World Journal of Advanced Engineering Technology and Sciences

eISSN: 2582-8266

Cross Ref DOI: 10.30574/wjaets

Journal homepage: https://wjaets.com/

(REVIEW ARTICLE)

Check for updates

Digital currency banking using block chain technology

N Sanchiga Nandhini * and Padmapriya Arumugam

Department of Computer Science, Alagappa University, Tamil Nadu, India.

World Journal of Advanced Engineering Technology and Sciences, 2023, 08(01), 053–061

Publication history: Received on 27 November 2022; revised on 08 January 2023; accepted on 10 January 2023

Article DOI: https://doi.org/10.30574/wjaets.2023.8.1.0011

Abstract

Banks are now the almost sole source of confidence for internet commerce when it comes to processing electronic payments. With a peer-to-peer electronic currency, payments can be conducted online directly between parties without going via a banking organisation. While signatures do contribute in some ways, the main benefits are lost if a trustworthy third party is still required to prevent double spending. So in this project we can implement Bit Coin based banking system can be implemented leveraging the technologies of block chains to create hash functions. Bit coin is a crypto currency, which is not supported by the government or central bank of any nation. It can be traded for goods or services with vendors who the use of bit coins payment. These bit coins are the blocks of secure data. It takes a lot of CPU resources to securely verify each individual transaction as the data is passed from one person to another while also spending money on the transaction.

The P2P network monitors and verifies the moving of bit coins between users. Bit coin is more secure than other currencies in terms of cryptographic implementation, and it is difficult to carry out fraudulent transactions. In a Bit coin transaction, the block chain will connect every user on the network, and each time a transaction is entered, the network will broadcast it to all other users after it has been validated. The network will also have a copy of every transaction. The network will group transaction data into blocks and broadcast them throughout the network rather than preserving any transactions in the block chain. Every block in this chain will link to the one before it, which is known as the genesis block. Peer-to-peer networks and a consensus mechanism are used in block chain systems, eliminating the potential of data alteration.

Keywords: Financial sector; Bit-coin transaction; Block chain; P2P network; Crypto currency

1. Introduction

A block chain is a distributed database that is shared by every node in a computer network. A block chain serves as a digital database for the storage of data. Block chains play a crucial role in maintaining a secure and decentralised record of transactions in crypto currency systems like Bit coin. A block chain is unique in that it promotes confidence without the need for a trustworthy third party by guaranteeing the security and integrity of a record of data. The data structure of a block chain and a normal database is one of their main distinctions. A block chain is a collection of information that is organized into blocks, each of which contains sets of data. Blocks contain a set amount of storage and, when filled, are closed and connected to the block that came before it, producing a data chain known as the block chain. Each piece of information that comes after the block that was just added is used to generate a new block, which is then added to the chain once the chain is full.

While a database normally arranges its data into tables, a block chain, as its name suggests, organises its data into chunks (blocks) that are connected together.

*Corresponding author: N Sanchiga Nandhini; Email Id: sanchiganathan19@gmail.com

This data format by default produces an irreversible temporal line of data when used decentralizedly. As blocks are completed, they take on a definite point in time and are added to the timeline. A precise time stamp is applied to each block as it is added to the chain. Block chain will make it possible to distribute and record digital data without modifying it. An immutable ledger, or a record of transactions that cannot be changed, erased, or destroyed, is built on a block chain in this way. Because of this, block chains are frequently referred to as distributed ledger technology (DLT).The block chain idea was initially put out as a research project in 1991, before its first significant implementation, Bit coin, which debuted in 2009. In Since then, the adoption of block chains has skyrocketed thanks to the development of various crypto currencies, decentralized finance (DeFi) applications, non-fungible tokens (NFTs), and smart contracts. The suggested structure is shown in fig 1.

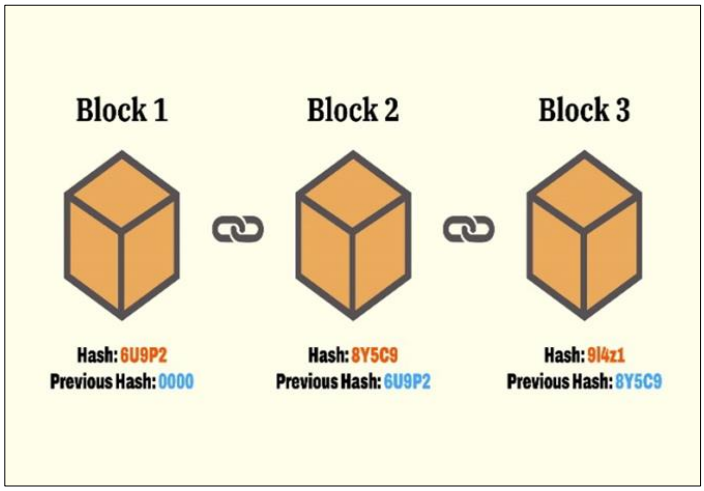

Figure 1 Block chain framework

2. Related Work

Taleb, Nasser, et.al, [1] Studied Applications that might be used in the future are provided together with an introduction of the Block chain and Bit coin technologies. Due to its safe peer-to-peer transactions and encrypted data, Block chain has recently attracted a lot of interest. Block chain implementation has a promising future since it can reduce working hours, eliminate millions of printed papers, reduce transaction costs, and guarantee the security of digital documents and transactions. This new innovative technology has its own both positive and negative aspects that receive some worries as well as some support. Future uses of Bit coin and block chain technology are reviewed in this essay. Block chain is a novel platform for digital information that is used to store encrypted data, perform safe digital transactions, and has recently attracted a lot of interest. Notably, the bulk of crypto currencies on the Block chain are built using the elliptic curves digital signature technique (ECDSA). Bit coin utilizes a particular type of ECDSA known as secp256k. Data security breaches on both a small-scale and large-scale employing conventional transactional and financial platforms resulted in the loss of personal and corporate data. Furthermore, it is assumed that data on platforms for bit coin and block chains is highly encrypted and secure.

Verma, Manish, et al. [2] attempted to examine a variety of the block chain technology's developing importance. It is essential for a system built on trust without the need for a third party. Based on the discussion in this article, a practical application may be created in the future. A mathematical and technical implementation of consensus and agreement built on trust is the Block chain. One of the main benefits of Block chain technology is the lack of third party verification when taking the consensus into account. This essay aims to investigate the numerous developing uses of block chain. A block chain does not incur trading fees. A framework has a real price, but there is no exchange fee. It is a simple yet effective method for sending data securely and mechanically from point A to point B. The process is started by one group to an exchange by creating a square. Thousands, perhaps many PCs transported over the internet, examine this square. The verified square is joined to a chain that is stored online, creating an amazing record with an intriguing record and a unique history. Misleading one record would entail misrepresenting the whole chain several times. That is really beyond comprehension. Although it frequently comes from other angles, Bit coin uses this approach for financial transactions.

To evaluate the objective, which is to understand how Bit coin characteristics (such as transaction volume, cost per transaction) might affect the following day change in price level of Bit coin, Sin et.al, [3], used a Genetic Algorithm-

based Selective Neural Network Ensemble Artificial Neural Network (ANN) ensemble technique (GASEN). The group will become accustomed to handling a binary distinction problem: the direction of Bit coin price will shift the following day. Back testing was performed to compare a trading approach and a general strategy that utilises the best MLP model in the ensemble to a "prior day trend following" approach in order to better understand and evaluate the usefulness of the ensemble's outcomes. In a different research, the binary classification method Bayesian Regression was used to forecast changes in the price of bit coin, and the prediction generated approximately 200% returns in less than a year is combined with a trading strategy, than 60 days. The study came to the conclusion that historical data for Bit coin may contain "information" that can be used to forecast price changes in the future. Atsidakos, George S.,

Atsidakos, George S.,Et al, [4] despite its importance for market practitioners, implemented models for predicting the price of bit coins have just recently emerged, and there is little empirical research in the area. In order to fill this vacuum in the literature, three computational intelligence models have been used in this work. The suggested paradigm, called PATSO, is a closed-loop, neuro-fuzzy controller with artificial intelligence. We compare its performance to both a hybrid ANFIS model and an artificial neural network-based model. It is the first time in the literature that the use of neuro-fuzzy models for forecasting Bit coin price changes is suggested. The suggested model is more accurate than both the ANN and the ANFIS models thanks to the usage of the inverse controller's feedback mechanism in the forecasting process. Additionally, When assessed over an out-of-sample time, the PATSOS model boosts the returns produced by a straightforward buy-and-hold investing strategy by 71.21%. When we test the PATSOS model using information on three more well-known crypto currencies, namely Ethereal, Lit coin, and Ripple, we get comparable findings. As a result, the PATSOS methodology seems to be a reliable way to predict Bit coin values. The forecasting system's buy-and-sell indications help to reduce the danger of losses during a market fall brought on by high price volatility. Additionally, the suggested forecasting system's user-friendliness and little computing overhead promote end users' adoption of the system.

Lin, Yu-Jing, et al,... [5] new features such as entity classification and a summary of transaction history for Bit coin addresses have been introduced. The core statistics, auxiliary statistics, and transaction moments make up the transaction history summary. The fundamental statistics have elements related to frequency and are based on earlier research. The additional information also include transaction totals and statistical measurements. The temporal distribution of transactions as well as transaction intervals are characterised by transaction moments. Our test illustrates the performance advantages of applying the criteria we've suggested for categorising Bit currency addresses and entities. The In terms of classification accuracy, feature combinations significantly improve performance. Furthermore, a well-trained LightGBM classifier finds that our suggested features outperform the ten main components. The Micro / Macro F1 scores in the address-based method are 87% / 86% as our best outcome. The great accuracy in each category is demonstrated by comparing Micro-F1 and Macro-F1 results. The matrix of misinterpretation of our best outcome serves as more evidence. However, data scarcity and imbalance are problems for entity-based classification. We design an experiment of Bit currency category categorization based on addresses and entities to assess the efficacy of the suggested features. First, we gathered address-label pair labelled data and retrieved all transactions associated with the addresses.

The addresses and entities are then condensed using these data into features. We used the extracted features to train eight supervised classifiers, and the performance was evaluated using the average Micro-F1 and average Macro-F1 scores of the 10-fold cross-validation.

3. Existing Methodologies

A credit network facilitates payments between any two agents and simulates trust between them in a distributed context. Due to their adaptable architecture and resistance to intrusion, Many Sybil-tolerant social networks, spam-resistant communication protocols, and payment systems are built on top of With Credit networks. The quantity and type of payment transactions, as well as agents' trust relationships, are considered sensitive information in social and financial contexts, but current systems reveal these details. This raises a difficult privacy issue that has largely gone unaddressed in the research on credit networks up to this point.

Privacy preserving Standards have lately been developed as a result of the frequent storage of sensitive data on Internet-connected machines. Additionally, a lot of jobs that were formerly completed by hand are now completed by computers, necessitating the need for information assurance (IA) and security. Maintaining privacy is crucial for preventing identity theft. Businesses also require security to protect their proprietary information and trade secrets. One of the main terrorist risks facing our country today is cyber terrorism. As we've already discussed, the enormous amount of information that is now accessible electronically and online exacerbates this issue.

Hommorphic encryption is a type of encryption that allows calculations to be performed on cipher text and yields an encrypted result that, when decoded, is the same as the results of operations performed on the plaintext. For instance, one person could then, after adding two encrypted numbers another person could decrypt the result, without either of them being capable find the value of the person numbers.

4. Bit Coin Based Net banking Transaction

Our transaction history has the potential to reveal a lot of personal information about each spender in the current centralised banking system, both to the financial sector and to the businesses that surround it (e.g., governments, industry etc.). Spending amounts, the things we buy with those amounts, where we spend our money, and the people we exchange money with are all examples of information that gets leaked.

Those who hold this information have tremendous power, and it can be used in a variety of ways, not all of which are good for us. Crypto currencies were introduced as a solution to address the drawbacks of centralised banking systems while also offering customers transactional data privacy, such as the well-known bit coin.

Algorithms for machine learning can be used to estimate the prices of crypto currencies thanks to the abundance of publicly available data on the market and social trends. Without explicitly programming the computer to perform a certain task, these algorithms are a collection of techniques for learning mathematical models from data.

But there is a need for various models that can capture more sophisticated representations of data as the complexity of the data for the crypto currency market increases. Recurrent neural networks, in particular, can be used to handle the time-series challenge of forecasting the prices of crypto currencies. In recent years, a wide range of writers have done numerous research to estimate the value of securities and stocks using machine learning and deep learning algorithms.

However, comparatively less research work has been carried out on predicting crypto currency price. E-commerce and online payment transactions are growing daily as a result of communications technology. Financial scams related to these transactions are likewise getting worse, costing billions of dollars annually throughout the globe.

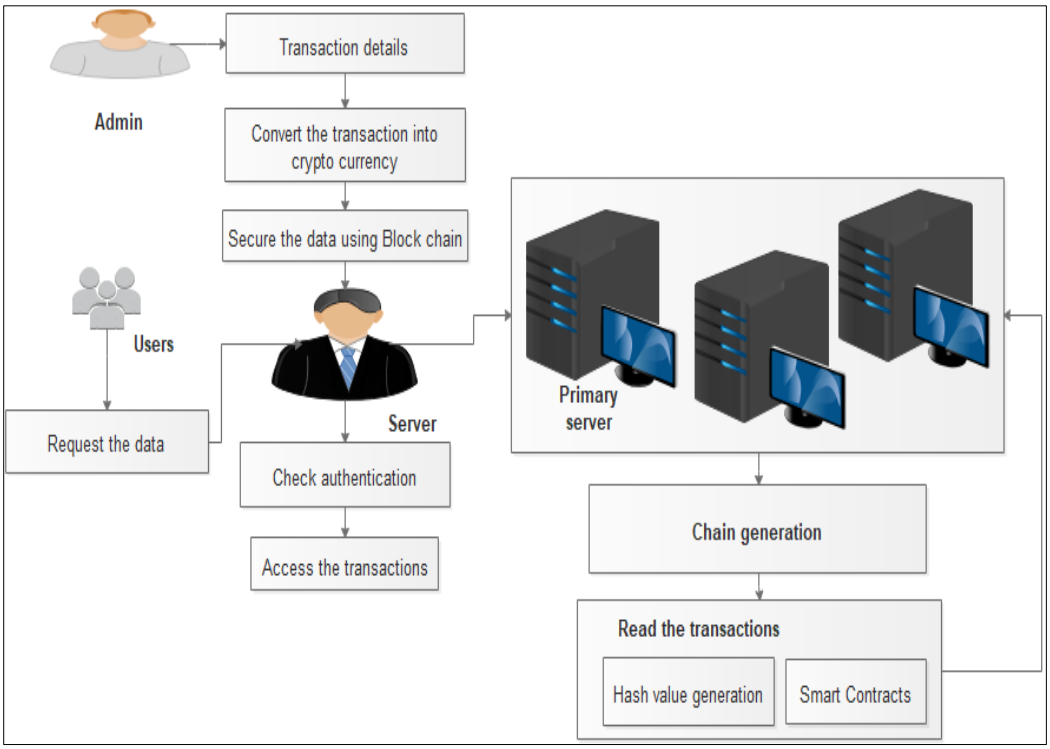

Figure 2 Proposed work framework

Additionally, a variety of benefits, such as cash back, reward points, interest-free credit, discount offers for purchases made at particular establishments, etc., attract customers to use a credit card rather than cash to complete transactions. The main issue facing today's e-commerce industry is that fraudulent transactions increasingly resemble legal ones, and

basic pattern matching tools are ineffective at spotting fraud. Bit coin is exchanged as crypto money in this decentralized system using a public ledger.

In the case of the bit currency, block chain creates a decentralised consensus among a large number of individuals who are not required to know or trust one another on the order of transactions. Additionally, each block makes reference to the hash of the block before it. By creating a connection between these blocks, this produces a block chain. Secondly, block chain technology combines a peer-to-peer network, cryptographic algorithm, distributed data storage, and a decentralised consensus mechanism to enable users to keep records in a safe and verifiable manner and successfully eliminates double spending.

Bit coin is a crypto currency, which is not supported by any government or the central bank of the nation. It can be traded for goods or services with vendors who the use of bit coins payment. These bit coins are the blocks of secure data. Design the system for banking system with improved security. Use block chain engineering to divide the information into blocks. Every transaction is completed using a crypto currency format.

4.1. Bank Interface Creation

Online banking, often known as internet banking, online banking, or home banking, is a type of electronic payment system that enables customers of banks and other financial organisations to execute a variety of financial transactions via the financial institution's website. Instead of using traditional branch banking, online banking systems usually connect to or are a component of the core banking system run by a bank to give users access to financial services. Online banking significantly reduces operational costs for banks by eliminating their reliance on a branch network, while also offering customers greater convenience by saving them time travelling to a branch and enabling them to make financial transactions even when such branches are closed. Banking services for individuals and businesses include You may connect with the bank in an efficient and automated manner thanks to the bank interface, an electronic information and payment system.

The term "banking transactions" describes the actions an account holder does at a communications facility to access his or her account, such as cash withdrawals, deposits, account transfers, payments from bank accounts, and payments made according to preauthorized credit agreements. A payment system is a device that makes it easier for people to conduct financial transactions by transferring money. It makes the two-way exchange of money for products and services in the economy. The most popular payment option that offers a number of features and advantages, such as ease and payment security, is the usage of banking cards. These cards also have the benefit of being compatible with many digital payment methods, such as PoS devices.

For instance, customers can store their information on cards the digital wallet and make cashless payments. VISA, MasterCard, and Rupay are a few of the well-known card payment methods. An institution in the financial sector with permission to accept deposits and make loans is known as a bank. Banks may also offer additional financial services including safe deposit boxes, currency exchange, and asset management.

Retail banks, commercial or corporate banks, and investment banks are just a few examples of the various types of banks. The national government or central bank controls banking in the majority of the world's nations. All transaction data is collected using this module. Customers of banks and other financial institutions can use the transaction detail, an electronic payment system, to conduct a range of financial transactions online.

In contrast to branch banking, which used to be the only option for customers to obtain financial services, an internet banking system would frequently link to or be a component of the primary banking system maintained by a bank. This web application allows for any transactions, including money transfers and withdrawals. Automatic updating of the amount occurs in the savings account. All transaction details are updated into single gateway. Gateway is responsible for transferring the amount to particular merchant without any leakages.

A crypto digital or virtual currency called currency is protected by encryption, making it almost difficult to forge or double-spend. A type of digital asset known as a crypto currency is built on a network that is dispersed among several computers.

A block chain's transactions are marked with an immutable cryptographic signature known as a hash. Cryptography is used to guarantee the block chain's integrity and chronological order. As a result, it would be obvious that it had been altered if a block appeared in just one chain.

Hackers would need to alter each block in a distributed copy of the chain in order to compromise a block chain system. Block chains like Bit coin and ether continue to expand as new blocks are added to the chain, significantly enhancing the security of the ledger. The use of block chain technology is global and decentralized. All of a block chain's records are not kept in a single place. Despite being stored on block chains, crypto currency may be accessed using mobile wallets. If you have a bit coin wallet, you may use it anywhere merchants who accept bit coins are located.

We may create authorized access to bank clients with this module. To access the transfer information, a user can log in using OTP security. OTP can be sent as an SMS alert and made visible after a certain amount of time. Users can securely see their personal information. On a computer system or other digital device, a one-time password (OTP) is a password that is only valid for one login session or transaction. Traditional (static) password-based authentication has a variety of drawbacks that OTPs do not, with their biggest benefit being that OTPs are not susceptible to replay attacks like static passwords are.

This ensures that an OTP that has previously been used to log into a service or complete a transaction cannot be abused by a future hacker because it will no longer be valid. A person who uses the same (or similar) password for numerous systems does not become susceptible on all of them if the password for one of them is discovered by an attacker, which is a second key benefit.

In order to reduce the attack surface, many OTP systems also try to prevent simple session interception or impersonation without knowledge of irregular data generated during the previous session. An authentication manager on the network server produces a number or shared secret using one-time password methods whenever an unauthorised user tries to enter a system or carry out a transaction on a device.

The security token on the smart card or device compares and authenticates the one-time password and user using the same number and procedure. A one-time passcode is frequently sent to customers via SMS as a second authentication step. Short Message Service, or SMS, is an acronym. Once the user enters his login and password, the temporary pass code is collected out of band via mobile phone connections on networked information systems and transaction-oriented web applications.

4.1.1. Hash and Block Generation

- A block containing the most recent transactional data.
- Each piece of data produces a hash.
- A hash is a string of numbers and characters.
- The order in which transactions happened is recorded.
- The previous transaction's hash, in addition to the current transaction, determines the hash.
- A transaction can change even slightly, creating a brand-new hash.
- To make sure that a transaction has not been changed, the nodes examine the hash.
- If a majority of the nodes approve a transaction, it is included in the block.
- Each block in the block chain has a reference to the one before it.
- A Block chain works because it is shared across many computers, each of which has a copy of it.

4.2. SHA-256 FUNCTION

Block chain is an organized data structure that holds blocks of transactions. Its hash value is 256. The chain's subsequent block is linked to every block that comes before it. The initial block in the chain is referred to as the stack's foundation. In order to construct the stack known as a block chain, each newly formed block is stacked on top of the one before it.The hash algorithm characteristic is characterised by susceptibility, unidirectionality, collision resistance, and great sensitivity. It reduces a series of messages of arbitrary length to a shorter fixed-length value. Hash is frequently used to guarantee data integrity, or to make sure the data hasn't been improperly altered with. The hash value of the tested data also adjusts as the data changes. Therefore, although the data is in a dangerous the hash value of the records may be used to determine the data's integrity in a given environment. The National Institute of Standards and Technology (NIST) released SHA as a particular type of cryptographic hash function with all the attributes of a cryptographic hash function. The SHA-2 algorithm cluster includes the SHA256 algorithm, which offers a 256-bit message digest.

The computation approach for the algorithm is broken down into the main loop and message pre-processing. Any length of data is exposed to message length filling and binary bit filling throughout the message preparation process. After then, the filled message is divided into numerous 512-bit message blocks. During the primary loop phase, each message block is handled by a compression mechanism. The original message's hash value is the result of the most recent

compression function, and the result of the previous compression function is the result of the previous compression characteristic. Hashing passwords is made safe by using the SHA-256 method. Verifying transactions in crypto currencies like Bit coin uses the SHA-256 algorithm.

On the block chain, hash functions may be used to confirm the accuracy of blocks and transactions. Every block on the block chain contains the hash value of the data from the previous block, and any user may compare the computed hash value to the recorded hash value. The integrity of the data in the previous block is so determined. Similarly, public-private key pairs can be generated using the hash function.

5. Experimental Results

The suggested structure implemented in Python Framework as web application in banking sectors. The currency and Block chain storage as shown in fig 3.

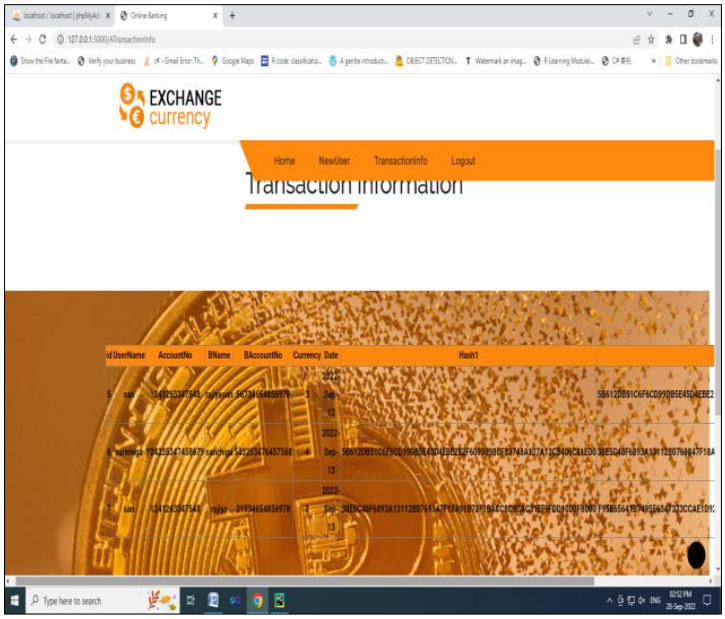

Figure 3 Block chain technology

Money to assess the system's efficiency in terms of the time it takes for each transaction to complete on each node. Execution time (t3): This is the duration for content of each transaction to appear in designated files of each node. The time was retrieved by setting on current the end of time nodes.

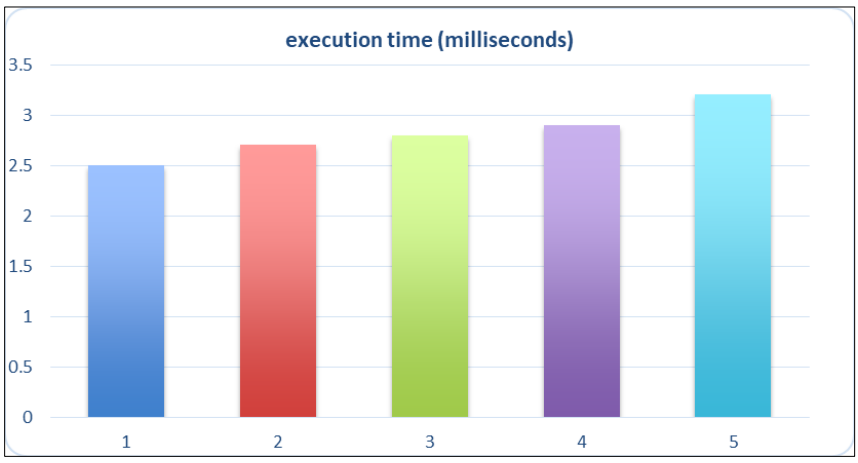

Figure 4 Execution time from the above fig displays the time for creating blocks for each transaction

6. Conclusion

Key management that is secure and reliable is becoming more and more important as the crypto currency market expands. The primary focus of this essay is the development of a decentralised crypto currency key management system.

Decentralized management, as opposed to local and central management, can prevent risk aggregation and use the entire network's storage capacity. The protection of personally identifiable information is the main objective of data privacy. Information is generally regarded as personally identifiable if it can be connected to a specific person either directly or indirectly. Therefore, the attribute values linked to specific individuals are private and must be kept secret when personal data are subjected to mining. Then, rather than learning from a specific person's traits, miners can draw from broad models. In this project, we may draw the conclusion that the suggested solution offered a net banking interface for accessing all transactions in crypto currency format and securing them with block chain technology.

Along with consumers' greed, one reason crypto currency scams are successful is because non-technical users sometimes struggle to discern between fraudulent and legitimate transactions. In particular, block chain-enabled financial services, are among the several new and disruptive technologies that we might expect as a result of the current surge in the crypto currency market. Crypto currency exchanges, in our opinion, will continue to offer fresh insights into various human social-economic activities in the future.

Compliance with ethical standards

Acknowledgments

The authors would like to acknowledge Department of Science and Technology, New Delhi for the financial support in general and infrastructure facilities sponsored under PURSE 2nd Phase programme (Order No. SR/ PURSE Phase 2/38 (G) dated: 21.02.2017).

Disclosure of conflict of interest

The authors declare that they have no conflict of interest.

References

[1] Taleb, Nasser. “Potential uses for the Block chain and bit coin crypto currencies. 48–55 in TEM Journal 8.1, 2019.

[2] Mr. Manish Verma "Emerging block chain technology applications." International Research Journal of Modernization in Engineering Technology and Science 3.4 (2021): 1258-1260

[3] Sin, Edwin, and Lipo Wang. "Prediction of the price of bit coin using neural network ensembles."13th international conference on fuzzy systems, natural computing, and knowledge discovery in 2017 (ICNC-FSKD).IEEE, 2017.

[4] Atsalakis, George S., et al. "Bitcoinprice prediction using neuro-fuzzy methods." Journal of Operational Research in Europe 276.2 (2019): 770-780.

[5] Lin, Yu-Jing, et al. “2019 IEEE International Conference on Blockchain and Cryptocurrency "An assessment of bitcoin addresses categorization based on transaction history summarising" (ICBC). IEEE, 2019.

[6] K. Liang, X. Huang, F. Guo, and J. K. Liu, “Regular language search over encrypted cloud data with privacy protection IEEE Trans. Inf. Foren. Secur., 2016, pp. 2365–2376, vol. 11, no.

[7] "Two birds with one stone: Two-factor authentication with security beyond traditional bounds," by D. Wang and P. Wang 2016's IEEE Trans. Depend. Secure Computing

[8] fully homomorphism encryption with an ideal lattice, C. GENTRY,” Proc. ACM STOC 2009, pp. 169–178.

[9] C. Gentry, A. Sahai, and B. "Homomorphism encryption from learning with errors: Conceptually-simpler, asymptotically quicker, attribute-based," by Waters, in Proc. CRYPTO 2013, pp. 75–92.

[10] Efficient completely homomorphism encryption from (standard) LWE by Z. Brakerski and V. Vaikuntanathan,” in Proc. IEEE FOCS 2011, pp. 97–106.

[11] Chen, Yan, and Cristiano Bellavitis. "Blockchain disruption and decentralized finance: The rise of decentralized business models." *Journal of Business Venturing Insights* 13 (2020): e00151.

[12] Schär, Fabian. "Decentralized finance: On blockchain-and smart contract-based financial markets." FRB of St. Louis Review (2021).

[13] Tran, Muoi, Inho Choi, Gi Jun Moon, Anh V. Vu, and Min Suk Kang. "A stealthier partitioning attack against bitcoin peer-to-peer network." In *2020 IEEE Symposium on Security and Privacy (SP)*, pp. 894-909. IEEE, 2020.

[14] Chohan, Usman W. "Non-fungible tokens: Blockchains, scarcity, and value." *Critical Blockchain Research Initiative (CBRI) Working Papers* (2021).

[15] He, Xiaojian, Jinfu Lin, Kangzi Li, and Ximeng Chen. "A novel cryptocurrency wallet management scheme based on decentralized multi-constrained derangement." *IEEE Access* 7 (2019): 185250-185263.