9th IEEE International Conference on Communication Systems and Network Technologies

# Blockchain for Cybersecurity: A Comprehensive Survey

Pranshu Bansal
Computer Science and Engineering Department
HMR Institute of Technology
Delhi, India
pranshubansal111@gmail.com

Rohit Panchal
Computer Science and Engineering Department
HMR Institute of Technology
Delhi, India
rohitxofficial@gmail.com

Sarthak Bassi
Computer Science and Engineering Department
HMR Institute of Technology
Delhi, India
sarthakbassi@hotmail.com

Amit Kumar
Computer Science and Engineering Department
Ambedkar Institute of Advance Communication
Technology and Research
Delhi, India
amitkr6002@gmail.com

***Abstract*—Blockchain is a decentralized ledger used to securely exchange digital currency, perform deals and transactions. Each member of the network has access to the latest copy of encrypted ledger so that they can validate a new transaction. Various features such as decentralization, trustworthiness, trackability and immutability are provided by the blockchain technology. This paper provides the blockchain architecture and explains the concept, characteristics, need of Blockchain in Security, how Bitcoin works and to enhance the security in the field of IoT. It attempts to highlights the role of Blockchain in shaping the future of Cyber Security, Cryptocurrency and adoption of IoT. This paper explains the need of blockchain technology in various technical fields and shows various advantages over conventional system.**

***Keywords-Blockchain; cybersecurity; DDOS; Bitcoin;***

## I. INTRODUCTION

Internet of Things (IoT) is an interconnection of various computing machines or various devices that can transfer data over a network. The potential of these devices and the way of interacting with such devices also gets enhanced by using IoT. The devices through cloud servers are connected and data get stored in these servers[1]. The data in such servers is trust dependent and centralized, due to which many loop holes are present in it and it is vulnerable to security threats. In order to make IOT system secure, trustworthy, decentralized and even more practical we need to use Blockchain technology.

The protection of any and all systems connected to the internet including hardware, software and data from cyber-attacks is known as Cybersecurity. For enterprises to secure their systems completely against any unauthorized access to any data or systems, security includes both cybersecurity and physical security [2]. Cybersecurity ensures the ability for one to maintain the integrity, confidential and ease of access to data.

A cryptocurrency is a tradable digital asset or digital form of money, built on blockchain technology that only exists online. Cryptocurrencies use cryptography to verify and secure transactions, hence their name. The most important feature of a cryptocurrency is that it is not controlled by any central authority, the decentralized nature of the blockchain makes cryptocurrencies theoretically immune to the old ways of government control and interference. Cryptocurrencies can be sent directly between two parties via the use of private and public keys. These transfers can be done with minimal processing fees, allowing users to avoid the steep fees charged by the mediator.

The main purpose of this research paper is to provide guidance in the field of blockchain technology and to implement blockchain technology in the field of Cyber Security, Cryptocurrency and IoT.

## II. LITERATURE SURVEY

Jing Li et. al[3] have proposed a decentralized platform with shard to reduce the latency in the transaction processing time due to complex maths puzzles and other task in the process of proof of work. Xinle yang et. al[4] have provided a solution for 51% attack on proof of work, which occurs when the attacker achieve the hash power which is more than the half of the total hash power to perform double spending.

Shu yang et. al[5] use Directed Acyclic Graph to enhance the linear structure of protocols used in traditional blockchain platforms. Ivan Homoliak et. al[6] on the basis of models of various threat-risks and threats stacked hierarchy proposed a security reference architecture using ISO/IEC 15408. S. Pavithra et. al[7] performed a survey which compare and analyze different security issues in cloud platforms and also proposed blockchain technologies as solution for various security issues. D. Tanana[8] proposed a method to use

978-1-7281-4976-9/20/$31.00 ©2020 IEEE
DOI: 10.1109/CSNT.2020.48

metastable blockchain protocol to preserve the integrity of data and also discuss the advantages of same over the traditional one to provide better security on different blockchain platforms.

## III. CYBERSECURITY

### A. *The importance of cybersecurity*

With continuously improving technologies, security trends are changing ever so often that threat intelligence teams find it cumbersome to keep up with the times. The need for cybersecurity is due to the huge amounts of data that is stored by different organizations like the military, corporate, financial and medical is in one way or another on systems that may be prone to attack [3]. The data on these systems may contain sensitive information which if illegally accessed or obtained can have negative and wide-ranging effects for an individual or even for the entire world. Ginni Rometty, IBM's chairman, president and CEO, said: "Cybercrime is the greatest threat to every company in the world."

### B. *Threats to cybersecurity*

Majority of cybercrimes are able to happen due to negligence and not taking proper security measures by ensuring only the use of protected software or applications. The process of committing a cybercrime is done by targeting unprotected computer and device networks. For effective cyber security, all elements of cyber have to be taken in consideration.

- Network security
- Application security
- Endpoint security
- Data security
- Identity management
- Database and infrastructure security
- Cloud security
- Mobile security
- Disaster recovery/business continuity planning

End-use education

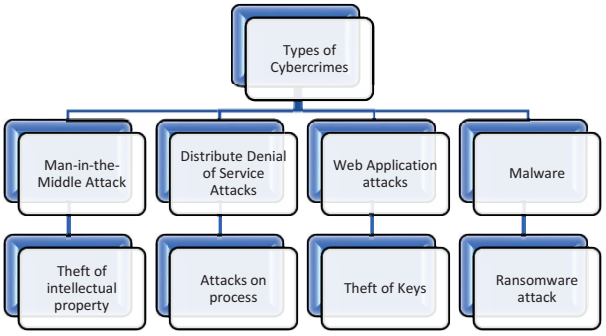


Figure 1. Types of Cybercrimes

## IV. ADDITION OF BLOCKCHAIN TO CYBERSECURITY

The Blockchain technology with its well defined and complex structure is one of the most secure technologies in the world. So, the addition of blockchain has started in different processes to ensure the prevention of fraud, hence increasing the security of data [9]. When it comes to cybersecurity, blockchain due to its method of maintaining a public leader it has a huge potential in-

- Big Data processing
- End point protection software
- Financial tools
- Supply chain management software

The HYPR Corp is a New York based company that provides enterprises with decentralized authentication solutions, which enable consumers and employees to securely and seamlessly access mobile, Web and Internet of Things (IoT) applications. It uses blockchain technology to decentralize credentials and biometric data to facilitate risk-based authentication. It invested US$ 10 million in 2018 on this platform[10].

### A. *How does blockchain help cyber security*

Elimination of human factor: The use of blockchain completely eliminates the need for businesses to authenticate and provide secure access to users and devices without using any password. The elimination of human error helps in avoiding an attack method. In many a case, even though businesses invest a large amount of money in security, all this money and effort is wasted if the employees and the customers use passwords that are easily crack able. Using Blockchain not only ensures a strong authentication process but also resolves point of the attack simultaneously [11]. A Blockchain based security can use distributed public key infrastructure that authenticates the devices. Each device is provided with an SSL certificate rather than a password by the security system. The certificate data is maintained and managed by blockchain,

hence making it impossible for an attacker to use fake certificates.

- Secured Private Messaging: Communication regarding documents and other work-related data, within an organization is necessary for work to be done, but many a time they may transfer this data or information over various messaging and social media apps due to which the data may get stolen. So Blockchain is used by companies to provide a secure platform for the transfer of information to the employees which can be accessed only on secure devices, hence making it impenetrable in case of an attack.
- Decentralized Storage: Blockchain allows users to maintain and store the data on their computer in their network, this ensures that the chain won't collapse [11]. If an attacker tries to change or make any action in regards to the data in a block, the system ensures the security by checking each and every data block by finding the tampered block from within the chain and recognizing it as fake and cutting it off from the chain. Blockchain ensures that no single storage location exists, every user or system that is on the network stores some or even the complete blockchain. This method ensures that every system on the network has the task of verifying the data that is shared and is being maintained to ensure that the existing data cannot be tampered with and false data can't be added.
- Traceability: Every transaction or action that takes place in a blockchain it may be public or private is signed digitally. This ensures that an organization or an entity can track down each and every transaction and also locate the corresponding entity on the blockchain using their public address[12]. Any new transaction leads to the change in the ledger, with the previous state being stored in the history log which makes it completely traceable. For Cybersecurity, this single feature adds an additional level of reassurance that the data has not been tampered in any way which makes it completely traceable.
- DDoS: A distributed denial-of-service (DDoS) attack is a major threat to integrity of blockchain, this is because the attack can easily stop a transaction if one of the units is stopped from sending transactions. This difficulty in stopping DDos attacks is due to DNS.
- DNS: Domain Name System is largely centralized, due to this attacking the connection between a website and IP address is comparatively easy, this give them the ability to cash website or even lead users to scam websites.

### *B. BRIEF INTRODUCTION TO BITCOIN*

The very first of its kind Bitcoin by invented in 2008 by an unknown person or group of people using the name Satoshi Nakamoto and started in 2009 when its source code was released as open-source software. Bitcoin is based on the Blockchain Technology [15]. Blockchain technology is a shared, secure ledger of transactions distributed among a network of computers, rather than resting with a single provider. Bitcoin is the most expensive digital currency or rather the most expensive currency at the time.

### *C. BITCOIN AND IT'S SECURITY*

Bitcoin works on the Blockchain Technology. Blockchain technology have various aspects of security such as Cryptographic Keys. There are two Public and Private Key for each user in the Blockchain. The public key is publicly known to everyone while the private key is known only to the user, now 0suppose A wants to send a data to B, so A can use the B's public key to encrypt the data and now the data can only be decrypted with B's private key. Another security aspect of Blockchain is that it is a decentralized peer to peer network, which means there is no one responsible to look over it, rather the copy of whole data of a blockchain is with each and every user [13]. Then there is Blockchain's protocol, a block contains a digital signature, timestamp, hash number and relevant information and is then broadcast to all nodes in the network. Each Block contains the hash of the previous block. Then there are miners who are responsible to add the block to the blockchain.

The bitcoin's current protocol is secure enough but still might fail with some sites or services that deals with bitcoin. In a paper proposed by Shervin Erfani and Majid Ahmadi a well-defined security functional architecture has been proposed. The security features and requirements of Bitcoin have been structured in layers by this model [14]. This model consists of 3 tiers: the protocol handling, the functional layers, and the distributed database.

This model is composed of mainly 4 layers. (I) Fundamental Mathematical Modules- such as pseudo number generator, (ii) Security Mechanism Layer- contains time stamp, digital signature, nonce and other algorithms, (iii) Security Service Layer, and (iv) Security Management Layer for bitcoin and another cryptocurrency. The security policy and business requirement- the top layer – is an added-on feature in this functional architecture, which provides the overall security supervision such as the difficulty rules for "target value" for mining, "legal views", "disaster recovery" and the rest.

### *D. BRIEF INTRODUCTION TO ETHEREUM*

Ethereum enables developers to build and deploy decentralized applications. A decentralized application or Dapp serve some particular purpose to its users. Bitcoin, for example, is a Dapp that provides its users with a peer to peer electronic cash system that enables online Bitcoin payments. Because decentralized applications are made up of code that runs on a blockchain network, they are not controlled by any individual or central entity[16]. Any services that are centralized can be decentralized using Ethereum. Ethereum is not "owned" by anyone, but all of the programs and services linked with the network require computing power, and that

power is not free, this is where ether comes in play. Ether is kind of fuel for the service fees or transaction fees or reward of miners on Ethereum.

### *E. ETHEREUM AND IT'S SECURITY*

Ethereum basically allows developers to make Dapps or Decentralized application. As the name suggests the decentralized, these Dapps works on the Blockchain Technology. Some of the key features of security of dapps build by Ethereum are:

Immutability: The data that is stored in a blockchain is recorded and the blockchain keeps track of all the changes that have been made to it from the beginning and it is not possible to change this history [17].

Protection against data corruption: Since each computer has a copy of the database, it is extremely difficult to hack this database. To alter the database, it would be necessary to simultaneously alter more than 51% of the participating computers simultaneously. The blockchain bitcoin exists since 2009 and it has never been corrupted by a computer attack [18].

Network security: The blockchain works with a very powerful encrypted protocol which also makes it very difficult to alter.

Reliability: It is virtually impossible to stop simultaneously all the computers participating in the Ethernet blockchain. Therefore, this database is always online and its operation never stops.

Another important feature of Ethereum is transparency. All contracts are publicly running on Ethereum and, with the necessary technical knowledge, anyone can check that everything is working properly.

## V. IOT FRAMEWORK AND SECURITY

IoT is basically an interconnection of devices and these devices are connected through internet. These devices send and receive all the data through internet and this data gets stored in cloud servers [19]. The basic principle of IoT is that the devices are made smarter by connecting them to internet. Through IoT technology user data is collected and processed and results in enhancing the experience of a user. IoT system is a centralized system in which all data is stored in few servers and all the powers lies in the hands of centralized authority.

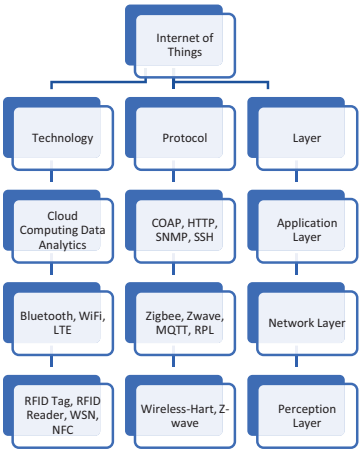


Figure 2. Layered architecture of IoT

Numerous applications are present in IoT namely autonomous vehicles, building smart cities, building smart homes, in health sectors. Various IoT devices like smart wearables, smart appliances and other smart thermostat systems.

Apart from all these security concern acts as the major concern in the field of IoT system where all information is stored in in one cloud servers only and works only on trust that's why IoT network is more prone to security threat and there are huge chances of data breach. If data breach occurs in IoT network, the hackers get access to the user's system through which privacy of user gets compromised and this can lead to harm to the user.so before the implementation of IoT there is a need for strengthening of systems and all bugs should be removed from the system. To accomplish the security of IoT devices are one of the difficult tasks to achieve but this can be achieved by using blockchain technology in the IoT systems [20].

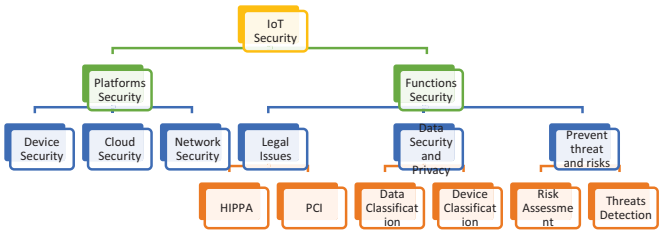


Figure 3. IoT Security Taxonomy

### A. BLOCKCHAIN

BLOCKCHAIN TECHNOLOGY uses a fully decentralized network in order to record and process the information. Ability for optimization and revolutionization of the global infrastructure of the technologies is only present in the blockchain technology. Blockchain technology helps to create a decentralized system that helps to provide interaction among users and the indulgence of central servers will remove. By using blockchain technology a fully transparent and open database can be created which provides transparency to the users.

### B. BLOCKCHAIN IN IoT FIELD

Blockchain system enables distributed data sharing. Blockchain technology does not allows any third party in between. Each user generates his own keys and in the distributed databases all the components like transactions and blocks are stored.

Basically, IoT system is more prone to attacks and data breach so we have to make it more secure and reliable. To make this happen we have to implement blockchain technology in the field of IoT. IoT system works on centralized system means server-client model but in order to make it more practical we need decentralization system. Decentralization system results in peer-to-peer communication model instead of the standard server-client communication mode and this can only be achieved by using Blockchain technology.

Blockchain technology is both decentralized and tamper proof means it is not vulnerable to cyber-attacks as compared to standard IoT system. Through blockchain technology there will be a distribution of both storage and computation needs across millions of IoT devices and by this the central failure will not leads to failure in whole system [21]. Cyber-attacks are impossible to occur in blockchain technology as it is very difficult to intercept any communication and it does not provide any space for middle men [22].

By using blockchain technology in IoT network, the billions of devices can be tracked [23]. Without having going through the traditional client-server model for each communication there can both coordination and processing can occur which results in low cost of installation and maintenance of the IoT networks and by these significant cost savings there will be massive scaling of IoT network can be done.

We can say that use of Blockchain technology in IoT can ensure that communication between different devices in the IoT network is secured and trustful. The combination of both BLOCKCHAIN and IoT will provide a decentralized secured network and smart devices can easily exchange data over a network reliably as there is no dependence on any centralised authority.

## VI. CONCLUSION

We conclude that Blockchain technology provides advancement in the field of cyber security, cryptocurrency and IoT. Blockchain Technology is useful for organisations and companies by providing them secure internet data, secure information and provides safety from cyberattacks. The main advantage of blockchain is that it is near impossible to break codes and keys as it combines many devices and computes which are anonymous or decentralised. By using blockchain technology business can easily authenticate users. The device cost is decreasing and computing power is increasing every day therefore Blockchain presents an immense possibility in Internet of Things (IoT) and providing security.

## REFERENCES


[1] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal and B. Sikdar, "A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures," in IEEE Access, vol. 7, pp. 82721-82743, 2019.

[2] Rainie, Lee, Duggan, M. “Privacy and Information Sharing” Pew Research Center, December 2015. Available at: http://www.pewinternet.org/2016/01/14/2016/Privacy-andInformation-Sharing/ (accessed 10 January 2017)

[3] J. Li, T. Liu, D. Niyato, P. Wang, J. Li and Z. Han, "Contract-Based Approach for Security Deposit in Blockchain Networks with Shards," *2019 IEEE International Conference on Blockchain (Blockchain)*, Atlanta, GA, USA, 2019, pp. 75-82.

[4] X. Yang, Y. Chen and X. Chen, "Effective Scheme against 51% Attack on Proof-of-Work Blockchain with History Weighted Information," 2019 IEEE International Conference on Blockchain (Blockchain), Atlanta, GA, USA, 2019, pp. 261-265.

[5] S. Yang, Z. Chen, L. Cui, M. Xu, Z. Ming and K. Xu, "CoDAG: An Efficient and Compacted DAG-Based Blockchain Protocol," 2019 IEEE International Conference on Blockchain (Blockchain), Atlanta, GA, USA, 2019, pp. 314-318.

[6] I. Homoliak, S. Venugopalan, Q. Hum and P. Szalachowski, "A Security Reference Architecture for Blockchains," 2019 IEEE International Conference on Blockchain (Blockchain), Atlanta, GA, USA, 2019, pp. 390-397.

[7] S. Pavithra, S. Ramya and S. Prathibha, "A Survey On Cloud Security Issues And Blockchain," 2019 3rd International Conference on Computing and Communications Technologies (ICCCT), Chennai, India, 2019, pp. 136-140.

[8] D. Tanana, "Avalanche blockchain protocol for distributed computing security," 2019 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom), Sochi, Russia, 2019, pp. 1-3.

[9] Shat, F. and Pimenidis, E. (2017) Social Media and e-Voting – Secure and Trusted Political Forum for Palestine, in Jahankhani, H, et.al. (eds.) Global Security, Safety and Sustainability - The Security Challenges of the Connected World, CCIS 630, pp. 290-302

[10] Kyle Croman, Christian Decker, Ittay Eyal, Adem Efe Gencer, Ari Juels,
Ahmed Kosba, Andrew Miller, Prateek Saxena, Elaine Shi, Emin Gun¨ Sirer, et al. On scaling decentralized blockchains. In International Conference on Financial Cryptography and Data Security, pages 106–125. Springer, 2016.

[11] Gillespie, M., Ampofo, L., Cheesman, M., Faith, B., Iliadou, E., Issa, A., Osseiran, S. and Skleparis, D. (2016) Mapping Refugee Media Journeys: Smartphones and Social Media Networks, Technical Report, DOI: 10.13140/RG.2.2.15633.22888

[12] Mousavi S.A.A., Pimenidis E, Jahankhani H. (2008) Cultivating Trust – An e-Government Development model for addressing the needs of developing countries, International Journal of Electronic Security and Digital Forensics (IJESDF), Vol. 1, No. 3, pp. 233-248.

[13] M. Conti, S. Kumar E, C. Lal, and S. Ruj, “A survey on security and privacy issues of Bitcoin,” arXiv preprint arXiv:1706.00916, 2017.

[14] J. Garay, A. Kiayias, and N. Leonardos, “The bitcoin backbone protocol: Analysis and applications,” in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*.Springer, 2015, pp. 281–310.

[15] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” 2008.

[16] I.Eyal, ‘‘Blockchain technology: Transforming libertarian cryptocurrency dreams to finance and banking realities,’’ *Computer*, vol. 50,no.9, pp. 38–49, 2017UNCHR (2017) Europe Monthly Report – May 2017,UNCHR TheUNRefugeeAgency.http://data2.unhcr.org/en/situations/mediterranean [online] (accessed 10 July 2017)

[17] Kacem, A., Belkaroui, R., Jemal, D., Ghorbel, H., Faiz , R. and Abid, I.H.(2016) Towards collaborative e-government improvement using social media-based citizen’s profile investigation, In Proceedings ICEGOV '15-16, March 01-03, 2016, Montevideo, Uruguay, DOI: http://dx.doi.org/10.1145/2910019.2910029

[18] Dincelli, E. and Goel, S. (2015) Research Design for Study of Cultural and Societal Influence on Online Privacy Behavior, In Proceedings of 2015 IFIP 8.11/11.13 Dewald Roode Information Security Research Workshop

[19] Dhir A, Torsheim T, Pallesen S and Andreassen CS (2017) Do Online Privacy Concerns Predict Selfie Behavior among Adolescents, Young Adults and Adults? Front. Psychol. 8:81

[20] T. M. Fernández-Caramés and P. Fraga-Lamas, ‘‘A review on the use of blockchain for the Internet of Things,’’ *IEEE Access*, vol. 6, pp. 32979–33001, 2018

[21] . M. Frustaci, P. Pace, G. Aloi, and G. Fortino, ‘‘Evaluating critical security issues of the IoT world: Present and future challenges,’’ *IEEE Internet Things J.*, vol. 5, no. 4, pp. 2483–2495, Aug. 2018.

[22] Flashpoint. *Mirai Botnet Linked to Dyn DNS DDoS Attacks*. Accessed: Dec. 18, 2018. [Online]. Available: https://www.flashpointintel.com/blog/cybercrime/mirai-botnet-linked-dyn-dns-ddos-attacks/

[23] G. Yang, M. Jiang, W. Ouyang, G. Ji, H. Xie, A. M. Rahmani, P. Liljeberg, and H. Tenhunen, ‘‘IoT-based remote pain monitoring system: From device to cloud platform,’’ *IEEE J. Biomed. Health Inform.*, vol. 22, no. 6, pp. 1711–1719, Nov. 2018.