I.J. Information Engineering and Electronic Business, 2024, 3, 47-56
Published Online on June 8, 2024 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijieeb.2024.03.05

A Progressive Key Administration for Block-Chain Technology with Lagrange Interpolation

Pradeep Kumar*
JSS Academy of Technical Education, Noida, Uttar Pradesh, India
E-mail: pradeep8984@jssaten.ac.in
ORCID iD: https://orcid.org/0000-0001-6177-8527
*Corresponding Author

Ajay Kumar
JSS Academy of Technical Education, Noida, India
E-mail: er.ajay.itcs@gmail.com
ORCID iD: https://orcid.org/0000-0002-3693-9701

Mukesh Raj
JSS Academy of Technical Education, Noida, India
E-mail: er.mukeshraj@jssaten.ac.in
ORCID iD: https://orcid.org/0000-0002-0829-3827

Priyank Sirohi
Assistant Professor, Sir Chhotu Ram Institute of Engineering and Technology, C.C.S. University, Meerut, India
Email: priyanksirohi01@gmail.com
ORCID iD: https://orcid.org/0009-0005-4334-1926

Received: 24 November, 2023; Revised: 11 January, 2024; Accepted: 18 February, 2024; Published: 08 June, 2024

Abstract: Block chain is a computerized data set containing data (like records of monetary exchanges) that can be at the same time utilized and shared inside an enormous decentralized, openly open organization. Block chain development has been a prominent occurrence of changing the statutes of wellbeing in money related trades and information exchange. It offers an extraordinary development for data integration with security. Block chain relies upon the norms of understanding, decentralization, and cryptography for following the trust in trades. In any case, block chain security issues have continued to agitate various affiliations and early adopters. It is sure that, even the grounded block chain new organizations experience burdens in block chain security. Without a doubt, block chain innovation has seen a far-reaching adaption lately. Aside from beginning adaption into digital currencies, today it is being utilized in medical care, land, shrewd contacts, and so forth. The ill-advised execution of innovation has been the reason for some block chain block protection concern, which can put the block chain vulnerable and can permit the aggressors to play out a few noxious exercises. To address the secrecy to the sensitive information in the Block chain organization, a proposed method namely progressive secure key administration for Block-Chain Technology with Lagrange Interpolation (PKABCLI) has been presented in this paper.

Index Terms: Block-chain, Lagrange Interpolation, Key Management, threshold value, modular arithmetic

1. Introduction

Block chain innovation or decentralized secure record is one of the most striking progressions, which can kill the need of outcast to embrace the exchanges over the Peer-to-Peer affiliation. Utilizing the agreement of the current individuals from the organization, exchanges over the organization are approved. In Block chain Technology, people from the association keep the trades' data in sort of record and this record is revived by adding of new block of trades to stay aware of the decency of the data. Satoshi Nakamoto suggested the Block chain based advance currency said to be Bit coin in 2009. In this Bit coin advanced money, exchanges are permitted among the companions to deal with the cash.

The significant benefit of this advanced virtual currency (Bit coin) is that there is no need of focal power to verify, control or approve the exchanges.

Block chain innovation is under creating stage. Nevertheless, this development has shown the likelihood to change the current business process, e-Governance associations, monetary associations, medical care associations, cultivation associations, etc into new aspects where additional advantages in term of usefulness, cost, trust, etc are guaranteed. Block chain innovation is helpful in numerous spaces which join e-Tender through Block chain, Block chain for IoT Devices, Block chain for banking, Block chain for Insurance ensure settlement, Block chain for Taxation, etc. Each block contains two segments namely the header and the body. The header includes block number, hash worth of past block to stay aware of the uprightness of the Chain, hash of collection of Current blocks to stay aware of the reliability of the trade data, timestamp, nonce, Block chain address of the block creator and other needed information. The body of the block includes no less than one trade as can be seen in the Fig. 1.

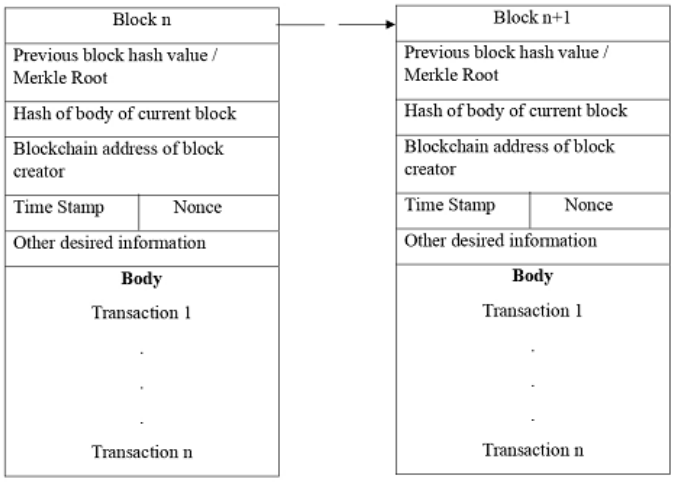

Fig. 1. Block Chain Block Structure

Block chain maintains data in a decentralized manner across the association and maintains a copy of every trade along with a hash of trade data in a form of record for every member of the association. Any intrusive party finds it challenging to alter the set apart data at greater proportion sets in a decentralized limit. As a result, decentralized limits offer greater cryptographic security than bound together limits. The majority of companions support trades. This evolution thus completely eliminates the role of central embracing authority. Because the transaction is underwritten decentralized, hacking is difficult, trades are maintained by arrangement shows, and security expenses are also reduced. Block chain ensures quick data certainty, security, insurance defence, and immutability of all changes requiring larger-part arrangement. Additionally guaranteed is the trade's quickness with the use of superb comprehension. Although the terms "block chain" and "digital money" are sometimes used synonymously, they differ greatly. Crypto-currency money is one of the most well-known uses of block chain technology. This invention has eventually made its way into many other industries. As a result, block chain is illustrated using the example of crypto-currency. Assume for the moment that A needs to send B one currency that Astra carried across the block chain. Public-key cryptography is therefore the most crucial idea to understand.

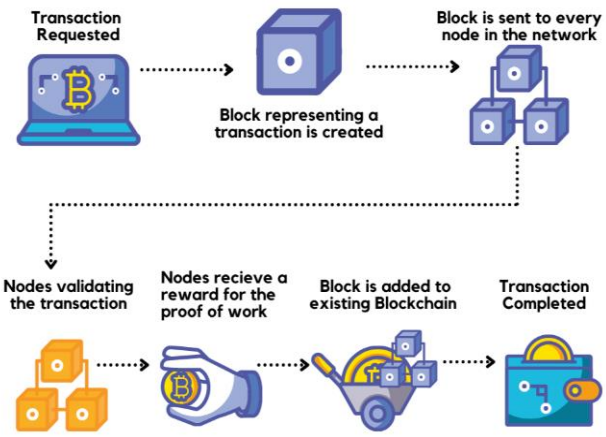

Fig. 2. Working of block chain

To put it another way, owning a crypto coin essentially entails possessing a key pair connected with it. User will now require the following items in order to complete the transaction:

- The private key related with the Astra coin that A holds
- A location on the block chain (his public key)
- B location on the block chain (his public key)
- What's more obviously, the sum ought to be available with A that he wishes to send.

The complete design of the paper is as per the following. Section 2 depicts related work of secret sharing of past approach. In section 3 examine about issue problem statement in block chain. In Section 4, the suggested method reliant on the multilevel secret key distribution reliant on the LaGrange polynomial was explored. The analysis and comparison of our methodology has been discussed in Section 5, and in Section 6 conclusion and future extension have been featured.

2. Related Work

A literature review on block chain technology's security typically encompasses a broad spectrum of research and findings. Security in block chain technology is a vast field with numerous related works and ongoing research.

Manal Alruqi *et al.*[1] Described a medical application that makes use of Mobile Agent Dr-MAPT to keep an eye on a patient's condition by giving the patient and the doctor access to information about their present state of health and by delivering alerts when critical situations arise. By integrating the mobile agent's smart contract, which is based on blockchain technology, with the stationary agent during communication, we have introduced a novel approach to safeguarding the Dr-MAPT. The smart contract, which is linked to the block chain, is a communication channel for the agents. The mobile agent's interactions with other agents are determined by four features of the smart contract. Block chain transactions help identify and stop malicious activity. In addition, the blacklist of the Block chain is employed to detect fraudulent Mobile Agents and obstruct further communication. Ultimately, the research shows how smart contract features meet security requirements like confidentiality, integrity, non-repudiation, authentication, and authorization.

shita Ishita *et al.*[2] In the paper, it was explained how to secure soft mobile agents in MAS using block chain technology. The proposed approach makes use of a Smart Contract that permits mobile agents to carry out a set of authorized operations and monitors deviations from those actions. The SC ensures that a Byzantine mobile agent is quarantined upon detection. Additionally, this technique supports and inhibits Byzantine mobile agent cloning at the SC's interface. Preliminary experiments have proven the effectiveness of the proposed approach. We intend to further study the system's behavior with Byzantine mobile agents and various node-to-mobile-agent ratios. Examining the effects of different network topologies—especially dynamic networks—is also essential. To significantly increase detection time, the one miner in the existing implementation might be increased. Ensuring the security of mobile agents will present fresh opportunities for their application in numerous fields, such as networked robots, IoT, MAS, and more.

Tianqi Zhou *et al.*[3] Block chain is explained, essentially based on engineering, and associated breakthroughs in cryptography are shown. Additionally, the block chain-based threshold key control plot is suggested. The situation sharing plans, which maintain threshold key sharing for two or three partners, are utilized to obtain threshold key control. Participants' health and capacity to adapt to internal failure measurements can be preserved by making use of the covert sharing arrangements. The association between CRT and Shamir's full key administration conspiracy based on secret sharing is also directed, showing that CRT's fundamentally based plan benefits more from recovery actions' complexity than does Shamir's plan.

Muqaddas Nazet al.[4] A block chain-based system for extremely comfortable information exchange and virtual goods delivery is described. The main goal of this scenario is to provide the buyer with amazing and valid data insights, all while maintaining a stable business endeavor stage for the owner. At the owner's stop, a decentralized stockpile IPFS controls the expense of responding to a swelling concern. Hashes of realities stored on the IPFS are encoded using SSS so that a client that does not have a virtual substance material charge recorded will not be able to access current realities. In this way, the owner is content with any form of hash leakage to unauthorized customers. With the use of a survey-based device that allows users to register their comments and rate existing realities, information authenticity is ensured. As a result, new clients can select the highest quality of data, potentially saving money when they cease using the service. Selective smart contracts are designed for various purposes, such as owner-driven settlement for importing the record onto IPFS and jumbling the hashes. The customer feature has the clever agreement on the other side. After verification by representative hubs, a buyer can access the record hashes from smart contact. Finally, both new and existing clients can benefit from the evaluation framework smart settlement's ability to look and register sentiments. The reproduction results for these devious agreements' gas consumption and cost evaluation have been completed. Every brand exhaust a unique fuel charge based on the justifications and intricacy of the actions carried out in each component. Furthermore, different encryption systems are compared based on their computational cost; this paper uses the primary scheme. The findings show that the encryption method that takes the least amount of time to compute is the one that is employed in this study to encrypt stocks.

Sheikh Mohammad*et al*. [5] Block chain generation, which was first proposed as the basis for the first digital currency, is currently being used in many software domain names due to its distinctive features, which guarantee the private, transparent, and easy exchange of data between peers within a distributed network. Their capabilities include time-stamped data, virtual signatures, consensus techniques, cryptographic hashing, and more. The blockchain has made it possible to handle data transfers in an immensely convenient framework without the need for middlemen. The blockchain also offers properties that provide data security and privacy for the community, making the device more comfortable. These qualities include pseudoidentity, resistance to tampering, consistency and secrecy of records, and more. An extensive examination of blockchain technology and its ramifications is given in this paper.

The block chain-based overall structure described by Chaitanya Singh *et al*. [6] cannot be immediately applied to the scientific field. We use the concepts of block chain and distributed storage to provide a user-friendly environment for sharing clinical data. Given the demands of the clinical industry, our proposed approach ensures green execution in terms of cost estimation, data sharing convenience, and reliability. We build an agreeable Medi-Block architecture for realities transfer that is fundamentally based on the decentralised and comfy transmission nature of block chain and local area form.

Om Pal *et al* .[7] Discussed the usage of block chain technology in the Internet of Things era. Additionally, we discussed the necessity of Key Control for Block Chain, which unifies the crucial management for Bit Coin Unknown Cash Pockets and Block Chain Public Key Infrastructure. In addition to ensuring that Block chain hubs are verified, it is essential to ensure that sensitive transactions made via the Block chain organization remain confidential. In order to address the problem of classifying sensitive documents, we suggested a group Key organization (GKM) plot for aesthetically beautiful affiliation dispatch.

Tsung-Chih Hsiao *et al.*[8] Described a key control scheme to improve the security issue in records get admission to. With the innovation of cell specialists, we can without issues fabricate a various levelled admittance make do. Then again, the Lagrange interpolation and get admission to control plans give the executives ability, and the sort and control of agreeable progressive system are accomplished. Moreover, the Lagrange interpolation approach gives elements of smooth computation and compromise obstruction. To cozy statistics access management efficiently, we put in force cell sellers to exclusive files across the device. Positive types of attacks are tended to. Proposed approach is comfortable in opposition to external assaults, reverse attacks, cooperative assaults, and equation assaults.

Tara Salman *et al.* [9] provided a comprehensive description of how block chain technology might be used to provide distributed security administrations. Element verification, classification, protection, provenance, and honesty affirmations are among the services provided. The public key cryptography, which employs encryption and mark plans, can provide element verification and privacy. Following that, we reviewed various block chain-based key management systems for public key cryptography. Furthermore, administrations for protection, provenance, and uprightness confirmation were concentrated in separate places. The qualities that make the block chain innovation a viable competitor for long-term applications is summarised. Then we described each aid, discussed its standards in contemporary systems administration programmes, and highlighted the typical approaches for providing the required assistance, as well as their challenges. Finally, we discussed how block chains can aid in the resolution of these difficulties; we looked into various block chain-based approaches and presented an analysis of them. Finally, we focused on the challenges that are currently restricting the block chain's suitability for security applications. The block chain innovation appears to have enormous promise in a variety of applications; nevertheless, its utility in security applications is still hazy due to a few issues. Future exploration goals include resolving these issues and putting various block chain techniques to the test in large-scale and ongoing scenarios.

Guy Zyskind*et al*. [10]Individual information, and delicate information as a rule, ought not be confided in the possession of outsiders, where they are vulnerable to assaults and abuse. All things considered, clients ought to possess and control their information without compromising security or restricting organizations' and specialists' capacity to offer customized types of assistance. Our foundation empowers this by joining a block chain, re-purposed as an entrance control arbitrator, with an off-block chain stockpiling arrangement. Clients are not needed to trust any outsider and are dependably mindful of the information that is being gathered with regards to them and how it is utilized. Likewise, the block chain sees the customers as the owners of their own data. Associations, subsequently, can focus in on utilizing data without being unreasonably stressed over fittingly getting and compartmentalizing them.

In ICN and similar designs, Nikos Fotiou *et al.* [11] introduced decentralised name-based security devices that mean to get content circulation. Our tools use Hierarchical Character Based Encryption (HIBE) to provide content storage authorization, provenance confirmation, and content integrity protection. Our solution is immune to the negative consequences of the key escrow issue, which is present in many other plans. Furthermore, our solution makes use of block chains to transmit the System Parameters, SP. Block chains don't rely on any central authority or pre-configured in hubs, and they have intriguing security qualities. Our scheme is sufficiently conventional that it can be incorporated into many ICN models or other analogous frameworks. We used Name coin's discrete, IP-based programming to connect to the block chain in our model execution.

Ao Lei *et al*. [12] Describes original key administration plot for key exchange among SMs in heterogeneous VCS organizations. It presents block chain idea and enhances the execution utilizing dynamic exchange assortment periods. The proposed block chain structure permits key exchange safely inside the decentralized SM organization. We fostered a successful and adaptable exchange assortment period choice technique to recoil the key exchange season of block chain plot. Two parts are talked about: block chain based key administration plan and dynamic exchange assortment

plot. We originally concentrated on cryptographic plans' handling time which creates the key exchange time. Also, by re-enacting a reach of 0 to 2000 exchanges move starting with one security space then onto the next, our block chain structure accomplishes more effectiveness and vigor contrasted with the customary design. At last, powerful exchange assortment period further streamline the key exchange time cost. With the assistance of our numerical model, SMs can choose how to utilize diverse exchange assortment periods.

Hsu CL *et al*[8]Here shown both the Wu-Chang and the Shen-Chen plans disregard the necessities characterized in a key task conspire for a poset client ordered progression. In the two plans, if there exist (at least two) security classes having the equivalent quick successor(s), the vindictive insider can approach the data things held by the people who are not his replacements without following the predefined to some degree requested connection. At long last, we utilize the single direction hash capacity to dispense with the security releases intrinsic in the two plans.

Chin-Chen Chang *et al*. [13] suggested a dynamic and flexible cryptographic key task conspire for admission control in a partially requested order. Certain substitutes' intrigue will almost certainly fail to unearth their archetype's secret key and will be comparatively incapable of creating their kin's mysterious key. As a result, our strategy is safe. By using the key acceptance, it is capable of inferring any of its swaps' keys for any security class. When a new class is introduced to the framework or an old one is removed from the framework, it can choose not to refresh those current keys.

Arcangelo Castiglione *et al*. [14] considered progressive key task plans supporting unique updates, like inclusions and erasures of classes and relations between classes, just as key substitutions and client repudiations. Broadened existing security thought for progressive key task plans, specifically, security regarding key lack of definition, by furnishing the foe with additional assault capacities. Then, using a symmetric encryption plot as a structure block, we described the optimal technique to create a progressive key task conspire that supports unique updates. It's important to note that this is the most accessible approach for non-static settings, in which the foe is allowed to gradually refresh the order. In terms of key indistinctness, the proposed development is provably secure and only requires a single computational suspicion. Furthermore, it provides efficient key determination and refreshing methods while only requiring each client to keep a single private key. The proposed strategy may become an important technique for various levelled admission control applications in powerful conditions due to its simplicity, feasibility, and vigour. Haowen Tan *et al*. [15] Describes wireless body area network (WBAN) framework model with a notice channel is planned. Also, an effective group key administration convention utilizing the Chinese remainder theorem (CRT) among healthcare centre (HC) and personal controller (PCs) is presented, which supports secure gathering key refreshing. Thusly, the HC is fit for broadcasting the message to various patient gatherings. In this way, the HC is fit for broadcasting the message to various patient gatherings. Furthermore, the group key plan among PC and sensors is planned, which is inspired by coded cooperative data exchange (CCDE). Formal security examination is given, demonstrating that the proposed convention can accomplish the ideal security properties. Besides, execution investigation shows that the proposed convention is effective contrasted and the best in class.

3. Problem Statement

Any cryptographic system finds it difficult to organise keys in a productive and secure manner. Gate crashers can take everything from the assigned structure if they can witness the keys through any means, such as noise power, side channel attack, actual system access, weak encryption, replay attack, and so on. As a result, the chiefs of keys are one of the most important components of the cryptographic system. No business can be considered secure if its keys aren't secure**.**

3.1 Proposed Key administration for Block chain organization

Protection of critical transactions' secrecy and competent encryption of payload are also significant issues of the Block chain Technology's setup time. We present a secure and Key Management framework for Block chain advancement to assure the security and successful encryption of payload at the understanding stage. When separate places are linked through a single layered plan, a piece of one region's transactions may not add any value to other regions. Complex designing is the best option in this situation. We anticipated a diverse architecture in our suggested system, with upper-layer hubs having a greater number of advantages and privileges than lower-level hubs.

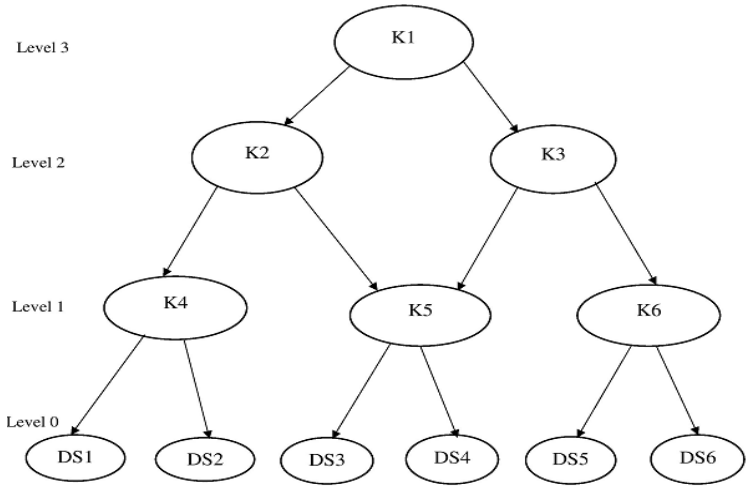

Fig. 3. Hierarchical key administration for Block-Chain

3.2 Secure key creation phase

Hierarchical Lagrange interpolation used to obtain the decryption key for every confidential blocks. The main steps proposed scheme as follow.

Step 1: Randomly chooses a huge prime number q= $2q' + 1$, where q' is additionally a huge prime number. Then, at that point, the picked r is a root of Galois field GF(q) and makes r, q and q' public.

Step 2: Blockchain chooses distinctive decryption keys DS_t(t = 1,2, …, n, with n being the quantity of decryption keys) for each secret report, where DS_t and q-1 are moderately prime.

Step 3: Blockchain chooses distinctive secret keys SK_i (i= 1,2, …, n, with n being the quantity of visited hosts), where SK_i and q-1 are moderately prime and SK_i is private.

Step 4: The interpolation work is set up as follows.

$$F_{DS_t}(x)=x \times DS_t \times \sum_{DS_t \le SC_i} X_{i,t}^{-1}\, m_{i,t}(x) \tag{1}$$

Where $m_{i,t}(x)$ is the Lagrange interpolation polynomial?

$$\left\{ m_{i,t}(x) = \prod_{s=1, s\neq i}^{n} \frac{x-x_{s,t}}{x_{i,t}-x_{s,t}} \right. \tag{2}$$

In the above equation, $DS_t \le SC_i$means that SC_i is approved to get to the private report t which is encrypted using the encryption keyDS_t; $x_{s,t} = ID_t || \ r^{sk_2} \ (\%q)$, where ID_t is the identity of the private record and || is the connection administrator.

$$\begin{cases} m_{1,5}(x) = \left(\frac{x-x_{2,5}}{x_{1,5}-x_{2,5}}\right)\left(\frac{x-x_{3,5}}{x_{1,5}-x_{3,5}}\right)\left(\frac{x-x_{4,5}}{x_{1,5}-x_{4,5}}\right)\left(\frac{x-x_{5,5}}{x_{1,5}-x_{5,5}}\right)\left(\frac{x-x_{6,5}}{x_{1,5}-x_{6,5}}\right) \\ = \frac{x-ID_5 || \ r^{sk_2}(\%q)}{ID_5 || \ r^{sk_1}(\%q) - ID_5 || \ r^{sk_2}(\%q)} \times \frac{x-ID_5 || \ r^{sk_3}(\%q)}{ID_5 || \ r^{sk_1}(\%q) - ID_5 || \ r^{sk_3}(\%q)} \\ \times \frac{x-ID_5 || \ r^{sk_4}(\%q)}{ID_5 || \ r^{sk_1}(\%q) - ID_5 || \ r^{sk_4}(\%q)} \times \frac{x-ID_5 || \ r^{sk_5}(\%q)}{ID_5 || \ r^{sk_1}(\%q) - ID_5 || \ r^{sk_5}(\%q)} \\ \times \frac{x-ID_5 || \ r^{sk_6}(\%q)}{ID_5 || \ r^{sk_1}(\%q) - ID_5 || \ r^{sk_6}(\%q)} \end{cases} \tag{3}$$

$$\begin{cases} m_{3,5}(x) = \left(\frac{x-x_{1,5}}{x_{3,5}-x_{1,5}}\right)\left(\frac{x-x_{2,5}}{x_{3,5}-x_{2,5}}\right)\left(\frac{x-x_{4,5}}{x_{3,5}-x_{4,5}}\right)\left(\frac{x-x_{5,5}}{x_{3,5}-x_{5,5}}\right)\left(\frac{x-x_{6,5}}{x_{3,5}-x_{6,5}}\right) \\ = \frac{x-ID_5 || \ r^{sk_1}(\%q)}{ID_5 || \ r^{sk_3}(\%q) - ID_5 || \ r^{sk_1}(\%q)} \times \frac{x-ID_5 || \ r^{sk_2}(\%q)}{ID_5 || \ r^{sk_3}(\%q) - ID_5 || \ r^{sk_2}(\%q)} \\ \times \frac{x-ID_5 || \ r^{sk_4}(\%q)}{ID_5 || \ r^{sk_3}(\%q) - ID_5 || \ r^{sk_4}(\%q)} \times \frac{x-ID_5 || \ r^{sk_5}(\%q)}{ID_5 || \ r^{sk_3}(\%q) - ID_5 || \ r^{sk_5}(\%q)} \\ \times \frac{x-ID_5 || \ r^{sk_6}(\%q)}{ID_5 || \ r^{sk_3}(\%q) - ID_5 || \ r^{sk_6}(\%q)} \end{cases} \tag{4}$$

$$\begin{cases} m_{6,5}(x) = \left(\frac{x-x_{1,5}}{x_{6,5}-x_{1,5}}\right)\left(\frac{x-x_{2,5}}{x_{6,5}-x_{2,5}}\right)\left(\frac{x-x_{3,5}}{x_{6,5}-x_{3,5}}\right)\left(\frac{x-x_{4,5}}{x_{6,5}-x_{4,5}}\right)\left(\frac{x-x_{5,5}}{x_{6,5}-x_{5,5}}\right) \\ = \frac{x-\mathrm{ID}_5||\ \mathrm{r}^{\mathrm{sk}_1}(\%q)}{\mathrm{ID}_5||\ \mathrm{r}^{\mathrm{sk}_6}(\%q)\ -\mathrm{ID}_5||\ \mathrm{r}^{\mathrm{sk}_1}(\%q)} \times \frac{x-\mathrm{ID}_5||\ \mathrm{r}^{\mathrm{sk}_2}(\%q)}{\mathrm{ID}_5||\ \mathrm{r}^{\mathrm{sk}_6}(\%q)\ -\mathrm{ID}_5||\ \mathrm{r}^{\mathrm{sk}_2}(\%q)} \\ \times \frac{x-\mathrm{ID}_5||\ \mathrm{r}^{\mathrm{sk}_3}(\%q)}{\mathrm{ID}_5||\ \mathrm{r}^{\mathrm{sk}_6}(\%q)\ -\mathrm{ID}_5||\ \mathrm{r}^{\mathrm{sk}_3}(\%q)} \times \frac{x-\mathrm{ID}_5||\ \mathrm{r}^{\mathrm{sk}_4}(\%q)}{\mathrm{ID}_5||\ \mathrm{r}^{\mathrm{sk}_6}(\%q)\ -\mathrm{ID}_5||\ \mathrm{r}^{\mathrm{sk}_4}(\%q)} \\ \times \frac{x-\mathrm{ID}_5||\ \mathrm{r}^{\mathrm{sk}_5}(\%q)}{\mathrm{ID}_5||\ \mathrm{r}^{\mathrm{sk}_6}(\%q)\ -\mathrm{ID}_5||\ \mathrm{r}^{\mathrm{sk}_5}(\%q)} \end{cases} \tag{5}$$

$$\mathrm{F}_{\mathrm{DS}_5}(x) = x \times\ \mathrm{DS}_5 \times \{\left(x_{1,5}\right)^{-1} m_{1,5}(x) + \left(x_{3,5}\right)^{-1} m_{3,5}(x) + \left(x_{6,5}\right)^{-1} m_{6,5}(x)\} \tag{6}$$

$$\begin{cases} m_{1,5}(x_{3,5}) = \left(\frac{x_{3,5}-x_{2,5}}{x_{1,5}-x_{2,5}}\right)\left(\frac{x_{3,5}-x_{3,5}}{x_{1,5}-x_{3,5}}\right)\left(\frac{x_{3,5}-x_{4,5}}{x_{1,5}-x_{4,5}}\right)\left(\frac{x_{3,5}-x_{5,5}}{x_{1,5}-x_{5,5}}\right)\left(\frac{x_{3,5}-x_{6,5}}{x_{1,5}-x_{6,5}}\right) \\ = \frac{x_{3,5}-\mathrm{ID}_5||\ \mathrm{r}^{\mathrm{sk}_2}(\%q)}{\mathrm{ID}_5||\ \mathrm{r}^{\mathrm{sk}_1}(\%q)\ -\mathrm{ID}_5||\ \mathrm{r}^{\mathrm{sk}_2}(\%q)} \times \frac{\mathrm{ID}_5||\ \mathrm{r}^{\mathrm{sk}_3}(\%q)-\mathrm{ID}_5||\ \mathrm{r}^{\mathrm{sk}_3}(\%q)}{\mathrm{ID}_5||\ \mathrm{r}^{\mathrm{sk}_1}(\%q)\ -\mathrm{ID}_5||\ \mathrm{r}^{\mathrm{sk}_3}(\%q)} \\ \times \frac{x_{3,5}-\mathrm{ID}_5||\ \mathrm{r}^{\mathrm{sk}_4}(\%q)}{\mathrm{ID}_5||\ \mathrm{r}^{\mathrm{sk}_1}(\%q)\ -\mathrm{ID}_5||\ \mathrm{r}^{\mathrm{sk}_4}(\%q)} \times \frac{x_{3,5}-\mathrm{ID}_5||\ \mathrm{r}^{\mathrm{sk}_5}(\%q)}{\mathrm{ID}_5||\ \mathrm{r}^{\mathrm{sk}_1}(\%q)\ -\mathrm{ID}_5||\ \mathrm{r}^{\mathrm{sk}_5}(\%q)} \\ \times \frac{x_{3,5}-\mathrm{ID}_5||\ \mathrm{r}^{\mathrm{sk}_6}(\%q)}{\mathrm{ID}_5||\ \mathrm{r}^{\mathrm{sk}_1}(\%q)\ -\mathrm{ID}_5||\ \mathrm{r}^{\mathrm{sk}_6}(\%q)} \\ = 0 \end{cases} \tag{7}$$

$$\begin{cases} m_{3,5}(x_{3,5}) = \left(\frac{x_{3,5}-x_{1,5}}{x_{3,5}-x_{1,5}}\right)\left(\frac{x_{3,5}-x_{2,5}}{x_{3,5}-x_{2,5}}\right)\left(\frac{x_{3,5}-x_{4,5}}{x_{3,5}-x_{4,5}}\right)\left(\frac{x_{3,5}-x_{5,5}}{x_{3,5}-x_{5,5}}\right)\left(\frac{x_{3,5}-x_{6,5}}{x_{3,5}-x_{6,5}}\right) \\ = \frac{\mathrm{ID}_5||\ \mathrm{r}^{\mathrm{sk}_3}(\%q)-\mathrm{ID}_5||\ \mathrm{r}^{\mathrm{sk}_1}(\%q)}{\mathrm{ID}_5||\ \mathrm{r}^{\mathrm{sk}_3}(\%q)\ -\mathrm{ID}_5||\ \mathrm{r}^{\mathrm{sk}_1}(\%q)} \times \frac{\mathrm{ID}_5||\ \mathrm{r}^{\mathrm{sk}_3}(\%q)-\mathrm{ID}_5||\ \mathrm{r}^{\mathrm{sk}_2}(\%q)}{\mathrm{ID}_5||\ \mathrm{r}^{\mathrm{sk}_3}(\%q)\ -\mathrm{ID}_5||\ \mathrm{r}^{\mathrm{sk}_2}(\%q)} \\ \times \frac{\mathrm{ID}_5||\ \mathrm{r}^{\mathrm{sk}_3}(\%q)-\mathrm{ID}_5||\ \mathrm{r}^{\mathrm{sk}_4}(\%q)}{\mathrm{ID}_5||\ \mathrm{r}^{\mathrm{sk}_3}(\%q)\ -\mathrm{ID}_5||\ \mathrm{r}^{\mathrm{sk}_4}(\%q)} \times \frac{\mathrm{ID}_5||\ \mathrm{r}^{\mathrm{sk}_3}(\%q)-\mathrm{ID}_5||\ \mathrm{r}^{\mathrm{sk}_5}(\%q)}{\mathrm{ID}_5||\ \mathrm{r}^{\mathrm{sk}_3}(\%q)\ -\mathrm{ID}_5||\ \mathrm{r}^{\mathrm{sk}_5}(\%q)} \\ \times \frac{\mathrm{ID}_5||\ \mathrm{r}^{\mathrm{sk}_3}(\%q)-\mathrm{ID}_5||\ \mathrm{r}^{\mathrm{sk}_6}(\%q)}{\mathrm{ID}_5||\ \mathrm{r}^{\mathrm{sk}_3}(\%q)\ -\mathrm{ID}_5||\ \mathrm{r}^{\mathrm{sk}_6}(\%q)} \\ = 1 \end{cases} \tag{8}$$

$$\begin{cases} m_{3,5}(x_{3,5}) = \left(\frac{x_{3,5}-x_{1,5}}{x_{6,5}-x_{1,5}}\right)\left(\frac{x_{3,5}-x_{2,5}}{x_{6,5}-x_{2,5}}\right)\left(\frac{x_{3,5}-x_{3,5}}{x_{6,5}-x_{3,5}}\right)\left(\frac{x_{3,5}-x_{4,5}}{x_{6,5}-x_{4,5}}\right)\left(\frac{x_{3,5}-x_{5,5}}{x_{6,5}-x_{5,5}}\right) \\ = \frac{x_{3,5}-\mathrm{ID}_5||\ \mathrm{r}^{\mathrm{sk}_1}(\%q)}{\mathrm{ID}_5||\ \mathrm{r}^{\mathrm{sk}_6}(\%q)\ -\mathrm{ID}_5||\ \mathrm{r}^{\mathrm{sk}_1}(\%q)} \times \frac{x_{3,5}-\mathrm{ID}_5||\ \mathrm{r}^{\mathrm{sk}_2}(\%q)}{\mathrm{ID}_5||\ \mathrm{r}^{\mathrm{sk}_6}(\%q)\ -\mathrm{ID}_5||\ \mathrm{r}^{\mathrm{sk}_2}(\%q)} \\ \times \frac{\mathrm{ID}_5||\ \mathrm{r}^{\mathrm{sk}_3}(\%q)-\mathrm{ID}_5||\ \mathrm{r}^{\mathrm{sk}_3}(\%q)}{\mathrm{ID}_5||\ \mathrm{r}^{\mathrm{sk}_6}(\%q)\ -\mathrm{ID}_5||\ \mathrm{r}^{\mathrm{sk}_3}(\%q)} \times \frac{x_{3,5}-\mathrm{ID}_5||\ \mathrm{r}^{\mathrm{sk}_4}(\%q)}{\mathrm{ID}_5||\ \mathrm{r}^{\mathrm{sk}_6}(\%q)\ -\mathrm{ID}_5||\ \mathrm{r}^{\mathrm{sk}_4}(\%q)} \\ \times \frac{x_{3,5}-\mathrm{ID}_5||\ \mathrm{r}^{\mathrm{sk}_5}(\%q)}{\mathrm{ID}_5||\ \mathrm{r}^{\mathrm{sk}_6}(\%q)\ -\mathrm{ID}_5||\ \mathrm{r}^{\mathrm{sk}_5}(\%q)} \\ = 0 \end{cases} \tag{9}$$

$$\begin{cases} \mathrm{F}_{\mathrm{DS}_5}(x_{3,5}) = \ x_{3,5} \times\ \mathrm{DS}_5 \times \{\left(x_{1,5}\right)^{-1} m_{1,5}(x) + \left(x_{3,5}\right)^{-1} m_{3,5}(x) + \left(x_{6,5}\right)^{-1} m_{6,5}(x)\} \\ = \ \mathrm{ID}_5||\ \mathrm{r}^{\mathrm{sk}_3}(\%q) \times\ \mathrm{DS}_5 \times \{\left(\mathrm{ID}_5||\ \mathrm{r}^{\mathrm{sk}_1}(\%q)\right)^{-1} \times 0 \\ +\left(\mathrm{ID}_5||\ \mathrm{r}^{\mathrm{sk}_3}(\%q)\right)^{-1} \times 1 + \left(\mathrm{ID}_5||\ \mathrm{r}^{\mathrm{sk}_6}(\%q)\right)^{-1} \times 0\} \\ = \mathrm{ID}_5||\ \mathrm{r}^{\mathrm{sk}_3}(\%q) \times\ \mathrm{DS}_5 \times \left(\mathrm{ID}_5||\ \mathrm{r}^{\mathrm{sk}_3}(\%q)\right)^{-1} \\ = \mathrm{DS}_5 \end{cases} \tag{10}$$

4. Implementation and Results

The proposed approach various levelled key administration dependent on Lagrange interpolation carried out in python programming language. Table 1 represents the comparison of proposed methodology with other methods das 2005, chang 2004 and haowen tan 2018 for key generation phase. Time required (sec) to generate secure key versus block size. As a result, if increasing the size of block the key generation time will increase. After the analysis of in term of time proposed methodology will take less time as compare to other method proposed by Haowen Tan 2018, and chang 2004 provide the multilevel security, multilevel security of secure key is another advantage as compare to other methods. But proposed methodology takes large time as compare to Das 2005 but advantage is multilevel security. Fig 4 addresses the time adopted by proposed strategy to produce key share. It is seen from the outcome that the execution time of proposed approach is very low.

Table 1. Comparison of proposed scheme with another scheme (secret key generation phase)

No of blocks (bit)	200	400	600	800	1000	1200	1400
Das 2005	2	5	8	14	21	29	34
chang 2004	3	8	15	22	31	41	49
Haowen Tan 2018	2.8	7	14	16	28	34	41
Proposed	**2.3**	**6**	**13**	**17**	**24**	**32**	**36**

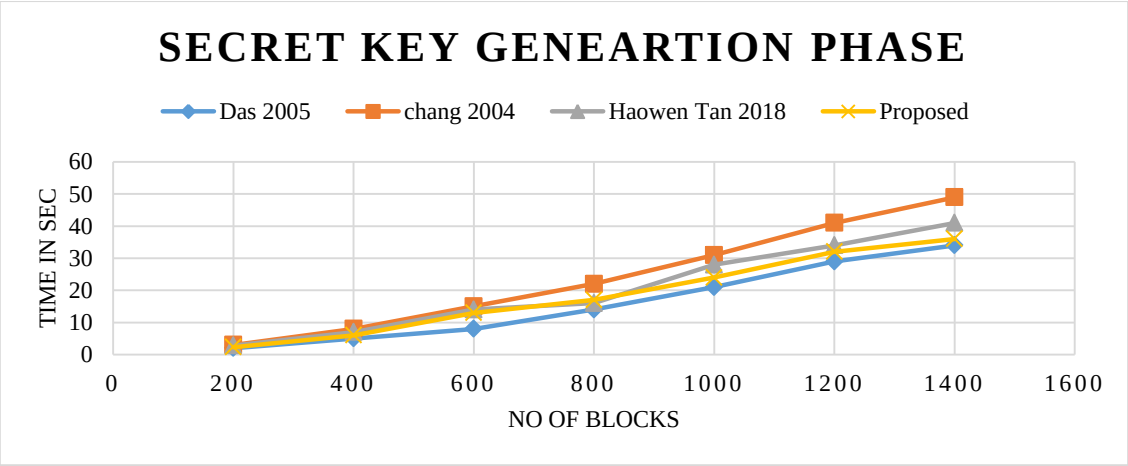

Fig. 4. Secret key generation for block chain

Table 2 represents the comparison of proposed methodology with other methods das 2005, chang 2004 and haowen tan 2018 for key derivation phase. Time required (sec) to derivation of secure key versus block size. As a result, if increasing the size of block the key derivation time will increase. After the analysis of in term of time proposed methodology will take less time as compare to other method proposed by Haowen Tan 2018, and chang 2004 provide the multilevel security, multilevel security of secure key is another advantage as compare to other methods. The proposed methodology takes large time as compare to Das 2005 but advantage is multilevel security. Figure 5 addresses the time adopted by proposed strategy to derivation of secure key. It is seen from the outcome that the execution time of proposed approach is very low. Another advantage of proposed methodology only upper level generates the key of lower level vice versa not possible.

Table 2. Comparison of proposed scheme with another scheme (secret key derivation phase)

No of blocks (bit)	200	400	600	800	1000	1200	1400
Das 2005	0.4	1.2	1.9	2.6	3.6	4.9	5.1
chang 2004	0.6	1.5	2.6	3.8	5.2	6.5	7.6
Haowen Tan 2018	0.58	1.4	2.4	3.1	4.9	5.9	6.9
Proposed Method	**0.5**	**1.3**	**2.1**	**3**	**4.1**	**5.2**	**6.1**

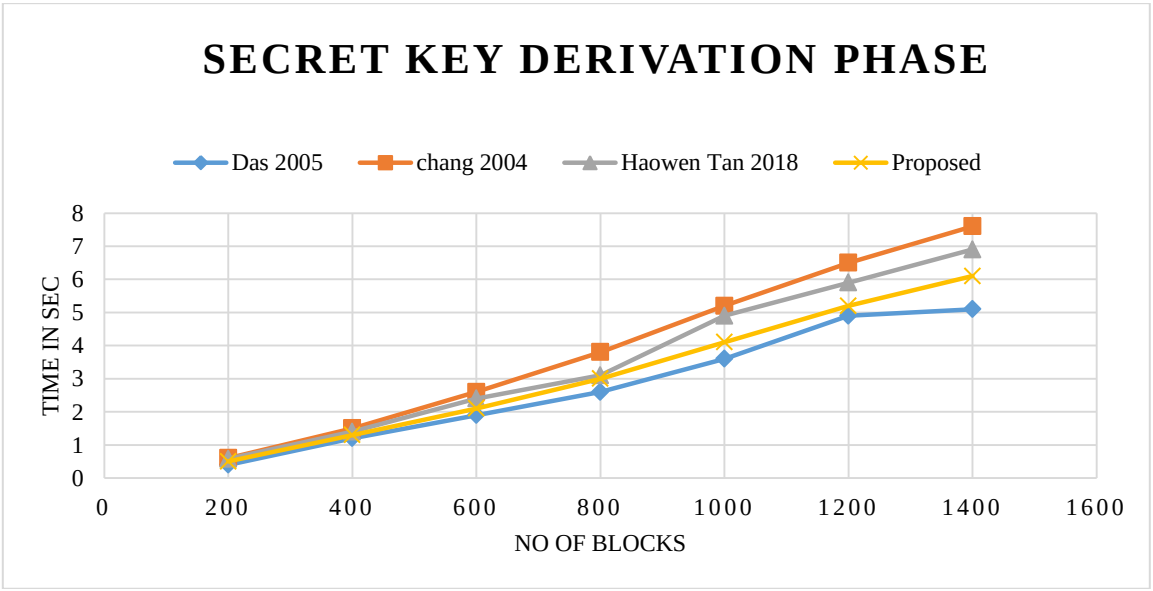

Fig. 5. Secret key derivation for Block Chain

5. Collusions and Future Scope

The scheme of safety for Blocks during the communication of blocks in block chain technology is as yet an essential issue. In this paper, another augmentation Lagrange interpolation has been intended to make a blocks security at multilevel. This new methodology gives the protection of key security utilizing limit esteems and a secret key administration conspires. This methodology assists with checking the security of access of blocks in block chain technology. The proposed authentication framework of blocks security expands the critical security just as key administration plot. The suggested method for key generation phase block size vs time analysis shows that it takes less time between 2.3 and 36 seconds. In comparison to the previous strategy, it is rather optimal. The derivation secret key similar takes 0.5 to 6.1 seconds to complete. In comparison to earlier tragedies, this is also the best. We focused towards further developing the security perspectives blocks in block chain and thus, it opens up new bearings of other examination to meet other security prerequisites. In future work other security models which will be more summed up and cater the need of block security just as distinguishing the Unreliable hosts will be helpful for basic application. This would assist with saving the figuring worldview of blocks from cheating and a few new application regions will be profited from the proposed work.

References

[1] M. Alruqi, L. Hsairi, and A. Eshmawi, *Secure mobile agents for patient status telemonitoring using blockchain*, vol. 1, no. 1. Association for Computing Machinery, 2020.

[2] I. Ishita, D. Kulkarni, T. Semwal, and S. B. Nair, "On securing mobile agents using blockchain technology," *2019 2nd Int. Conf. Adv. Comput. Commun. Paradig. ICACCP 2019*, 2019, doi: 10.1109/ICACCP.2019.8882907.

[3] T. Zhou, J. Shen, Y. Ren, and S. Ji, "Threshold Key Management Scheme for Blockchain-Based Intelligent Transportation Systems," *Secur. Commun. Networks*, vol. 2021, 2021, doi: 10.1155/2021/1864514.

[4] M. Naz *et al.*, "A Secure Data Sharing Platform Using Blockchain and Interplanetary File System," *Sustain.*, vol. 11, no. 24, pp. 1–24, 2019, doi: 10.3390/su11247054.

[5] I. Applications, "Security Aspects of Blockchain Technology Intended for," pp. 1–24, 2021.

[6] C. Singh, D. Chauhan, S. A. Deshmukh, S. S. Vishnu, and R. Walia, "Medi-Block record: Secure data sharing using block chain technology," *Informatics Med. Unlocked*, vol. 24, no. April, p. 100624, 2021, doi: 10.1016/j.imu.2021.100624.

[7] O. Pal, B. Alam, V. Thakur, and S. Singh, "Key management for blockchain technology," *ICT Express*, vol. 7, no. 1, pp. 76–80, 2021, doi: 10.1016/j.icte.2019.08.002.

[8] T. C. Hsiao, Z. Y. Wu, T. L. Chen, Y. F. Chung, and T. S. Chen, "A hierarchical access control scheme based on Lagrange interpolation for mobile agents," *Int. J. Distrib. Sens. Networks*, vol. 14, no. 7, 2018, doi: 10.1177/1550147718790892.

[9] T. Salman, M. Zolanvari, A. Erbad, R. Jain, and M. Samaka, "Security services using blockchains: A state of the art survey," *IEEE Commun. Surv. Tutorials*, vol. 21, no. 1, pp. 858–880, 2019, doi: 10.1109/COMST.2018.2863956.

[10] G. Zyskind, O. Nathan, and A. S. Pentland, "Decentralizing privacy: Using blockchain to protect personal data," *Proc. - 2015 IEEE Secur. Priv. Work. SPW 2015*, pp. 180–184, 2015, doi: 10.1109/SPW.2015.27.

[11] N. Fotiou and G. C. Polyzos, "Decentralized name-based security for content distribution using blockchains," *Proc. - IEEE INFOCOM*, vol. 2016-September, pp. 415–420, 2016, doi: 10.1109/INFCOMW.2016.7562112.

[12] A. Lei, H. Cruickshank, Y. Cao, P. Asuquo, C. P. A. Ogah, and Z. Sun, "Blockchain-Based Dynamic Key Management for Heterogeneous Intelligent Transportation Systems," *IEEE Internet Things J.*, vol. 4, no. 6, pp. 1832–1843, 2017, doi: 10.1109/JIOT.2017.2740569.

[13] C. C. Chang, I. C. Lin, H. M. Tsai, and H. H. Wang, "A key assignment scheme for controlling access in partially ordered user hierarchies," *Proc. - Int. Conf. Adv. Inf. Netw. Appl.*, vol. 2, pp. 376–379, 2004, doi: 10.1109/aina.2004.1283826.

[14] A. Castiglione, A. De Santis, B. Masucci, F. Palmieri, A. Castiglione, and X. Huang, "Cryptographic Hierarchical Access Control for Dynamic Structures," *IEEE Trans. Inf. Forensics Secur.*, vol. 11, no. 10, pp. 2349–2364, 2016, doi: 10.1109/TIFS.2016.2581147.

[15] H. Tan and I. Chung, "A secure and efficient group key management protocol with cooperative sensor association in WBANs," *Sensors (Switzerland)*, vol. 18, no. 11, pp. 1–25, 2018, doi: 10.3390/s18113930.

Authors' Profiles

Pradeep Kumar is completed Ph.D. in computer engineering and engineering at Department of Computer Engineering Shobhit Institute of Engineering & Technology (Deemed-to-be University), Meerut, 250110. He has obtained his M.Tech. in Computer Science and engineering Department of Computer Engineering Shobhit Institute of Engineering & Technology (Deemed-to-be University), with first class. He obtained his B.Tech in Computer Engineering and engineering degree from college of engineering Roorkee, India in 2006 with first class.

Ajay Kumar, Assistant Professor in the Department of Computer Science & Engineering at JSS Academy of Technical Education, Noida. He has received his M. Tech (Computer Engineering) from YMCA University of Science & Technology, Faridabad, India, and B. Tech (Computer Engineering) from University Institute of Engineering & Technology, M.D.U. Rohtak. He has more than 10 years of academic experience. He has contributed 09 Research papers in International Journal and 11 Research papers in International/National Conferences/proceedings and Edited Books. He has added 02 Patents with his name out of which 01 has granted. His areas of research are Machine Learning, IOT & Network Security. He has organized various workshops and FDPs in these areas. He is the lifetime member of International Association of Engineers (IAENG).

Mukesh Raj, Assistant Professor in the department of Computer Science and Engineering at JSS Academy of Technical Education Noida (UP) having a teaching experience of approx. 10 Years. Has taken his Bachelor of Engineering in CSE from Rajiv Gandhi Proudyogiki Vishwavidyalaya, Bhopal Madhya Pradesh. There after done the M Tech in CSE from Maulana Abul Kalam Azad University of Technology, Kolkata West Bengal and working as Assistant Professor. Pursuing PhD in Computer Science & Engineering from NIT Jamshedpur (Jharkhand). Domain of research is ML in information and network security, ML in medical diagnosis.

Priyank Sirohi is a Ph.D. student of computer engineering and engineering at Department of Computer Engineering Shobhit Institute of Engineering & Technology (Deemed-to-be University), Meerut, 250110. He has obtained his M.Tech. in Computer Science and engineering Department of Computer Engineering Shobhit Institute of Engineering & Technology (Deemed-to-be University), with first class. He obtained his B.Tech degree in Information Technology engineering from RGEC Meerut *college of UPTU,* India in 2006 with first class. Presently he is working as Assistant Professor in the department of Information Technology at Sir Chhotu Ram Institute of Engineering & Technology, Chaudhary Charan Singh University, Meerut.

How to cite this paper: Pradeep Kumar, Ajay Kumar, Mukesh Raj, Priyank Sirohi, "A Progressive Key Administration for Block-Chain Technology with Lagrange Interpolation", International Journal of Information Engineering and Electronic Business(IJIEEB), Vol.16, No.3, pp. 47-56, 2024. DOI:10.5815/ijieeb.2024.03.05