Enhancing Cybersecurity Through Blockchain Technology Enhancing Cybersecurity Through Blockchain Technology

9 authors, including:

Shouvik Sanyal
Dhofar University
74 PUBLICATIONS   **661** CITATIONS

SEE PROFILE

Madan Laddunuri
The Papua New Guinea University of Technology
7 PUBLICATIONS   **17** CITATIONS

SEE PROFILE

Sp Mathiraj Subramanian
Alagappa University
139 PUBLICATIONS   **173** CITATIONS

SEE PROFILE

Dhanabalan Thangam
Presidency Business School
35 PUBLICATIONS   **428** CITATIONS

SEE PROFILE

Chapter 11
Enhancing Cybersecurity Through Blockchain Technology

Sriram V. P.
Acharya Bangalore B School, Bengaluru, India

Shouvik Sanyal
Dhofar University, Oman

Madan Mohan Laddunuri
Malla Reddy University, India

Mathiraj Subramanian
Alagappa University, India

Vijay Bose
Vaagdevi College of Engineering, India

Bharath Booshan
Acharya Institute of Graduate Studies, India

Chethan Shivaram
Acharya Institute of Graduate Studies, India

Manasa Bettaswamy
PES University, Bengaluru, India

Shabista Booshan
ISBR Business School, Bengaluru, India

Dhanabalan Thangam
iD https://orcid.org/0000-0003-1253-3587
Presidency Business School, Presidency College, Bengaluru, India

ABSTRACT

Blockchain technology ensures data security through an integrated system whereby it collects, arranges, stores, and disseminates information in different blocks. This technology thus enables adding the data to the network. Once data has been added to the network, no one can alter the data set either by adding or deleting it. Further, this technology also helps to track and check the changes if anything is made to a blockchain, as the changes remain in the database forever. Since this technology uses lots of systems in a blockchain, it will regularly download its data, arranging, and keeping the copy locally. Locating the data errors and cyberattacks in advance by analyzing the data documented, it employs the consent of various participants and accomplishments in cryptography. With this backdrop, the chapter has attempted to disclose the basics of blockchain technology in data security, why blockchain in cybersecurity, how it ensures cybersecurity, its benefits, its innovative uses, and the future of cybersecurity in the online business platforms.

INTRODUCTION

The conventional economy has rejuvenated itself as a digital economy by incorporating the latest digital technology advancements in its business process. Its result transfer and so on. Hence the business houses have to understand deeply that now almost all the sectors such as manufacturing and services sectors have started to use the Information and Communication Technology (ICT) enabled digital gadgets into their business operations for designing, executing, supervising, and augmenting the business technologies have been supporting a lot to the business process, they are not free from data security issues such as cybercriminal and cyber attack, particularly in the operations by administering business and customers' data. Thus data has made a revolution in the recent business world, along with Internet technologies (Verma Mudit Kumar, 2020). Though the online business growing day-by-day, data security threats also have been growing along with the online business in various forms and distress the acuities of the way consumers are using online platforms for various purposes such as online purchasing, ticket booking, and money these threats will destroy their businesses which are operating on the online platform. Therefore the business houses need to take appropriate safety precautions to eliminate the data threats as possible as to increase consumers' self-confidence towards the online business, and thus it would be an option to maintain a tempo in online shopping (Liao and Fan, 2020). As these measures are used to secure the customer base, it is called cybersecurity, and it has been instituted to make sure the security of consumers' seclusion and data and thus it ensures a hassle-free shopping experience to the consumers. Hence there is a requirement for promoting cybersecurity measures at all levels of the online business to condense the impact of cybercrime and to promote the benefits connected with cybersecurity (Aboul-Enein, 2017).

Moreover Investing in cybersecurity has been increasing in recent times at all businesses to save customers' data. As far as the investment over cybersecurity has been concerned, it has been increased aggressively in the times of yore, with no sluggish. Further, it is also estimated that the business organizations planned to invest more than 1 trillion USD globally between 2017 and 2021 to protect their business houses and customers' data from online security threats (Morgan, 2019). Even though the business houses have invested a huge amount and efforts on cybersecurity, but still internet hackers prolong to assail business processes by hacking data and making the business units weak, interrupting data storage devices and their applications, and thus creating network errors or traffic. There was the worst experience in the past and they have insisted on the importance of developing cybersecurity systems. There were more than 4500 cyber assails have took place every day in the year 2016, and it is 300 percent more than the attacks that took place in 2015, while 1,000 assails were found approximately daily. In the case of Uber, around 60 million data of various drivers and riders have hacked in the year 2016. In the case of Facebook, about 5335 million users' details were hacked from 105 countries, of which 30 million users' records were from the USA, 11 million users from the UK, and 6.5 million were data from India (Holmes, 2021). Hacked data includes names, mobile numbers, user locations, birthdates, bios, and email addresses. Thus it is understood clearly that no industrial sectors are safe online, and hackers are continuously seeking new ways from new landscapes to the crook. CB Insights report has estimated that between 2017 and 2018 around 6 billion secret files were stolen one side. On the other side, the number of cyberattacks has also increased. These complicated attacks have collapsed the conventional data security methods, thus creating privacy challenges for business organizations. In the wake of the covid-19 outbreak, a large number of companies have insisted their employees work from home by connecting themselves with internet technology, and it is also created a new way of data threats to the company and employees (World Economic Forum, 2019). Therefore, instead of developing more potential tools, many

business organizations have started to rethink the existing systems that formed these vulnerabilities in the primary place. As a result, there are technologies such as Artificial Intelligence (AI), Big-data analytics, Internet of things (IoT), and blockchain technology have been developed for strengthening the business process effectively, of which blockchain technology is one of the technologies that have played a major role and ensures smooth flow of the business process with adequate data security in the online business environment. Blockchain technology presents a diversified pathway towards better data and cybersecurity, one that is travelled a smaller amount and almost avoids the cybercriminals (Infosys, 2021). These moves trim down the susceptibility, present sturdy encryption, authenticate the ownership of the data and also assess the genuineness of the data. Still, this technology can reduce the requirement of some passwords, which are often making cybersecurity weak. The primary benefit of using blockchain in the business process is dispersed data ledger. A distributed communal key infrastructure model decreases numerous risks connected with the data stored in the centralized storage, by removing the most noticeable marks. Business transactions or dealings will be recording each node in the entire network, thus it ensures the data is secure and free from cyberattacks, hacking, data stealing, or meddling with data, unless the susceptibility exists at the platform level (Jamie Condliffe, 2016).

The combined consensus algorithm of the blockchain technology helps to remove the traditional data threats, by observing the malevolent activities, irregularities, and removing those problems by devoiding the requirement of the authority center. Thus this technology makes stronger the validation of the data and protects the data communications by maintaining a digital ledger. Even though blockchain technology holds various futuristic characteristics, it does not operate itself, and it is taking the support of cybersecurity technology called encryption (Mukundan, 2019). The dispersed data ledger can employ the public key platform to ensure data communication, by authenticating the devices, validating the changes in the configurations, and finding out secret devices in the IoT environment. Blockchain technology can protect various attached thermostats, security cameras, smart doorbells, and other susceptible technologies from side to side encryption and digital signatures. A report published by Palo Alto Networks reveals that 98 percent of the traffic of the IoT-enabled device was due to unencrypted and it paves a way for the cyberattack (Paloalto Networks, 2020). Thus blockchain technology act as a warhead against dispersed denial-of-service (DDoS) assails. Hence all the Industries irrespective of manufacturing or services require an excellent cybersecurity solution and depend on blockchain technology to distribute the goods and services without mistakes and fraud. Further, this technology also supports digitizing the business and customers' data. Hence all the industries, online business houses, in particular, are using this astonishing technology to make stronger their business processes by ensuring cybersecurity processes (Javaid, Haleem, Singh, Khan, & Suman, 2021).

This technology provides an essential as well as an effective platform to share the data securely, in relation to different financial, business transactions as well as contracts. In such process blockchain uses a technology called cryptography to transfer the data with utmost accuracy and safety. The data transfers happening in blockchains are just a transferring the assets and the assets are fundamentally data that may expose various personal as well as business data such as personal data, healthcare data, financial data or even companies data. One of the best applications of this technology is Bitcoin, where it has been using mostly for the secure transfer of bitcoins from one to another by executing the contract through blockchains. Further, this technology also used in smart contracts, for its safety. Etherium is a yet another application of blockchain, and it has been developed to execute smart contracts with predefined rules and regulations. Such type of smart contracts are having various application in different areas like Internet of Things (IoT), in which billions of devices need to function collectively, to build smart contracts for

swapping data and carry out the process. Basically it is a peering technology without a centralised control of blockchains fundamentally deals with contracts and contracts involve data. Thus a huge volume of data will be collected, classified, processed, assessed and disseminated in different transactions. Since the data science technology is the heart of various business transactions, blockchain technology ensures a system to execute the transactions firmly (Thuraisingham, 2020). With this backdrop this present chapter will reveal about blockchain technology, its working structure, role of blockchain technology in data science and cybersecurity, how it ensures cybersecurity, blockchain technology and its benefits to cybersecurity, innovative uses of blockchain technology in cybersecurity, blockchain technology and future of cybersecurity subsequently. Finally this chapter concludes in the last part of the chapter.

WORKING STRUCTURE OF BLOCKCHAIN TECHNOLOGIES

Blockchain is a technology that works with group of blocks, which are linked with each other through chains. Each block will act as a file that restrains the data related to each transaction. Further the stored data can be transferred from one block to multiple blocks, in the same way one block also can collect the data from different blocks simultaneously. The data stored in the blocks will be permanent and irreversible. Thus the number of blocks can also be added to the chain depends upon the number of transactions, and each transaction will be verified to ensure the authenticity of the data. According to NIST technical publication, blocks can be used without permissions, it means anybody can use a block; on the other hand blocks can also be used with permissions, with the consent of centralized or decentralized authority (Kshetri, 2017). Thus in the blockchain there is an important component called cryptographic hash and it is playing major functions. Further it is a kind of data assimilates where multiple checks are calculated depends upon the content. It seems as one of the important component that ensures security for the blockchain. Notion of transaction is a yet another component of this technology that ensures the communication interface with two blocks or parties. Through this cryptocurrency transactions are passed between different users of this technology. This technology also uses asymmetric key method, as it is being an essential one in the public key cryptography. This blockchains also collects the network details which are derived from the communal key cryptography. The notion is considered as the central part of blockchain, as it is being a ledger of various transactions. Further these transactions are performed through a decentralized fashion, and hence this structural design supports blockchain as a distributed ledger. As the business transactions are performed, blocks will be added to the existing blockchain which have the data of authenticated business transactions and the metadata about those transactions. Each block will have the data, and the blocks are linked together to build the blockchain. Thus huge volume of relevant information available about the blockchains, it includes smart contracts and consensus model forks. With the help of these models, users can publish next block by showing the proof of completion of work. This model is also used in bitcoin transactions. In various cases blockchains required to do alteration and those alterations are called as forks (Casino, Dasaklis & Patsakis, 2019).

Blockchain is acting as a ledger of all the business transactions that have been performed, shared, and confirmed by various users in the blockchain system. Further, it is administered by a peer-to-peer network that is accountable for authenticating new-blocks and instituting inter-node communication. Whichever the changes need to do in the dataset in a blockchain will necessitate changes in all the consequent blocks in the chain, and it is making the assignment enormously as well as resource-extensive. Thus, blockchain technology is one of the most protected technologies for various types of business

transactions, to date. The blockchain technology is a setup of linear association of blocks, in that such data is added sequentially on it. Thus the data is added to the chain by utilizing procedures that assist to evade faulty functioning of the system of blockchain. The requirement for unity protocol materialized from the thought of Hashcash, as a result of a poor working of cryptography methods like Elliptic Curve Digital Signature Algorithm (ECDSA) to alleviate the risks of dual expenditure and Sybil molests (Sankar, Sindhu & Sethumadhavan, 2017). Figure 1 explains the complete structure of stack of blockchain technology. This structure stack advocates how various layers of a blockchain work together with each other to get an operational blockchain.

Figure 1. Working structure of Blockchain Technology in the Data Security
Source: Mittal, Gupta, Chaturvedi, Chansarkar & Gupta (2021).
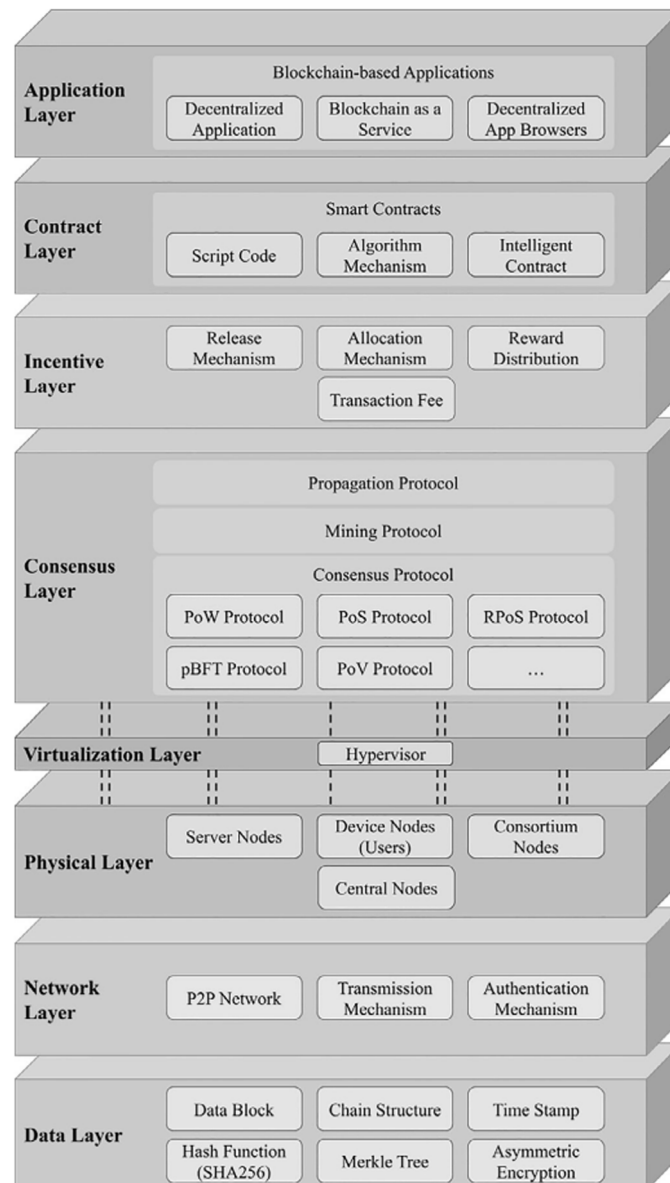
Homoliak et al., (2020) have proposed that the blockchain structure should contain seven layers right from Data layer, Network layer, Physical layer, Consensus layer, Incentive layer, Contract layer, and Application layer. Besides, they also have proposed the Virtualization layer to bridge the Physical layer to the Consensus layer. Yli-Huumo, Ko, Choi, Park, and Smolander (2016) revealed that in spite of the exposure of blockchain technology into different fields, the familiarity of the ordinary public about blockchain enabled systems has not highly developed, as research about it. Therefore, people must comprehend about blockchain technology and become skilled to promote the business applications to distribute their software applications and dealings across the network, and thus, afford enhanced cyber-security to the developing cyber-infrastructure.

ROLE OF BLOCKCHAIN TECHNOLOGY

With the growth and development of internet technology, our entire life has been changed in all aspects. Computing systems have occupied the entire world, and it is spreading from mobile technology to au-tonomous vehicles. All these things are possible only because of the data and its related science. With the help of the data and its related science, it is easy to collect, accumulate, administer, and analyze a huge volume of data collected from various sensors and devices, with the help of IoT (Demirkan, Demirkan, & McKee, 2020). In this process, a huge number of self-functioning systems and devices are connected through internet technology and thereby synchronize their activities. Still, data security and solitude for the substantial number of data systems within the IoT have become a question mark. As, IoT collects huge volumes of assorted data from various sources with numerous devices, conventional data and cyber security methods such as encryption are not competent to safeguard the IoT and data systems. Hence to ensure efficient cybersecurity, more number of researches has been happening in recent times to examine the developments happening in data science for protecting such systems (Sarker, 2020). As a result, a new technology called blockchain has developed and it plays a major role as expected, in safeguarding data science and ensuring cybersecurity, and the same has been elucidated as follows;

In Data Science

Blockchain technology is an emerging one that ensures data safety and thus supports data science techniques also. It means this technology ensures the data collection in a highly secured environment, and it also helps to process the data, manage the data, analyze the data, and share the data in a secured manner. Yaga, Mell, Roby and Scarfone, (2018) mentioned in their work that data analysis is feasible in recent days due to blockchain technology, even from the basic individual devices. Furthermore, this technology also validated the data generated by it, in a planned and irreversible manner. Thus, block-chain technology ensures the genuineness of data, and thus improves big data. Tasnim, Omar, Rahman, Bhuiyan and Alam (2018) mentioned in his paper that blockchain is very much useful to data scien-tists to validate and verify the data at each block on a chain. As it is being immutable security, for this reason, it is treated as the main driver for its implementation. Further the decentralized ledger system available in blockchain shields data through manifold signatures, thus it helps to avoid data leaks and lacerates. As a result blockchain technology is ensuring and maintaining data security, and trust, helps to get better data quality, and firmly disseminates the data to the required parties. In several institutions, transaction or business trust is imposed by a centralized controlling authority; as a result, it is having

the possibility to be a single point of the malfunctioning state. Where in the case of blockchain technology, it ensures the transactions trust in a decentralized manner, by utilizing a group of a system in the peer-to-peer network. In the same way, this technology also enables data sharing by enabling manifold parties to collect and disseminate the data firmly (Marr, 2018). This technology also helps to verify the reliability of the data at every transaction. The main component of blockchain technology called Distributed ledger is also playing a major role in deciding the derivation of the data, as it is an essential part of data science. The role of Blockchain technology in the supply chain is more significant as it is keep on tracking the data, and thus it is also helpful in the data supply chain process (Hamlen & Thuraisingham, 2013). This technology also invested a lot of effort in data science; especially in big data analytics for assessing private data, based on the hyper ledger framework (Lampropoulos, Georgakakos & Ioannidis, 2019). Data safety and solitude spread across all parts of data science and then converse with the help of blockchain with its decentralized system (Liu, Peng, Long, Wei, Liu, & Tian, 2020). Houben and Snyers (2018) have presented in their paper that blockchain-enabled cryptocurrencies will have transaction history and graphs to facilitate the public to access them. Thereby public can have detailed information about the impact of price on the underlying cryptocurrency. Further, a topological enabled data system helps to assess graph dimensions with the help of the data collected through blockchain, and it can be utilized to forecast the price structure of Bitcoin. Thuraisingham (2018) explained in their paper that blockchain technology ensures data safety and security in the whole data lifecycle process, right from data collection to data dissemination, and the same examined by (Thuraisingham, 2018) about different ways of combining cyber security process into the data science. The same data-driven approach has also suggested by (Thuraisingham et al, 2016).

In Cybersecurity

The ultimate objective of Blockchain technology is to ensure secured business transactions, especially in the case of the cryptocurrency business. As data security is at the forefront of this technology, it reached all the spheres of the business easily. With this backdrop, this section presents various applications of blockchain technology in cybersecurity (Zhuang, Zamir & Liang, 2020). There are four areas identified based on the blockchain-enabled security such as distributed ledger, IoT security, Domain Name System, and end-to-end encryption. As mentioned earlier, centralized data storage is not safe due to single point authorization, as it is having the possibility of massive errors. To replace the same issue, this technology uses the component called distributed ledger process, through this data can be managed in a decentralized manner and disseminated among numerous devices. With the help of distributed ledger architecture, blockchains enabled decentralized data storage, and also use Cryptographic checksums to make sure data security. The second area where this technology ensures security is IoT, as it is having association with numerous connected devices, and cybersecurity is a must for this case. Hence, blockchain technologies can be used to ensure secure data transfer between the systems and not have centralized control. Domain Name Systems (DNS) are typically functioning under a centralized controlling setup and it would be easy for the hackers to break the system and steal the data easily without complexity (Parizi, Dehghantanha, Azmoodeh & Choo, 2020). On the other hand blockchain technology facilitates distributed nature data storage, and it would be a challenge for the hackers to find out the place where the data is stored exactly, and it is more complicated to discover the point of entry. Thus the data can be safe and without any manipulation. In recent times all the applications are using more number of messaging services, for the same they are using the end-to-end encryption, to ensure secured data transfer. For the same, this

end-to-end encryption system is started to use blockchain technology (Bansal, Panchal, Bassi, & Kumar, 2020). Where this technology enables a homogeneous way of communication in messaging systems, by utilizing distributed processing. Thus, there are researchers have discussed a lot of the uses of blockchain for security. Demirkan, Demirkan, and McKee (2020) presented in their work that blockchains technology has the potential to enhance the cybersecurity, and thus it acts as the safest platform to avoid deceitful activities through various consent mechanisms, and it also notices data corruption depending on its fundamental characteristics of functional resilience, data encryption, review, clearness, and immutability. Further, this technology also enhances security by removing human beings in the validation process, condensing the attacks happening through distributed denial of service (DDoS), affording data identifiably, and supporting scattered storage. Such parallel applications have also discussed in various research works including (Goldstein, 2020) where the author explained the extent to which blockchain technology improves cybersecurity, data privacy, and veracity are provided.

HOW THE BLOCKCHAIN TECHNOLOGY DOES ENSURES CYBERSECURITY

Blockchain Technology incorporates a system called decentralized distributed ledger on which business and other related transactions' data would be recorded with the help of diversified computer networks. The specialty of this technology is any type of data that can be stored on the blockchain, irrespective of the industries. This technology further assures absolute security against data breaches, cyber assails, and identifying potential data thefts. This technology also ensures that all our business transactions with fully protected and shielded from unlawful data access. With data hacking occurrences and this process reaching more concentrated and modernized over the years, and thus it moved the online business world securely and it had become a genuine concern. The conditions of the individual and business houses data security have become and no proper resolution was found until the arrival of blockchain technology in the cybersecurity field (Horbenko, 2017). Thus the application of blockchain technology in the industrial sectors has transformed various industries such as the IT industry, health sector, online business and banking, and financial sector from an unsecured zone to a well secure zone. Business experts from various industries state that this technology offers unconquerable safety from unlawful access of the customer and business data and avoid cyber-assail. Thus this technology can be used to keep the business process in the protected environment and thereby it enhances cybersecurity almost in all industries (IBM, 2021). The application of blockchain technology in business processes helps to deal with data in the protected environment by ensuring a scatter form of data storage. This method of data management helps individuals and business people to safeguard themselves from data threats, and it avoids hackers from the manipulation of the data storage. On the other side companies which are providing storage services are also evaluating the capability of blockchain technology in protecting data from hackers (Cloudtweaks, 2019). Thus this technology offers a secured environment for doing business in the following manner;

Ensures the Safety of the Private Messages

Due to the ICT developments, the usage of social media has popularized among the public, and the number of social and digital media platforms have also been increasing day by day, and the number of social media applications is also developed every day. Its a result online business is getting popular among the public. A huge volume of metadata would be collected during these transactions. Thereby

it shields business accounts, transactions, and customers' data which have been used in social media. Many of the messaging companies have now started to use this technology than end-to-end encryption as it is being the best option for the collection of genuine data. Further, this technology also enables the security protocol consistently and it can be used to create a single Application Programming Interface (API) architecture to serve better communication capabilities among various messengers. It was experienced that numerous attacks have taken place recently against various social media platforms such as Facebook, Twitter, and Instagram. Crores of accounts were hacked as a result of these cyberattacks, as the users' data were into the erroneous points. These kinds of cyberattacks can be avoided easily if the social media platforms deployed this technology in their messaging systems, and it will also help these sectors to shun cyberattacks in the future (Arnold, 2019).

Ensuring the Safety of the Internet of Things

Due to the introduction of various edge devices like routing switches, Integrated Access Devices (IADs), thermostats, metropolitan area network (MAN), and routers, these are some of the devices used by the hackers progressively to access the data anonymously from a large number of networks. Increasing usage of AI and its enabling technologies make the hackers easy to get access to residence automation systems through these edge devices such as smart televisions, and smart switches. In many cases, the IoT-enabled gadgets are insecure, at this juncture, blockchain-enabled technologies can be an effective alternative to manage more systems, and thereby it secures those systems (Arnold, 2019). Thus this method will be helping to leverage the ability of the gadgets and make them do judge the security position of the systems. This technology also supports perceiving and reacting to various commands rose from the unidentified networks without depending upon the centralized systems; thereby it saves the edge devices from cyberattacks. As this technology deals with decentralized systems, it will make the hackers lose their control over the systems. Thus blockchain technology is operating with decentralized systems; it avoids cyberattacks and data threats and saves the entire network (Yatsenko and Sotnichek, 2021).

Protection From Domain Name System

In some cases, the users will be denied to access the resources from the target resource enters such as servers, networks, and websites when they have a DDoS attack, as a result, the system would be shutting down or slowing down. Another resource center called Domain Name System (DNS) would be monitored through a centralized system, however, it is having higher possibilities for hacking the sites, as it is monitored by the centralized system, and it is being a perfect place for the hackers to control the linkage between a website address and an IP address (Surajdeep Singh, 2021). This kind of assails will turn the websites into out of order, cashable, and even redirectable to various bogus websites. Fortunately, blockchain technology will avoid such issues by the distributed DNS entries, and it may also be used to diminish such assails in the future. Thus this technology would be removing the feeble points of the areas demoralized by hackers by distributed systems solutions (Sheikh, 2019).

Decentralization of Storage

Data contravene and thefts are common nowadays in the place of work, however it is a mounting issue for the business houses, as they are still using an integrated storage system. The integrated data storage

system makes the hackers' job so easy, as they require only one vulnerable point to enter into the storage system and exploit the data easily (Underwood, 2016). Thus an illicit can get access to an organization's confidential and sensitive data, such as firms' financial records, customer databases, diplomacy, and another database. Hence the blockchain experts suggest using a blockchain-enabled decentralized data storage system, thereby the sensitive data can be stored and maintained without cyberattack or hacking threats. By this setup, the hacker will be finding it difficult to break the data storage systems and hack the data. Thus cloud storage service providers are started to use this blockchain technology to keep the data safe from cyberattacks (Arnold, 2019)

Helps to Verify the Cyber-Physical Infrastructure

The reliability of the data generated by the cyber-physical systems would be damaged by various factors such as corruption of data, wrong configuration of the systems, failure of the components, and so on. However, these problems can be rectified or avoided by incorporating blockchain technology into cyber-physical systems to generate reliable data. This technology ensures data integrity and authentication, and it can be used to authenticate the significance of various cyber-physical systems and their infrastructure. Thus the data developed by blockchain technology based on the components of the cyber-physical infrastructure would be more supportive to the whole chain of protection (Infosecurity magazine.com, 2018).

Enhances Data Diffusion Security

Blockchain technology would be used across various sectors in the future to limit unauthorized access to data while transiting the data. As a result, the transmission of Data can be shielded by incorporating this technology's widespread encryption technique to avert dreadful users from getting access to it, and the users may be organizations or individuals. This technique thus enhances the overall fidelity and veracity of data transmitted through blockchain technology. It also challenges the hackers having the intention to interrupt, change and erase the data transiting through this technology (Andrew, 2019).

BENEFITS OF ADOPTING BLOCKCHAIN IN CYBERSECURITY

A blockchain-enabled security structure will be performing in a decentralized environment, and it never compromises its operations and thus it is being a challenge for the hackers and the cyberattacks. This technology helps a lot across the sectors and users, especially for the internet users, it is offering huge benefits. Like that this technology offers various benefits in various ways, of which some of the benefits have been presented in the following manner;

It Ensures the Security of the Data Storage

Once the data has entered into blockchain it cannot be either changed or altered. If in case of any changes made in the data set on the blocks it would reveal the same transparently, as this technology has the feature of non-erasable, irreversible, and unchangeable. As a result, the saved data on the blockchain would be safe and sound than data maintained on conventional physical or digital records (Shrestha, Vassileva, & Deters, 2020).

Helps to Transfers the Data Securely

This emerging blockchain technology enables the users to accomplish the swift and secure data transit of various business and personal data such as banking and financial transactions, customer database, and information. It also supports executing Smart contracts by allowing the data safely and facilitating to implementation of the agreements among numerous parties automatically with cent percent data security (Sam Ingalls, 2021).

Minimize the Chances of Process Failure

As blockchain technology uses a decentralized storage system, it does not require permission for storing, and hence it is more flexible in its operations than the traditional system. Since it is using a decentralized storage system, its performance or safety will not be damaged even if a single node of the chain is compromised. It means though the storage system is subjected to cyberattacks, DDoS attacks, and hacking the system will prolong its performance usually without any data and speed loss, as it is having a huge number of copies in the data ledger (Shrimali, & Patel, 2021).

Augmenting Accuracy and Traceability of Data

Usually, all the business transactions will be stored in the blockchain with digitally encrypted technology along with time-stamped, and thus it keeps on recording the transactions as per the time it has collected. As a result, it records each and every transaction in different nodes. Thereby it helps network members to track various business, financial, personal transactions without any confusion along with the activity record. This way of data dealing ability aids business people to distribute the assets properly without any discrepancies, and all these benefits are possible only because of blockchain technology.

Protect Users' Privacy

Blockchain also supports a lot to increase users' privacy by employing public-key cryptography technology in its process. In that way, it authenticates the privacy of users' data, thus it also ensures the data secrecy of the users. Based on this privacy model some of the blockchain-based companies apply this technology in their business operations to move forward safely by leveraging its data privacy. One more advantage of this technology called Keyless Signature Infrastructure (KSI) enables the users to ensure the legality of their signs without using their keys (Shrimali, & Patel, 2021).

INNOVATIVE USES OF BLOCKCHAIN TECHNOLOGY

The growth and development of ICTs induce people to use internet technologies in all spheres of life and technologies keep on updating themselves on par with the developments in the ICTs. Thus the ICT-enabled technologies have changed the business landscape into more data-oriented. As a result all the industries now started to concentrate on various data such as business and customers. As the business houses need to forecast their business trend and customer base for the sustainability of the business (Business Insider Intelligence, 2020). Hence irrespective of the type of industries all the industries started to collect and

use different types of data. Though the data have been collected and stored in a safe environment, they are not free from the threats such as cyberattacks, hackers, and so on. Millions of hackers are available throughout the world to steal business and customer data or try to corrupt the data. This is a great challenge to industries and business houses to safeguard the data and employ different technologies for the same, but they have attacked easily. At this juncture, blockchain technology has developed and started to deploy in business operations to safeguard the database (Sam Daley, 2021). Thus the technology served effectively for the purpose it has developed. This technology is also having a versatile application capable and providing more constructive and useful to the future of Internet technologies, helping users to secure the data from cyber threats. The groundbreaking application of blockchain technology has already been explored a lot in various fields such as banking and finance, online business, e-governance of government, further than bitcoin, cryptocurrency, and it thus has enhanced cybersecurity against cyber threats and hacking. Any industry can safeguard its data with the help of blockchain technology, as it is operating with precise encryption technology and well-established data circulation protocols. Thus this technology ensures data safety from various cyberattacks, and thus it keeps the data remain securely intact away from hackers (Ryo Takahashi, 2017). Thus blockchain technology has a striving feature in cybersecurity, and it may be implemented in the business houses for making numerous benefits to the business and customers.

BLOCKCHAIN AND THE FEATURE OF CYBERSECURITY

Cybersecurity is a major concern of all businesses nowadays and all industries have started to invest more in cybersecurity-related technologies. This tension has reduced now due to the arrival of blockchain technology. As this technology saves the data into different blocks from time to time, it is hard for hackers to attack the specific point. Moreover, this technology uses a decentralized data storage system, and thereby it saves the data in different blocks. By this means, even if the hackers try to attack the storage they have to get access to thousands of nodes, on a similar system (Neeraj, 2021). Even if we do any changes to the data stored in a block will consequence in the whole system will get alert of the same. Hacking or attacking a blockchain-based data system is equal to larcening hundreds of banks all at a time and makes sure that no alarm should be triggered while doing the same. This technology also helps to build a unanimity system and thereby it trims down deceptions and data corruptions by inculcating fresh blocks along with the various security features such as verifying and validating the data by the digital signature, recording the data from time to time with time-stamped, and connected the data to the preceding blocks, and compared the same with remaining blocks (Alex, 2019). Thus the blockchain would be a sound technology in the future for cybersecurity, and it can be possible through utilizing the available resources optimally and understanding this technology deeply. Further, this technology also trims down human involvement in the cybersecurity process, thereby it eliminates possible human error from the process, and thus it reduces the possibility of data violations as much as possible. However, there are chances for human error in the process, due to carelessness, and descends of operations will be the major threats to the data security in near future and it cannot solve these issues completely by the blockchains overnight. Hence, industries need to understand clearly about the blockchain and use it in their business operations appropriately to avoid cyberattacks in the future (Bansal, Panchal, Bassi, and Kumar, 2020).

CONCLUSION

For various reasons Blockchain technology has been used across industries, and it supports to avert cyber threats and attacks, data violence, individual data theft, and ensures the collected data is confidential and safe. As this technology is in the beginning phase, the developers need to build its advanced versions to manage the business operations and data in an enhanced manner. This technology can also supervise and forecast the cyberattacks with the help of AI and alarming the inward cyberattacks and threats, and thereby it helps the business and other organizations to minimize the cost incurred for data security and keep the data in a safe environment. Though blockchain technology ensures cybersecurity, it is not providing the solution for the global security requirements; however, it is an imperative tool for developing next-generation security systems. This technology also helps to build a reliable security system, well-designed storage system for recording business events, and it would be more helpful for various functions such as signing and tracking documents, individual data management, and tracking access. Further, this technology also empowers the data sharing process across the company and outside of the companies by establishing secured networks with no individual control over its process, but anybody can authenticate and validate it. Since millions of people use internet technologies globally, online-based business platforms have been growing every day. Since online-based businesses are more data-driven, millions of data have been generated every day from every business. On the other side, the number and type of hackers are also growing and they tried to attack, hack or corrupt that data sources. In many of the cases, hackers had already attacked social media such as Facebook and Twitter and hacked crores of users' data. All these issues have been rectified now with blockchain technology. As this technology has versatile and unbelievable safety features, it would be more useful for the Internet and internet-based businesses in the future, by establishing safety environment for the users and their data. The groundbreaking application of blockchain technology becoming an element of various business fields already beyond bitcoin business, cryptocurrencies and can also be used to boost cybersecurity further in the future. Thus any industry can ensure the cybersecurity environment comfortably and keep the business and users' data safely by deploying the blockchain technology into their business operations. Thus hack free and cyberattack-free business environment can be established for the smooth conduct of the business.

REFERENCES

Aboul-Enein, S. (2017). Cybersecurity challenges in the Middle East. *GCSP*, *17*, 5–49.

Arnold, A. (2019). Promising use cases of blockchain in cybersecurity. Forbes.

Bansal, P., Panchal, R., Bassi, S., & Kumar, A. (2020, April). Blockchain for cybersecurity: A comprehensive survey. In *2020 IEEE 9th International Conference on Communication Systems and Network Technologies (CSNT)* (pp. 260-265). IEEE. 10.1109/CSNT48778.2020.9115738

Benjamin, N. (2021, July 23). *Is Blockchain the Ultimate Cybersecurity Solution for My Applications?* https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2021/is-blockchain-the-ultimate-cybersecurity-solution-for-my-applications

Business Insider Intelligence. (2020, March 2). *The growing list of applications and use cases of block-chain technology in business and life*. https://www.businessinsider.in/finance/news/the-growing-list-of-applications-and-use-cases-of-blockchain-technology-in-business-and-life/articleshow/74447275.cms

Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telematics and Informatics*, *36*, 55–81. doi:10.1016/j.tele.2018.11.006

Cloudtweaks.com. (2019, February 26). *How Blockchain Is Transforming Cyber Security*. https://cloud-tweaks.com/2019/04/how-blockchain-is-transforming-cyber-security/

Condliffe, J. (2016, July 28). *Massive Internet Outage Could Be a Sign of Things to Come*. https://www.technologyreview.com/2016/10/21/156505/massive-internet-outage-could-be-a-sign-of-things-to-come/

Daley, S. (2021, March 31). *30 Blockchain Applications and Real-World Use Cases Disrupting the Status Quo*. https://builtin.com/blockchain/blockchain-applications

Demirkan, S., Demirkan, I., & McKee, A. (2020). Blockchain technology in the future of business cyber security and accounting. *Journal of Management Analytics*, *7*(2), 189–208. doi:10.1080/23270012.2020.1731721

Demirkan, S., Demirkan, I., & McKee, A. (2020). Blockchain technology in the future of business cyber security and accounting. *Journal of Management Analytics*, *7*(2), 189–208. doi:10.1080/23270012.2020.1731721

Goldstein, K. (2020). Blockchain and Distributed Ledger Technology: Insurance Applications, Legal Developments, and Cybersecurity Considerations. *Conn. Ins. LJ*, *27*, 511.

Hamlen, K. W., & Thuraisingham, B. (2013). Data security services, solutions and standards for out-sourcing. *Computer Standards & Interfaces*, *35*(1), 1–5. doi:10.1016/j.csi.2012.02.001

Holmes, A. (2021). *533 million Facebook users' phone numbers and personal data have been leaked on-line*. https://www.Businessinsider.com/stolen-data-of-533-million-facebook-users-leaked-online-2021-4

Homoliak, I., Venugopalan, S., Reijsbergen, D., Hum, Q., Schumi, R., & Szalachowski, P. (2020). The security reference architecture for blockchains: Toward a standardized model for studying vulnerabilities, threats, and defenses. *IEEE Communications Surveys and Tutorials*, *23*(1), 341–390. doi:10.1109/COMST.2020.3033665

Horbenko, Y. (2017). *Using Blockchain Technology to Boost Cyber Security*. Retrieved from Steel Wiki: https://steelkiwi. com/blog/using-blockchain-technology-to-boost-cybersecurity

Houben, R., & Snyers, A. (2018). *Cryptocurrencies and blockchain: Legal context and implications for financial crime, money laundering and tax evasion*. https://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf

IBM. (2021, August 16). *What is blockchain security?* https://www.ibm.com/in-en/topics/blockchain-security

Infosecurity magazine.com. (2018, August 7). *How Blockchain Is Revolutionizing Cybersecurity.* https://www.infosecurity-magazine.com/next-geninfosec/blockchain-cybersecurity

Infosys. (2021, July 29). *Assuring Digital-trust.* https://www.infosys.com/services/cyber-security/insights/assuring-digital-trust-cybersecurity.html

Ingalls, S. (2021, July 28). *The State of Blockchain Applications in Cybersecurity.* https://www.esecurityplanet.com/applications/cybersecurity-blockchain-applications/

Javaid, M., Haleem, A., Singh, R. P., Khan, S., & Suman, R. (2021). Blockchain technology applications for Industry 4.0: A literature-based review. *Blockchain: Research and Applications, 100027*.

Kshetri, N. (2017). Blockchain's roles in strengthening cybersecurity and protecting privacy. *Telecommunications Policy*, *41*(10), 1027–1038. doi:10.1016/j.telpol.2017.09.003

Lampropoulos, K., Georgakakos, G., & Ioannidis, S. (2019, September). Using blockchains to enable big data analysis of private information. In *2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)* (pp. 1-6). 10.1109/CAMAD.2019.8858468

Lampropoulos, K., Georgakakos, G., & Ioannidis, S. (2019, September). Using blockchains to enable big data analysis of private information. In *2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)* (pp. 1-6). IEEE. 10.1109/CAMAD.2019.8858468

Liao, R., & Fan, Z. (2020, April). Supply chains have been upended. Here's how to make them more resilient. In *World Economic Forum* (Vol. 6). Academic Press.

Liu, J., Peng, S., Long, C., Wei, L., Liu, Y., & Tian, Z. (2020, March). Blockchain for data science. In *Proceedings of the 2020 The 2nd International Conference on Blockchain Technology* (pp. 24-28). 10.1145/3390566.3391681

Liu, J., Peng, S., Long, C., Wei, L., Liu, Y., & Tian, Z. (2020, March). Blockchain for data science. In *Proceedings of the 2020 The 2nd International Conference on Blockchain Technology* (pp. 24-28). 10.1145/3390566.3391681

Marr, B. (2018). How is AI used in education--Real world examples of today and a peek into the future? *Forbes Magazine*, 25.

Mathew. (2019). Cyber Security through Blockchain Technology. *International Journal of Engineering and Advanced Technology*, *9*(1).

Morgan, S. (2019). Global cybersecurity spending predicted to exceed $1 trillion from 2017-2021. *Cybercrime Magazine, 10*.

Networks, P. (2020, August 6). *2020 Unit 42 IoT Threat Report*. https://unit42.paloaltonetworks.com/iot-threat-report-2020/

Ocampos. (2020). *Contribution of Blockchain to Cybersecurity*. Blockchain Land.

Parizi, R. M., Dehghantanha, A., Azmoodeh, A., & Choo, K. K. R. (2020). Blockchain in cybersecurity realm: An overview. *Blockchain Cybersecurity, Trust and Privacy*, 1-5.

Sankar, L. S., Sindhu, M., & Sethumadhavan, M. (2017, January). Survey of consensus protocols on blockchain applications. In *2017 4th international conference on advanced computing and communication systems (ICACCS)* (pp. 1-5). IEEE. 10.1109/ICACCS.2017.8014672

Sarker, I. H., Kayes, A. S. M., Badsha, S., Alqahtani, H., Watters, P., & Ng, A. (2020). Cybersecurity data science: An overview from machine learning perspective. *Journal of Big Data*, *7*(1), 1–29. doi:10.118640537-020-00318-5

Sheikh, A., Kamuni, V., Urooj, A., Wagh, S., Singh, N., & Patel, D. (2019). Secured energy trading using byzantine-based blockchain consensus. *IEEE Access: Practical Innovations, Open Solutions*, *8*, 8554–8571. doi:10.1109/ACCESS.2019.2963325

Shrestha, A. K., Vassileva, J., & Deters, R. (2020). A blockchain platform for user data sharing ensuring user control and incentives. *Frontiers in Blockchain, 48*.

Shrimali, B., & Patel, H. B. (2021). Blockchain state-of-the-art: architecture, use cases, consensus, challenges and opportunities. *Journal of King Saud University-Computer and Information Sciences*.

Singh, S. (2021, July 16). *Potential Use Cases of Blockchain Technology for Cybersecurity*. https://www.itbusinessedge.com/security/potential-use-cases-of-blockchain-technology-for-cybersecurity/

Takahashi, R. (2017, August 7). *How can creative industries benefit from blockchain?* https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/how-can-creative-industries-benefit-from-blockchain

Tasnim, M. A., Omar, A. A., Rahman, M. S., Bhuiyan, M., & Alam, Z. (2018, December). Crab: Blockchain based criminal record management system. In *International conference on security, privacy and anonymity in computation, communication and storage* (pp. 294-303). Springer.

Thuraisingham, B. (2020, October). Blockchain Technologies and Their Applications in Data Science and Cyber Security. In *2020 3rd International Conference on Smart BlockChain (SmartBlock)* (pp. 1-4). IEEE. 10.1109/SmartBlock52591.2020.00008

Thuraisingham, B., Kantarcioglu, M., Bertino, E., Bakdash, J. Z., & Fernandez, M. (2018, June). Towards a privacy-aware quantified self data management framework. In *Proceedings of the 23nd ACM on Symposium on Access Control Models and Technologies* (pp. 173-184). 10.1145/3205977.3205997

Thuraisingham, B., Kantarcioglu, M., Hamlen, K., Khan, L., Finin, T., Joshi, A., . . . Bertino, E. (2016, July). A data driven approach for the science of cyber security: Challenges and directions. In *2016 IEEE 17th International Conference on Information Reuse and Integration (IRI)* (pp. 1-10). IEEE.

Thuraisingham, B., Kantarcioglu, M., Hamlen, K., Khan, L., Finin, T., Joshi, A., . . . Bertino, E. (2016, July). A data driven approach for the science of cyber security: Challenges and directions. In *2016 IEEE 17th International Conference on Information Reuse and Integration (IRI)* (pp. 1-10). IEEE.

Underwood, S. (2016). Blockchain beyond bitcoin. *Communications of the ACM*, *59*(11), 15–17. doi:10.1145/2994581

Verma, M. (2018). Artificial intelligence and its scope in different areas with special reference to the field of education. *Online Submission*, *3*(1), 5–10.

Vijayaraj, M. (2019). *Rethinking Security in IT by Incorporating Blockchain Technology*. https://www.relevance.com/rethinking-security-in-it-by-incorporating-blockchain-technology/

World Economic Forum. (2019). *World Economic Forum Annual Meeting 2019*. Davos: World Economic Forum.

Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2019). *Blockchain technology overview*. arXiv preprint arXiv:1906.11078.

Yatsen, M., & Sotnichek, M. (2021, February 4). *Blockchain for Cybersecurity: Pros and Cons, Trending Use Cases*. https://www.apriorit.com/dev-blog/462-blockchain-cybersecurity-pros-cons

Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where is current research on blockchain technology? A systematic review. *PLoS One*, *11*(10), e0163477. doi:10.1371/journal.pone.0163477 PMID:27695049

Zhuang, P., Zamir, T., & Liang, H. (2020). Blockchain for cybersecurity in smart grid: A comprehensive survey. *IEEE Transactions on Industrial Informatics*, *17*(1), 3–19. doi:10.1109/TII.2020.2998479