WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Cryptocurrency

Dr. Shubhangi DC [a], Dr. Basavaraj Gadgay [b], Ayesha Mohammadi Qureshi [c], Dr. M.A Waheed [d]

[a,d] *Professor, Department of Computer Science and Engineering, VTU Centre for PG Studies, Kalaburagi, Karnataka.*
[b] *Regional Director, VTU Regional Office, Kalaburagi, Karnataka.*
[c] *Student, Department of Computer Science and Engineering, VTU Centre for PG Studies, Kalaburagi, Karnataka.*

ABSTRACT

Despite the widespread interest in cryptocurrencies and the many studies into DLT, very little has been done to examine cryptocurrencies themselves. This paper presents a landscape of a subset of cryptocurrencies in order to give business and technical analysis to practitioners in light of the fast growing quantity and variety of cryptocurrencies. Specific details are provided that shed light on usual cryptocurrency's layout and operation in business world. The study's created landscape reports current status of cryptocurrencies and may be utilized as a foundation for further cryptocurrency research and analysis.

Keywords- Cryptocurrency, Blockchain, Distributed Ledger Technology.

1. Introduction

Bitcoin and other cryptocurrencies are relatively new types of digital cash that provide quick and easy transactions between buyers and sellers inside the same secure network. Invented by Satoshi Nakamoto in 2008, it employs a distributed ledger called a "blockchain" to ensure the safety of financial transactions. The cryptocurrency sector has evolved unexpectedly and at an unprecedented rate in recent years. It has helped fund a new kind of applied research, the full extent of whose promise is not yet known. However, in its present state, it serves a purpose somewhat dissimilar to that of more conventional assets. The Blockchain technique is a bitcoin explorer service that maintains a public ledger of all past transactions, so guaranteeing the safety and transparency of any and all cryptocurrency dealings. Since decentralized networks lack a central authority to provide privileges, users are protected against being scammed. The data in a blockchain consists of interconnected records called blocks, which are encrypted against tampering and are added to continuously. Due in large part to the blockchain system, which is widely regarded as a key component of the continuing global revolution, cryptocurrencies have seen a dramatic increase in both quality and popularity within monetary systems in recent years. Since Nakamoto's introduction of Bitcoin in 2008, blockchain technology's explosive development has been a driving force in the evolution and improvement of the financial sector. Bitcoins are widely hailed as the world's first decentralized, peer-to-peer digital money. Domain "Bitcoin.org" was registered on August 13, 2008, and the name Bitcoin was approved by Bitcoin's cryptography creator that same day. Electronic money shared between users. Bitcoins are a forward-thinking medium of exchange. While many other cryptocurrencies, such as Ethereum, Ripple, Litecoin, etc., have since been registered, Bitcoin still stands out as the most valuable, with a market value of $1.7 trillion [8; 3]. Multiple experts agree that Bitcoin, Ethereum, Ripple, or Litecoin are the most prominent cryptocurrencies now in use. As a stand-alone investment, Ripple offers the highest profits, following Litecoin & Bitcoin. However, Ripple also has the biggest volatility, followed by Litecoin and Bitcoin.

2. Literature Review

2.1 Cryptocurrencies overview:

[1].Geiregat (2018), An unregulated, decentralized, and entirely anonymous method of payments direct between individual to individual with no bank account or card, Bitcoin was created by a group of researchers & activists worried about security and individual liberty. Decentralization, absence of central oversight, and anonymity are three defining features of cryptocurrencies. [2].Nakamoto (2008), focused upon issues of transaction privacy and security, and offered a well-considered solution in form of blockchain to address them. The blockchain's distributed ledger system is original inspiration for decentralized character of cryptocurrency. [3].Foley et al. (2019) prove that a significant percentage of Bitcoin users (around a quarter) may have engaged in criminal behavior. According to their research, Bitcoin might be involved in annual criminal activities worth over $76 billion. They also provide evidence that the proportion of Bitcoin transactions that are conducted illegally has decreased as both Bitcoin and other, more anonymous cryptocurrencies have gained popularity. Investing in cryptocurrencies has a number of real-world challenges, including volatility, low market liquidity, theft, fraud, ransomware, and potentially onerous government regulation. There are no safeguards, liability provisions, or insurance for cryptocurrency transactions since industry is unregulated, decentralized, untraceable, & anonymous. [4]. Radovanov et al. (2018), The unit values, market capitalizations, and user applications of these cryptocurrencies are vastly distinct from one another, despite fact that there is some degree of link between them. Bitcoin

is the most well-known, widely used, and technically advanced cryptocurrency to date. [5]. Velde, (2013), Value has increased by a factor of 10 between 2013 and 2018 since the launch in 2009. Bitcoin's value in the 2010s is seen in Figure 1 in comparison to Dow Jones Industrial Average. The tremendous rise and fall of Bitcoin's value during the cryptocurrency meltdown of January 2018 is clearly seen. [6]. In his 2008 manifesto, Satoshi Nakamoto introduced Bitcoin and the blockchain as a way to make low-cost, secure payments that did not need a trusted third party or central authority.

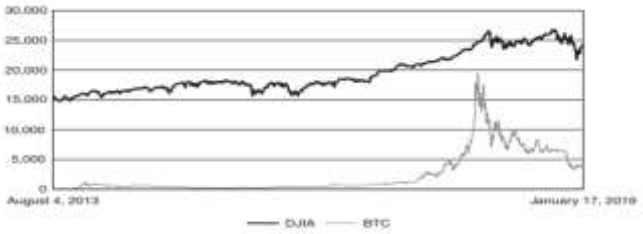

Fig 1: Depicts the Bitcoin price vs the Dow Jones Industrial Average

3. Objective Of the Study

The objective of the study is:

- Examining whether or not Bitcoin, Ethereum, Litecoin, and Ripple values share any discernible pattern.
- See if there's a link between Bitcoin and other cryptocurrencies by comparing its price to that of Ethereum, Litecoin, and Ripple.

4. Research Methodology

The research makes use of both primary and secondary data gathered from a variety of online resources and surveys. Secondary data includes the average daily price of all cryptocurrencies under consideration from 2015–16 to 2020–21. To serve as a main data point, West Bengal was selected. The grade and quality of the study is raised as a result of the outlining and encapsulation of the data. You may find these resources at book stores, on the internet, etc.

Table 1: Model Summary

MODEL	R	R SQUARE		ADJUSTED R SQUARE	STD. ERROR OF THE ESTIMATE
1	.887A	.787		.786	3571.4861
A. PREDICTORS: (CONSTANT), RIPPLE_PRICE, ETHEREUM_PRICE, LITECOIN_PRICE					

The regression model's goodness-of-fit to data is shown in table 1, the model summary table. R, often known as multiple correlation coefficients, is a statistical measure of the accuracy with which a model can predict its dependent variable. The multiple correlation coefficient, shown by the number R, is 0.887, as shown in Table 3, indicating a high degree of accuracy in predictions. R Square, also known as the coefficient of determination, is a measure of the extent to which one independent variable accounts for variation in a set of dependent variables. The R Square score of 0.787 shows that the variability in our dependent variable is explained by independent factors.

Table 2 : ANOVA

Model		Sum of Squares	Df	Mean Square	F	Sig.
1	Regression	77417938168.659	3	25805979389.553	2023.124	.000[b]
	Residual	20995574122.983	1646	12755512.833		
	Total	98413512291.641	1649			
a. Dependent Variable: BITCOIN_PRICE						
b. Predictors: (Constant), RIPPLE_PRICE, ETHEREUM_PRICE, LITECOIN_PRICE						

Table 2 shows the results of an analysis of variance performed to see whether the study's regression model is a good match for data. The p-value for the regression model's ability to predict dependent variable is less than 0.05, as seen in table provided.

Table 3 : Coefficient

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	*Std. Error*	*Beta*		
1	(Constant)	2498.721	139.992		17.849	.000
	ETHEREUM_PRICE	23.360	.472	.954	49.458	.000
	LITECOIN_PRICE	26.314	3.415	.190	7.705	.000
	RIPPLE_PRICE	-10782.54	469.255	-.427	-22.97	.000

a. Dependent Variable: BITCOIN_PRICE

Table 3 shows the coefficients, which are what you need to forecast dependent variable as from independent factors and to determine whether or not the independent variables are substantially contributing to model of research. You can see how the "Ethereum Price," "Litecoin Price," and "Ripple Price" are contributing to people's happiness in the above table. Each of these factors is statistically significant (because its value is less than 0.05, or 0.000) and may be used to construct regression model (see below).:

BITCOIN PRICE=2498.721+.954(ETHEREUM PRICE) + .190 (LITECOIN PRICE) - .427 (RIPPLE PRICE)

5. Results And Analysis

We present just the domains, consensus procedures, issuance techniques, and popularity data that is important because to space constraints. The remaining research findings will be released at a later date. Several use cases for the chosen cryptocurrencies are shown in Fig. 1. There is a predominant emphasis on monetary issues among cryptocurrency ventures. Much research effort is focused on study platforms for developing decentralized apps and payment, which is a method of payment for a genuine commercial transaction, whereas currency is solely for bitcoin. Both safety & scalability might be affected by consensus process used.

Fig. 1: Domain.

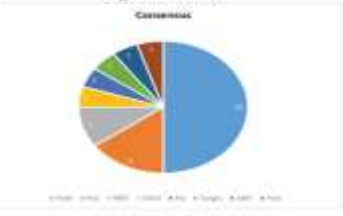

Fig. 2: Consensus protocol.

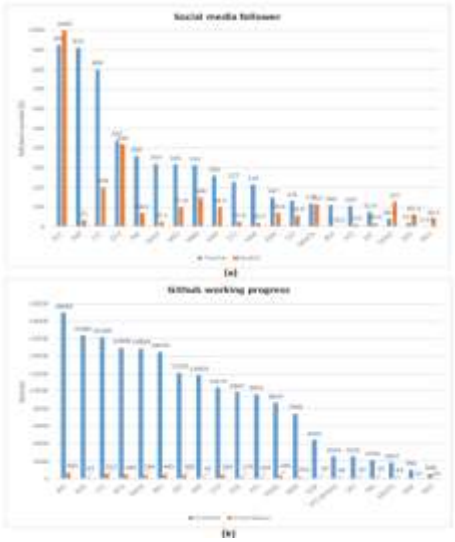

Fig 2: Popularity attributes.

In eight of the cryptocurrencies we looked at, the sponsors and founding team have access to a sizable currency supply that will be used to fund future growth and research. Reducing the reward is another kind of distribution approach that might help keep cryptocurrency prices stable. The mining process often uses a block reward mechanism to distribute newly created cash. The genesis block is where the code is used to create the premining currency, which can only be traded for other cryptocurrencies. You can gauge interest in cryptocurrency by looking at its popularity on social media platforms like Twitter and Reddit, and you can gauge optimism about a project's future success, the pace at which it is adding new features, and the likelihood that it is a scam by looking at its activity on the code repository GitHub.

Table 4: Issuance Attributes.

Coin	Issuance policy	Issuance method
BTC	Reward halves every four years.	mining
XRP	Founders 20%.	premining
ETH	Contributors 60 million.	mining
XLM	Individuals-50%, partners-25%, BTC&XRP holders-20%, Stellar.org-5%.	premining
BCH	Reward halving every four years.	mining
EOS	"Founders' Tokens" 10%.	premining
BSV	Reward halving every four years.	mining
LTC	N/A	mining
TRX	N/A	premining
ADA	Cardano community 20%.	mining
XMR	Smoothness of the emission using a specific formula.	mining
XEM	N/A	mining
MIOTA	N/A	premining
DASH	7% reduction of the supply per year.	mining
ETC	N/A	mining
NEO	50 million for supporters and 50 million for NEO Council. Mining generates gas decreasing every year.	mining & premining
ZEC	Founders 10%.	mining
DOGE	Inflationary coin with no production limit.	mining
XTZ	N/A	mining & bond
VET	Public token sale-41%, private investors-9%, enterprise investors-23%, co-founders-5%, continuous operation-12%,business case development-10%.	mining & premining

6. Experiment Results

We sourced all of our numbers from the ever-reliable Cryptocurrency Market Capitalizations1. Cryptocurrencies developed using the same language were downloaded for analysis. In this study, we focused on comparing four distinct digital currencies. One of the cryptocurrencies we used to prove the viability of our method had been fork of other one. There is no connection between the other two coins we picked at random. Therefore, we anticipate a significantly greater level of resemblance between the forked cryptocurrencies and one another than between the forked cryptocurrencies & other non-related currency. Table 5 shows that the degree of similarity between any two crypto projects is between 54.3 and 74.3 percent, whereas the degree of similarity between the source codes of a branched cryptocurrency & original cryptocurrency is between 82.9 and 84.1 percent.

Table 5: The Similarity in each cryptocurrency

	JPlag	SIM	Fuzzy Hash
Coin A - Coin A′	82.9%	83.1%	84.1%
Coin A - Coin B	54.3%	59.3%	60.2%
Coin B - Coin C	71.9%	72.7%	74.3%
Coin C - Coin A	64.6%	68.7%	67.4%

7. Research Materials And Methods

We'll evaluate the method's viability using Bitcoin as an example due to the lack of a Litecoin API that allowed for fast enough data collecting. The Bitcoin & Litecoin protocols are quite similar. Just four key distinctions separate them from one another: Bitcoin's Proof-of-work is encrypted using SHA256; Litecoin's is script; Litecoin's transaction times are four times those of Bitcoin; and Litecoin has four times as many coins in circulation. Digital currency Bitcoin operates on a blockchain-based peer-to-peer network. [5] The term "blockchain" refers to the series of linked records that make up the system (Fig. 3). Users throughout the network have copied this structure to their own hard disks. The system's essential data, including transaction records, is stored in blocks, which are connected by hash values.

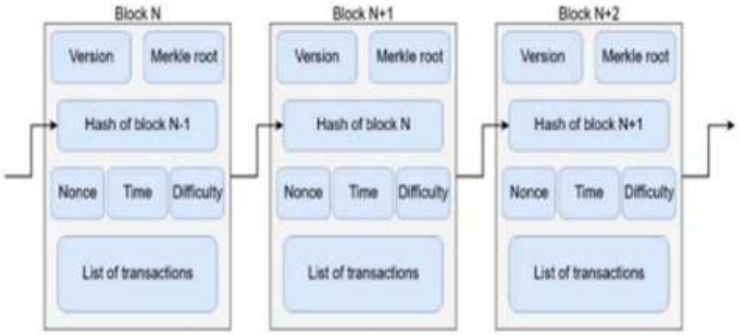

Fig 3: Blockchain.

Blocks consist of a magic number (an identifier for the blockchain network), a block size, a block header, the total number of block data, & list of records detailing those transactions. All data is stored in a binary form, & special decoding software is needed to decipher it.

Field	Description	Size
Magic no	Value always 0xD9B4BEF9	4 bytes
Blocksize	Number of bytes	4 bytes
Blockheader	Consists of 6 items	80 bytes
Transaction counter	Positive integer	1-9 bytes
Transactions	The list of transactions	variable

Block versions, the hash of the preceding block (HashPrevBlock), hash of all transactions in block (HashMerkleRoot), the time the block was generated, the number of bits representing difficulty of computing its hash, and creation time are all part of blockheader structure. It is the miners' job to alter this field, known as the nonce, in order to provide a unique hash for this block.

Table 6: Block Structure

Field	Description	Size
Version	Block version number	4 bytes
HashPrevBlock	Hash of the previous blockheader	32 bytes
HashMerkleRoot	Hash based on the transactions in this block	32 bytes
Time	Timestamp(sec) since 01.01.1970 00:00 UTC	4 bytes
Bits	Current target in compact format	4 bytes
Nonce	Using for generating current block hash	4 bytes

In order to keep track of user-to-user monetary dealings, each such exchange is recorded as a new entry in a block. Table 7 lays out the various parts that make up a single transaction, including the version, the flag indicating whether or not witnesses were present (if it is always equal to 0001, witnesses were present), the total count of currency senders, record of entrances (senders),amount of currency recipients, collection of exits (receivers), list of witnesses, & time.

Table 7: Transaction Structure

Field	Description	Size
Version	Currently 1	4 bytes
Flag	If present, always 0001	2 byte array
In-counter	Positive integer	1-9 bytes
Inputs	The list of inputs	variable
Out-counter	Positive integer	1-9 bytes
Outputs	The list of outputs	variable
Witnesses	A list of witnesses, 1 for each input	variable
Lock time	Timestamp when transaction is final	4 bytes

The matching records may be found in the input and output lists. The entry's structure (Table 8) includes the sender's address, encoded in scriptSig (the script also includes information about the recipient's wallet's real balance).

Table 8 : Transaction Input Structure

Field	Description	Size
Previous transaction hash	doubled SHA256-hashed	32 bytes
Previous txout-index	Non negative integer indexing an output	4 bytes
Txin-script length	Non negative integer	1-9 bytes
ScriptSig	Contains information about input addrs	variable
Sequence no	Irrelevant unless tx's lock time is > 0	4 bytes

Using scriptPubKey, output record structure (Table 9) encodes recipient's address & amount received.

Table 9 : Transaction Output Structure

Field	Description	Size
Value	Non negative integer (number of Satoshis)	32 bytes
Txout-script length	Non negative integer	1-9 bytes
ScriptPubKey	Contains information about output addrs	variable

The following diagram, therefore, may serve as a representation of the blockchain's underlying structure:

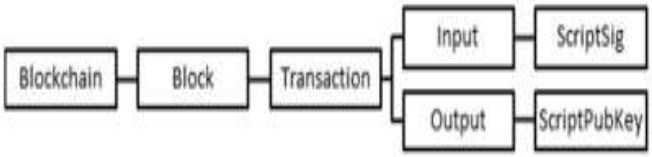

Fig 4: Blockchain scheme.

The API is used to decrypt scriptSig and scriptPubKey, which yields the necessary data for the procedure. Every cryptocurrency "wallet" is really a pair of keys, one that is kept secret and one that may be shared with others. The owner alone has access to the private key, but anybody with access to the public key may conduct financial transactions. An asymmetric private key encryption technique is used to get the public key, making the two inseparable. There is no practical way to reverse-engineer the private key into the public key using the technique, hence the monies are safe. [10] Given the length of a Bitcoin public key, a public address is used to represent it. Hashes of public keys are used to create public addresses. The initial value of a brand-new digital wallet is zero.

Each wallet falls into one of three categories: active, inactive, and forgotten. Hot wallets are online wallets that can be accessed from any device; with them, you don't have to download the complete blockchain. "Cold" wallets are offline Bitcoin wallets that require installing software and storing the whole blockchain on a physical device like a thumb drive.

Wallets that have been left unused for an extended period of time are considered abandoned. Since the descriptions of "cold," "hot," and "abandoned" wallets imply that these wallets have distinct transaction activity, we may evaluate belonging of wallets to such kinds by examining their activity, for instance to locate wallets that are likely to have been abandoned.

Concise explanation of the procedure:

1) A database for wallets is being created.

a) The database stores following data for each wallet: wallet's address & time of its most recent transaction.

b) In order to add new wallet to list, it must first be verified that it does not already exist in the database..

2) Using the defined criteria, examine the produced data set. This method is written in Python 3.7 and runs on Linux. The code was written in Python, and it makes use of the requests, json, and pymysql libraries. For safekeeping, wallet details were entered into a MySQL database. The blockchain.info API, which returns results in JSON format, was utilized to get at the blockchain data.

Detailed explanation on how to put up a databset of wallets:

The analysis of the blockchain's blocks begins at its head. The API receives data in JSON format about each block. The JSON data is being converted into Python's native data types using the library's in-built support for the format. The list serves as a repository for addresses and associated data. Then, the block's transactions are all making phone calls. After a transaction's outputs have been recorded, any input addresses that were used will be stored. The block's received data list is now unloading in database. From 3 seconds to 9 seconds is the duration of the whole cycle.

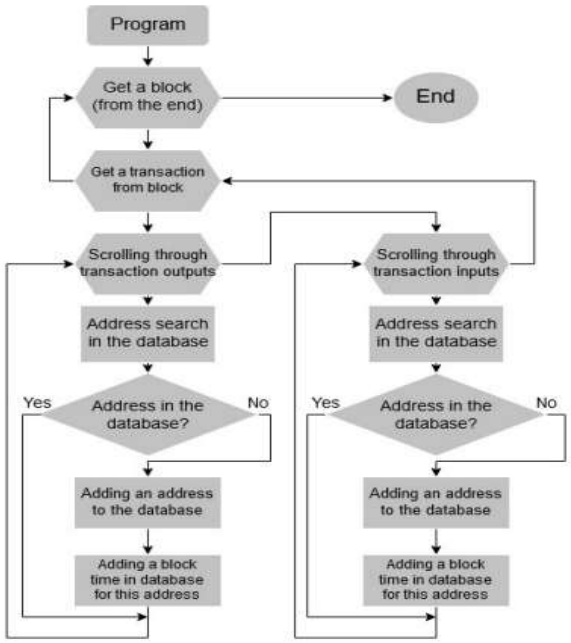

Fig 5: Scheme of the algorithm

Following this, you may use the API to get each wallet's balance by sending a request to wallet's unique address. Additionally, JSON representations of the data are made available.

8. Results

In the first place, the data shown above serves as proof that the stated procedure is effective. The present database was built over the course of around 29 hours. From 2019-03-17 00:13 (height: 581026) to 2019-11-13 19:16 (height: 603597), the database containing statistics for 52017587 wallets was collected and evaluated thanks to the application running at that time. The number of wallets that have not been used to make a purchase since November 13 at 19:16 (as seen in Fig. 6) is shown below. For the chosen time period, it is shown that the dependency is linear. This suggests that volume of Bitcoin transactions has been rather stable over the last year, with no obvious peaks or valleys.

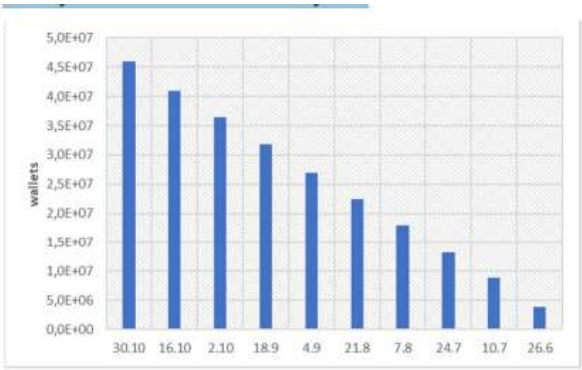

Fig 6: Inactive wallets with non-zero balance

Wallets with no balance as of 13.11.2019 19:16 are shown in the following figure (Fig. 7), which also displays the period span during which no transactions were made using these wallets.

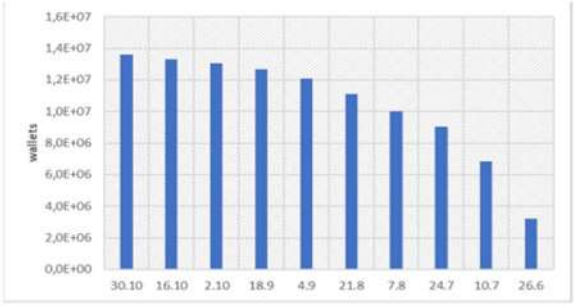

Fig 7: Inactive wallets with zero balance

Here, after ten weeks, the growth in number of empty wallets slows down noticeably. This implies that after around 10 weeks, the majority of wallets are deactivated and can no longer be used in any transactions.

The percentage of wallets with no balance compared to total number of wallets on wall as of November 13 at 19:16 UTC is then plotted.

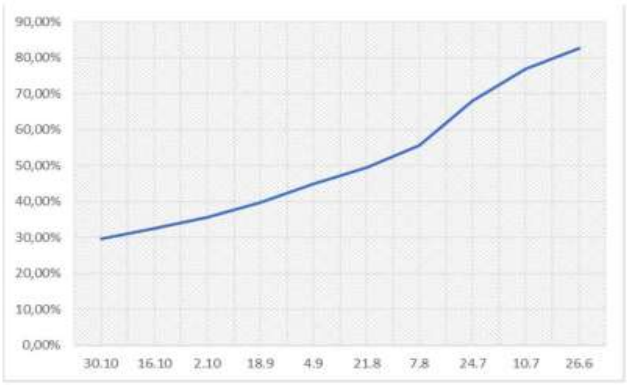

Fig 8: Ratio of inactive wallets

When this graph is superimposed on the preceding one, we see that wallets that haven't been used in more than 10 weeks tend to have empty balances. Currency depositories which are not actively engaged in transactions may also be identified using this graph (they account for around 8% of the total throughout the 20-week timeframe).

9. Conclusion

For those unfamiliar, cryptocurrency refers to a digital currency built on the decentralized ledger technology known as the blockchain. First introduced in 2008, it was created by Satoshi Nakamoto. In 2008, the domain name Bitcoin.org was registered as the birthplace of the world's first cryptocurrency. The Bitcoin market capitalization accounts for 66% of the whole cryptocurrency market, making it among the largest cryptocurrencies. Bitcoin, Ethereum, Litecoin, and Ripple are the four most popular cryptocurrencies used in this study. The prices of several cryptocurrencies have been discovered to be very correlated. The investigation also revealed a correlation between Bitcoin and altcoin values. It is generally assumed that Bitcoin prices would increase in tandem with those of Ethereum and Litecoin, but that if Ripple's value increases, Bitcoin's value will decrease. It's safe to say that social influence has a significant role in determining cryptocurrency prices, however other variables, such as the price and performance of competing cryptocurrencies, may play a role as well. Further, the findings demonstrate the value of doing even modest studies and research before investing in cryptocurrencies.

REFERENCES

Spithoven, A. (2019). Theory and reality of cryptocurrency governance. Journal of Economic Issues, 53(2), 385-393. DOI-: https://doi.org/10.1080/00213624.2019.1594518.

“Distributed ledger technology: beyond blockchain,” Tech. Rep., 2016, uK Government Chief Scientific Adviser.

Andrianto, Y. and Diputra, Y. (2017), “The effect of cryptocurrency on investment portfolio effectiveness”, Journal of Finance and Accounting, Vol. 5 No. 6, pp. 229-238.

Anyfantaki, S., Arvanitis, S. and Topaloglou, N. (2018), “Diversification, integration and cryptocurrency market”, working paper, Bank of Greece, Athens, March 1.

Biais, B., Bisière, C., Bouvard, M. and Casamatta, C. (2019), “The blockchain folk theorem”, Review of Financial Studies, Vol. 32 No. 5, pp. 1662-1715.

Borri, N. (2019), “Conditional tail-risk in cryptocurrency markets”, Journal of Empirical Finance, Vol. 50 No. C, pp. 1-19.

H. Adams, N. Zinsmeister, and D. Robinson, “Uniswap v2 core,” tech. rep., 2020.

M. Egorov, “Stableswap-efficient mechanism for stablecoin liquidity,” tech. rep., 2019.