DIGITAL CURRENCY BASED BANKING SYSTEM USING BLOCK CHAIN TECHNOLOGY

Ajaykumar.. K
ComputerScience and Engineering
E.G.S.Pillay Engineering College,
Nagapattinam, India
ajvinajay@gmail.com

Dinesh.A.R
ComputerScience and Engineering
E.G.S.PillayEngineering College,
Nagapattinam, India
dineshramesh065@gmail.com

Sivaganesh.S
ComputerScience and Engineering
E.G.S. Pillay Engineering College,
Nagapattinam, India
smsganesh143@gmail.com

Dr.N.Murali M.E,PhD.
Associate Professor
E.G.S.PillayEngineering College,
Nagapattinam, India
muraliegspec.org

Abstract—Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. So in this project we can implement Bit Coin based banking system can be implemented using Block chain technology to create hash functions. Bit coin is a crypto currency, which is not backed by any country's central bank or government. It can be traded for goods or services with vendors who accept bit coins as payment. These bit coins are the blocks of secure data. This data is transferred from one person to another and verifying the transaction, i.e., spending the money that requires high computing power to safely verify the individual transactions. The P2P network monitors and verifies the transfer of bit coins between users. As per to cryptographic implementation bit coin is more secure than other currencies and it is impossible to do fake transactions. In a Bit coin transaction, block chain will create an interconnection between all users connected to network and every time when entering a transaction to the network after validating it will broadcast to other users and also network will have a copy of every transaction. Instead of saving any transaction in the block chain, the network will bundle transaction information into a block and it will broadcast into the network. Each and every block link to the previous block this chain will trace to the first block which is called genesis block. Block chain systems work with peer-to-peer networks and also uses a consensus algorithm that's why there is no possibility of data modification.

Index Terms— **Financial sector, Bit-coin transaction, Block chain, P2P network, Crypto currency**

I. INTRODUCTION

A block chain is a distributed database that is shared among the nodes of a computer network. As a database, a block chain stores information electronically in digital format. Block chains are best known for their crucial role in crypto currency systems, such as Bit coin, for maintaining a secure and decentralized record of transactions. The innovation with a block chain is that it guarantees the fidelity and security of a record of data and generates trust without the need for a trusted third party. One key difference between a typical database and a block chain is how the data is structured. A block chain collects information together in groups, known as blocks that hold sets of information. Blocks have certain storage capacities and, when filled, are closed and linked to the previously filled block, forming a chain of data known as the block chain. All new information that follows that freshly added block is compiled into a newly formed block that will then also be added to the chain once filled. A database usually structures its data into tables, whereas a block chain, like its name implies, structures its data into chunks (blocks) that are strung together. This data structure inherently makes an irreversible time line of data when implemented in a decentralized nature. When a block is filled, it is set in stone and becomes a part of this time line. Each block in the chain is given an exact time stamp when it is added to the chain. The goal of block chain is to allow digital information to be recorded and distributed, but not edited. In this way, a block chain is the foundation for immutable ledgers, or records of

1

transactions that cannot be altered, deleted, or destroyed. This is why block chains are also known as a distributed ledger technology (DLT). First proposed as a research project in 1991, the block chain concept predated its first widespread application in use: Bit coin, in 2009. In the years since, the use of block chains has exploded via the creation of various crypto currencies, decentralized finance (DeFi) applications, non-fungible tokens (NFTs), and smart contracts. The proposed framework is shown in fig 1.

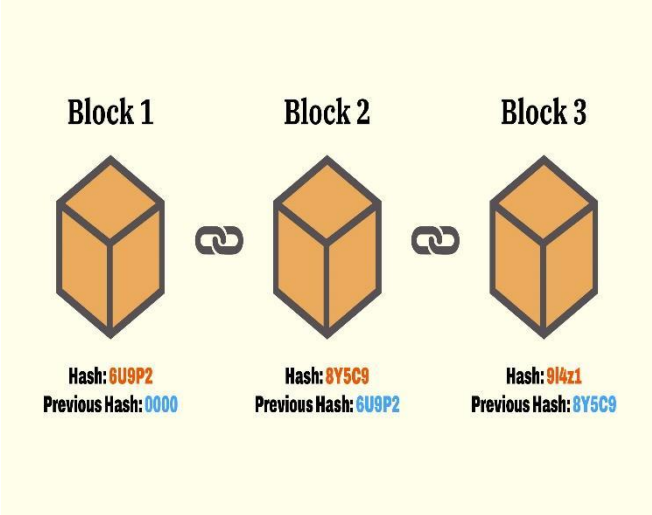

Fig 1: Block chain framework

II. RELATED WORK

Taleb, Nasser, et.al,…[1] studied an overview of Blockchain and Bitcoin technology is presented along with prospective and future applications. Recently Blockchain has received special attention due to its encrypted data and secure digital of peer-to-peer transactions. The implementation of Blockchain has a promising future represented in: saving working hours, saving million printed documents, saving money in transactions, and ensuring the digital security of documents and transactions. This new innovative technology has its own advantages and disadvantages that receives some support as well as some concerns. This paper presents a literature review of Blockchain and Bitcoin technology future applications. Recently Blockchain has received special attention and is used as a new platform for digital information and to store encrypted data and process secure digital transactions. Noticeably, the majority of Blockchain cryptocurrency is structured based on the elliptic curves digital signature algorithm (ECDSA). In particular, Bitcoin uses special ECDSA called secp256k. Losses of personal and organizational data occurred due to security breaches of data at small and large scales using traditional transactional and financial platforms. Furthermore, data on Blockchain and Bitcoin platforms are assumed to be highly encrypted and in secured state.

Verma, Manish, et.al,…[2] tried to explore a range of the emerging relevance of Block chain technology. It is crucial for a trust-based system without requirement for a third party. In future, the practical application could be developed based on this paper discussion. The Blockchain has been a mathematical and technical application of consensus and agreement based on trust. The absence of third party verification considering the consensus is a major advantage of the Blockchain technologies. This paper tries to explore the emerging applications of Blockchain in various domains. A Blockchain conveys no exchange cost. A framework cost truly, yet no exchange cost. It is a clear yet sharp technique for passing information from A to B in a totally mechanized and safe manner. One gathering to an exchange starts the procedure by composing a square. Thousands check this square, maybe a sizable number of PCs conveyed around the net. The confirmed square is added to a chain, which is stowed on the internet, making a remarkable record, yet an interesting record with a one of a kind history. Distorting a solitary record would mean misrepresenting the whole chain on a large number of times. That is essentially incomprehensible. Bitcoin utilizes this model for money related exchanges, yet it tends to be sent from various perspectives

Sin, Edwin, et.al,…[3] analyzed the objective which is to understand how features of Bitcoin (such as transaction volume, cost per transaction) can affect the next day change in price level of Bitcoin through the use of an Artificial Neural Network (ANN) ensemble approach called Genetic Algorithm based Selective Neural Network Ensemble (GASEN). The ensemble will be used to solve a binary classification problem: the next day change in the direction of the price of Bitcoin. To better understand and evaluate its effectiveness, back testing was done to see how a trading strategy based on the results of the ensemble can compare against a “previous day trend following” trading strategy as well as a trading strategy that follows the single, best MLP model in the ensemble. As the market is relatively new, existing works related to forecasting in this market is fairly limited. One study showed that Google Trends data and volume of tweets related to Bitcoin on Twitter have positive correlation with Bitcoin’s price and hence may be able to predict the fluctuations in price of Bitcoin. In another study, Bayesian Regression, a binary classification algorithm, was used to predict price variation in Bitcoin and the prediction gave almost 200% returns in less than 60 days when used with a trading strategy. The study concluded that there may be ‘information’ in Bitcoin’s

historical data that can help predict future price variations.

Atsalakis, George S., et al,…[4] implemented Bitcoin price forecasting models that have only recently appeared, and despite their significance for market practitioners, the empirical work in the field is scarce. To fill this gap in the literature, three computational intelligence models have been employed in the present study. The proposed model, namely PATSO is an artificially intelligent, neuro-fuzzy controller incorporating a closed-loop. We benchmark its performance against a hybrid ANFIS model, and an artificial neural network model. The application of neuro-fuzzy models for the forecasting of Bit coin price movements is proposed for the first time in the literature. The use of the feedback mechanism of the inverse controller in the forecasting process improves the accuracy of the proposed model, making it superior to both the ANN and the ANFIS models. Additionally, when tested in an out-of-sample period, the PATSOS model improves the returns earned by a naive buy-and-hold investment strategy by 71.21%. We obtain similar results when testing the PATSOS model with data on three other well-known cryptocurrencies, namely Ethereum, Litecoin, and Ripple. Therefore, the PATSOS system appears to be an efficient method to forecast Bitcoin prices. The buy-and-sell signals, produced by the forecasting system, minimize the risk from losses that may occur during the decline of the market due to high price volatility. Additionally, the easiness of dealing with the proposed forecasting system and the short computational time that is required encourage its adoption by end users

Lin, Yu-Jing, et al,…[5] introduced new features as transaction history summary for Bitcoin address and entity classification. The transaction history summary is composed of basic statistics, extra statistics, and transaction moments. The basic statistics are based on the previous work and capture the features in the aspect of frequency. The extra statistics additionally contain total amounts and statistical measures of transactions. The transaction moments characterize the temporal distribution of transactions as well as transaction intervals. Our experiment showcases the performance benefits from using our proposed features for Bitcoin address/entity classification. The combinations of features make huge progress in terms of classification accuracy. Moreover, our proposed features dominate the ten most important features according to a well-trained LightGBM classifier. As the best result we achieve, the Micro / Macro F1 scores are 87% / 86% in the address-based scheme. The high accuracy in each category is indicated from measuring the similarity between Micro-F1 and Macro-F1. Also, the confusion matrix of our best result further proves it. The entity-based classification, however, suffers from data imbalance and data scarcity. To evaluate how effective the proposed features are, we design an experiment of Bitcoin category classification based on addresses and entities. Firstly, we collected labeled data of address-label pairs and fetched all transactions associated with the addresses. The addresses and entities are then be summarized into features with the use of these data. We trained eight supervised classifiers on the extracted features and evaluate the results by average Micro-F1 scores and average Macro-F1 scores of 10-fold cross-validation.

III. EXISTING METHODOLOGIES

A credit network models trust between agents in a distributed environment and enables payments between arbitrary pairs of agents. With their flexible design and robustness against intrusion, credit networks form the basis of several Sybil-tolerant social networks, spam-resistant communication protocols, and payment systems. Existing systems, however, expose agents' trust links as well as the existence and volumes of payment transactions, which is considered sensitive information in social environments or in the financial world. This raises a challenging privacy concern, which has largely been ignored by the research on credit networks so far. Privacy preserving standards have been created recently because sensitive information is now frequently stored on computers that are attached to the Internet. Also many tasks that were once done by hand are carried out by computer; therefore there is a need for Information Assurance (IA) and security. Privacy preserving is an important in order to guard against identity theft. Businesses also need security because they need to protect their trade secrets and proprietary information. Cyber-terrorism is one of the major terrorist threats posed to our nation today. As we have mentioned earlier, this threat is exacerbated by the vast quantities of information now available electronically and on the web. Homomorphic encryption is a form of encryption which allows specific types of computations to be carried out on cipher text and obtain an encrypted result which decrypted matches the result of operations performed on the plaintext. For instance, one person could add two encrypted numbers and then another person could decrypt the result, without either of them being able to find the value of the individual numbers.

IV. BIT COIN BASED NETBANKING TRANSACTION

In the existing centralised banking system, our transaction history has the potential to reveal a great deal of personal information about each spender, both to the banking system and to the companies that surround it (e.g., governments, industry etc.). The amounts spent, the things on which the amounts were spent, the spending locations, and the users with whom we exchange money are all examples of leaking information. This knowledge is extremely powerful in the hands of those who possess it, and it may be applied in a variety of ways, not all of which are beneficial to us. Crypto currencies, such as the well-known bit coin, were offered as a way to remedy the shortcomings of centralised banking systems while also providing users with transactional data privacy.

Having vast amounts of openly available data on the Cryptocurrencies market and social trends information, machine learning algorithms can be used to forecast the prices with Cryptocurrencies. These algorithms are a set of methods for learning mathematical models from data without explicitly programming the computer to do a specific task. But, with an increase in the complexity of the data for the Cryptocurrency market, there is a need of different models, which can capture more complex representations of data. Deep learning models specifically recurrent neural networks can be used to solve the time-series problem of predicting the prices of Cryptocurrencies. Numerous research has been explored by various authors in the last to predict the value of equity and securities using machine learning and deep learning algorithms. However, comparatively fewer research work has been carried out on forecasting the price of Cryptocurrencies.

With the advent of communications techniques, e-commerce as well as online payment transactions are increasing day by day. Along with this financial frauds associated with these transactions are also intensifying which result in loss of billions of dollars every year globally. Also the various types of benefits like cash back, reward points, interest-free credit, discount offers on purchases made at selected stores, and so forth tempt the customers to use credit card instead of cash for their purchases. The major problem for e-commerce business today is that fraudulent transactions appear more and more like legitimate ones and simple pattern matching techniques are not efficient to detect fraud. Using a public ledger, bit coin is transacted as crypto currency in this decentralized system. In the bit coin, blockchain establishes a decentralized consensus about the order of transactions among a large number of members who need not to know or trust anyone. Furthermore, each block references the hash of the previous block. This establishes a link between these blocks, thus, it creates a blockchain. Then, by combining peer-to-peer network, cryptographic algorithm, distributed data storage and a decentralized consensus mechanism, blockchain technology provides a way for people that record in a secure and verifiable manner, and it can prevent double spending effectively. Bit coin is a crypto currency, which is not backed by any country's central bank or government. It can be traded for goods or services with vendors who accept bit coins as payment. These bit coins are the blocks of secure data. Design the system for banking system with improved security. Implement block chain technology to split the details in the form of blocks. All transactions are done with help of crypto currency format.

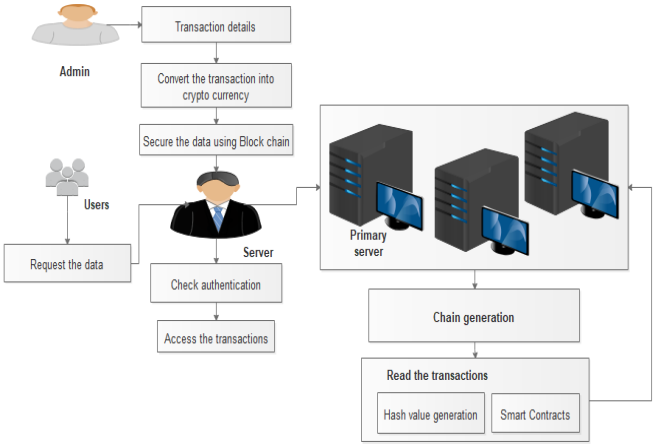

Fig 2: Proposed work framework

BANK INTERFACE CREATION

Online banking, also known as internet banking, web banking or home banking, is an electronic payment system that enables customers of a bank or other financial institution to conduct a range of financial transactions through the financial institution's website. The online banking system will typically connect to or be part of the core banking system operated by a bank to provide customers access to banking services in place of traditional branch banking. Online banking significantly reduces the banks' operating cost by reducing reliance on a branch network, and offers greater convenience to customers in time saving in coming to a branch and the convenience of being able to perform banking transactions even when branches are closed. Internet banking provides personal and corporate banking services offering features such as viewing account balances, obtaining statements, checking recent

transactions, transferring money between accounts, and making payments. The bank interface is an electronic information and payment system that enables you to communicate with the bank in an automated and operative way. The bank interface allows you to integrate the company's accounting system with the bank service. Online Banking System is a web application that ensures a registered user to enjoy banking online. This Online Banking project is a web application where you can transfer money to other users and can have a close watch on all your transactions. Also we have added extra security features to our Online Banking System project. This module is used to create a web based application specially for banking sector. This application will be used by bank administrator and user only. By using this application user can perform online transactions

TRANSACTION DETAILS

Banking transactions means cash withdrawals, deposits, account transfers, payments from bank accounts, disbursements under a preauthorized credit agreement, and loan payments initiated by an account holder at a communications facility and accessing his or her account. A payment system is a mechanism that facilitates financial transactions via the transfer of monetary value. It makes the two-way flow of payments in exchange for goods services in the economy. One of the most used payment methods that come with several features and benefits, such as security of payments, convenience, etc., are the banking cards. An alternative advantage of these cards is that you can use them to make various kinds of digital payments, PoS machines, etc. For instance, customers can store their card information on the digital wallet and make cashless payments. Some of the well-known card payment systems are VISA, MasterCard, and Rupay. A bank is a financial institution licensed to receive deposits and make loans. Banks may also provide financial services such as wealth management, currency exchange, and safe deposit boxes. There are several different kinds of banks including retail banks, commercial or corporate banks, and investment banks. In most countries, banks are regulated by the national government or central bank. This module is used to collect the all transactions data. The transaction detail is an electronic payment system that enables customers of a bank or other financial institution to conduct a range of financial transactions through the financial institution's website. The online banking system will typically connect to or be part of the core banking system operated by a bank and is in contrast to branch banking which was the traditional way customers accessed banking services. Any transactions like money deposit, withdrawal, money transfer, are available by using this web application. The amount is automatically updated to saving account. All transaction details are updated into single gateway. Gateway is responsible for transferring the amount to particular merchant without any leakages.

CONVERT CRYPTO CURRENCY

A crypto currency is a digital or virtual currency that is secured by cryptography, which makes it nearly impossible to counterfeit or double-spend. A crypto currency is a form of digital asset based on a network that is distributed across a large number of computers. This decentralized structure allows them to exist outside the control of governments and central authorities. The advantages of crypto currencies include cheaper and faster money transfers and decentralized systems that do not collapse at a single point of failure. Bit coin is a decentralized digital currency, without a central bank or single administrator that can be sent from user to user on the peer-to-peer bit coin network without the need for intermediaries. Crypto currencies run on a distributed public ledger called blockchain, a record of all transactions updated and held by currency holders. Units of cryptocurrency are created through a process called mining, which involves using computer power to solve complicated mathematical problems that generate coins. Users can also buy the currencies from brokers, then store and spend those using cryptographic wallets. If you own cryptocurrency, you don't own anything tangible. What you own is a key that allows you to move a record or a unit of measure from one person to another without a trusted third party. Although Bitcoin has been around since 2009, crypto currencies and applications of block chain technology are still emerging in financial terms, and more uses are expected in the future. Transactions including bonds, stocks, and other financial assets could eventually be traded using the technology.Coin value is trained by the admin. Amount of the transactions are converted into coin values

BLOCK CHAIN IMPLEMENTATION

Many crypto currencies are decentralized networks based on block chain technology—a distributed ledger enforced by a disparate network of computers. A defining feature of crypto currencies is that they are generally not issued by any central authority, rendering them theoretically immune to government interference or manipulation. Every new block generated must be verified by each node before being confirmed, making it almost impossible to forge

transaction histories. The contents of the online ledger must be agreed upon by the entire network of an individual node, or computer maintaining a copy of the ledger. The block chain is a shared public ledger on which the entire Bit coin network relies. All confirmed transactions are included in the block chain. It allows Bit coin wallets to calculate their spendable balance so that new transactions can be verified thereby ensuring they're actually owned by the spender. Blockchain is a system of recording information in a way that makes it difficult or impossible to change, hack, or cheat the system. A blockchain is essentially a digital ledger of transactions that is duplicated and distributed across the entire network of computer systems on the blockchain. Each block in the chain contains a number of transactions, and every time a new transaction occurs on the blockchain, a record of that transaction is added to every participant's ledger. The decentralised database managed by multiple participants is known as Distributed Ledger Technology (DLT). Blockchain is a type of DLT in which transactions are recorded with an immutable cryptographic signature called a hash. The integrity and the chronological order of the block chain are enforced with cryptography. This means if one block in one chain was changed, it would be immediately apparent it had been tampered with. If hackers wanted to corrupt a blockchain system, they would have to change every block in the chain, across all of the distributed versions of the chain. Blockchains such as Bitcoin and Ethereum are constantly and continually growing as blocks are being added to the chain, which significantly adds to the security of the ledger. Blockchain technology is decentralized and distributed all over the world. There is no single location where all records of a blockchain are stored. Cryptocurrencies, although held in blockchains, can be accessed via mobile wallets. If you have a bitcoin wallet, you can use it anywhere for transacting with parties accepting bitcoins.

AUTHORIZED ACCESS

In this module, we can design authorized access to bank customers. User can be login to view the transfer details with OTP security. OTP can be send as SMS alert and visible with particular seconds. User can view their details in secure manner. A one-time password (OTP) is a password that is valid for only one login session or transaction, on a computer system or other digital device. OTPs avoid a number of shortcomings that are associated with traditional (static) password-based authentication; the most important advantage that is addressed by OTPs is that, in contrast to static passwords, they are not vulnerable to replay attacks. This means that a potential intruder who manages to record an OTP that was already used to log into a service or to conduct a transaction will not be able to abuse it, since it will no longer be valid. A second major advantage is that a user, who uses the same (or similar) password for multiple systems, is not made vulnerable on all of them, if the password for one of these is gained by an attacker. A number of OTP systems also aim to ensure that a session cannot easily be intercepted or impersonated without knowledge of unpredictable data created during the previous session, thus reducing the attack surface further. When an unauthenticated user attempts to access a system or perform a transaction on a device, an authentication manager on the network server generates a number or shared secret, using one-time password algorithms. The same number and algorithm are used by the security token on the smart card or device to match and validate the one-time password and user. Many companies use Short Message Service (SMS) to provide a temporary passcode via text for a second authentication factor. The temporary passcode is obtained out of band through cell phone communications after the user enters his username and password on networked information systems and transaction-oriented web applications.

ALGORITHM - BLOCKCHAIN TECHNOLOGY

A blockchain is a digital idea to store **data**. These blocks are chained collectively, and this makes their data immutable. When a block of information is chained to the other blocks, its data can never be changed again. It will be publicly available to anyone who wants to see it ever again, in exactly the way it was once introduced to the blockchain.

The most adopted secure algorithms associated with the blockchain technology are (SHA-1, SHA2, and SHA-256) encryption because of their unique quality of hash function that creates unique outputs when given different inputs. The hash characteristic here is a unique key created to identify a transaction that at the same time identifies an individual in the petroleum supply chain.

Blockchain Technology is reliable for use in a hashing crypto method, which facilitates create an adequate and strong hashing code and convert it from a bit of fixed size data to strings of character. Each transaction proposed in a blockchain are hashed together before shoving in a block, and the hash pointers connect every block to the next block for holding of previous hash records as it is undisputable. Therefore, any modifications in the blockchain transaction of hashing function will result in different hash string of character and affect all the involved blocks.

Block and Hash Generation

1. A block carrying current transaction information.
2. Each data generates a hash.
3. A hash is a numbers string and letters.
4. Transactions are recorded in the sequence in which they occurred.
5. The hash is determined not only by the transaction, but also by the hash of the prior transaction.
6. Even a small modification in a transaction generates a completely new hash.
7. The nodes inspect the hash to ensure that a transaction has not been altered.
8. A transaction is written into a block if it is approved by a majority of the nodes.
9. Each block references to the previous block and forming the Blockchain.
10. A Blockchain is effective because it is distributed among multiple computers, each with a copy of the Blockchain.

HASH FUNCTION SHA 256:

Blockchain is an ordered data structure that stores blocks of transactions. Each block in the chain is connected to the previous block in the chain. The foundation of the stack refers to the first block within the chain. Each new block created receives layered on top of the previous block to form a stack known as a Blockchain.

The hash algorithm is a feature that transforms a chain of messages of any length to a shorter fixed-length value, and is characterized by susceptibility, unidirectionality, collision resistance, and extreme sensitivity. Hash typically used to ensure data integrity, that is, to verify the data has been illegally tampered with. When the data tested changes, its hash value additionally changes correspondingly. Therefore, even if the data is in a dangerous environment, the integrity of the data can be determined based on the hash value of the records. The National Institute of Standards and Technology (NIST) issued SHA as a type of cryptographic hash function having the general features of a cryptographic hash function. The SHA256 algorithm, which provides a 256-bit message digest, is a subset of the SHA-2 algorithm cluster. The computation approach for the algorithm is divided into two stages: message preprocessing and the main loop. In the message preprocessing stage, binary bit filling and message length filling are performed on the data of any length, and the filled message is split into numerous 512-bit message blocks. In the primary loop phase, every message block is handled by a compression function. The output of the previous compression characteristic is the input of the current compression function, and the hash value of the original message is the output of the last compression function.

The SHA-256 algorithm is used to secure password hashing. The SHA-256 algorithm is used to verify transactions in cryptocurrencies like Bitcoin. Hash functions can be used to verify the integrity of blocks and transactions on the blockchain. The hash value of the preceding block's data is kept in the header of each block in the blockchain, and any user can compare the calculated hash value to the stored hash value. As a result, the integrity of the previous block's information is determined. Similarly, public-private key pairs can be generated using the hash function

V EXPERIMENTAL RESULTS

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

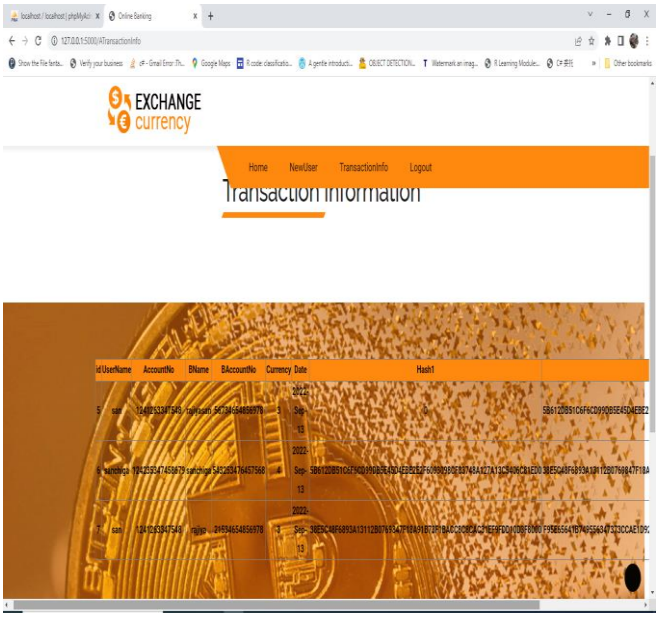

Fig 3: Currency and Block chain technology

To evaluate performance of our system in terms of execution time at every transactions on nodes.

Execution time (t3): This is the time taken for content of each transaction to appear in designated files of each node. The time was retrieved by setting on current time for all nodes.

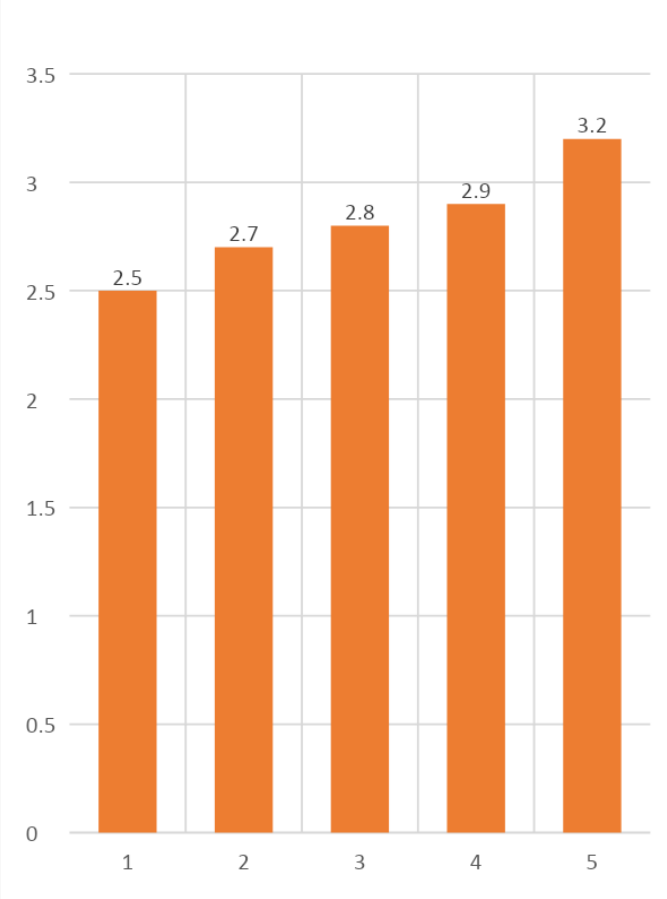

Fig 4: Execution time

From the above fig displays the time for creating blocks for each transactions

VI CONCLUSION

As the crypto currency market continues to expand, secure and stable key management is becoming more and more important. This article focuses on designing a decentralized crypto currency key management scheme. Compared with local management and central management, decentralized management can avoid risk aggregation and make use of the whole network storage resources. The primary goal of data privacy is the protection of personally identifiable information. In general, information is considered personally identifiable if it can be linked, directly or indirectly, to an individual person. Thus, when personal data are subjected to mining, the attribute values associated with individuals are private and must be protected from disclosure. Miners are then able to learn from global models rather than from the characteristics of a particular individual. In this project, we can conclude that the proposed system provided net banking interface to access the all transactions in crypto currency format and secure the transactions using Block chain technology. A success factor of crypto currency scams, besides users' greediness, is that non-technical users often find it difficult to distinguish fraudulent transactions from legit ones. With the crypto currency economy booming in recent years, we can foresee an abundance of new and disruptive innovations, especially blockchain-enabled financial services. We believe that crypto currency transactions will continuously provide new knowledge of various human social-economic behaviours in the future.

References

[1] Taleb, Nasser. "Prospective applications of blockchain and bitcoin cryptocurrency technology." TEM Journal 8.1 (2019): 48-55.
[2] Verma, Manish. "Emerging applications of blockchain technology." International Research Journal of Modernization in Engineering Technology and Science 3.4 (2021): 1258-1260
[3] Sin, Edwin, and Lipo Wang. "Bitcoin price prediction using ensembles of neural networks." 2017 13th International conference on natural computation, fuzzy systems and knowledge discovery (ICNC-FSKD). IEEE, 2017.
[4] Atsalakis, George S., et al. "Bitcoin price forecasting with neuro-fuzzy techniques." European Journal of Operational Research 276.2 (2019): 770-780.
[5] Lin, Yu-Jing, et al. "An evaluation of bitcoin address classification based on transaction history summarization." 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC). IEEE, 2019.
[6] K. Liang, X. Huang, F. Guo, and J. K. Liu, "Privacy-preserving and regular language search over encrypted cloud data," IEEE Trans. Inf. Foren. Secur., vol. 11, no. 10, pp. 2365–2376, 2016.
[7] D. Wang and P. Wang, "Two birds with one stone: Two-factor authentication with security beyond conventional bound," IEEE Trans. Depend. Secur. Comput., 2016.
[8] C. GENTRY, "Fully homomorphic encryption using ideal lattice," Proc. ACM STOC 2009, pp. 169–178.
[9] C. Gentry, A. Sahai, and B. Waters, "Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically faster, attribute-based," in Proc. CRYPTO 2013, pp. 75–92.
[10] Z. Brakerski and V. Vaikuntanathan, "Efficient fully homomorphic encryption from (standard) LWE," in Proc. IEEE FOCS 2011, pp. 97–106.