Safeguarding the Financial Transactions with the Aid of Blockchain Technology

A. Dr. Sameena Banu[1], B. Shaista Shireen[2]
[1]*Associate Professor, Dept. of Computer Science and Engineering, KBNU, Kalaburagi, Karnataka, India*
[2]*PG Scholar, Dept. of Computer Science and Engineering, KBNU, Kalaburagi, Karnataka, India*

Abstract **- The emergence of digital technology has changed people's lives forever. In the financial sector, there have been numerous hazards and scams discovered. Banking systems have a centralised database, making it easier for an attacker to gain access to data and making the system insecure. The problems of this centralised approach can be minimised by changing the structure and using block-chain technology instead of tokens. Block-chain uses a decentralised design to store and retrieve data across a database. Database hacking attacks are reduced as a result. Each block in the network confirms block-chain transactions, increasing their security and supporting the financial system.**

Index Terms **- Blockchain Technology; Bitcoin; Hacking.**

I.INTRODUCTION

Bitcoin was the main cryptographic money to utilize block-chain innovation. This procedure was at first recommended in 2008 for the improvement of bitcoin, a well-known digital currency that was carried out in 2009. Square chain innovation supports and powers automated money. In a computerized cash, block-chain is basic for confirming and approving exchanges. It has a novel construction that doesn't need the inclusion of an outsider. By approving a current square when another exchange is mentioned, another square is shaped in a current square chain, and the chain grows. Banking as an assistance requires the support and security of buyer data to protect it from programmers, who are turning out to be more common constantly.

In this day and age, business banks assume a significant part in monetary foundations, since information should have the option to withstand information breaks and assailants while furnishing customers with dependable administrations. An elective choice is provided for this security reason, but it comes at an enormous expense and consumes a large chunk of the day, making it wasteful. Clients will profit from a more reliable and less tedious framework because of square chain. Therefore, the square chain is the inclined toward choice. The square chain is utilized to build a distributed organization. In the square chain, adaptation to non-critical failure and extensibility are two of the main qualities of this disseminated framework. Shielding the geologically scattered information structure from information misfortune, interior disappointment, and framework end is basic.

II RELATED WORK

Natalia A. Popova and Natalia G. Butakova et al[1], mentioned that this article researches the utilization of Block-tie innovation to shield information about monetary exchanges without the utilization of tokens, explicitly, move aggregates, card nuances, names of individuals, etc This point is huge, since the high level economy is transforming into an essential piece of present day life. The took care of information goes through the data base of banks and portion systems, which potentially makes it open to the aggressor. The article examines the confirmation parts of scattered informational collections, proposes an answer for the issue of staying aware of the independence of information in them dependent on Advancement without tokens, and makes suggestions for how Block-chain progression ought to be introduced in current monetary systems.

ZibinZhengl, ShaoanXiel, Hongning Dai, Xiangping Chen and Huaimin Wang et al[2], mentioned that Square chain, the establishment of Bitcoin, has as of late acquired a ton of consideration. The square chain fills in as an extremely durable record that takes into consideration de-concentrated exchanging. Square chain-based applications are multiplying in an assortment of spaces, including monetary

organizations, notoriety the executives, and the Internet-of Things (IoT). Regardless, there are different difficulties to obstruct chain advancement, for example, flexibility and security concerns, that should be survived. This article gives a thorough outline of square chain development. As a matter of first importance, we give an outline of square chain design prior to considering some normal arrangement calculations utilized in assorted square chains.

WatcharaChatwiriya, et al [3] mentioned that Our overall market is emerging change framework that can have the impact among progress and dissatisfaction. Sharp agreement structures through headways of mechanical improvements are logically viewed as elective developments to influence restrictive cycles out and out. Square chain is a shrewd agreement show with trust offering the potential for making new trade stages and subsequently shows an outrageous distinction in the current core value creation in outcasts. These results in enormous cost and time speculation reserves and the lessened risk for the get-togethers. This audit proposed a procedure to chip away at the usefulness of dispersed understanding in block-chains using pandemic estimation. The results showed that disease shows can pass on the information like square chain

J. Yli-Huumo, D. Ko, S. Choi, S. Park and K Smolander et al,[4] mentioned that Square chain is a decentralized exchange and information the bosses progression grew first for Bitcoin mechanized money. The interest in Block-chain improvement has been stretching out since the examination was made in 2009. The legitimization behind the interest in Block-chain is its focal qualities that give security, secrecy and information reliability with essentially no unapproachable relationship answerable for the exchanges, and in this way it makes fascinating evaluation areas, particularly according to the viewpoint of specific inconveniences and cutoff focuses. In this evaluation, we have composed a careful orchestrating focus on totally reason on get-together all colossal examination on Block-chain headway. We will probably get a handle on the cadenced development research subjects, difficulties and future direction seeing Block-chain advancement according to the particular viewpoint. We have secluded 40 key papers from shrewd information bases. The outcomes show that concentration in more than 81% of the papers is on Bit-coin structure and under 19% plans with other Block-chain applications including for example savvy arrangements and endorsing. Most of evaluation is zeroing in on revealing and further making limits of Block-chain from affirmation and security viewpoints, yet a colossal number of the proposed blueprints need extensive examination on their plentifulness. Different other Block-chain flexibility related difficulties including throughput and inaction have been left unstudied. Taking into account this review, thoughts on future evaluation headings are obliged specialists.

A. Prakash et al[5] mentioned that By and by a days, people are attracting towards demonetization, a quickly evolving globe, and worldwide portion choices, among different variables, have brought about advanced cash. Ventures are searching for an answer that works in cutting edge cash conditions and has a record of an enormous number of trades.. In this paper, we have analyzed Block-chain advancement, a propelling development, which gives an assistance to the endeavors in automated money environment with the record of each trade. We have talk about the various kinds of square chain with the middle thought of hashing computation. We have discussed the utilization of square chain in different endeavors and how it can have the gigantic impact on the business. The paper also revolves around the troubles of square chain which are expected to address before execution. Thusly, With the dread and grin of the beginning of another season of straightforwardness, this paper gives understanding with regards to impede chain advancement.

A. Proposed system

The most astounding feature of bitcoin is its decentralisation, which, thanks to its block-chain-based features, may essentially remove the power of traditional banking systems and monetary institutions. Furthermore, because Bitcoin's digital payment system is based on cryptographic evidence rather than mutual belief, and because its transactions can't be changed without redoing all proofs of work on all block-chains, it can act as a crucial trust intermediary and be widely used in practise, such as recording charitable donations to avoid bribery.

Advantages of proposed system:

We may take use of bitcoin's customizable anonymity method, which improves user safety and privacy, by leveraging this technology. This capability of block-

chain, for example, can be used to produce discovery cards, which not only secure our privacy but also verify our identification. We use two alternative artificial intelligence systems to investigate and predict the price movements of Bit-coin and other digital currency: fully-connected Artificial-Neural Networks and fully-connected Artificial-Neural Networks (A-NN). The use of a block chain provides more security.

B. System Architecture

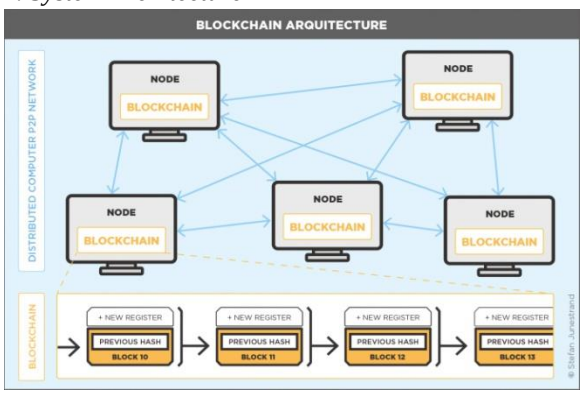

Fig 1: System Architecture

III. METHODOLOGY

The system uses SHA-256 computation. SHA tends to Secure Hashing Function, and 256 grant the numerical proportion of the appropriate piece length. This recommends the objective is right 256 piece, and as alluded to, Bit-coin utilizes a 65-hexadecimal hash regard. Using the SHA-256 breaking point makes it difficult to copy a hash for making the hash a motivating force for a specific square which is also used for endorsing a comparable square. The hashing strategy amasses input information into a respectable size. Hashes see, examine, or run figuring against records and strings of information. When attempting to add to some extent block-chain, the program ought to illuminate for the objective hash with the target for it to appear at attestation as another square. The endorsement is done by PC centers related in the square chain. It ponders the previous hash regard set aside in the system with another hash worth of a square. It makes a hash worth of data in the square. The length and size of the hash regard are something almost identical for a wide scope of data.

In the structure, where two people wish to lead an exchange of money, each with a public and a private key, block-fasten licenses individual A to utilize their private key to mix data concerning the exchange to the public key of individual B. This data together developments some piece of a square, which contains an electronic imprint correspondingly as a timestamp and other pertinent data about the exchange, yet not the characters of people related with that exchange. That square is then conveyed over the square chain system to the total of the focuses, or other part pieces of the structure, which will by then go about as validators for the exchanging of money. Sending of data and supporting square requires enormous extents of figuring power. This is done by diggers present in the structure which supports the square and a short time later places it in the square chain, during the time spent square chain underwriting, a system who surrenders a little piece of their computational ability to offer assistance to the system suitably wins a prize.

IV. PERFORMANCE ANALYSIS

The simulation was performed to test the performance of the existing and proposed work by considering the blocks viz, 10, 20, 30, 40 where the Delay, overhead and throughput was calculated, and the comparison was done for existing as well as for the proposed system. Following are graphs which mention variations with existing and proposed system.

1. Delay(ms)

The time it takes a node to create a new block and validate it on a blockchain is known as delay. The time it takes miners to construct and validate blocks is longer in the existing system than it is in the proposed scheme. This is because the current system necessitates human intervention. In this case, the delay is measured in milliseconds.

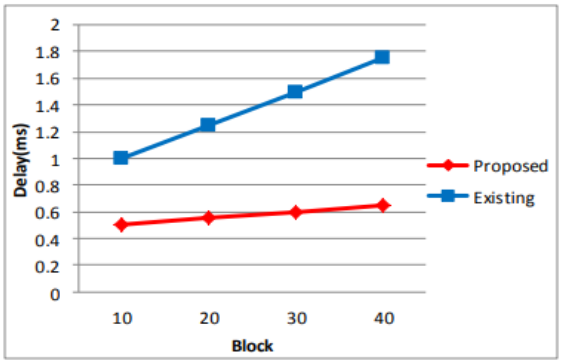

Fig 2: Delay Comparison for Validating Block in Blockchain

Fig 2 shows a comparison of delay with respect to the existing and proposed model, which stated that the performance of proposed is appreciated.

2. Overhead:

Unlike the delay which accounts for single block, the overhead helps us keep track of time lapse of overall blockchain. In a blockchain, multiple copies of blocks have to be maintained in every system. This results in requirement of high network connectivity. Automation techniques are provided for miners thereby making it easier to share the workload while validating and creating new blocks.

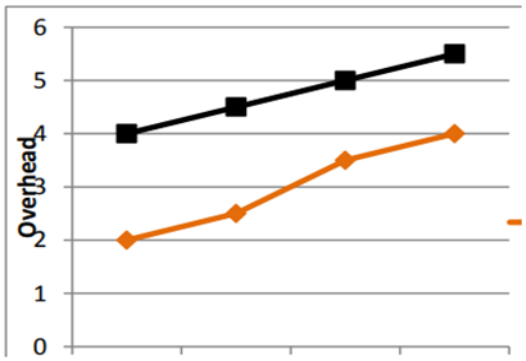

Fig 3: Overhead Comparison in Blockchain

Fig 3 provides a comparison of overhead between the existing and proposed models, indicating that the proposed model's performance is preferred.

3. Throughput:

Throughput is measure of rate of validation of blocks by nodes in a network. In the existing system, humans are miners which take more time, because they have to solve the given mathematical problem to validate and create a new block. In proposed system, nodes take lesser time than the existing system.

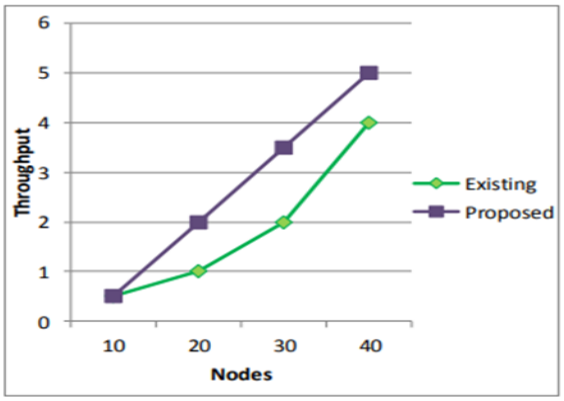

Fig 4: Throughput comparison in the Blockchain

Fig 4 Above figure provides a throughput comparison between the existing and new models, concluding that the proposed model's performance is superior.

V. SNEAKPEEKS OF IMPLEMENTATION

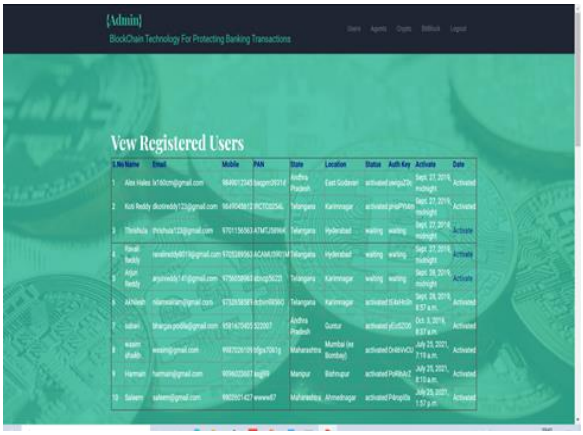

Fig 5: The information about the users and agents registered and admin have to activate the users after this only the users can login successfully.

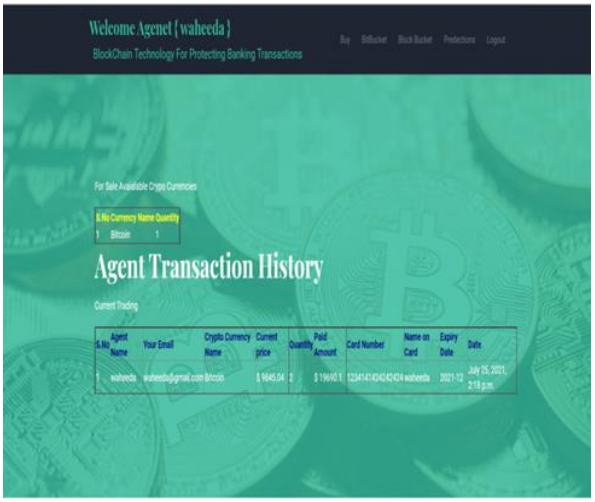

Fig 6: Transaction details

VI. CONCLUSION

Finally, the study finds that the suggested system achieves system security. Block-chain technology is a distributed system that relies on complete data validation and verification without the need of miners or tokens. Eliminating the usage of miners or tokens may result in a more transparent and load-free network, increasing transaction durability. By incorporating block-chain into the distribution of datasets on financial systems, threats on the system

can be reduced. Without tokens, block-chain plays a critical role in constructing a system that is more dependable for banking to conduct transactions that must be extremely safe.

REFERENCES

[1] Natalia A. Popova, Natalia G. Butakova" Research of a Possibility of Using Block-chain Technology without Tokens to Protect Banking Transactions",‖ 978-1-7281-0339-6/19/$31.00 ©2019 IEEE.

[2] Zibin Zheng1, Shaoan Xie1, Hongning Dai2, Xiangping Chen4, and Huaimin Wang3 "An Overview of Block-chain Technology: Architecture, Consensus, and Future Trends" 2017 IEEE sixth International Congress on Big Data

[3] PasuPoonpakdee∗, Jarotwan Koiwanit∗, Chumpol Yuangyai∗ and Watchara Chatwiriya "Applying Epidemic Algorithm for Financial Service dependent on Block-chain Technology" 978-1-5386-4956-5/18/$31.00 ©2018 IEEE

[4] J. Yli-Huumo, D. Ko, S. Choi, S. Park and K Smolander, "Where Is Current Research on Block-chain Technology?- A Systematic Review", PLoS ONE, vol. 11, no. 10, pp. 1-27, 2016.

[5] T. K.Siba, and Prakash, A. (2016). Square Chain: An Evolving Technology. Worldwide Journal of Enterprise Information System, 8(4), 29–35.

[6] Sachchidan and Singh, Nirmala Singh ‖ Block-chain: Future of Financial and Cyber Security‖ 463978-1-5090-5256-1/16/$31.00 c˘2016 IEEE || second International Conference on Contemperary Coumputing and informatics (IC3I)

[7] Rohmat Taufiq, Meyliana, Achmad Nizar Hidayanto and Harjanto Prabowo, "The Affecting Factors of Block-chain Technology Adoption of Payments Systems in Indonesia Banking Industry",

[8] Xin Wang, Xiaomin Xu, Lance Feagan, Sheng Huang, Limei Jiao and Wei Zhao, "Between Bank Payment System on Enterprise Block-chain Platform", 2159–6190/18/\$31.00 ©2018 IEEEDOI 10.1109/CLOUD.2018.00085.2018 IEEE eleventh International Conference on Cloud Computing.

[9] Satoshi Nakamoto " ‖ Bitcoin: A Peer-to-Peer Electronic Cash System"

[10] Soto Méndez Jomar "Present status of Block-chain Technology A Literature Review" Tareq Ahram1, Arman Sargolzaei2, Saman Sargolzaei3,4, Jeff Daniels5, and Ben Amaba6 Block-chain Technology Innovations‖ 2017 IEEE Technology and Engineering Management Conference (TEMSCON).