies on bitcoin date back to 2013 on the subject of the Zero-coin protocol. Individuals such as Becker et al (2013), Dwyer (2015), Segendorf et al. (2014), Brandvold et al (2015) and Roth (2015) have explained the behavior of this phenomenon. Of course, the role of this phenomenon in the foreign exchange market was not significant until 2013, but in the following years Bitcoin accounted for about 80% of the market value of cryptocurrencies (Al-Yahyaee et al., 2018). In the years since 2013, Bitcoin has gained a share of over $ 120 billion in the international capital market (Troster et al., 2018). These changes have encouraged people to study the behavior of bitcoin.

The creation of bitcoin follows strict financial rules such as the gold market, and the value of bitcoin is created by solving encrypted issues and

validating transactions (Briere et al. 2015). This value is formed based on a process called mining. Bitcoin is formed through a peer-to-peer network on the Internet. The main concept of mining is based on the proof of work protocol (Brandvold et al., 2015). Shortly before the proof-of-work protocol was developed, people like Dwork & Naor in the field of computing introduced the basis of "pricing by processing" in 1992.

In the process of proving of work, people use home processors to solve difficult mathematical problems. Solving these problems is rewarded with a cryptocurrencies form. This process of encoding, converting and re-validating it, the existence of nodes, validators and block architecture mediators is in the form of a blockchain. In fact, the Proof of work process is a protocol that creates a hash. A hash is a mathematical algorithm that converts all types of data, including letters or numbers, into a fixed numeric string (Bhaskar & Chuen, 2015). This creation mechanism is related to algorithms in cryptocurrencies because valid algorithms affect the validity of cryptocurrencies and are effective in its price (Turpin, 2014).

Now, after explaining the consensus, this article will explain the issue of bitcoin consensus as one of the successful cryptocurrencies. This article seeks to investigate whether the mechanisms of creation and consensus have an effect on the time series behavior of the price of cryptocurrencies. Also, do cryptocurrencies fall into a certain group with the same mechanism or not?

2-1. Consensus

Consensus is a common acceptance among users. Mainly in cryptocurrencies, algorithms have created consensus by creating a validation process among network members in the form of blockchain (Aruna Sri and Lalitha Bhaskari, 2020).

One of the pillars of all blockchain systems is consensus algorithms (Yu et al., 2019; Feng et al., 2020). Reaching an agreement in the blockchain is a matter of consensus (Hosseini Bamkan et al., 2020). To understand the

mechanism of consensus in cryptocurrencies, we must first look at blockchain technology. A blockchain is a chain of blocks, each of which stores a set of information. Blockchain consists of two basic concepts: peer-to-peer network and distributed database (Oliveira et al., 2020). Digital identity creation, storage of registry data and creation of immutable data are among the activities that lead to the validation of blocks which mainly lead to the validation of cryptocurrencies. In blockchain, information is linked to the next block through a special complex mathematical function called a hash, which is the most important step in reaching a consensus (Lafourcade et al., 2020).

Consensus is an interactive process in which decision-makers reach an agreement (Kacprzyk & Fedrizz, 1988). Although the concept of consensus is formed in creating an agreement, but in the system of cryptocurrencies, in addition to social consensus, there is a technical consensus based on algorithms (Aggarwal et al., 2020). The main consensus algorithms include the algorithm designed to proof (work, stake or a subject), the algorithm designed for voting and the Directed Acyclic Graph algorithm that each of them has unique characteristics and a group of the cryptocurrencies follow them.

Technical consensus includes Proof of Work (POW), Proof of Stake, Proof-of-Weight, Proof of Authority, Byzantine Fault Tolerance, etc algorithms. Each of these algorithms has advantages and disadvantages and they are used in different cryptocurrency protocols. One of the differences between cryptocurrencies and real money is consensus. Technical algorithms also lead to consensus. On the other hand, encouraging users to receive rewards, or forcing them to follow a validation protocol, also leads to consensus. In the process of consensus, cryptocurrencies become valuable.

Numerous people have discussed consensus mechanisms and their models (Dong & Cooper, 2016; Dong et al., 2015; Zhang et al., 2020). Consensus can be explained as a percentage of trust that arises in the decision-making process (Liu et al., 2017). Several methods for consensus have been defined in the

cryptocurrency's algorithm, one of the most important of which is measures to avoid double spending (Gilad et al., 2017). It can be said that consensus is formed through agreements between miners[1], key node[2] owners and programmers. These agreements can become rule in the cryptocurrency network. The most important criteria in consensus algorithms include the basis of agreement, how to add to the network or node, decentralization processes, trust building, user identity, security and the amount of reward provided in the algorithm.

Due to the novelty of the subject of cryptocurrencies, studies on the mechanism of consensus are few. Pournaras (2020) emphasizes that blockchain consensus can strengthen trust in smart city systems. Gramoli (2020) examines the differences between cryptocurrency consensus protocols. The results of his study show the benefits of consensus algorithms such as proof of work and proof of stake and emphasize that the design of new consensus algorithms is very important in process validation. Oliveira et al. (2020) explain the mechanism of consensus and their problems such as energy consumption. In their study, it is noted that the mechanisms of consensus lead to agreement among the users in the blockchain. Bugday et al (2019) in their paper have shown the Byzantine Fault Tolerance algorithm to be important for solving the problem of scalability. In their study, they introduced an algorithm that increases credibility in the network by building a consensus committee. Zhang & Le (2020) have categorized the strengths and weaknesses of each by classifying consensus protocols. In their study, it was stated that a good consensus mechanism can ensure error tolerance and increase the security of the blockchain system. Viriyasitavat & Hoonsopo (2019) in their paper entitled Blockchain Properties and Consensus in New Business Processes examines the consensus process in business process architecture.

1. Computational processes for creating credit are defined as extraction. Mining in cryptocurrencies means generating and verifying cryptocurrency transactions by solving mathematical problems.
2. Any computer connected to a blockchain network is called a node. Nodes are responsible for verifying, reviewing, and performing transaction calculations.

Their research shows that consensus leads to increased stability and credibility.

A review of consensus research shows that consensus protocols are an integral part of cryptocurrencies and all protocols have led to the validation and increase of the value of cryptocurrencies. In this section, cryptocurrencies are categorized by consensus protocols. The types of consensus algorithms and cryptocurrencies based on it are shown in Table 1. This content shows that all cryptocurrencies have a consensus mechanism and, cryptocurrencies have not been successful without a consensus mechanism and have not found an external existence. Cryptocurrencies are also categorized based on consensus protocols and consensus-related technology.

Cryptocurrencies are classified based on the mechanism of creation and consensus, including SHA-256, Ethash, Scrypt, Equihash, Crypto Note, X11, Lyra2. Bitcoin, Bitcoin Cash, Counterparty, Namecoin, Peercoin, Titcoin, Maza Coin cryptocurrencies in SHA-256 technology category, Ethereum, Ethereum classic cryptocurrencies in Ethash category, Aurora coin cryptocurrencies, Bitconnect, Bitcoin Gold, Coinye, Dogecoin, Litecoin in Scrypt category Zcash cryptocurrencies are in the Equihash category, Monero cryptocurrencies are in the Crypto Note category, Petro cryptocurrencies are in the X11 category, Taler cryptocurrencies are in the Lyra2 category, and Amba Coin, IOTA, Primecoin, Zcoin, Vert coin, Verge cryptocurrencies are in the category of other proof-of-work protocols. Also, Tron, Tezos, Steem, NXT, Grid coin, EOS.IO, Cardano cryptocurrencies are in the Proof of stake protocol group and Kodak Coin, INX, Bancor, Aventus, Augur, Maker DAO, Minds, The DAO cryptocurrencies are in the tokens group. And the cryptocurrencies of File coin, GNUTaler, Libra, Nano, NEO, Ripple, Tether, USDCoin are in the other categories.

Table1. Classification of cryptocurrencies

Algorithm group	Algorithm name	Available cryptocurrencies
Proof-based algorithms	Proof of work	Bitcoin, Litecoin, Ethereum Monero, Dash, Verge, Bitcoin Cash, Counterparty, Namecoin, Titcoin, MazaCoin
	Proof of stake	Cardano, Peercoin, Dash, Decred, Ethereum
	Proof of Authority	Kovan, Giveth, TomoChain, Rublix, SwarmCity, Colony, Rinkeby
	Proof of Reputation	GoChain
	Proof-of-Weight	Algorand, Filecoin, Chia
	Other methods of proof	Peercoin, Zcash, ZCoin, vertcoin, Bitcoin Gold, Petro, Dash, Auroracoin, Bitconnect, Coinye, Dogecoin
Voting-based algorithms	Delegated proof of stake	Steem , eos, BitShares ,Tron
	Byzantine Fault Tolerance	Hyperledger, Stellar, Ripple ,Neo
	Other methods of proving stake	Tezos, nxt, Gridcoin
New algorithms of consensus	Directed Acyclic Graph algorithm	IOTA ,NANO, ByteBall, Hashgraph, Neo*
Token	ERC20	USD Coin, KodakCoin, INX, Bancor, Aventus, Augur, Minds, The DAO

Source: cryptocurrencies websites available in the market.

*** Note:** Some cryptocurrencies use two or more consensus mechanisms.

2-2. Consensus on Bitcoin

Bitcoin consensus is formed from the rules designed by programmers in a process involving the modification of the original software and the implementation of new algorithms. In the free software model, ideas are voted on after discussing bug fixes or process optimization. Then the best idea that gets the highest votes is turned into software by miners, programmers and with the financial support of investors and payment system managers in the bitcoin market. Consensus in bitcoin is formed in two ways: first, that the people who do the extraction work correctly receive a reward, and second, that the distribution of the prize is randomly divided among the nodes. In the bitcoin creation process, several important features such as the authenticity of the passwords, the unique time stamp and the lack of a double spending process are the main factors in creating credibility and trust among users. Time stamp is based on a server that records the time of the first entry and exit and is a tool to prevent double spending of credit in the blockchain. The Time stamp uses algorithms to maintain the exact time of creation and transfer (Nakamoto, 2009). This tool has created trust among cryptocurrency traders, including Bitcoins.

Another vital component of Bitcoin authentication is the digital signature, which includes a function[1] that converts the two elements of the private key[2] and the public key[3] into one code. Bitcoin's reputation as a cryptocurrency depends on its digital signature (Feld et al., 2014). A digital signature is a valid proof of recognition (Authority) that uses an elliptic curve algorithm. This process is equivalent to the bank's action in validating paper money. As a result, this trust among cryptocurrency users has led to consensus.

1. An algorithm that, by combining public and private keys, verifies the authenticity of the message and the sender.
2. A confidential text collection, which is a combination of letters and numbers used to send or spend bitcoins in an e-wallet.
3. It is a set of combinations of letters and numbers obtained from the private key using mathematical cryptocurrencies functions.

The most important protocols that lead to the validity of bitcoins and similar cryptocurrencies are the Proof of work and stake proof process. In the process of proving work, people use electronic processors to solve difficult mathematical problems. Solving these problems has a reward system. They receive bitcoins in exchange for this processing (Das & Dutta, 2020). The hash equation must also be solvable at an appropriate time (Puzzle friendliness). In the Bitcoin creation mechanism, transactions and calculations must be done in such a way that the appropriate hash is extracted.

Proof of reserve and Merkle tree methods are among the most important methods that have led to the validation of bitcoin. According to the proof of reserve method, a certain amount of money is transferred in the network and then people in all block chains check this claim, and if the claim is confirmed, the validity of the collection will increase In the Merkle tree method, the number of real users and their validity are checked and verified by node members with an algorithm (Xu et al., 2018) .This protocol shows that when a user's transaction is invalidated on the network, that user is denied access to all nodes, thus eliminating the possibility of collusion for violating miners. Also, in Bitcoin, due to the existence of distributed Ledger and information transparency, there are no discriminatory policies in mining, and all this has led to an increase in its credibility (Killin, 2015).

Given the above, the technical methods of valuing Bitcoin led to consensus. Other cryptocurrencies such as Litecoin, Zcash, etc. also use consensus protocols. Now, considering the mechanisms of consensus in cryptocurrencies, the question arises whether cryptocurrencies have the same behavior with the same consensus tasks? To answer this question and better understand the behavior of cryptocurrencies in this article, time series clustering method has been used.

3. Research method

3-1. Time series clustering

Now, according to the results presented in the theoretical foundations of this article, there is a need for statistical study of the subject. To achieve this goal, the time series data of cryptocurrency prices is evaluated using time series clustering algorithm. Time series clustering is one of the common methods in time series data analysis. In the clustering process, the data are placed in a certain cluster with the most similarity using econometric models and data mining algorithms. In time series clustering method, algorithms such as K-Mean algorithm are mainly used to determine clusters (Ruiz et al., 2020). In these algorithms, the most important factor for clustering is the similarity criterion, which is defined as a mathematical function. In time series clustering method, mainly data mining is done as unsupervised data mining. For clustering in this data mining method, the default is not given to the algorithm. The main purpose of clustering algorithms is to create clusters with the most similarity within clusters and the least similarity between each cluster (Jahanpal et al., 2020)

The time series clustering process usually consists of three steps: determining the distance (quantifying the dissimilarity), determining the prototype, or in other words, summarizing the time series specifications in a cluster and then using the clustering algorithm to execute the cluster process. The main clustering algorithms in the third stage include two categories: Hierarchical algorithm and Partitional algorithm. Hierarchical algorithm is mainly used in models with smaller sample size (Javed et al., 2020)

3-1-1. Distance measures

To determine the similarity criterion, mainly mathematical functions such as Euclidean distance function or Dynamic time warping (DTW) function are used. Due to the limitations of the Euclidean distance function, such as forcing the time series data to be equal, the Dynamic time warping method is more

suitable for comparing time series. In this method, time series are grouped according to shape (Berndt & Cliffor, 1994). In Dynamic time warping function, actions such as selecting the pattern step, selecting the local cost matrix, creating computational ability for time series with unequal length and creating alignment and divergence functions as functions 1 and 2 are created. Then, by determining the general alignment or homogeneity core, the simulation between the existing time series is performed and by determining the function 1, the regional simulation is performed and this path continues again to obtain the optimal solutions. Functions 1 and 2 represent the minimum alignment or similarity and divergence functions. In this function, two time series x and y with lengths n and m are measured. In function number 3, the Global alignment kernel is calculated between two time series.

$$DTW(x,y) = min\pi \in \mathrm{A(n,m)Dx,y(\pi)} \quad (1)$$

$$DTW(x,y) = \sum_{i=1}^{\Pi} \varphi(\mathrm{x}_{\Pi 1^{(i)}}, \mathrm{y}_{\Pi 2^{(i)}}) \quad (2)$$

$$\kappa\mathrm{GA} = \sum\nolimits_{\pi \in A(n,m)} \prod_{i=1}^{\pi} K(\mathrm{x}_{\Pi 1^{(i)}}, \mathrm{y}_{\Pi 2^{(i)}}) \quad (3)$$

The alignment between several time series with different lengths is done with the above
pattern and the similarity criterion is obtained in this way.

3-1-2. Determining the prototype

Several methods have been developed to determine the prototype in clustering algorithms or machine learning languages. Common methods for determining these prototypes include the mean or median method, Partition around medoids, Dynamic time warping barycenter averaging, Shape extraction, and Fuzzy-based prototypes. In studies that use time series clustering to identify time series, the formal or mean method is used (Sarda-Espinosa, 2017).

3-1-3. Time series clustering algorithm

For the next step in time series clustering, using the hierarchical clustering algorithm requires the following steps:

First, hierarchical grouping should be done to create clusters.

Summarize the clusters.

The criterion of similarity between groups is measured and determined in pairs and groups.

Near and far pairs are determined by linkage methods.

Using a diagram, the best clustering number is extracted.

3-1-4. Evaluation of clusters

To select the optimal number of categories, the Cluster validity index is used after executing the clustering algorithm. In this method, the set of Silhouette, Dunn, Calinski-Harabasz, COP, Davies-Bouldin indicators has been used. Each of these indicators can lead to the selection of the best number of clusters (Wang & Zhang, 2007). The programming of this algorithm is taken from the algorithm designed by Marques in 2018 using Rstudio software.

3-1-5. Data

In this section, the cryptocurrencies used to evaluate time series clustering are described in Table 2. The data used in this research is the price of cryptocurrencies available in the market. These cryptocurrencies are divided into three groups: proof of work, proof of stake, and new methods of consensus. These data are daily and in US dollars from 2015 to 2020. The price of cryptocurrencies, which is presented in Table 2, has been extracted from coin Marketcap website (https://www.coinmarketcap.com/) as one of the cryptocurrency prices references as well as the website of each cryptocurrency.

Table 2. Variables used in clustering algorithm

raw	name of cryptocurrencies	Symbol	consensus protocols
1	Bitcoin	BTC	Pow
2	Binance Coin	BNB	DPoS
3	BitShares	BTS	DPoS
4	Dash	DASH	pow
5	EOS.IO	EOS	DPoS
6	Ethereum	ETH	Pow/ POS
7	Iota	IOTA	DAG
8	Litecoin	LTC	Pow
9	Monero	XMR	Pow
10	Neo	ANS	Practical Byzantine Fault Tolerance (PBFT
11	Nano	NANO	directed acyclic graph (DAG)
12	Namecoin	NMC	POW
13	Obyte		directed acyclic graph
14	Peercoin	PPC	PoS
15	PotCoin	POT	Proof of Stake Velocity
16	Ripple	XRP	Byzantine Fault Tolerance
17	Stellar	XLM	Federated Byzantine Agreement
18	Steem	steem	pos
19	Tron	TRX	DPOS
20	Zcash	ZEC	pow

Source: Cryptocurrencies websites available in the market**.**

4. Results of time series clustering algorithms

Control chart sequences are one of the statistical tools for monitoring clustering processes. When control charts are entered outside the range, it means that the trend of a time series has changed (Ghazanfari et al., 2008). Figure 1 shows the control diagrams created by RStudio software from the time series data of the selected cryptocurrencies. Control chart sequences are used to examine the time series shape within the defined range. If the time series process goes beyond the range defined in the algorithm, that time series is transferred to another category.

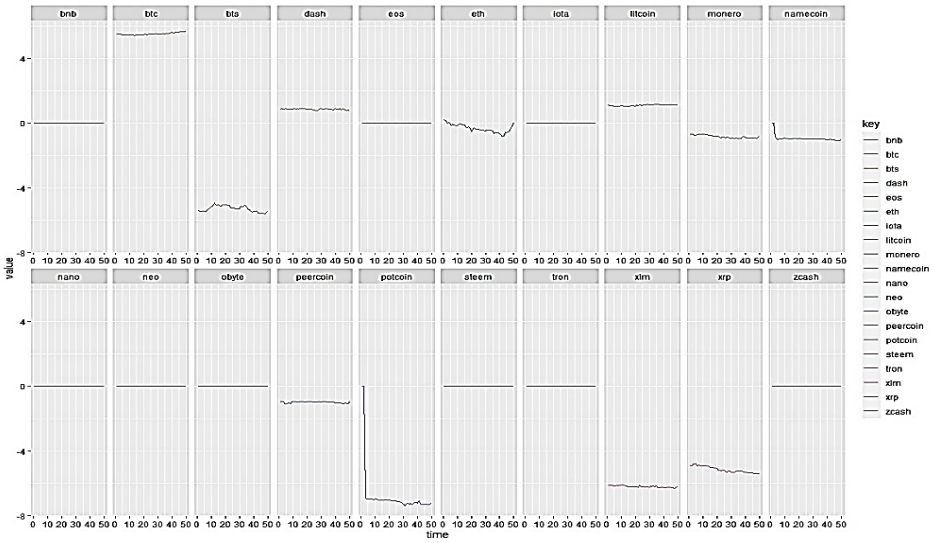

Figure 1. Control chart sequences
Source: Compiled by Authors

The results of time series clustering based on Figure 2 obtained by average distance method show that Bitcoin and Litecoin cryptocurrencies are in the same group. Also, Tron, Steem, Obyte, Neo, Nano, Iota, BNB and Eos are in their own category. Also, Stellar, Ethereum, Monero and Ripple are in the same group. These results show that cryptocurrencies with the same creation mechanism are in similar categories.

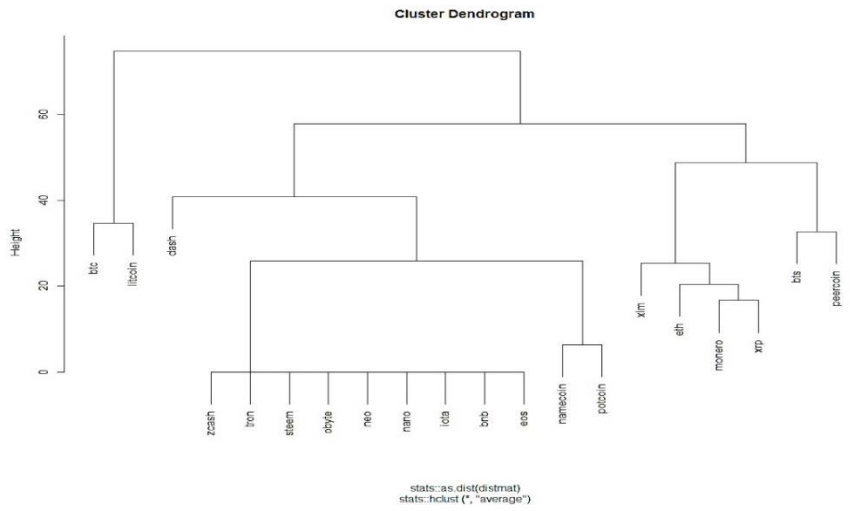

Figure 2. Time series clustering with average distance methodology
Source: compiled by Authors

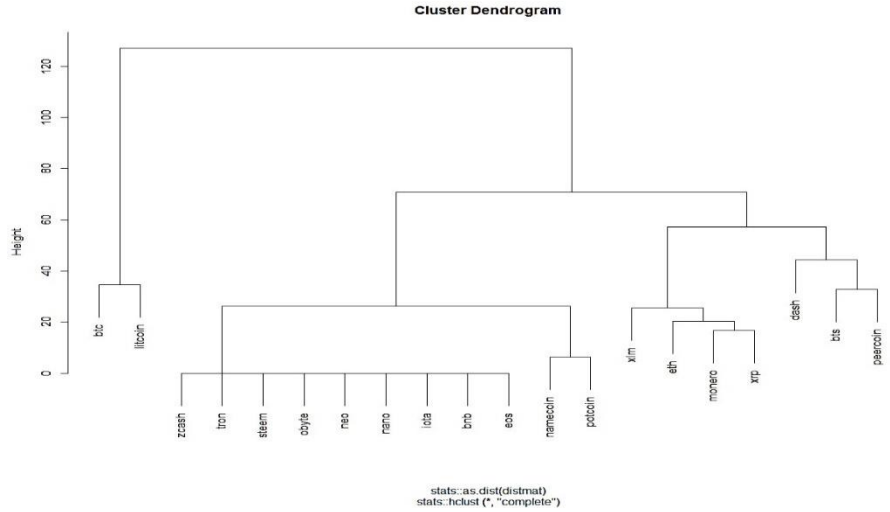

Figure 3. Time series clustering with complete distance methodology
Source: compiled by Authors

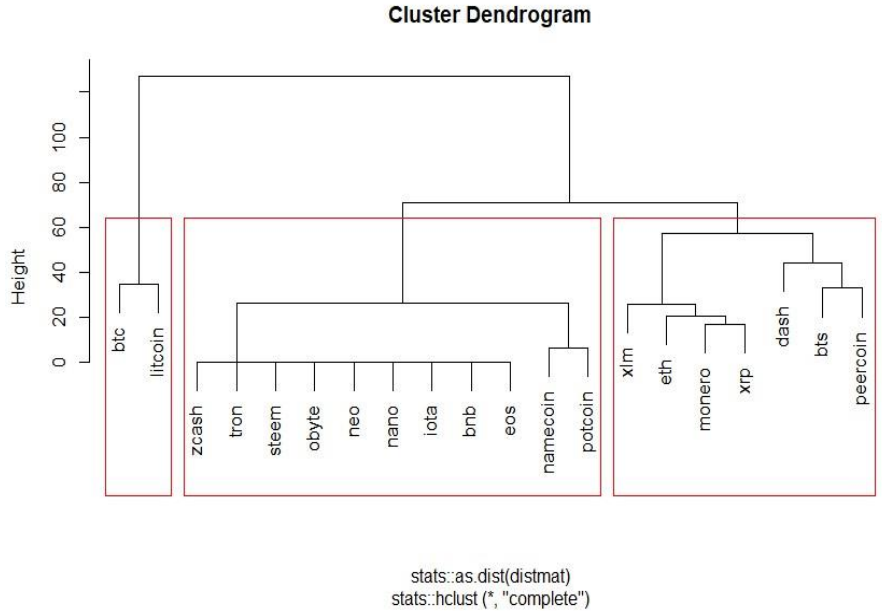

Figure 4. Classification of the results of clusters obtained from the algorithm
Source: compiled by Authors

The results of time series clustering based on Figure 3 obtained by complete distance method show that bitcoin and Litecoin cryptocurrencies are in the same group. Also, Tron, Steem, Obyte, IOTA, BNB and Eos are in their own category. With the improvement of the clustering algorithm and the use of the mean method, we see minor changes in the groupings. In Figure 4, grouping is also done. This figure shows that Bitcoin and Litecoin are in the same group. Ethereum, Ripple, Monero and stellar currencies are in a similar group. Bit Shares and Peercoin are grouped with Dash. These results indicate that according to the grouping performed, the cryptocurrencies behave similarly with the same consensus algorithms, including proof of work and proof of stakes, and a directed acyclic graph. Also, cryptocurrencies with the same creation mechanism show similar behavior over time and fall into similar groups.

5. Conclusion and recommendations

A review of consensus studies shows that consensus protocols are an integral part of cryptocurrencies and most consensus protocols have led to the validation and increase in the value of cryptocurrencies. The important point is that the consensus in cryptocurrencies is in the form of technical consensus resulting from algorithms and socio-economic relations resulting from these consensuses. Although the study of the mechanisms of creating cryptocurrencies and its relationship with their value needs further investigation, but in this study, the statistical evaluation of the time series clustering algorithm shows the accuracy of what is said about the consensus on value creation in cryptocurrencies.

The results of the time series clustering algorithm show that the Bitcoin and Litecoin cryptocurrencies are in the same group with the proof-of-work mechanism. Also, Zcash, Tron, Obyte, Neo, Iota and Eos cryptocurrencies mainly with new consensus mechanisms such as directed acyclic graph algorithm in a group and Stellar, Monero and Ripple cryptocurrencies with almost similar mechanisms (using two or more consensus mechanisms together). They are clustered in a group. These results indicate that the time series of cryptocurrencies with similar creation mechanisms and consensus have the same behavior over time and are in the same cluster.

Based on the results, one of the important recommendations for cryptocurrency market investors is to use three different groups of cryptocurrencies with different consensus mechanisms in the investment portfolio.

Cryptocurrencies, with newer consensus mechanisms, have had similar and positive price trends. These cryptocurrencies which have entered the market with consensus processes aimed at reforming monetary and banking systems, have a similar price behavior with each other, but have significant differences

with cryptocurrencies with older mechanisms. By choosing cryptocurrencies with new mechanisms, investors have put less risk into their portfolio. The use of three different groups of cryptocurrencies also reinforces this issue.

In addition, the classification of cryptocurrencies into groups with certain consensus mechanisms can be of great help to monetary authorities in managing the cryptocurrency market. The existence of newer consensus mechanisms that have reduced governments' concerns about energy consumption and money laundering indicates an important path for governments to enter the management of the cryptocurrency market. Cryptocurrencies with newer capabilities, which also show their behavior in the price trend, can be the basis for the government to enter them. New mechanisms, such as proof of stake, in addition to solving the problems of monetary and banking systems, have also been effective in preserving public capital, and their price trends have behaved quite positively and similarly. Therefore, monetary authorities are advised to pay more attention to cryptocurrencies with new mechanisms, instead of deciding to enter the market of traditional cryptocurrencies.

References

Aggarwal, S. Kumar, N. Chelliah, P. R. (2021). Cryptographic consensus mechanisms. Advances in Computers, 121: 211-226.

Al-Yahyaee, K. H. Mensi, W. Yoon, a. (2018). Efficiency, multifractality, and the long-memory property of the Bitcoin market: A comparative analysis with stock, currency, and gold markets, Finance Research Letters, 27: 228-234.

Arbelaitz O, Gurrutxaga I, Muguerza J. (2013). An extensive comparative study of cluster validity indices. Pattern Recognition, 46:243–256.

Aruna Sri, P.S.G, Lalitha Bhaskari, D. (2020). Blockchain technology for secure medical data sharing using consensus mechanism, Materialstoday.

Becker, J., Breuker, D., Heide, T., Holler, J., Rauer, H., Böhme, R. (2013). Can we afford integrity by proof-of-work? Scenarios inspired by the Bitcoin currency.In: Böhme, R. (Ed.), The Economics of Information Security and Privacy. Springer Berlin Heidelberg, 135–156.

Berndt, D., Clifford, J. (1994). Using Dynamic Time Warping to Find Patterns in Time Series, Proc. AAAI-94 Workshop Knowledge Discovery in Databases, 359-370.

Bhaskar, N. D., Chuen D. L. K. (2015). Chapter 3 - Bitcoin Mining Technology, Handbook of Digital Currency Bitcoin, Innovation, Financial Instruments, and Big Data, 45-65.

Brandvold, M., Molnár, P., Vagstad, K., Valstad, C. (2015). Price Discovery on Bitcoin Exchanges. Journal of International Financial Markets, Institutions and Money, 36:18-35 .

Briere, M. Oosterlinck, K. Szafarz, A. (2013). Virtual Currency, Tangible Return: Portfolio Diversification with Bitcoin. Journal of Asset Management,16(6): 365-373.

Bugday, A. Ozsoy, A. Öztaner, S. M. Sever, H. (2019). Creating consensus group using online learning-based reputation in blockchain networks, Pervasive and Mobile Computing, 59: 101056.

chaum D. fait A. & naor M. (1988). Untraceable Electronic Cash Conference on the Theory and Application of Cryptography CRYPTO: Advances in Cryptology- CRYPTO, 88: 319-327.

Cheah E., Fry J. (2015). Speculative bubbles in Bitcoin markets? An empirical investigation into the fundamental value of Bitcoin, Economics Letters,130: 32–36.

Corradi, F., Höfner, P. (2018). The disenchantment of Bitcoin: unveiling the myth of a digital currency, International Review of Sociology, 28:1.193-207.

Das, D. Dutta, A. (2020). Bitcoin's energy consumption: Is it the Achilles heel to miner's revenue? Economics Letters, 186: 108530.

Dong, Q.X., & Cooper, O. (2016). A peer-to-peer dynamic adaptive consensus reaching model for the group AHP decision making. European Journal of Operational Research, 250(2): 521-530.

Dong, Y.C., Li, C.C., Xu, Y.F., & Gu, X. (2015). Consensus-based group decision making under multi-granular unbalanced 2-tuple linguistic preference relations. Group Decision and Negotiation, 24(2): 217-242.

Dwork, C. Naor, M. (1992). Pricing via Processing or Combatting Junk Mail, Annual International Cryptology Conference, CRYPTO 1992: Advances in Cryptology- CRYPTO, 92: 139-147.

Dwyer, G. P. (2015). The economics of Bitcoin and similar private digital currencies, Journal of Financial Stability, 17: 81-91.

Feld, S., Schönfeld, M., Werner, M. (2014). Analyzing the Deployment of Bitcoin's P2P Network under an AS-level Perspective, Procedia Computer Science, 32: 1121-1126.

Feng, J. Zhao, X. Chen, K. Zhao, F. Zhang, G. (2020). Towards random-honest miners' selection and multi-blocks creation: Proof-of-negotiation consensus mechanism in blockchain networks" Future Generation Computer Systems, 105: 248-258.

Ghazanfari, M. Alaeddini, A. Akhavan Niaki, S. T. Aryanezhad, M. (2008). A clustering approach to identify the time of a step change in Shewhart control charts, Quality and Reliability Engineering, 24(7):765-778.

Gilad, Y. Hemo, R. Micali S., Vlachos, G., Zeldovich, N. (2017). Algorand: Scaling byzantine agreements for cryptocurrencies, in: Proceedings of the 26th Symposium on Operating Systems Principles, ACM, 51–68.

Gramoli, V. (2020). From blockchain consensus back to Byzantine consensus, Future Generation Computer Systems, 107: 760-769.

Horra, L. P.de l., Fuente, G. l., Perote, J. (2019). The drivers of Bitcoin demand: A short and long-run analysis", International Review of Financial Analysis, 62: 21-34.

Hosseini Bamakan S. M. Motavali, A. Bondarti, A. B. (2020). A survey of blockchain consensus algorithms performance evaluation criteria, Expert Systems with Applications, 154, 15: 113385.

Javed, A. Lee, B. S. Rizzo, D. M. (2020). A benchmark study on time series clustering, Machine Learning with Applications 1, 100001, 1-13.

Ji, Q., Bouri E., Gupta, R., Roubaud, D. (2018). Network causality structures among Bitcoin and other financial assets: A directed acyclic graph approach, The Quarterly Review of Economics and Finance, 70: 203-213.

johnpaul, c., prasad, m. v., nickolas, s., & gangadharan, g. (2020). trendlets: a novel probabilistic representational structure for clustering the time series data. expert systems with applications,145, 113119.

Kacprzyk, J., & Fedrizzi, M. (1988). A 'soft' measure of consensus in the setting of partial (fuzzy) preferences. European Journal of Operational Research, 34: 316–325.

Killeen, A. (2015). The Confluence of Bitcoin and the Global Sharing Economy, Chapter 24, Handbook of Digital Currency Bitcoin, Innovation, Financial Instruments, and Big Data, 485-503.

Lafourcade, P. Lombard-Platet, M. (2020). About blockchain interoperability, Information Processing Letters, 161, 105976.

Levin, R. B. O'Brien,A. A. Zuberi, M. M. (2015). chapter 17 - Real Regulation of Virtual Currencies, Handbook of Digital Currency Bitcoin, Innovation, Financial Instruments, and Big Data, 327-360.

Liu, Yujia. Liang, Changyong. Chiclana, Francisco. Wu, Jian. (2017). A trust induced recommendation mechanism for reaching consensus in group decision making. Knowledge-Based Systems,119: 221-231.

Matta, M. Lunesu, I. Marchesi, M. (2015). Bitcoin Spread Prediction Using Social and Web Search Media. Università degli Studi di Cagliari Piazza

d'Armi, 09123 Cagliari, Italy, Conference: Workshop Deep Content Analytics Techniques for Personalized & Intelligent Services.

Oliveira, M. T. d. Reis, L.H.A. Medeiros, D. S.V. Carrano, R. C. Olabarriaga, S. D. D. Mattosa, M.F. (2020). Blockchain reputation-based consensus: A scalable and resilient mechanism for distributed mistrusting applications, Computer Networks, 179: 107367.

Pieters G., Vivanco, S. (2017). Financial regulations and price inconsistencies across Bitcoin markets, Information Economics and Policy, 0 00, 1–14.

Pournaras, E. (2020). Proof of witness presence: Blockchain consensus for augmented democracy in smart cities, Journal of Parallel and Distributed Computing, 145:160-175.

Roth, N. (2015). An Architectural Assessment of Bitcoin: Using the Systems Modeling Language, Procedia Computer Science, 44: 527-536.

Ruiz, L.G.B., Pegalajar, M.C. Arcucci, R. Molina-Solana, M. (2020). A Time-Series Clustering Methodology for Knowledge Extraction in Energy Consumption Data, Expert Systems with Applications, 160: 113731.

Sarda-Espinosa A. (2017). Comparing Time-Series Clustering Algorithms in R Using the dtwclust Package, 1–41.

Segendorf, B. (2014). What is bitcoin? Sveriges Riksbank Econ, Rev. 2, 71–87.

Shin, D. H, (2008). Understanding purchasing behaviors in a virtual economy: Consumer behavior involving virtual currency in Web 2.0 communities, Interacting with Computers, 20: 433-446.

Systems with Applications, 145, Article 113119.

Troster, V., Tiwari A. K., Shahbaz M., Macedo D. N. (2019). Bitcoin returns and risk: A general GARCH and GAS analysis. Finance Research Letters, 30: 187-193.

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, 21: Iss. 1, Article 13 .

Viriyasitavat, W. Hoonsopon, D. (2019). Blockchain characteristics and consensus in modern business processes, Journal of Industrial Information Integration, 13, 32-39.

Wang W., Zhang Y. (2007). On fuzzy cluster validity indices. Fuzzy sets and systems, 158(19): 2095–2117.

Xu, J., Wei, L., Zhang, Y., Wang, A. Zhou, F. Gao, C. (2018). Dynamic Fully Homomorphic encryption-based Merkle Tree for lightweight streaming authenticated data structures, Journal of Network and Computer Applications, 107: 1.113-124.

Yu, B. Liu, J. Nepal, S. Yu, J. Rimba, P. (2019). Proof-of-QoS: QoS Based Blockchain Consensus Protocol, Computers & Security, 87: 101580.

Zhang, H.J., Zhao, S.H., Kou, G., Li, C.C., Dong, Y.C., & Herrera, F. (2020). An overview on feedback mechanisms with minimum adjustment or cost in consensus reaching in group decision making: Research paradigms and challenges. Information Fusion, 60: 65-79.

Zhang, S. Lee, J. H. (2020). Analysis of the main consensus protocols of blockchain, ICT Express, 6(2): 93-97.