MATHEMATICAL MODELING APPROACHES FOR BLOCKCHAIN TECHNOLOGY

K Suresh Kumar¹, R Rajeswari², Ch Vidyadhari³, B Santhosh Kumar⁴

¹Assistant Professor/ECE, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Andhra Pradesh.
²Professor/ECE, Rajalakshmi Institute of Technology, Chennai, India,
³Assistant Professor/CSE, Gokaraju Rangaraju Institute of Engineering and Technology Hyderabad, Telangana, India
⁴Sr. Assistant Professor/CSE, GMR Institute of Technology, Rajam Andhra Pradesh, India

E-Mail: m.k.sureshkumar@kluniversity.in

Abstract. These days blockchain innovation has become a significant issue as of late and greatly affected the business. Even though blockchain innovations was reliable for security issues, advantageous administrations, and difficulties for procedure assumes a significant key job that we have to break down. To have a superior observation about this square chain innovation, we will find out about the essential security highlights like-expanded limit, better security, unchanging nature, quicker settlement, and decentralized framework. The range of blockchain applications limits from budgetary, human services, vehicle, chance administration, Internet of things to open and social administrations. In this paper, by examining its structure to various agreement calculations just as difficulties and openings, we endeavor to lead an expansive going review on blockchain innovation and also the few mathematical models behind this blockchain technology.

Keywords: Security, Privacy, Bitcoin, Smart contract

1. INTRODUCTION

A Blockchain is an information structure that makes it conceivable to imagine a computerized record of information and offer among a system of independent gatherings. Blockchain assembles changeless records and accounts of different exchanges, however, nothing is truly persevering. At the point when we talk about the blockchain innovation, the primary component that strikes to our brain is Bitcoin. The absolute first utilization of blockchain is Bitcoin which is a kind of advanced money built upon blockchain innovations. A blockchain is a distributed framework with no noteworthy coordinating information stream. To expel an essential control while keeping up information honesty is, by having an expansive circulated system of independent clients. This implies the PCs that make up the system are in more than one area. To
restrain the system from being debased, not exclusively are square chains decentralized, yet they frequently utilize digital currency. Cryptographic money is an advanced symbolic that has market esteem. Cryptocurrencies [1] are substituted on trades like stocks. Essentially the product pays the equipment to lock-in. This product has notable blockchain conventions that incorporate Bitcoin [2], Ethereum, Ripple, Hyper record, and Factom. The equipment exists of full hubs accomplishing the information in the system. Bitcoin brought the idea of blockchain and keen agreements into the consciousness of everybody.

**Figure 1. Simple blockchain architecture**

Blockchain isn’t only a solitary thought, anyway it is a blend of various thoughts like cryptography, science, sorting out, scattered arrangement advancement, calculations. It is awkward to deal with issues with spread information base synchronization with the appropriated accord. The qualities are Transparent, Distributed, Autonomy, Immutable Anonymity, and Open-source. Smart contracts [3] [4] are fundamentally PC programs loaded in a blockchain. These agreements are utilized to imbrute the tenacious exchange of crypto-tokens between clients. It is a code running in the head of the blockchain innovation containing a lot of rules with which parties under that agreement will concede. The understanding will without a doubt be required. This is one of the basic types of decentralized robotization. The essential nature of the brilliant agreements is Self-executing, Self-confirming, and Tamper safe.

Blockchain is a variety of square having the exhaustive rundown of exchange records. The engineering contains a few layers explained below. Accord layer, a convention that plots the configuration of a record that is freely obvious and an agreement work that anybody can use to direct which of different competitor records is according to record. The convention should likewise permit new squares to be added to the record. Mining layer, a protocol that urges gatherings to keep up the accord and add different squares to the record. Spread layer, a convention that rules how the record and squares are communicated between hubs in the network. Semantic layer, a specification of how new squares must identify with past squares and
a convention for validating similarity with the determination. Application layer, application code that instruments some ideal usefulness. In the field of Machine Learning, we can provide security using blockchain technology like Machine Learning, Plant Disease Prediction [5] [6], Security [7] [8], Forgery Detection [9], and so on.

In a large portion of these applications, they manage sensitive information, so security ought to be required, to give protection, information trustworthiness, and accessibility [2] [3]. The organization incorporates a social event of lightweight battery controlled devices and a distant establishment to record and screens the overall condition (building, city, wild regions, and so on). The intrinsic issue of the characteristic issue of as far as possible limited shared exchange speed, low estimation power, low stockpiling, and confined battery life [10]. Right when centers are passed on in closed-off scenes or catastrophe help domains constrain of the sensor hubs is an enormous test. In light of its confined resources, giving computationally genuine security features is a tremendous test. Be that as it may, offering security to the hub and guaranteeing information correspondence mystery is basic to keeping up the mystery, respectability, and openness (CIA) so required. In such organizations, the security shortcomings of different layers of the association from physical to the application layer are highlighted by [11] [12]. One such advancement that ensures the utilization of the CIA gathering of three as a group in security is Blockchain innovation. Blockchain gives an overall advanced record to be used for each structure of trade and record in a deliberate request. It is public, regardless, it’s fixed, hub disappointment lenient, and secure without the need or help of any confined in an outsider. This makes it an intriguing methodology to apply concerning such an appropriated network and is used for cryptographic forms of money (Bitcoin, Etherium, Ripple, etc) [13] with remarkable accomplishment, however grows a danger to the conventional monetary financial framework. A remote sensor network framework is wanted to plan to help a Blockchain by contemplating the confined computational power, battery life, and limit of the sensor hubs in a solitary hand and leads engineering advancement to decrease control overhead required for directing and square updates and equalizations energy among bunch heads.

2. RELATED WORK

In a trade, the record is made: For instance, Mr. An is offering four of his coins to Mr. B for Rs.3000. This record plans the nuances close by electronic mark from each fighting gathering. The information which gets recorded is affirmed on a framework. The center points on this framework will check the nuances of record to persuade the authenticity of the trade. The record which has been supported by a framework is added to the square. Every square will contain a particular code which is called the hash. It contains a hash of the past square of the chain. Directly the square is added to the blockchain. The hash code will relate the squares in a specific solicitation. This hash code watches the record with paying little brain to the record size. Any change to the current record will make a new hash. Finally, this will change the whole course of action of hash. Hash will hint that data has been modified or not.

An elective arrangement between various social events is drafted as code into the blockchain. The substances included are unidentified, anyway, the understanding is open record. A made an event like pass date and strike cost is hit and the understanding hangs itself as demonstrated by the coded things. Regulators can have the utilization of blockchain to understand the activity in the market while sparing the security of individual performers’ positions. There are a couple of preferences for the on-screen character under savvy contracts [14] [15] like Autonomy, Trust, Backup, Safety, Speed, Savings, and Accuracy. Hash, at whatever point the trade is drilled, it had been hash to code and subsequently convey to every center. There is an enormous number
of trades that are contained in a couple of center points. Blockchain uses the Merkle tree ability to make last hash regard which is in like manner called the Merkle tree root. Timestamp, Time of the square made.

A touch of data verification is difficult to make implies that at any rate direct for others to affirm and satisfied certain essentials. Bitcoin uses Hash cash insistence of the work structure. Mining implies that by determining the Proof of Work. The confirmation of work must pass on a value that makes header regard, but it’s anything but a "Weight Target"[23]. Diggers must complete a proof of work to ensure the attestation by engineering individuals. The work trouble is changed to limit the rate at which new squares could be made by the framework ordinarily. The low chances of powerful age, made it blemished which authority Personal Computer in the framework will make the going with the square. This procedure needn’t lounge around with any expensive dealing with force. A Proof of stake may give extended security from a subverting attack on the framework. With Proof of Stake, the favored position that is pondered is the whole minor holds. For example, a person having one percentage of the bitcoin can mine the one percentage of the "Certification of Stake squares"[24]. Additional affirmation begins with two extraordinary sources. One is Executing an attack would be through and through more exorbitant and another is Reduce reason for the attack. The assailant needs to have a near a huge amount of all bitcoins.

3. MATHEMATICAL APPROACHES AND CHALLENGES IN BLOCKCHAIN

In the previous hardly any years, analysts and experts have featured the likelihood of Blockchain and appropriated record innovation to reevaluate the administration forms. Blockchain innovation empowers disseminated power and implanted security. As such, blockchain is viewed as a broadly useful innovation, offering better approaches for association in numerous spaces. The Ethereum [16] blockchain is one of the most progressive and accessible blockchains in the biological systems. It has its Turing- complete Programming language (the full working programming language that awards engineers to construct a kind of utilization). It obtained the most elevated situation in blockchain advancement and use cases. It might be one of the most confounded blockchains ever constructed. The Ethereum biological system is by and by the best spot to build up the decentralized applications. Fast advancement time, security for little applications and the capacity for applications to effectively team up with each other are the fundamental key attributes of this framework. In the research community working in the Markov process as follows,

\[ P[X(t_n) \leq x_n | X(t_{n-1}) \leq x_{n-1}, X(t_{n-2}) \leq x_{n-2}, \ldots, X(t_0) \leq x_0] = P[X(t_n) \leq x_n | X(t_{n-1}) \leq x_{n-1}] \ldots \]

Turing-Complete Programming Language (TCPL) is the key component that creates the Ethereum blockchain tremendously more impressive than the Bitcoin blockchain for building new projects. Ethereum’s scripting language makes things like Twitter application conceivable in scarcely any lines of code, and exorbitantly secure. The most radical and contested clarification of Ethereum is oneself overseeing and decentralized application (DAPP). It can oversee things like computerized resources and DAOs (Decentralized Autonomous Organization). These applications run on an exclusively manufactured blockchain, an incredibly ground-breaking shared worldwide framework that can move an incentive around and speak to the responsibility for.

This e-government [17] [18] requires part of utilizations for its working. The blockchain was gathering the information and use with respect to e-government are to some degree new in insightful composition. In this e-government process, the significant inclination depends on genuine sources and electronic distinguishing proof, clearness in the exchanges, cross fringe
adaptability and the whole procedure being client-driven. The e-government fit for blockchain innovation is so far under mishandled [19][22]. A report from the European commission when discussing the infiltration and digitalization of the government in different kinds of sections have been summed up for various nations in four distinct regions of advantageous, expandable, unexploited, and non-unified types of e-government. In Blockchain technology the acceptance of payment through elliptic curve digital signature algorithm. The elliptic curve equation is,

\[ b^2 = a^3 + xa + y \]

(2)

Normally in Bitcoin the value of \( x=0, y=7 \), so simply \( b^2 = a^3 + 7 \). In particular, in elliptic curve digital signature algorithm addition of two points \((r1,r2)\) and \((s1,s2)\), and the doubling of \((r1,r2)\), are performed as follows:

- Addition of \((r1,r2)\) and \((s1,s2)\): \( c = (r2 - r2) / (s1 - s1) \mod M \)
  \[ t1 = c^2 - r1 - r1 \mod M \]
  \[ t2 = c (r1 - t1) - p2 \mod M \]

- Doubling of \((r1,r2)\): \( c = (3 r1^2) / (2 r2) \mod M \)
  \[ t1 = c^2 - 2r1 \mod M \]
  \[ r2 = c (r1 - s1) - r2 \mod M \]

**Figure 2. The elliptic curve for Bitcoin**

Blockchain innovation execution is being examined in countless enterprises, extending from flexible chain to money related administrations. No scrutinizing that dispersed record innovation is probably the best development of late occasions, almost certainly, it will take an unprecedented measure of time before the innovation is embraced generally. To oversee security blockchain has given a solid help, still, it is confronting difficulties. There is an expansion in blockchain use volume and advance in the number of exchanges happening regular schedule, blockchain has gotten immense. Exchanges are put away in hubs for getting approval. To begin with, the current exchange source should be evaluated before the exchange itself. Both Bitcoin and Ethereum, the well-known blockchain systems, have encountered eased back exchange speeds and higher expenses charged per exchange because of a significant increment in clients.
Protection leakage: The primary powerlessness of the blockchain is spillage of exchange security because the specifics of the open keys and the equalizations are seen to every single one. The Markov chain\cite{23} property is,

$$P(X_{t+1} = s \mid X_t = s_t, X_{t-1} = s_{t-1}, \ldots, X_0 = s_0) = P(X_{t+1} = s \mid X_t = s_t)$$

This can be disseminated in the unknown arrangement and blending arrangement.

The Markov chain\cite{1} transition probability $T_r(y_2|y_1)$ is,

$$T_r = (T_1)_{r=0,1,2}$$

The distribution of probability $p(t)$ is,

$$p(t) = Tp(0)$$

Childish Mining is a significant danger in the blockchain. A square is available for cheating regardless of whether a little intensity of hashing power is utilized. The specific mined square is kept with the digger with no correspondence on arranging and will assemble a different branch in the wake of meeting the necessities. The fitting excavators will sit around idly and assets and the private chain will be mined without anyone else focused diggers. Individual Identifiable Information\cite{20} is the tale identified with blockchain and character is that blockchain bears perfect dispersed option rather than concentrated database stockpiling for Personal Identifiable Information. Blockchain can bolster laying Personal Identifiable Information on the chain or used to imagine proof on the chain which focuses on off-chain for Personal Identifiable Information stockpiling\cite{21}. The Criminal Connection of bitcoin has been for quite some time associated with the obscure dealings of the bootleg market and the dull web. Since this is the primary collaboration of the general population with blockchain innovation, this association has sought after with bitcoin, and the tech hidden it too.

4. CONCLUSION

Blockchain has indicated its likelihood of changing the standard industry with its key qualities like decentralization, persistence, and riddle and survey limit. This paper we are using the wide chart to give an investigation of various blockchain types of progress which includes the blockchain arranging and we explain the key assigns of blockchain. By then discussion about the regular accord figuring which we are used in the blockchain methods. The government needs to make some similar laws for this innovation, and undertaking ought to prepare for getting a handle on the blockchain innovation. To determine the mechanical difficulties, we propose the investigation into blockchain innovation norms and reference engineering for e-government applications. Likewise, a way to deal with study the mathematical modeling outcomes with greater force on the authoritative setting in creating blockchain-based applications is required.

References

\[1\] H. Wang, Y. Li, X. Zhao, and F. Yang, “An algorithm based on markov chain to improve edge cache hit ratio for blockchain-enabled IoT,” China Communications, vol. 17, no. 9, pp. 66–76,
Sep. 2020..

[2] S. Bagad and S. Vijayakumaran, “On the Confidentiality of Amounts in Grin,” 2020 Crypto Valley Conference on Blockchain Technology (CVCBT), Jun. 2020.

[3] P. Gururaj, “Identity management using permissioned blockchain,” 2020 International Conference on Mainstreaming Block Chain Implementation (ICOMBI), Feb. 2020.

[4] C. P. Jagrat and J. Channegowda, “A Survey of Blockchain Based Government Infrastructure Information,” 2020 International Conference on Mainstreaming Block Chain Implementation (ICOMBI), Feb. 2020.

[5] R. Cristin, B. S. Kumar, C. Priya, and K. Karthick, “Deep neural network based Rider-Cuckoo Search Algorithm for plant disease detection,” Artificial Intelligence Review, vol. 53, no. 7, pp. 4993–5018, Feb. 2020.

[6] K. Loheswaran, T. Daniya, and K. Karthick, “Hybrid Cuckoo Search Algorithm with Iterative Local Search for Optimized Task Scheduling on Cloud Computing Environment,” Journal of Computational and Theoretical Nanoscience, vol. 16, no. 5, pp. 2065–2071, May 2019.

[7] S. Vellianigiri, R. Cristin, and P. Karthikeyan, “Genetic Gray Wolf Improvement for Distributed Denial of Service Attacks in the Cloud,” Journal of Computational and Theoretical Nanoscience, vol. 15, no. 6, pp. 2330–2335, Jun. 2018.

[8] B. S. Kumar, R. Cristin, K. Karthick, and T. Daniya, “Study of Shadow and Reflection based Image Forgery Detection,” 2019 International Conference on Computer Communication and Informatics (ICCCI), Jan. 2019.

[9] A. Kaur, S. Kumar Arora, and M. Masud, “Comparative Analysis of Clustering using AODV DSDV and CBRP,” International Journal of Engineering & Technology, vol. 7, no. 3.8, p. 131, Jul. 2018.

[10] A. K. Bashir, R. Arul, S. Basheer, G. Raja, R. Jayaraman, and N. M. F. Qureshi, “An optimal multitier resource allocation of cloud RAN in 5G using machine learning,” Transactions on Emerging Telecommunications Technologies, vol. 30, no. 8, May 2019.

[11] N. B. Gayathri, G. Thumbur, P. Rajesh Kumar, M. Z. U. Rahman, P. V. Reddy, and A. Lay-Ekuakille, “Efficient and Secure Pairing-Free Certificateless Aggregate Signature Scheme for Healthcare Wireless Medical Sensor Networks,” IEEE Internet of Things Journal, vol. 6, no. 5, pp. 9064–9075, Oct. 2019.

[12] B. Santhosh Kumar, M. P. Geetha, G. Padmapriya, and M. Premkumar, “AN APPROACH FOR IMPROVING THE LABELLING IN A TEXT CORPORA USING SENTIMENT ANALYSIS,” Advances in Mathematics: Scientific Journal, vol. 9, no. 10, pp. 8165–8174, Sep. 2020.

[13] T. M. Thekkil and N. Prabakaran, “Minimizing Remote Monitoring Service Cost of Wireless Sensor Networks Using Krill Swarm Optimization,” Wireless Personal Communications, vol. 109, no. 2, pp. 1429–1448, Jun. 2019.

[14] S. D. M. Achanta, K. T., and V. K. R., “A wireless IOT system towards gait detection technique using FSR sensor and wearable IOT devices,” International Journal of Intelligent Unmanned Systems, vol. 8, no. 1, pp. 43–54, Jul. 2019.

[15] S. P. Reddy Karri and B. Santhosh Kumar, “Deep Learning Techniques for Implementation of Chatbots,” 2020 International Conference on Computer Communication and Informatics (ICCCI), Jan. 2020.
[16] Brahman, P. K., Suresh, L., Lokesh, V., & Nizamuddin, S. (2016). Fabrication of highly sensitive and selective nanocomposite film based on CuNPs/fullerene-C 60 /MWCNTs: An electrochemical nanosensor for trace recognition of paracetamol. Analytica Chimica Acta, 917, 107–116. doi:10.1016/j.aca.2016.02.044

[17] G. V. S. Karthik, S. Y. Fathima, M. Z. U. Rahman, S. R. Ahamed, and A. Lay-Ekuakille, “Efficient Signal Conditioning Techniques for Brain Activity in Remote Health Monitoring Network,” IEEE Sensors Journal, vol. 13, no. 9, pp. 3276–3283, Sep. 2013.

[18] B. S. Kumar and R. Cristin, “A Survey on Efficient Power Management Using Smart Socket and IoT,” Review of Computer Engineering Research, vol. 5, no. 2, pp. 25–30, 2018.

[19] R. Rajakumar, J. Amudhavel, P. Dhamavelan, and T. Vengattaraman, “GWO-LPWSN: Grey Wolf Optimization Algorithm for Node Localization Problem in Wireless Sensor Networks,” Journal of Computer Networks and Communications, vol. 2017, pp. 1–10, 2017.

[20] B. S. Kumar, T. Daniya, N. Sathya, and R. Cristin, “Investigation on Privacy Preserving using K-Anonymity Techniques,” 2020 International Conference on Computer Communication and Informatics (ICCCI), Jan. 2020.

[21] K. Girija Sravani, G. Sai Lakshmi, and K. Srinivasa Rao, “Design and Optimization of Piezoresistive Materials Based Microbridge for Electro-osmosis Pressure Sensor,” Transactions on Electrical and Electronic Materials, vol. 20, no. 3, pp. 198–205, Feb. 2019.

[22] P. Goswami, Z. Yan, A. Mukherjee, L. Yang, S. Routray, and G. Palai, “An energy efficient clustering using firefly and HML for optical wireless sensor network,” Optik, vol. 182, pp. 181–185, Apr. 2019.

[23] T. Daniya, M. Geetha, and K. Suresh Kumar, “Classification And Regression Trees with Gini Index,” Advances in Mathematics: Scientific Journal, vol. 9, no. 10, pp. 8237–8247, Sep. 2020.

[24] C. C. Vignesh and S. Karthik, “Predicting the position of adjacent nodes with QoS in mobile ad hoc networks,” Multimedia Tools and Applications, vol. 79, no. 13–14, pp. 8445–8457, Apr. 2018.