International Journal of Scientific Research in Science and Technology
Available online at : www.ijsrst.com
OPEN ACCESS
Print ISSN: 2395-6011 | Online ISSN: 2395-602X
doi : https://doi.org/10.32628/IJSRST524111100

Study of Web Security Using Blockchain Technology and Its Application in Education

Satyam Anand
Department of Computer Science Engineering, Dayanand Sagar University, Bangalore, India

ARTICLEINFO

Article History:
Accepted: 05 Feb 2024
Published: 24 Feb 2024

Publication Issue :
Volume 11, Issue 1
January-February-2024

Page Number :
590-597

ABSTRACT

Present paper discussed about Blockchain Technology and its application in Education. Cybersecurity offers protection from cyberattacks for protected data on internet-connected devices as well as for hardware and software. A set of regulations, guidelines, and laws that apply to hardware, software, programmers, and secure information provide defense against dangers from without, such as destruction, theft, manipulation, and unauthorized access [1]. The words "cyber" and "security" are combined to form the compound word "cybersecurity." The network of protected devices, services, networks, and data is referred to as "cyber". On the other hand, security is concerned with safeguarding data, networks, applications, and systems. The application of blockchain technology to improve data security, dependability, and device security has increased significantly in a number of industries in recent years [3]. A number of cryptographically chain blocks can be eagerly decoded from the blockchain technology.

Keywords : Blockchain, Cybersecurity, IoT.

I. INTRODUCTION

Timestamp, version, merkle tree, difficulty target, nonce, and prior hashing are the six elements that make up the data structure header. In addition to providing a specific dependence order between blocks, this guarantees the blockchain's overall integrity. The hashing will change if even minor data changes occur in any of the blocks. Since the hashing of the related blocks will no longer be acceptable as a result of this, the transactions on the blockchain will become unchallengeable [5]. This architecture not only offers cybersecurity solutions in complex domains like networks, data storage, IoT, machine learning, transmission, and transaction, but it may also be very useful. Blockchain is a cutting-edge technology that is expected to transform computing in the future and provide more creative solutions in a number of industries. Since it is distributed, immutable, and open, it can be used usefully in a variety of settings. Although the technology has many uses outside of finance, the rise of cryptocurrencies gave it a huge boost in popularity. A loose translation of the term "blockchain" is multiple cryptographically chained blocks [1]. A block in a data structure is made up of three things: the data, the hash of the block that came before it, and the combination of the data and the preceding hash [2]. As a result, it is possible to exploit the order of reliance between blocks to guarantee the integrity of the entire Blockchain [3]. Any time the contents in a block changes, the block's hash will also change. The hashes of the succeeding blocks will become invalid as a result of the spiral effect that will result from this. Because of this, blockchain transactions are unchangeable [4]. It can be very beneficial to provide cybersecurity solutions in complex domains like IoT devices, networks, and data transmission across this infrastructure.

II. Blockchain Technology

Blockchain, also known as distributed ledger technology (dlt), ensures that every digital asset's past is both transparent and irreversible through the use of cryptographic hashing and decentralization. A Google Doc can be used as an easy analogy to explain blockchain innovation. When we produce a report and give it to a group of individuals, we distribute it rather than copy it or move it precisely. This establishes a decentralized network of distribution that gives everyone instant access to the report. The steady recording of all modifications to the document makes changes incredibly simple, so nobody has to depart in expectation of updates from another meeting [6].

Blockchain technology and other distributed ledger technologies (DLTs) have demonstrated to exhibit a number of properties, including decentralization, replication, transparency, timestamping, immutability, digital signatures, automation, and smart contracts. Recent developments have made it possible for parties who are distantly located or who have little to no trust in one another to with few to no centralized intermediaries, communicate and exchange value and information on a totally dispersed basis, enabling not only straightforward network transactions but also complex computation. Numerous widely popular applications utilize the cloud. Consumers should take control of their online presence by employing these built-in building blocks, in addition to the widely used apps in the banking sector, new advancements in internet applications have enabled in the fields of healthcare, social media, and other digital services. Collaboration between Zhejiang University Press and Elsevier produced Blockchain: Research and Applications. This journal aims to establish itself as a premier venue for corporate innovators, academic researchers, and practitioners to collaborate in order to accept, advance, and improve blockchain technology and its applications. We think it will help the global community and improve blockchain technology[7].

III. Challenges to the acceptance of Blockchain Technology

Nowadays we all are living in a fast-changing, highly technological era, where online / live is the essential and common habit of the consumer of normal society too. However, everything had to be built up from nothing at all. In this section, we explored traditional security mechanisms through web-based security using blockchain technology systems, challenges, and technological improvisations.

3.1 Technological Challenges

Blockchain technology (BT) is a decentralised system that manages transactions and data in a way that guarantees data integrity, secrecy, and privacy without subjecting the transactions to the control of outside parties. Blockchain technology (BT) has the ability to manage equity by employing electronic invoice ledgers for online transactions [1]. Supply chain, gaming, gambling, manufacturing, trading, and e-commerce are some industries that are utilizing blockchain technology (BT) [2]. The BT system is an immutable database that contains a digital ledger of every past transaction. Additionally, every node (user) on the distributed blockchain network has access to and control over the shared ledger [3]. Blocks are stacked when they are organized in chains, with the bottom block acting as the stack's base [4]. In the chain, each brick is connected to the one before it. Each block is identifiable by a produced hash created using cryptographic hash methods. Despite the possibility of just one parent block, a block in the chain may include a large number of child blocks [6]. A block has a header that links it to its parent blocks in a chain and consists of a unique hash of those parent blocks [7]. The initial block is called a genesis block and in 2009, the initial Bitcoin block was generated. The blockchain technology (BT) system is a decentralized database that functions as a digital record of ownership and maintains an expanding list of transaction records, in contrast to traditional centralized database systems [8]. The early age file system and live access mechanism were the simplest architecture, as shown in figure 1. The file system was not that efficient for data storage, processing, and retrieval. File Systems require procedures to be written by users for managing the records, even from the security point of view there was no crashing mechanism, on a crash system will certainly lose data.

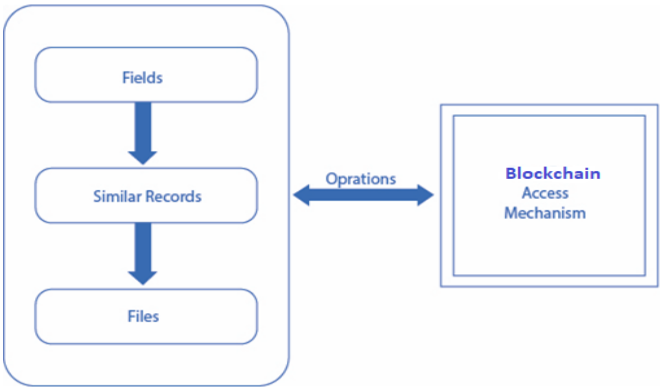

Figure 1. File System Based Live / Blockchain Mechanism

3.2 Legal Challenges in the acceptance in India

Even though blockchain technology is incredibly promising and brilliant, India still has some issues with it. The first and most significant issue is the lack of a clear legislation for blockchain technology from the Indian government. The adoption of technology would increase after the rules are established.The RBI and tax authorities do not promote cryptocurrencies because of worries about tax fraud and a lack of regulatory monitoring of digital currencies, which is the third problem. Due to the same, blockchain technology-based projects are reluctant to move forward. Additionally, a lack of knowledge and a general mistrust of technology prevent many supply chain providers from implementing the technology. India is eager to adopt blockchain, despite the fact that it is only now beginning to gain traction. Despite all of these unique difficulties, widespread adoption of this technology across industries will show to be a game-changer. The future of this next-generation technology in India will be shaped by policies, as well as by the efforts of the government and various sectors.Blockchain-based cryptocurrency has been outlawed in many nations, including China and India. Due to several worries and problems associated with it, individuals were first hesitant to employ blockchain technology in Indian marketplaces, which led to a gradual increase in its importance. Users in the Indian markets were unaware of the potential of blockchain technology. The government initially decided to forbid all activities connected with it from taking place in the Indian markets due to its low credibility and high danger [5].

But in 2018, the Supreme Court overturned the Reserve Bank of India's (RBI) prohibition on cryptocurrencies by ruling in favor of blockchain technology. The decision was made following the filing of numerous petitions in the Supreme Court in 2018 contesting the RBI's decision. Additionally, the court noted that this technology can be used in India in accordance with the appropriate laws and regulations with the creation of a framework by the government.

Blockchain is a key technology on the market, and many parties are exploiting it to their advantage in the commercial enterprises. But some of its most important characteristics come with legal, regulatory, and technological problems. It is made out of network data that has been recorded in "blocks" and concatenated in a specific way; the data cannot be changed or altered in any way. The development of data that enables a decentralised network on blockchain technology, which can confront new risks and challenges in the modern era, is a goal of many organizations and stakeholders. As a result, the vast majority of nations have laws and regulations that represent a centralized system of governance and organizations that offer responsibility and control. By departing from existing framework of governance, blockchain technology law may face new obstacles and problems. In the monolithic design of blockchain diagram shown below in figure 2 that shows data flow through the file organization system in different stages through different blocks and reflect internal cryptographically process using hash function for output.

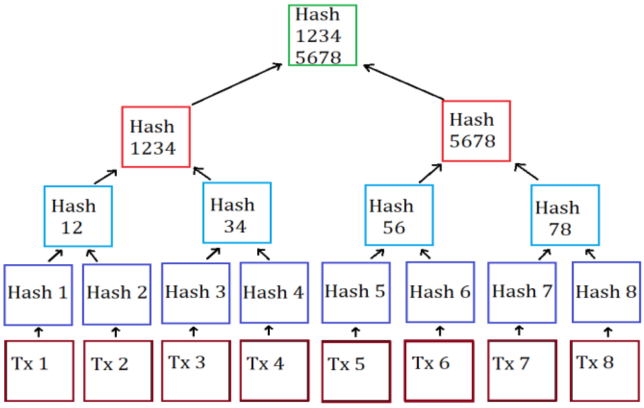

Figure 2. : Monolithic Design of Blockchain Diagram

Every block in the chain confirms the validity of all earlier blocks and transactions. If a valid additional block does not satisfy these requirements, the network as a whole will reject it. In distributed systems, blockchain is employed. There is a chance that the system's various participants will disagree. There isn't a reliable adjudicator to judge who is correct. Any blockchain must find a way to address the problems, as shown in figure 3 below.

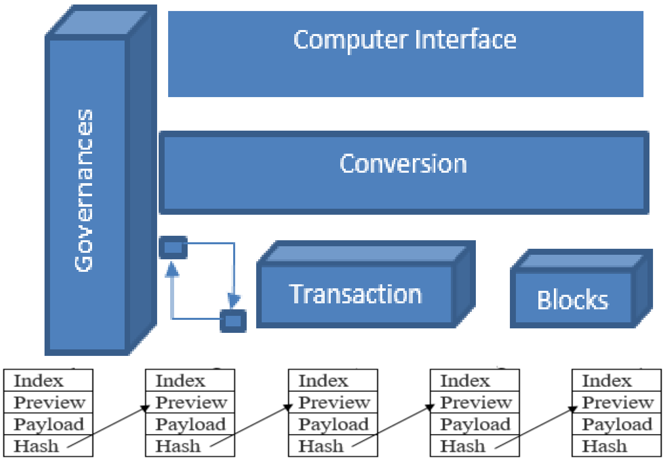

Figure 3 : A set of records that are linked together, with each record containing the previous record's hash value

The way incentives are aligned in the design of bitcoin is truly brilliant. The miners who run the system are dishonest and self-centred. They have strong incentives to abide with the rules. They also have an interest to prevent any attack that might jeopardize their investment because they have significant capital invested in bitcoin. The fact that Bitcoin is mostly used for money transfers makes it simple to incorporate payoff into the protocol, which is why everything works. Alternatives to incentives that aren't immediately apparent must be found for other blockchains, especially permissioned ones, in order to incorporate a playout into a protocol for storing medical records.

The retargeting method and chain measurement cast doubt on the viability of a long-range attack in the way previously mentioned. Despite being difficult across the entire multi branch ecosystem, there is still a chance that a multi branch account may launch a close-range attack [19].

Hash-based proof of work
I give you a challenge C and limit L = 2220.
Ask you to find N such that
SHA256(C||N) <L
Expected work = 236
Each New N has prob 2-36 of success
When you succeed, only take me one hash to check.

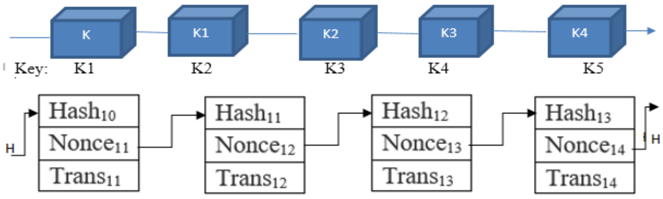

Figure 4: The first block's nonce is chosen to ensure that the second block's hash value as can be seen in the first block, is smaller than L.

3.3 Evolution and Need of the Web Security in Blockchain

The network and internet (network of networks, the early 1980s) were the first-ever causes behind the web-based storage mechanism evolution. All above databases except Client / Server were initially standalone storage and accessed databases. The client / Server model first-ever forced things to put storage on a remote/central server publicly. The Study of Web Security using Blockchain Technology (SWSUBT) access interfaces were also getting improvements after the evolution of the internet and was necessary too, to remote usage of the databases. The applications/interfaces also needed to have the user usage orientation to make them more adaptable and securable transaction data. In this section, we explored web-based data security through blockchain technology.

Web-Based Study in Blockchain Technology

The essential part of web-applications / services is the web-based databases to store, process and retrieve the data behind. Web-based programmes and services, such as e-commerce, emailing, message boards, business websites, sports and news portals, etc., frequently employ a blockchain that is accessible via the internet. You must create a blockchain application in order to create a contemporary website. In banking transaction, IoT devices, transport service health care services many more are used for housed amount of data for transaction that is not fully secured, they are partially secured. The blockcahin technology provide secured transaction data in the app and web application.

Requirement of Web Integration

Technological improvement without web-support is unimaginable, in this fast and exponentially grown technological era, everyone looking to control things/systems/consumables from remote without much human/manual intervention. After Google's publication on distributed file systems, GFS, and NFS, the storage method [2006]. Making storage ubiquitous/transparent/fault-tolerant become research trend among vendors, there are many organizations that are providing the opportunities for database connectivity solutions over the web. Many of them are working for more advance technologies to work upon to preventing them by being stuck on one single technology only.

IV. The Problem Statement with Blockchain Technology

Advanced web Security using Blockchain Technology (SWSUBT) as the name of the technology might lead you to believe, Blockchain is simply a network of blocks—at least conceptually. Here, "blocks" refer to digital data that are connected to other blocks via a cryptographic hash of the preceding block. The majority of its applications are in this space because of its distinctive structure, which makes it extremely safe and resistant to any type of data tampering. You must first and foremost keep in mind that there is no centralized authority in charge of blockchain. As a result, the system is entirely democratic. Additionally, the immutability of the information makes it simple to distribute and make public, enabling extraordinary amounts of openness. Because of these two aspects, blockchain is essentially the biggest development since the creation of the internet. Although cryptocurrency exchanges have historically used the blockchain, its applications in other fields are growing [12]. The issue is that non-cryptocurrency programmed frequently use untested, highly experimental software, which makes it possible for hackers to uncover and exploit weaknesses.

An append-only data structure is the foundation for systems based on Blockchain Technology (BT), and it stores each network transaction. As a result of a network's individual blocks maintaining a reference to the previous version (hash), the genesis block is referenced in a chain of blocks. When any time a fresh block is inserted into the network chain, all subsequent blocks must be mined because of the parent-child relationship between the blocks. Once a block has been on the chain for a while, it is methodologically difficult to reverse it later. A blockchain is produced by decentralized nodes cooperating in a PoW consensus architecture and exchanging information over a network. Interestingly, since a transaction can be completed without the approval of a trustworthy third party, this gives a state akin to an unidentified network. The distributed maintenance approach of the blockchain results in a system with complete transparency. In this scenario, every processed transaction is verified before being added to the blockchain and is kept transparent within the system. This may significantly limit users' capacity to "double spend" on their particular digital resources. A strong hashing power attacker might still insert erroneous transactions within a block, nevertheless. As the attacker would be in complete control of the network in this scenario, he or she might restrict service to particular users. This type of assault, known as a 51 percent attack by network security professionals, can make a blockchain exceedingly vulnerable. As a result, when a mining pool holds 50% share of the hash rate, a PoW consensus architecture is susceptible to 51% assaults.

After Bitcoin's launch, PoW quickly rose to prominence as the most widely used architecture for cryptographic assembly (peer-to-peer system) authentication. Nonetheless, it has flaws, especially in terms of how challenging and intricate mining is and how much energy it uses. It has been suggested to use a proof-of-stake (PoS) architecture as a replacement for proof-of-work (PoW) that depends on the financial investment a certifier makes in the network [17]. In the BT system, a proof-of-stake (PoS) mining algorithm replaces a different depending on a user's perspective ownership or stake in a digital money. A user purchases mining hardware under a PoW architecture and receives a mining incentive for confirming transactions. Users that acquire as a stake in the blockchain, cryptocurrencies network equivalent to their investment can take part in the block construction as certifiers utilizing the PoS design. When constructing blocks, the PoS architecture chooses certifiers at random. Therefore, no certifier can anticipate when it will turn [18]. However, PoS have a significant flaw known as nothing-at-stake [19]. The best course of action for any miner in the event of a fork is to mine on each chain, guaranteeing that he or she will be rewarded regardless of which fork prevails, whether the fork was unintentional or a consequence of an intentional attempt to alter the chain's history and reverse a transaction. If it is anticipated that there will be a many who are economically motivated using miners as intermediaries, an attacker might be able to submit a transaction for specific digital goods and receive them. Instead of starting the blockchain transaction from the previous block, the fork will transmit the money. The attacker's fork would triumph even with 1% of the total stake each node engages in mining on both. Ethereum tried to use the PoS approach to circumvent the PoW security restrictions, reduce the possibility of centralization and boost energy effectiveness [20]. As a result, while the PoW architecture has numerous potential security vulnerabilities, PoS enables a consensus to be built on the network [21]. The operational tenets of a double-spending attack are as follows: after adding TrA to a memory pool, other entered transactions involving TrA will be rejected. All other attacks will be rendered ineffective because TrA will always be validated as the first block added to the chain [15]. The aforementioned justification and Figure 5 illustrates the twofold expenditure attack's basic idea.

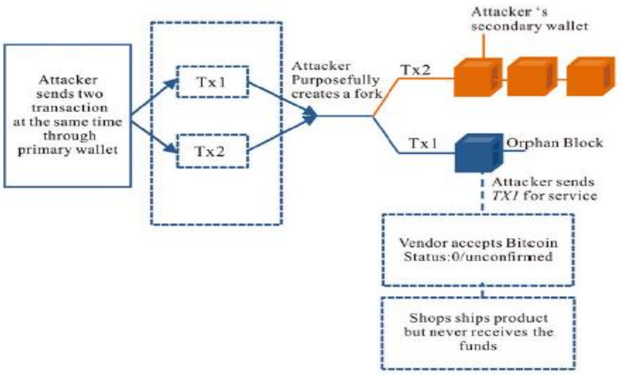
Attacker sends two transaction at the same time through primary wallet
Tx1
Tx2
Attacker Purposefully creates a fork
Attacker 's secondary wallet
Tx2
Tx1
Orphan Block
Attacker sends TX1 for service
Vendor accepts Bitcoin Status:0/unconfirmed
Shops ships product but never receives the funds

Figure 5: Working process of double - spending attack.

V. Blockchain in Education

Every educational institution is required to maintain records of student test scores, teacher demographic data, and certifications and diplomas granted to students. It need the participation of many stakeholders to monitor all of these elements. Blockchain is recognized as the best solution for reliably and adaptable record-keeping [11], [12]. In many nations, improving the teaching and learning processes presents numerous difficulties. By maintaining data in an effective and accurate manner, blockchain can aid in managing these difficulties. Furthermore, neither geography nor time can impede learning. In partnership with British Telecommunications, the Knowledge Media Institute of the Open University in the United Kingdom has launched a blockchain-based project called Open Blockchain [13]. When used in educational institutions, blockchain offers several advantages:

Information about students and/or departments that is safe and secure.

You can define access restrictions effectively.

The consistency of the data is maintained.

All users build trust with one another.

Prices are decreased.

Identity verification is possible for both students and resource owners.

It is quick and easy to evaluate student performance.

6. Conclusions

There is no imagination of world without internet and the applications based on the same. Web-based applications are the only driving forces that making us to think about future smart. Keeping data persistent, processing relevant towards information, secure and available for on-demand real-time access is the main data-computing phenomena. Designing next generation applications with aim of low cost, efficiency and true sense ubiquitous usage is the demand of current time.

Blockchain is a cutting-edge technology that is expected to transform computing in the future and provide more creative solutions in a number of industries. Since it is distributed, immutable, and open, it can be used usefully in a variety of settings. Although the technology has many uses outside of finance, the rise of cryptocurrencies gave it a huge boost in popularity. A loose translation of the term "blockchain" is multiple cryptographically chained blocks. Blockchain technology and other distributed ledger technologies (DLTs) have demonstrated to exhibit a number of properties, including decentralization, replication, transparency, timestamping, immutability, digital signatures, automation, and smart contracts. Recent developments have made it possible for parties who are distantly located or who have little to no trust in one another to with few to no centralized intermediaries, communicate and exchange value and information on a totally dispersed basis, enabling not only straightforward network transactions but also complex computation. Numerous widely popular applications utilize the cloud. Consumers should take control of their online presence by employing these built-in building blocks, in addition to the widely used apps in the banking sector, new advancements in internet applications have enabled in the fields of healthcare, social media, and other digital services.

VI. REFERENCES

[1]. Shah, P. K., Pandey, R. P., & Kumar, R. (2016, November). Vector quantization with codebook and index compression. In 2016 International Conference System Modeling & Advancement in Research Trends (SMART) (pp. 49-52). IEEE.

[2]. Kumar, P., Kumar, M., Singh, K. B., Tripathi, A. R., & Kumar, A. (2021, December). Blockchain Security Detection Condition Light Module. In 2021 10th International Conference on System Modeling & Advancement in Research Trends (SMART) (pp. 363-367). IEEE.

[3]. Asad, M., Kumar, M., Shah, P. K., & Sinha, A. K. (2021, December). Business Growth Forecast using Saket Data Mining Methodology. In 2021 10th International Conference on System Modeling & Advancement in Research Trends (SMART) (pp. 99-103). IEEE.

[4]. Pandey, R. P., & Shah, P. K. TRANSFERRING SECRET ELECTRONIC PAYMENT.

[5]. Received November 30, 2017, accepted January 21, 2018, date of publication January 30, 2018, date of current version March 15, 2018.

[6]. International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-9 Issue-1, October 2019.

[7]. www.javatpoint.com/cyber-security-introduction, copyright 2011-2018. All rights reserved. Developed by JavaTpoint.

[8]. Iansiti, Marco, and Karim R. Lakhani. "The truth about blockchain." Harvard Business Review 95.1 (2017): pp. 118-127.

[9]. Crosby, Michael, et al. "Blockchain technology: Beyond bitcoin." Applied Innovation 2.6-10 (2016): pp. 71.

[10]. Cachin C. Architecture of the hyperledger blockchain fabric. InWorkshop on distributed cryptocurrencies and consensus ledgers 2016, 310(1), pp. 4.

[11]. Li, Wenting, et al. "Securing proof-of-stake blockchain protocols." Data Privacy Management, Cryptocurrencies and Blockchain Technology. Springer, Cham, 2017, 8(1), 297-315.

[12]. Nabil El Ioini and Claus Pahl. A review of distributed ledger technologies. In Herve Panetto, Christophe Debruyne, Henderik A. Proper, Claudio Agostino Ardagna, Dumitru Roman, and Robert Meersman, editors, On the Move to Meaningful Internet Systems. OTM 2018 Conferences, pages 277{288. Springer International Publishing, 2018.

[13]. S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system, 2009.

[14]. Gao Y, Nobuhara H. A proof of stake sharding protocol for scalable blockchains. Proceedings of the Asia-Pacific Advanced Network. 2017; 44:13-6.

[15]. Digital Communications and Networks 6 (2020) 147–156, Paul J. Taylor, Tooska Dargahi , Ali Dehghantanha , Reza M. Parizi , Kim-Kwang Raymond Choo.

[16]. Authors: Eric Piscini (Deloitte U.S.), David Dalton (Deloitte Ireland) and Lory Kehoe (Deloitte Ireland).

[17]. Institute for Information & Communications Technology Promotion (IITP), Grant/Award Number: 2018-0-00539-001.

[18]. Yeoh P. Regulatory issues in blockchain technology. Journal of Financial Regulation and Compliance. 2017, 25(2), pp. 196-208.

[19]. Internet of Things Volume 11, September 2020, 100227.

Cite this article as :

Satyam Anand, " Study of Web Security Using Blockchain Technology and Its Application in Education ", International Journal of Scientific Research in Science and Technology(IJSRST), Print ISSN : 2395-6011, Online ISSN : 2395-602X, Volume 11, Issue 1, pp.590-597, January-February-2024. Available at doi : https://doi.org/10.32628/IJSRST524111100

Journal URL : https://ijsrst.com/IJSRST524111100