A STUDY ON ADOPTION OF BLOCKCHAIN TECHNOLOGY IN CYBERSECURITY

Aditya Routh[1], Koushik Pal[2], Subhomoy Das[3], Jishnu Nath Paul[4]

Department of Electronics& Communication Engineering, Guru Nanak Institute of Technology, Kolkata, India

---***---

Abstract *- Since Satoshi Nakamoto published white Paper on Bitcoin in 2008, blockchain has (slowly)became one of the foremost mentioned strategies for securing data storage and transfer through decentralized, trust-less, peer-to-peer systems. This analysis identifies peer-reviewed literature that seeks to utilize Blockchain for cyber security functions and presents a scientific analysis of the foremost often adopted blockchain security applications. In this proposed work, we are introducing blockchain technology in cybersecurity where IOT security, availability and decentralized storage of data and many more applications will be add on into the system. Thus the Intelligence Agencies and Cybersecurity Cell does not face any issues or drawbacks while operating, although cybersecurity is itself a very secure but after introducing blockchain in it, it will be impossible to seize.*

Keywords **– Blockchain in cybersecurity, roles, uses cases, methodology, making of more secure system.**

I. INTRODUCTION

India is home to a population that is unmoving in numerous socio-economic backgrounds. As per the living standards of individuals, a large vary of devices area unit in use - from high-end secured electronic devices to inexpensive mobile phones. This makes it troublesome for authorities to line uniform legal and technical standards to control data-protection. Additionally, digital attainment and awareness among the population is very low.

Cyber-Security refers to the act of protective and making certain the protection of laptop systems and electronic devices from targeted cyber-attacks, opportunist malware (- viruses, trojans and bugs) or accidental introduction of malware by users.

So, the main motto of this project is to ensure more secure system which is unbeatable and overcome the drawbacks which was faced earlier. This proposed application of blockchain in cybersecurity will work as decentralized system i.e. it every user will get to know activities and with the help of it, it will notify whenever any outsider tries to invade it and if somehow if invasion is successful it will be impossible to change aur retrieve the data as each block in blockchain requires a security key if anyone to tamper it, it will automatically become invalid.

II. OBJECTIVE

Cybersecurity protects both raw and meaningful data, but only on internet-based threats. Organisations implement information security for a wide range of reasons. The main objectives are typically related to ensuring confidentiality, integrity, availability of company information.

The main objective of this proposed work is to enhance cybersecurity by using blockchain technology. As we all know cybersecurity is itself a very secured network, but at some instances it is not so efficient as any organisations or anyone can tamper the data if equipped with the knowledge. As result the data will be in a threat, but by introducing blockchain in it we overcome this issue.

The goal of blockchain is to **permit digital information, to be recorded and distributed, however not altered.** During this manner, a blockchain is that the foundation of immutable ledgers, or records of transactions that **can't be altered, deleted or destroyed.** Here we minimize the chance to a bigger extent. We also can't ignore the point that it is decentralized service i.e. **nobody should apprehend or trust anyone else.** Every user within the network features a copy of actual same data within the variety of distributed ledger. If the user's ledger is altered or corrupted in any manner, it'll be rejected by the bulk of the users within the network. In particular every block within the chain needs a security key, if anybody tried to counter that, the information can become invalid for the trespasser and can't operate any more. So, this method ensures most security of the information and prevents any variety of malpractice. This can facilitate the security agencies that's serves for the nation.

III. METHODOLGY AND BLOCK DIAGRAM

This research will be qualitative analysis to evaluate the applicability of Blockchain technology in today's cybersecurity industry. The paper will focus on two aspects of all the highlighted papers, to begin with will look at the latest implementations of the evolving Blockchain technology in cybersecurity. Second, it'll check out the strategies available for deploying Blockchain cybersecurity solutions. The main takeaways from the research findings will be used to form a discussion on how Blockchain can afford security in today's IT user environments.

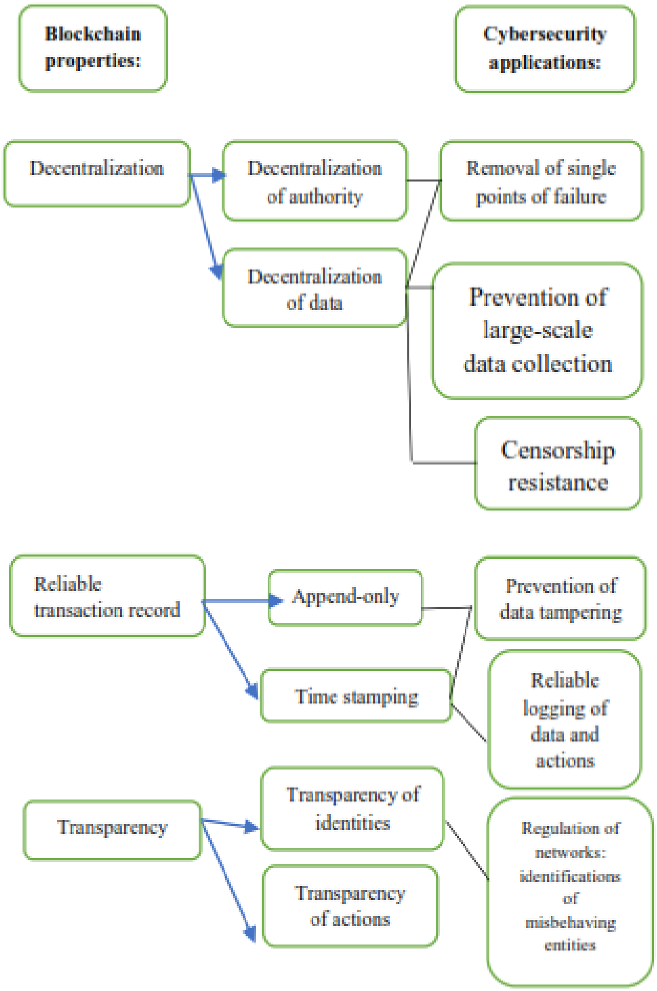
Blockchain properties:
Cybersecurity applications:
Decentralization
Decentralization of authority
Decentralization of data
Removal of single points of failure
Prevention of large-scale data collection
Censorship resistance
Reliable transaction record
Append-only
Time stamping
Prevention of data tampering
Reliable logging of data and actions
Transparency
Transparency of identities
Transparency of actions
Regulation of networks: identifications of misbehaving entities

Fig1.Blockdiagram of blockchain

IV. GENERAL DESCRIPTION

Use cases of blockchain in cybersecurity:

Decentralized storage of crucial data: The blockchain-based decentralized storage system splits users' files into varied tiny chunks of information, mentioned as "blocks". It then encrypts every block with a unique hash or with public-private keys and distributes the blocks across multiple computers or "nodes". This method of distributing information across the network of node is called 'sharding'.

Likewise, all information gets distributed and hold on at decentralized locations. If interlopers decide to hack into these locations, they hit encrypted blocks of information. What's more, they will only be able to obtain a chunk of information, not the entire file. This, in sum, is however blockchain-based decentralized storage systems ensure data security.

Availability: In recent times, cyberattacks trying to impact technology services availableness square on the surge with DDoS (Distributed Denial-of-Service) being the foremost common types of attacks. However, in blockchain-based systems, DDoS attacks square measure expensive as the assaulter makes an attempt to overpower the network with an excellent variety of tiny transactions. Blockchains haven't any single purpose of failure that decreases the possibilities of IP-based DDoS attacks disrupting the traditional operation. Information remains accessible through numerous nodes and so full copies of the ledger are often accessed the least bit times. The mixture of multiple nodes and distributed operation makes the platforms and systems resilient.

IoT security: As far much IoT thinks about, Blockchain technology stands out due to its ability to unravel measurability, reliability and privacy problems. It allows coordination between devices, furthermore as chase of immeasurable connected devices and process transactions. This is a decentralized approach in which cryptographic algorithms square measure enforced so client information get pleasure from bigger privacy. It's associate degree approach that eradicates faults and offers a resilient scheme. With the increasing application of AI and IoT, the protection of information and systems from hackers has forever been a serious concern. Usage of Blockchain for improved security by victimization device-to-device encryption to secure communication, key management techniques, and authentication is a potential use case to keep up cybersecurity within the IoT system.

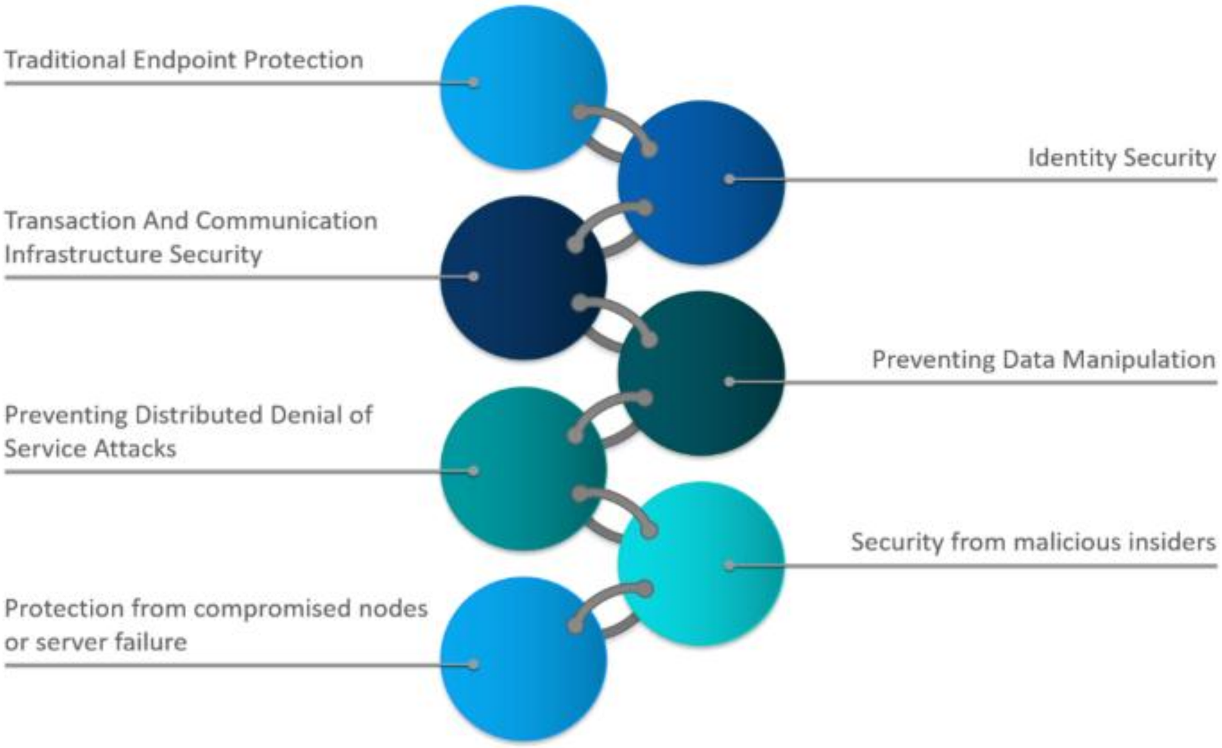
Traditional Endpoint Protection
Identity Security
Transaction And Communication Infrastructure Security
Preventing Data Manipulation
Preventing Distributed Denial of Service Attacks
Security from malicious insiders
Protection from compromised nodes or server failure

Fig2. Blockchian in cybersecurity

Cybersecurity Threats and Incidents on Blockchain Network: Around 65 real world cybersecurity incidents have occurred round the globe amid2011 and 2019. The incidents have adversely affected the Blockchain system. We calculate the impact based on price of the cost coins at the time the attacks were discovered. However, these reports were discovered. However, these reports may differ a little from reality since the lack real life circumstances. We broadly divide the incidents as – **hacks, scams and smart contract flow**. The highest lose relates to hacking followed by scams and the contract flows. Figure-1, shows that the number of incidents reduced as the price of BTC fell. But as soon as the price soared up, so did the number of attacks.

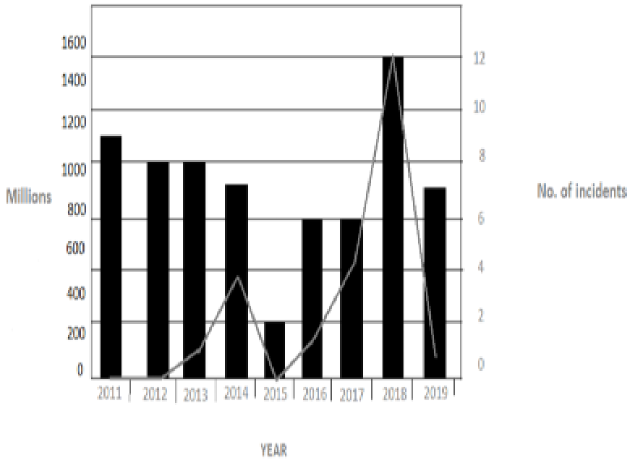

Fig-3. Blockchain incidents 2011-2019.

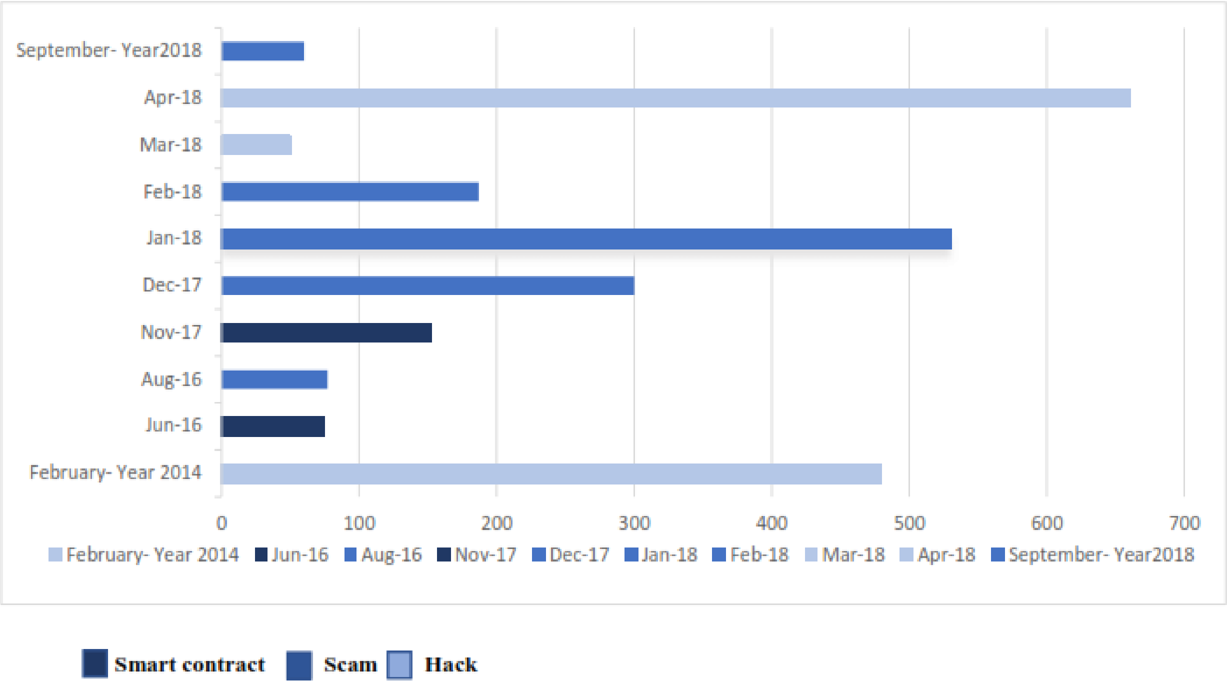

Fig-4.. Top 10 most affected blockchain incidents.

V. WORKFLOW OF THE SYSTEM

For better understanding of the working of this proposed system, we can divide the whole procedure in two parts- firstly, the working of blockchain technology and secondly, how the cybersecurity system works.

So, in the first section we are going to discuss about the process of the blockchain technology. Blockchain is system of recording information in a way that makes it difficult or impossible to change, hack or cheat the system. A blockchain is basically a digital ledger of transactions that's duplicated and distributed across the complete network of computer systems on the blockchain. Each block in the chain contains a number of transactions, and every time a new transaction occurs on the blockchain, a record of that transaction is added to every user's ledger. The decentralized information managed by multiple users is known as Distributed Ledger Technology. Now, within the second part we are going to discuss regarding the cybersecurity and the way it works. It's sub-categorized in 3 points- **analysis, implementation and support.**

Analysis- It includes an intensive analysis of infrastructure, necessities and effective cyber threat scenario. Solid reasons for and against solutions. Joint realization of proof of construct, trial and take a look at surroundings

Implementation- Licensing support, consulting and deployments with the expertise from thousands of difficult IT security projects. Know how across industries and company sizes and a high level of routine.

Support- Troubleshooting, support and 24/7 instant facilitate with qualified contact persons. Certified power concerning product moreover as data concerning individual- environments. Enhancements, reviews and potential analyses.

VI. LITERATURE SURVEY

In the paper 1: Cybersecurity through Blockchain technology: A Review. In October 2019, this paper was published by Alex. R. Mathew. It was published in International Journal of Engineering and Advanced Technology (IJEAT). This paper looked at several use cases of Blockchain in the cybersecurity industry as envisioned by 30 researchers. It found that most researchers are concentrating on the adoption of Blockchain to protect IoT (Internet of Things) devices, networks, and data.

In the paper 2: Blockchain for Cybersecurity and Privacy: Architectures, Challenges, and Applications: A Review. In July 2020, this paper was published by Malehe Yassine, Mamoun Alajab, Imed Romdhani. It was published in The Internal Audit and IT Audit. This paper looked at Blockchain has moved beyond hype to real-world implementation in a broad range of industries (eg, finance, supply chain management, and Internet of Things) and applications (eg, cybersecurity and digital forensics), partly evidenced by its evolution over the last decade or so.

This book focuses on the applications of blockchain in cybersecurity, privacy, and digital forensics, for different industry sectors such as Internet of Things and health-care.

In the paper 3: A systematic literature review of blockchain cyber security, in June 2020, this paper was published by Paul J. Taylor, Tooska Dargahi, Ali Dehghantanha, Reza M. Parizi, Kim-Kwang Raymond Choo. This research has identified available recent research on how blockchain solutions can contribute to cyber security problems. The initial keyword searches for this research and current media reports

highlight blockchain as a standalone technology that brings with it an exorbitant array of possible solutions for finance, logistics, health, cyber security.

This research has focused solely on cyber security. Undoubtedly, there are worthy applications for blockchain; however, a decentralized, trustless system cannot by itself solve all problems one may uncover in the field of cyber security.

VII. CONCLUSION AND FUTURE SCOPE

Blockchain technology continues to evolve and notice additional use cases within the modern times. One in every of the viable areas where it's been studied and applied is cybersecurity. The Blockchain infrastructure makes it extremely sensible in addressing the present security challenges in areas like as IoT devices, and information in transmission and storage. Alongside this, alternative major area units as of Blockchain security are networks and information. As ascertained within the discussion, the Blockchain technology is be want to secure IoT devices through additional reliable authentication and information transfer mechanisms. This will forestall hackers from breaching into these devices which frequently ship with poor security configurations.

In future, for obvious reasons, Blockchain technology's scope lies within the field of Cybersecurity. Though the Blockchain ledger is open and distributed, **the information is secured and verified.** The encryption is finished through cryptography to eliminate vulnerabilities like as unauthorized information tampering bolstered the existing efforts to enhance security and to deter malicious actors.

VIII. REFERENCES

1. Swan, Melanie. Blockchain: Blueprint for a new economy. " O'Reilly Media, Inc.", 2015.
2. Crosby, Michael, et al. "Blockchain technology: Beyond bitcoin." Applied Innovation 2.6-10 (2016): pp. 71.
3. Iansiti, Marco, and Karim R. Lakhani. "The truth about blockchain." Harvard Business Review 95.1 (2017): pp. 118-127.
4. Cachin C. Architecture of the hyperledger blockchain fabric. InWorkshop on distributed cryptocurrencies and consensus ledgers 2016, 310(1), pp. 4.
5. Coindesk: Bitcoin venture capital funding, www.coindesk.com/bitcoin-venture-capital, 17 July 2019.
6. CoinMarketCap: Cryptocurrency market capitalizations—Coinmarketcap, https://coinmarketcap.com/, 17 July 2019.
7. Chowdhury, M.J.M., Colman, A., Kabir, M.A., Han, J., Sarda, P.: Blockchain as a notarization service for data sharing with personal data store. In: Trust-Com/BigDataSE 2018, IEEE (2018) 1330–1335.
8. V. Buterin, A Next-Generation Smart Contract and Decentralized Application Platform, Etherum, 2014 [Online].
9. T. Salman, M. Zolanvari, A. Erbad, R. Jain, M. Samaka, Security services using blockchains: a state of the art survey, in: IEEE Communications Surveys & Tutorials, 2018.
10. S. Nakamoto, Bitcoin: a peer-to-peer electronic cash system, 2008.