IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

Impact Factor: 7.301

Volume 3, Issue 5, June 2023

Block Chain Management based for Security of Cognitive Radio

Parmod Kumar[1] and Dr. Hitanshu Saluja[2]

Research Scholar, Department of ECE, Ganga Technical Campus, Soldha, Bahadurgarh, India[1]

Head of Department, Department of ECE, Ganga Technical Campus, Soldha, Bahadurgarh, India[2]

Abstract: *The recent advances in wireless communication have led to the problem of growing spectrum scarcity. The problem of spectrum allocation is due to advance research in wireless communication. As new wireless applications are emerging, day after another, and making use of the available wireless spectrum for communication, the demand for spectrum increase makes the available spectrum scarcer. Mostly part of the spectrum is not utilized significantly in the wireless network. Cognitive Radio (CR) is a new technology that enables an unlicensed secondary user to coexist with licensed primary users in licensed spectrum bands without inducing interference to licensed primary users communication. This technology can significantly ease the spectrum redundancy problem & enhance the efficiency of utilization of spectrum. Cognitive Radio Networks (CRN) or Dynamic Spectrum Access Networks are formed by several CR nodes and they are often called NeXt Generation (XG) communication networks. This XG communication network is expected to give high transfer speed to versatile clients through heterogeneous remote designs and dynamic range access procedures. CRNs have drawn in incredible exploration interest in the new years. Nonetheless, research on the security parts of CRNs has been exceptionally restricted. As CRN is like a remote organization, the idea of the remote media is outside, it is more helpless against assaults when contrasted with that of a wired organization. This channel might be stuck/abuse due to remote media information is to be listened to*

Keywords: Blockchain, CRN Security, Error Rate, NES Algorithm

I. INTRODUCTION

Blockchain adoption is gaining huge momentum as industry is evolving at a fast pace. Many startups have initiated use cases and there is significant rise in investments in blockchain projects as well. Although blockchain is still evolving in terms of technological maturity, innovative experimental adoption and customization are continuously rising. Blockchain has the potential of displacing a setup innovation and stirs up the business or a pivotal item that makes a totally new industry and initial trends with the rise of crypto currencies has signaled that blockchain has been disruptive for the banking industry and financial services.

Crypto currency has the potential of shaking a centralized banking system by eliminating the need to pay fees for using credit or debit cards. Recent Trends have shown that blockchain is turning out to be a sustaining technology rather disruptive and has huge potential in supply chain, healthcare, Internet of Things (IoT), education and public services.Commercial viability and acceptability of blockchain are on the rise and 3021 patent families related to blockchain applications are divided into four sub-categories based on different types of application like Payments and Transaction systems, Financial services business, Administration and E-commerce. Extensive use of cryptography and decentralization makes it highly secure. Privacy issues over public blockchains can be addressed by implementing blockchain in a controlled manner (permissioned blockchain). Blockchains can be named public, private or half and half variations, contingent upon their application[4].

- Public – No one owns Public blockchains, they are fully decentralized and are visible by anyone.
- Private – These are also referred to as permissioned blockchains and uses privilege to control who can peruse from and write to the blockchain.
- Hybrid – These blockchains are public just to an advantaged bunch. Agreement measure is constrained by special workers utilizing a bunch of rules consented to by all gatherings

DOI: 10.48175/568

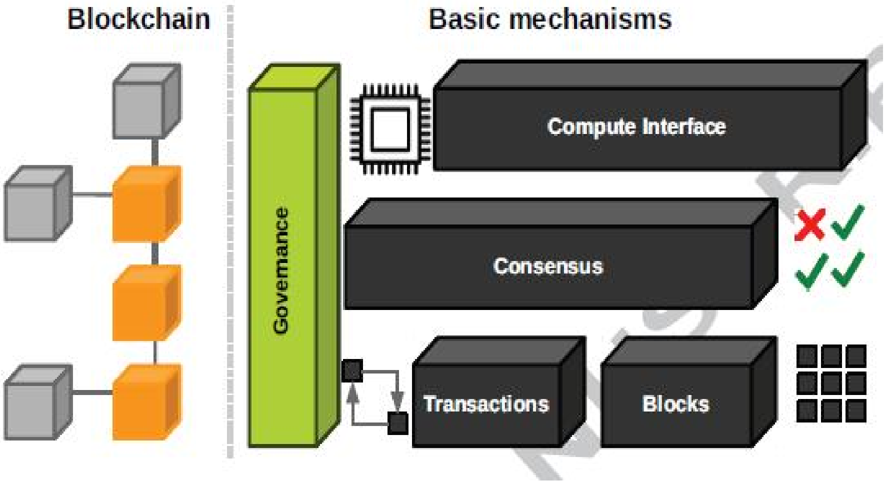

Figure 1: An Overview Of Block Chain Architecture[4].

Blockchain may record exchanges, contracts, data resources or for all intents and purposes whatever can be put away in advanced structure. Blockchain records are lasting, carefully designed, straightforward, and accessible. Each new "block" created is added to the furthest limit of a "chain." Initiation, validation, storage, and distribution of each new block is managed by a protocol. Blockchain replaces the need of third-party intermediaries and participants of blockchain run complex algorithms to certify the integrity of records in the block.

Blockchain hence is an interesting alternative to how data is stored. Databases have been the way to store data in databases. Though databases are quite fast and user friendly, they too have limitations and issues like lack of immutability. Following table highlights key differences between blockchain and databases[5]

Table 1: Comparison of Databases With Blockchain[5]

Criteria	Databases	Blockchain
Data Integrity	Records and Data items can be changed.	Transaction data is immutable, can’t be changed after the transaction.
Authority	Administrator or selected people have authoritative control	No central authority.
Transparency	All transactional data is hidden from each other.	All transactional data is open for everyone.
Cost	Implementation Process is costly.	It can help in cutting down excessive costing.
Performance	They are comparatively faster.	They are slow.
Trust	Suitable for organizations having mutual trust.	Suitable for organizations where people don’t trust each other.

Blockchain is a system having various components that work together to perform transactions of business operations. Each element in the blockchain has a specific role to play as listed below[4].

Node: Node is a computing device within a blockchain that can initiate, receive or validate a transaction. A node operates with the help of a software application that offers various functionalities related to the business use case. Blockchain typically has two kinds of nodes i.e., validator nodes and member nodes. Validator nodes have more capabilities as compared to member nodes as they could initiate, received & validated a transaction whereas defined nodes can only initiate & receive a transaction.

- Transaction: Transaction in a blockchain is a collection of various data items that carries facts about the exchange of something like product, service, entity, event or anything that carries value. For example, it could be transfer of ownership, issue of certificate etc.
- Block: A Block is a data structure that keeps a set of transactions. Every block on successful verification is distributed to all nodes of the blockchain network. A block contains various elements as shown in Table 2.

Block number can be used for unique identification of blocks in a chain of blocks. Nonce is a random number that helps generate a hash code with reasonably difficult mathematical computation. Previous represents the hash code of the previous block and Hash represents hash code of current block.

- Chain: Chain in a Blockchain is an interconnected sequence of blocks in chronological order with the latest block in the last with each block having reference to its previous block to trace back the complete blockchain.

Table 2. Block Structure in A Blockchain Radio Networks Summary[5]

Block	# 1				
Nonce	36584				
Transaction	Rs 65	from	Ravi	to	Mohit
	Rs 30	from	Pankaj	To	Vishal
Transaction	Rs 65	from	Ravi	to	Mohit
	Rs 30	from	Pankaj	To	Vishal
	Rs 45	from	Ravi	To	Mohit
	Rs 50	from	Rohit	To	Sonu
	Rs 30	from	Mohit	To	Kunal
Previous	0000000000000000000000				
Hash	0000ab2des234f453f4r5tfe34				

- Miners: a blockchain may have two kinds of nodes Miner nodes (also called Network nodes) and User Nodes. Miners are the one who have the copy of the blockchain and they also participate in the block verification process, whereas User nodes can only initiate a transaction[5].
- Consensus: Consensus algorithms are used to assure necessary conformity on a single state of the network consisting of distributed machines or network nodes in a blockchain system. The consensus is assessed by comparing the hash codes of all copies of the chain. This assessment involves mathematical problem solving that requires a lot of computing power. For this provision of reward is required for people to contribute resources for maintaining the network. Following are some popular consensus algorithms
- Proof of work (PoW) mechanism: In this mechanism all the network nodes or participants on the network fetch recent transactions as a block. Each block within the chain must have hash code of the previous block. To select a network node who will be assigned to process the block, a reasonably complex mathematical problem is created. The node that solves the given mathematical problem first is allowed to process the block. For doing this job, the network node is rewarded that could be transaction fee or some bitcoin. The complexity of the mathematical problem increases after every successful transaction i.e. the network node needs to compute larger hash codes. The complexity of the mathematical problem is also determined by the number of network nodes in the blockchain network[4].
- Proof of stake is a mechanism that requires network nodes to invest a native currency to perform a transaction i.e. users need to possess stake in the transaction. For example ether is the native currency in Ethereum blockchain, and a fraction of ether is invested by network nodes for processing of transactions and achieving consensus.
- Proof of activity this scheme of consensus combination of work proof & stake proof mechanisms. A random number of network nodes have to perform complex mathematical problems and need to digitally sign the block using a crypto key to make a block official.
- Proof of capacity This scheme is depend on the idea of contribution of storage and computation resources by all network nodes. This requires network nodes to allocate a portion of their hard drive for block verification, while proof of storage requires network nodes to reserve a portion of disk space either in machine or a distributed cloud.
- Ripple (XRP) Ripple follows a different approach and involves social networks for achieving consensus on the basis of value of network nodes. This value is computed on the basis of the number of unique nodes one connects to. This may encourage biasing where newcomers need social intelligence and reputation to participate. This scheme is more suitable for permissioned or private blockchain systems[5].

II. BLOCKCHAIN USE CASE SELECTION AND DESIGN PROCESS

- Blockchain use case selection involves many decisions based on following criteria and NITI Ayog has published a blockchain use case selection framework [4] as shown in Figure 2 that covers all these.
- Is there a compelling business case to reduce intermediaries?
- Are Multiple Stakeholders Involved?
- Are we working with advanced resources rather than actual Assets?
- Do numerous gatherings require shared compose access?
- Do we require superior and fast exchanges?
- Do we plan to store non-conditional information as a feature of your answer?
- Do we need to depend on believed parties for consistence reasons?
- Do we have a powerful Tokenomics Model?
- Do we need the capacity to control usefulness?
- Should exchanges be public?
- The structure presents following four potential results dependent on models,
- Don't use blockchain

Blockchain can't do this effectively yet solutions are in development shown fig 3

- Strong case for public blockchain
- Strong case for private blockchain

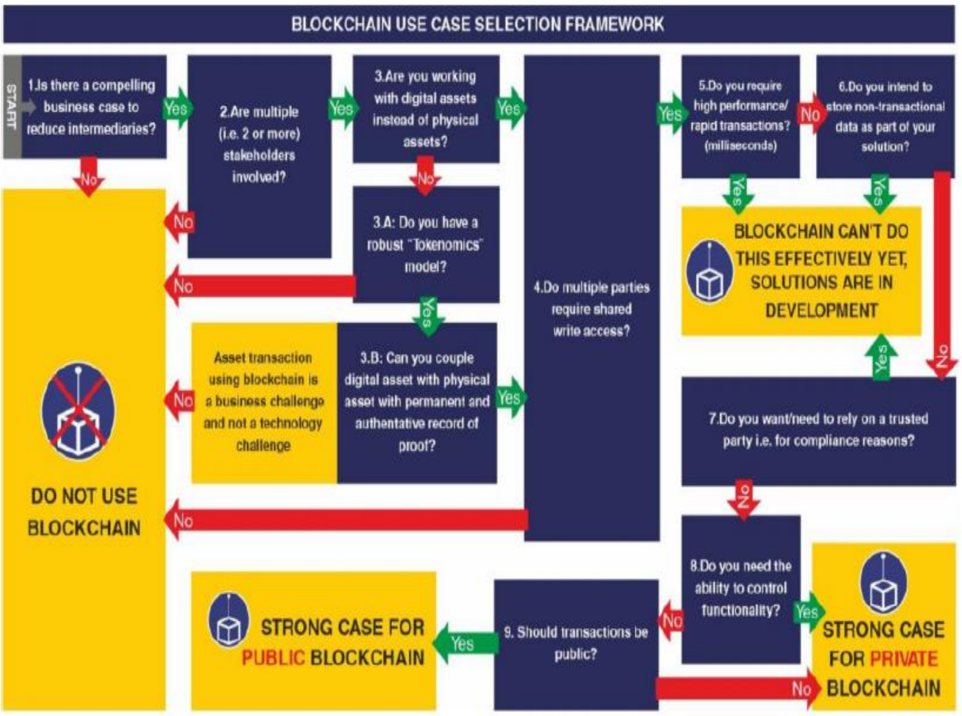
BLOCKCHAIN USE CASE SELECTION FRAMEWORK
START
1.Is there a compelling business case to reduce intermediaries?
Yes
No
2.Are multiple (i.e. 2 or more) stakeholders involved?
Yes
No
3.Are you working with digital assets instead of physical assets?
Yes
No
3.A: Do you have a robust "Tokenomics" model?
No
Yes
3.B: Can you couple digital asset with physical asset with permanent and authentative record of proof?
Yes
No
Asset transaction using blockchain is a business challenge and not a technology challenge
DO NOT USE BLOCKCHAIN
4.Do multiple parties require shared write access?
Yes
No
5.Do you require high performance/ rapid transactions? (milliseconds)
No
Yes
6.Do you intend to store non-transactional data as part of your solution?
Yes
No
BLOCKCHAIN CAN'T DO THIS EFFECTIVELY YET, SOLUTIONS ARE IN DEVELOPMENT
Yes
7.Do you want/need to rely on a trusted party i.e. for compliance reasons?
No
8.Do you need the ability to control functionality?
Yes
No
STRONG CASE FOR PRIVATE BLOCKCHAIN
9. Should transactions be public?
Yes
No
STRONG CASE FOR PUBLIC BLOCKCHAIN

Figure 2. Framework for Blockchain use Case Evaluation[5]

From that point onward, an assortment of plan choices around blockchain arrangement should be made, similar to the sort of blockchain, agreement convention, block size and recurrence. The bolts just represent one of the potential groupings to settle on plan choices. A few choices are required to set up acceptable levels of expansion (like block size and rate of occurrence), security, cost of processing and performance [5].

III. BLOCK CHAIN BASED CRN SECURITY TECHNIQUE

Block chaining is a basic innovation preoccupied via Bit-coined. It is another use of conventional innovation in the web period, that incorporates conveyed information stockpiling innovation, remote organizations, agreement system and cryptography [29]. As a decentralization publically data set, block-chaining utilizes publically keying cryptographical calculations, hashing capacities, agreement instruments & different innovations to fabricate a decentralization non-verification framework that could be utilized in internet business to guarantee client data security. Basically, blockchaining could be broadly utilized in web nance or a more extensive market. It would additionally advance the course of monetary globalisation& would enormously affect the current monetary marketingdesign& surprisingly the socially design [30].

Block chained innovation enjoys the benefits of least exchange costing, solid straightforwardness, & highest securities. It could adequately work on the proficiency of data usage, make-out the exchange interaction straightforward, share management, and secure the authentic rights and interests, all things considered, to the exchange. Normal issues like significant expense, low effectiveness, and low information stockpiling security in the normalized data set give groundbreaking thoughts [31]. Blockchain is a sort of carefully designed, full history information base stockpiling innovation, ordinarily utilizes highlight direct innovation toward coordinate every hub. Every hub understands the elements of steering, new hub distinguishing proof and information dispersal via multicast. It could show up at any hub in the framework. By utilizing cryptography's, it can create relating information blockings. The created information could actually look at the legitimacy of the data, & could likewise understand the solid connection via the following information [32]. In remote organization correspondence, blockchain innovation is a sort of innovation that can't be altered among similar level auxiliary clients who don't confide in one another or have feeble trust without go-between investment. With respect to authentic cooperation in the information base as a publically record books, every hub storing the chronicled association recording of the entire organization, & records of information assortment, exchange, flow and computation and examination are kept on the blockchain, which causes the nature of information to acquire exceptional solid trust support, and guarantees the rightness of information investigation outputs& the impact of mined data [33]. Taking into account the benefits of blockchain innovation, this chaptergives a psychological remote organization security calculation dependent on block-chaining

A. Algo Design Structure

The examination objects of such articles is 2-waying confirmation issue bet^{n} the block chained IoT gadget & the psychological remote organization combination focus

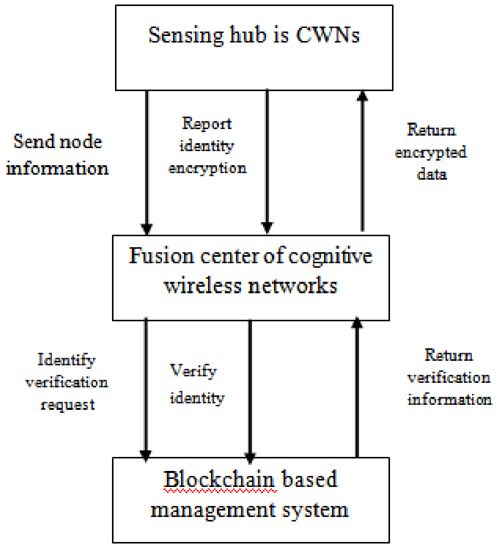
Sensing hub is CWNs
Send node information
Report identity encryption
Return encrypted data
Fusion center of cognitive wireless networks
Identify verification request
Verify identity
Return verification information
Blockchain based management system

Figure 3 Security calculation construction of intellectual remote organization

Thusly, the framework in this article is basically made out of the blockchain framework, the psychological remote organization combination focus, & the block chaining IoT gadget. Clients speak via the block chaining framework via the combination place.

The particular construction is displayed in Fig 3 The I.o.T gadget sending hub data to the combination place, & the combination community inquiries the blockchain framework for the presence of its hub data, & afterward the hub sending the information endorsed via the privately keying to the combination place, & checks whenever the detecting hub had a relating privately keying pairedsignture it. Assuming it is, forward the hub's solicitation to the block chaining framework, and forward the reaction of the block chained framework back to the detecting hub. The information endorsed by the detecting hub can affirm the character of partaking in range detecting, and can likewise guarantee that its information has not been altered or produced.

IV. BLOCKCHAIN TECHNOLOGY BLOCK CHAIN BASED SECURE SPECTRUM

This report presents the blockchain innovation and notoriety system into the range detecting measure. Another safe range detecting strategy is proposed. This security detecting strategy incorporates the assessment of the client's immediate standing and suggestion notoriety

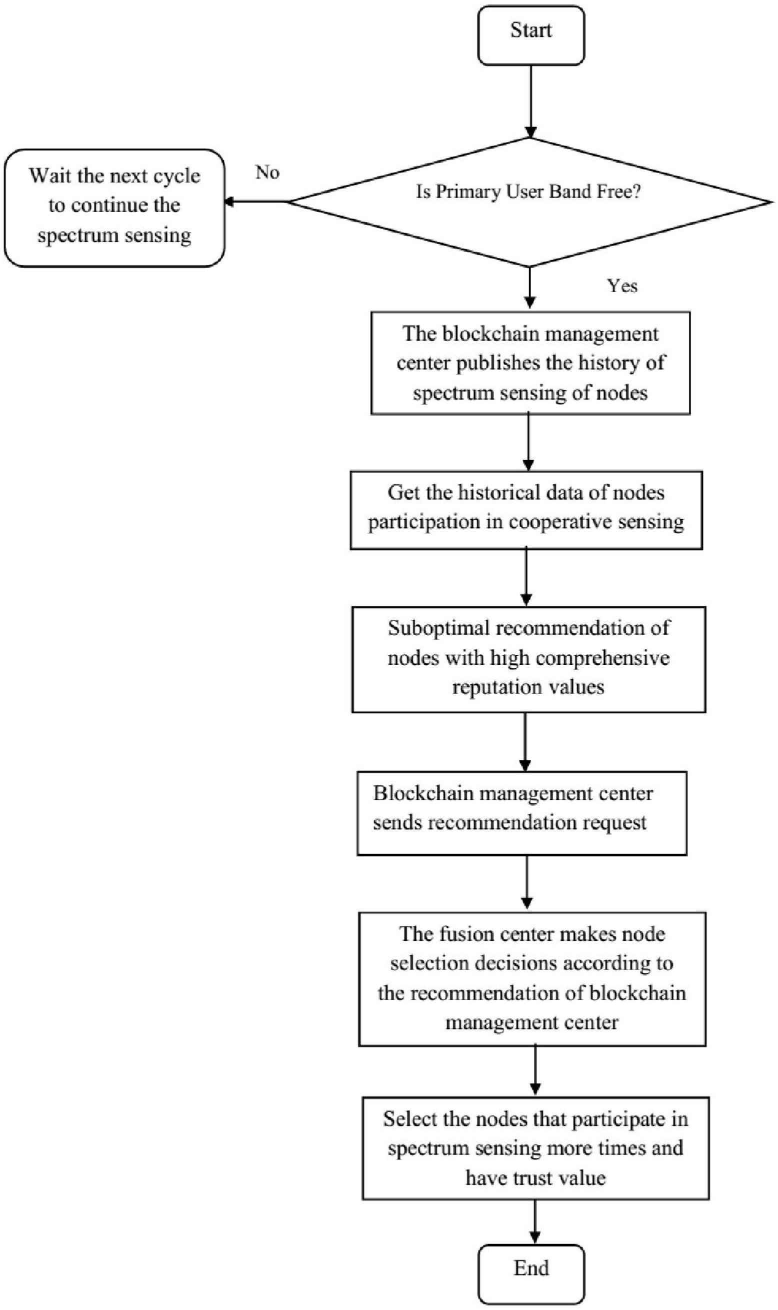
Start
Is Primary User Band Free?
No
Wait the next cycle to continue the spectrum sensing
Yes
The blockchain management center publishes the history of spectrum sensing of nodes
Get the historical data of nodes participation in cooperative sensing
Suboptimal recommendation of nodes with high comprehensive reputation values
Blockchain management center sends recommendation request
The fusion center makes node selection decisions according to the recommendation of blockchain management center
Select the nodes that participate in spectrum sensing more times and have trust value
End

Figure 4Secure Spectrum Sensing Algorithm Based on Blockchain In Cognitive Wireless Networks

At the point when a helpful hub solicitation to get to a specific recurrence band, it needs to detect whether the recurrence band is inactive. In case it is inactive, it will send a proposal solicitation to the combination place. To stay away from conspiracy assault and malevolent hub conduct, the detecting results are more precise. Utilizing the blockchain innovation, the verifiable detecting records in the data set and the distance of cooperation history is viewed as a public record, which can be shared by each neighbor hub, and no hub in this situation can change the record data. The particular working course of safety range detecting dependent on blockchain innovation is displayed in Figure 4

After the combination place sends a discernment demand, the assessment of a hub's nearby standing worth is identified with the friend requester. It is important to acquire the requester's discernment computation record from the public record book of the blockchain to ascertain its immediate standing worth. For the sender, the neighborhood direct standing worth is determined by recipe

$$T_i = \frac{N_i}{k}\theta\omega_i \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (3.14)$$

In equation 3.14, T_i addresses the ith detecting period, N_i is the quantity of all the detecting periods up to T_i time-frame. The significance of k is equivalent to and showing the right number of intuitive detecting in history [34], θ implies the detecting activity force, and its worth is determined by recipe (14), ω_i is the impact coefficient of the detecting times in the public record book, and its worth is determined by equation 3.15.

$$\theta = 1 - e^{\left|-\frac{k}{mn}\right|} \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (3.15)$$

$$\omega_i = \sum_{i=1}^{n}\left|\frac{h_1}{m}.\frac{l}{n}\right| \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (3.16)$$

where h_1 is the quantity of cooperations in l period and m is the size of detecting period in every period, n is the all out association time frame. It tends to be seen from equation that the nearer is the cooperation history in the public record book, the extent will be the more prominent, and the effect on trust worth will increment as needs be [35].

At the point when the trust worth of the hub isn't in the front line, everything being equal, the hub is chosen by figuring the extensive trust esteem, and the thorough trust worth of the hub is determined by (3.17)

$$T_{i,c} = \emptyset T_i + \varphi\left|T_i + \theta \textstyle\sum_i w_i\right| \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (3.17)$$

The security range detecting innovation dependent on the blockchain, through the computation of the extensive trust worth of the hubs in the organization. A ultimate conclusion making measure utilizes the exemplary trust esteem dynamic calculation. The hubs in the organization are grouped by setting the relating dismissal limit and trust edge. On the off chance that the far reaching trust esteem is not exactly the dismissal limit, the hub is viewed as a malignant client; if the exhaustive trust esteem is more noteworthy than the trust edge, the hub is viewed as a typical client; if the thorough trust esteem is between the dismissal edge and the trust edge, the hub is viewed as a hub to be noticed. The hub gets the option to take part in helpful detecting through the ceaseless update of the trust esteem.

V. RESULT ANALYSIS

In this section, we have to discuss the result analysis of Blockchain technology in cognitive radio network. The simulation parameter is discussed in the table 1

Table 1 Simulation Parameter

Sr. No.	Parameter	Value
1	Simulation Area Setting	A Circular area with a radius of m
2	Primary User	Place a primary user anywhere on the edge of circular area
3	Working Parameters of primary user	BPSK signal with power of 100 MW and bandwidth of 100 kHz.
4	Number of Nodes	Randomly place 15 nodes (5 nodes with SNR = -18 dB and -14 dB respectively)
5	Noise Settings	AWGN
6	Average Detection Times	10000

7	Auxiliary Node	3
8	Spectrum Detection Method of Node Front End	Energy Detection

The circular area with radius m is define as simulation area of the network. The primary users are placed anywhere on the edge of circular area. The signal power is 100 MW and bandwidth of 100 kHz. Similarly, 15 nodes are placed in the system. Beyond this SNR of these nodes are -18 dB and -14dB respectively. The noise used in the proposed system is AWGN. The average detection time and auxiliary nodes are 10000 and 3 respectively. Energy detection method is used as spectrum detection.

The cognitive radio topology is defined in the fig 5. The different no. of primary and secondary users is placed in particular geometry. The range of network lies between -500 to 500 m. There is one primary user and multiple secondary users. The primary user is located at the center of area while secondary users are locating around the primary users with the specific pattern.

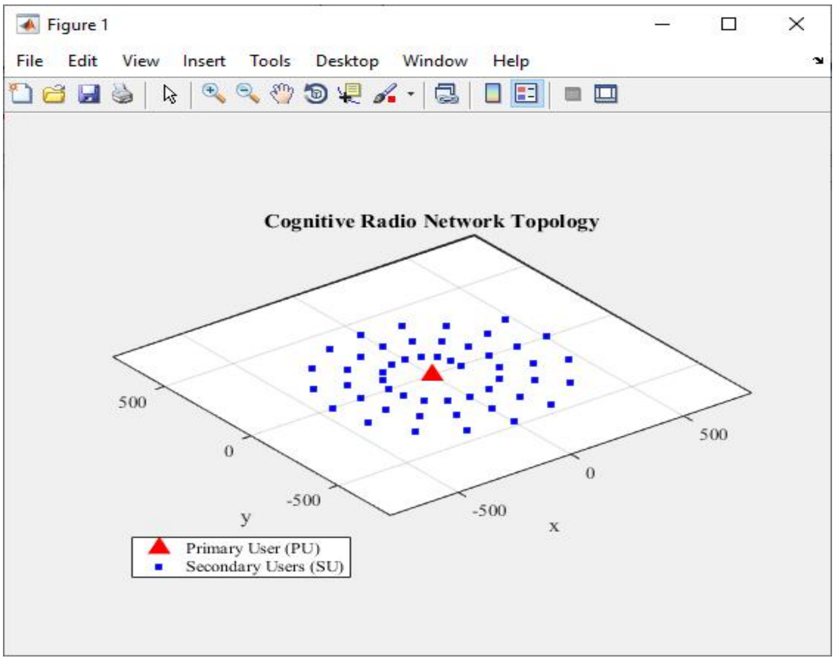

Fig 5 Cognitive Radio Topology

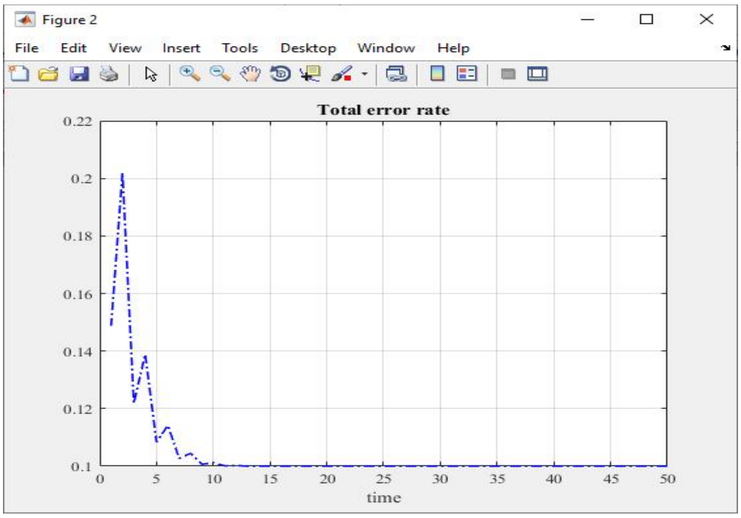

Fig 6 Total Error Rate

The Total error rate is shown in the fig 6. The total error rate is start 15 % for 1 sec. As the graph shows that total error rate increases to 20.05 % with the time period of 2 sec. Suddenly, the total error rate is decrease to 10%. The steady state error is 10%.

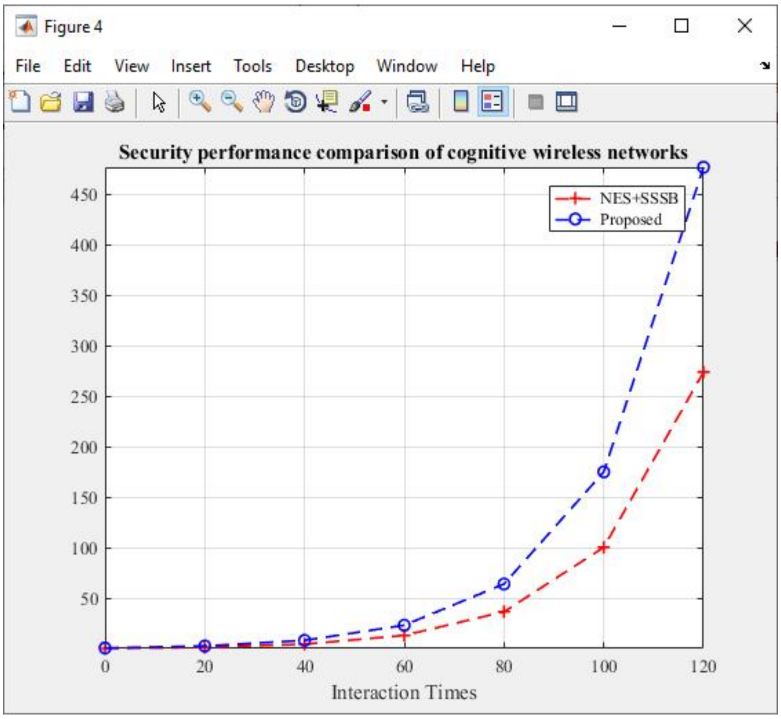

Fig 7 Comparative Analysis of Security in Cognitive Radio

Similar Analysis of Security in Cognitive Radio is displayed in fig 7. It tends to be seen from Figure that when the NES and SSSB calculations are utilized in mix, as expanding the quantity of associations between the detecting hub, combination focus and blockchain the board community, the security file of the psychological remote organization rises fundamentally quicker. At the point when the quantity of associations surpasses multiple times, the security list utilizing the SSSB calculation rose quicker than the wellbeing file utilizing just the NES calculation, which completely mirrors the adequacy of the SSSB calculation. This is on the grounds that the SSSB calculation joins blockchain innovation. It can extraordinarily further develop the counter assault capacity and security capacity of psychological remote organization. The security execution of proposed calculation is better when contrasted with NES+SSB calculation.

VI. CONCLUSION

This paper design an inside and out examination on the model of intellectual remote organizations. In the pragmatic application situations of intellectual remote organizations, there are typically genuine mistakes when the hubs detecting the information, which causes the detecting esteems to go amiss from the ordinary reach, or a few hubs purposely, send some unacceptable information to the combination community. Accordingly, focusing on the security issue of noxious hub assault in intellectual remote organization, this paper proposes the hub assessment and planning (NES) calculation and the Secure Spectrum Sensing, which respects the client's collaboration history and association distance as a public record book, and is overseen by the blockchain the executives community, which is helpful for the combination place to call hubs with astounding execution to take an interest in agreeable detecting

REFERENCES

[1] Abbas, Sana-e-Zainab, S & Wajahat 2010, 'An Efficient Algorithm for Secure & Fair Dynamic Spectrum Access in Cognitive Radio Networks', Canadian Journal on Multimedia and Wireless Networks, vol. 1, no. 3, pp. 173-177.

[2] Amarnathprabhakaran, A & Manikandan, A 2013, 'An Efficient Communication and Security for Cognitive Radio Networks', International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, vol. 2, issue 4, pp. 1689-1696.

[3] Anand Z Jin & Subbalakshmi, KP 2008, 'An analytical model for primary user emulation attacks in cognitive radio networks', DySPAN 2008, 3rd IEEE Symposium, IEEE, pp. 1-6.

[4] Atta & Alireza 2012, 'A Survey of Security Challenges in Cognitive Radio Networks: Solutions and Future Research Direction', Proceeding of IEEE, pp. 3172-3186.

[5] Bhattacharjee, Suchismita & Ningrinla Marchang 2015, 'AttackResistant Trust-Based Weighted Majority Game Rule for Spectrum Sensing in Cognitive Radio Networks', International Conference on Information Systems Security, Springer, pp. 441-460.

[6] Bhattacharya, PP, Khandelwal, R, Gera, R & Anjali Agarwal 2011, 'Smart radio Spectrum management for Cognitive radio', International journal of Distributed and parallel systems, vol. 2, no. 4, pp. 12-24.

[7] Cabric Danijela M Mishra & Brodersen, RW 2004, 'Implementation issues in specrtum sensing for cognitive radios. Signal Systems and Computers', Conference record of 38th Asilomer Conference, IEEE, vol. 1, pp. 772-776.

[8] Chen, R, Park, J & Reed, JH 2008, 'Toward secure distributed spectrum sensing in cognitive radio networks', Communications Magazine, IEEE, vol. 46, no. 4, , pp. 50-55.

[9] Dubey Rajni, Sanjeev Sharma & Lokesh Chouhan 2012, 'Secure and trusted algorithm for cognitive radio network', Ninth International Conference on Wireless and Optical Communications Networks (WOCN), IEEE, pp. 1-7.

[10] Etkin, R, Parekh, A & Tse, D 2005, 'Spectrum sharing for unlicensed bands', Proc. IEEEDySPAN 2005, IEEE, pp. 251–258.

[11] FCC 2003, 'Notice for Proposed Rulemaking (NPRM 03-322)', Facilitating Opportunities for flexible, Efficient, and Reliable Spectrum Use Employing Cognitive Radio Technologies. ET Docket, pp. 03- 108.

[12] Feng Lin, Robert C Qiu, Zhen Hu, Shujie Hou, Lily Liy, James P Browningz & Michael C Wicks 2012, 'Cognitive Radio Network as Sensors: Low Signal-to-Noise Ratio Collaborative Spectrum Sensing', Proceedings of Aerospace and Electronics Conference (NAECON), IEEE, pp. 978-985.

[13] Harish Ganapathy, Constantine Caramanis & Lei Ying 2010, 'Limited Feedback for Cognitive Radio Networks Using Compressed Sensing', IEEE 48th Annual Allerton Conference on Communication, Control, and Computing (Allerton), IEEE, p. 10901097.

[14] Haykin & Simon 2005, 'Cognitive radio: brain-empowered wireless Communication. Selected Areas in Communications', IEEE Journalon, vol. 23, no. 2, pp. 201–220.

[15] Haykin & Simon 2010, 'Cognitive radio: brain-empowered wireless communications', IEEE Journal of Selected Areas of Communication, vol. 2, pp. 201-220.

[16] Ian F Akyildiz, Won-Yeol Lee & Kaushik R Chowdhury 2006, 'Next generation/dynamic spectrum access/cognitive radio wireless networks: a survey', Computer networks, vol. 50, no. 13, pp. 2127- 2159.

[17] Januszkiewicz & Lukasz 2010, 'Simplified human body models for interference analysis in the cognitive radio for medical body area networks', 8th International conference on Medical Information and Communication Technology, IEEE, pp. 15-24.

[18] Juebo & Long Tang 2012, 'Research and Analysis on Cognitive Radio Network Security', Wireless Sensor Network, vol. 4, pp. 120-126.

[19] Khuong Ho-Van & Thiem Do-Dac 2018, 'Reliability-Security Tradeoff analysis of Cognitive Radio Networks with jamming and licensed interfernce', Wireless Communication and Mobile Computing, Hinadwi, vol. 2018, pp. 1-15.

[20] Kwang Cheng Chen, Peng-Yu Chen, Neeli Prasad, Ying-Chang Liang & Sumei Sun 2009, 'Trusted cognitive radio networking. Wireless Communications and Mobile Computing'.

[21] León, Olga, Juan Hernández-Serrano & Miguel Soriano 2010, 'Securing cognitive radio networks', International journal of communication systems no. 5, pp. 633-652.

DOI: 10.48175/568

[22] León, Olga, Juan Hernández-Serrano & Miguel Soriano 2010, 'Securing cognitive radio networks', International Journal of Communication Systems, vol. 23, issue 5, pp. 633-652.

[23] Mao, Huaqing & Li Zhu 2011, 'An investigation on security of cognitive radio networks', International Conference on Management and Service Science (MASS), IEE, pp. 1-4.

[24] Matteo Cesana, Francesca Cuomo & Eylem Ekici 2010, 'Routing in cognitive radio networks: Challenges and solutions', Ad Hoc Networks, Elsevier., pp. 18-39.

[25] McLoone, Safdar, GA & O'Neillne, M 2009, 'Common Control Channel Security Framework for Cognitive Radio Networks', IEEE 69th, Vehicular Technology Conference, VTC Spring 2009, IEEE, pp. 26-29.

[26] Meng, T 2015, 'Spatial Reusability-Aware Routing in Multi-Hop Wireless Networks', IEEE TMC, DOI 10.1109/TC.2015.2417543 .

[27] Mitola, J & Maguire, GQ 1999, 'Cognitive Radio: Making software radios more personal', IEEE personal Communications, vol. 6, no. 4 , pp. 13-18.

[28] Muhammad Ayzed Mirza, Mudassar Ahmad, Muhammad Asif Habib,Nasir Mahmood, Nadeem Faisal, CM & Usman Ahmad 2018, 'CDSS:Cluster-based distributed cooperative spectrum sensing model against primary user emulation cyber attack', The Journal of Supercomputing, Springer, Available Online, pp. 1-17.

[29] Parvin Sazia & Farookh Khadeer Hussain 2012, 'Trust-based security for community-based cognitive radio networks', IEEE 26th International Conference on Advanced Information Networking and Applications, IEEE, pp. 518-525.

[30] Parvin, Sazia & Farookh Khadeer Hussain 2011, 'Digital signature based secure communication in cognitive radio networks', Broadband and Wireless Computing, Communication and Applications (BWCCA), IEEE, pp. 230-235.

DOI: 10.48175/568