STUDY OF BLOCKCHAIN TECHNOLOGY AND DATA COMPRESSION TECHNIQUE

[1]BRIJENDRA KUMAR, [2]DR. AMIT KUMAR, [3]DR. TAPAN BHATTACHARYA
[1]Research Scholar, [2]Professor & Head, [3]Principal & PGT
[123]Department of Mathematics
[12]B. R. A. Bihar University, Muzaffarpur-842001, [3]DAV Public School, Chatro, Giridih, Jharkkhand

***Abstract*—In this paper, we focus our attention on the study of Blockchain technology and data compression techniques. 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].**

***Index Terms*—Blockchain, Cybersecurity, Compression techniques.**

I. Introduction

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 safe guarding 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. 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 for financial transactions.

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.

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. I anticipate your continuous involvement in this project whether it be as a writer, critic, reader, or in any other capacity.

The usage of Blockchain Technology (BT) in the November 2008-launched cryptocurrency Bitcoin is largely to blame for the rise in concentration in Blockchain Technology (BT). A distributed peer-to-peer digital currency is called Bitcoin that maintains a public log of all digital transactions. It keeps track of all shared transactions between parties and verifies them with the agreement of users of the shared system. A digital event's recorded data cannot be changed once it has been saved. As a result, every occurrence is continuously and verifiably recorded in Bitcoin. In the market for digital currencies, Bitcoin is very contentious in terms of security. The application of Blockchain Technology (BT) in both the financial and non-financial sectors has expanded, nevertheless. A blockchain gives organizations a safe platform for keeping historical records of digital activity and establishes a distributed consensus in the digital world by producing an immutable record on a public ledger.

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].

A blockchain is a list of documents, or blocks, that are linked together and encrypted using cryptography. Since a blockchain records every transaction made by an individual, we can all agree on the system's present

status. Using a platform for decentralized computing and information sharing, various authoritative domains that do not trust one another can coordinate and work together to make reasonable decisions. A blockchain is a collection of hash chain records, where once you see record N, there is no going back. A process for selecting the best possible candidate blockchain. There is a way for Alice and Bob to eventually agree on who wrote history when they have differing perspectives on it.

Even the live meaning here is only the information access mechanism. The file system in web based security mechanism through blockchain technology was following the storage rule like- the file was the collection of similar records; a record was the collection of fields. The live processing and registration mechanism was also completely dependent, and in the early phase of system design and refinement, the major thing was the repetitive relations that were dependent on the storage, processing, and access mechanism. Data and information security was also the new dimension for continuous system evaluation. The early age file system and live access mechanism were the simplest architecture, as shown in figure 1.

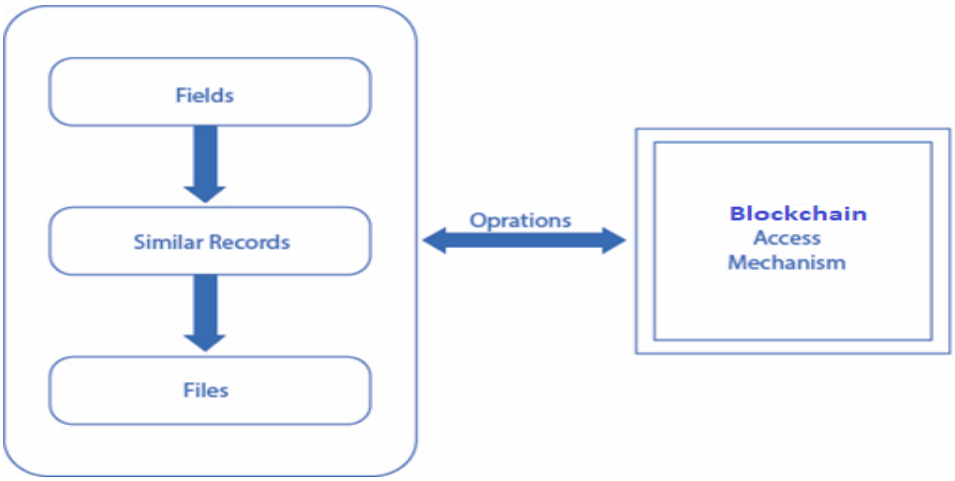


Figure 1. File System Based Live / Blockchain Mechanism

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.

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.

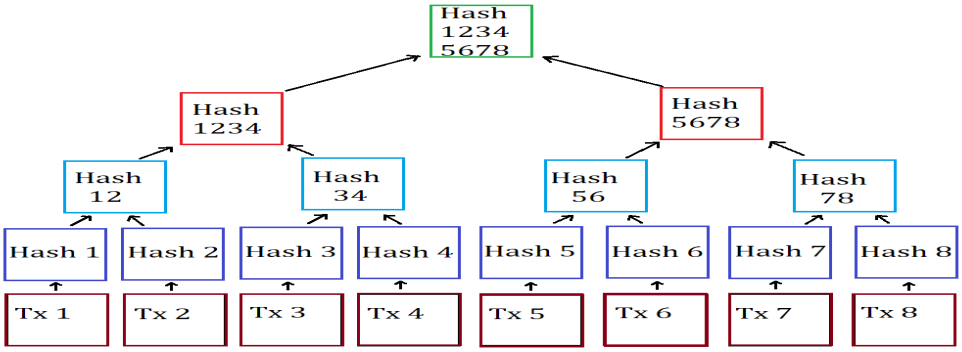


Figure 2: Monolithic Design of Blockchain Diagram

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.

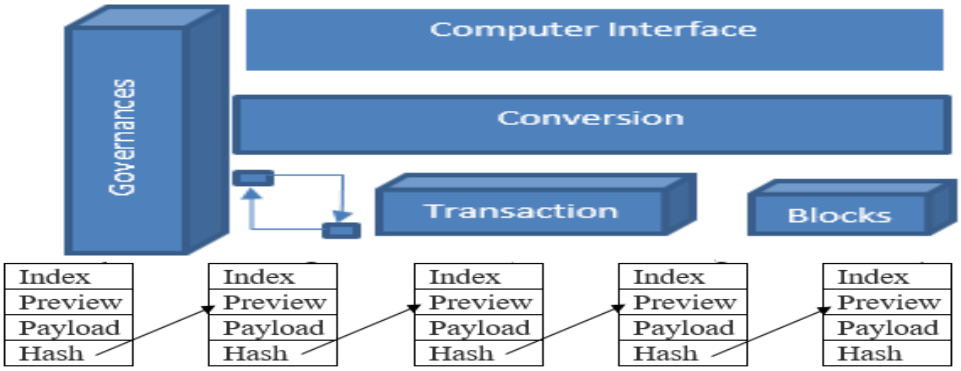


Figure 3: A set of records that are linked together, with each record containing the previous record's hash value

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.

If we have a group of reasonably trusted entities that can cooperate to add records to the blockchain, an alternate proof-of-work could be used. For instance, if three of the five trustees enough people vote to approve it, a block will be added to the chain. 3/5 signatures are required for a block to be validly added. There should not be any branched chains since that would require someone to cast a vote for two rival blocks, and the resolution for conflicting chains is to find the longest chain with 3/5.

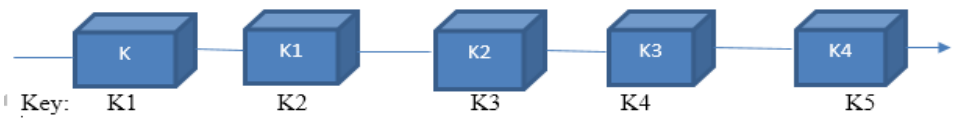
Any blockchain system must decide who is allowed to add additional blocks to the chain and how it should be done. There are four main ideas are Proof-of-work(POW), Permission blockchain(PB), Proof-of-stack(POS) and Proof-of-storage(POS). In below figure 4 shows that each blocks contains the value of previous blocks. The hash value contains previous value hash, Nonce contains previous value of nonce and transaction contains previous value of transaction, so that each block contains information of previous block like chain system. In blockchain Proof-of-Work (POW) change making before block has to be validated. It takes at least 10 minutes to add the block in blockchain. The blockchain will be store in multiple machines.

Every block's PoW ensures that a certain amount of difficulty is required to create it, and the PoS is based on the idea that only those with assets in the system are permitted to take part in the consensus process that expands the blockchain.

The majority of present stakeholders stay truthful when a stake is moved since they can still bargain for former account keys without a current stake. This is a significant problem for PoS-based blockchains as dishonest shareholders can quickly build one using current accounts due to how simple it is to create a blockchain [12]. It is generally simpler to launch a nothing-at-stake attack against one by shareholders running numerous blockchains concurrently and taking use of the fact that a blockchain with a PoS model only requires a small amount of resources in terms of processing power to be built. Stakeholders have a motivation to behave responsibly in a stake through the longest chain because doing otherwise could result in losing the amount they invested. It ignores a number of issues, though. There is a 1% chance that a stakeholder will be a key component of an attack that fails without them. This means that only a small bribe—1 percent of the amount of each stakeholder's deposit—is needed to persuade each one of them to join an attack. The essential sharing bribe can therefore only be between 0.5 and 1 percent of the whole deposit. This presumption states that since everyone would have a 0% probability of becoming crucial, a scenario with a 0% likelihood of failure cannot be in a constant state of equilibrium. The PoS architecture is additionally weak to a long-distance attack, in which a culprit with 1% of the coins forges without referencing the most recently generated blocks on the main chain. After the genesis block, by producing only fresh blocks and the longest chain possible, the attacker attempts to fork the network is possible. Because many blocks in these situations are unlawful, a new user cannot determine which blockchain is the longest. One possible solution to this problem is to require a timestamp to be present in every block, in order to reject chains whose timestamps are too far in the future of their own timestamp, a user would need this capability. Because it happens infrequently and would eventually vanish, this is a short-range strike. In some circumstances, the attacker can wait until the generated blocks can be regarded as a local maximum before releasing and routinely executing the best chain. This causes the assault to proliferate locally before being duplicated. In a 500-step run, the attacker can still construct 28 to 30 pieces of blocks even with a stake of 30 percent. However, the likelihood of an attack is completely eliminated after 1000 steps. As a result, the attacker in the finest blockchain assault on the local level may be easily identified by the series of blocks they produced. 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 $L = 2^{220.}$
  - Ask you to find N such that

    $$SHA256(C||N) < L$$
  - Expected work = 2^{36}
  - Each New N has prob 2^{-36} of success
  - When you succeed, only take me one hash to check.



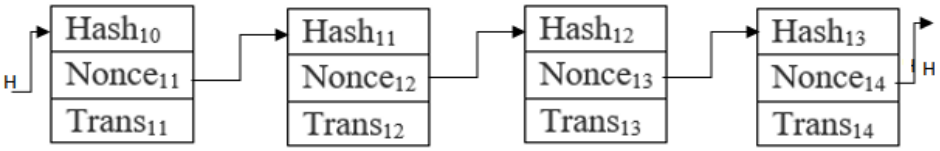


Figure 4: The first block's nonce is chosen to ensure that the second block's hash value as can be seen in the first block, is smaller than L.

IV. 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.

The necessity of having integration of a storage mechanism to the web is essential from various facet. Here are some of the lists of the most important requirements for database integration Web applications. These standards aren't totally attainable right now because they're standards. The standard requirements to have such applications are mentioned as follows-

- **Security:** Right to use valuable data in a secure manner that has been authenticated.
- **Flexibility:** By providing the flexibility in selecting the data for their current use as well as upcoming also.
- **Interface Independence:** web application independence from any Web Browser/ Server is one of the essential requirements while selecting proper application.
- **Versatile Features:** One more requirement while choosing any particular data. It must provide such kind of connectivity solution those benefits in all features of selected data.
- **Interoperability:** As it points to platform and device independence, web application's structure must be open-ended and must provide interoperability in comparison to be rigid. It must be able to run variety of Web servers.
- **Java/ RMI, XML Support:** Some advanced features and support for various technologies must be there in an effective web application.
- **Web Services:** It can perform similar with multiple web service types like SOAP, and UDDI etc.

- **Cost Effectiveness:** It should provide a cost effective way for maintenance, scalability, development for various applications.
- **Optimized Transactions:** It must provide an optimized transaction support with multiple integrated applications.
- **User Friendliness-**It must be user-friendly while working with it by allowing minimal overhead of administration.

The Website

Understanding the high-level organizational structure of the web and how it forces the governance and structural evolution of the various web-based applications that we will be exploring in the next chapter as part of a literature review and types of integration is necessary in order to comprehend the above-mentioned necessities and requirements of having integration of storage mechanisms with the web towards ubiquitous and versatile facilitation. If we talk about a simplest scenario, the web is everything while working with internet. Either we are requesting some resource from the server, or the server is responding to the corresponding request, all we do by filling some kind of forms, filling the data over that forms, entering some specific URLs in the address bar of the browser or by clicking some links. While working with any of the mentioned task, we deal with the web pages are generally used to display any of the content on the browser. Figure 5 shows how a blockchain communicates with a blocks to retrieve data and display to the specific users. This demonstrates the most common method, which is to repeat this process for every block in order to maintain the previous block.

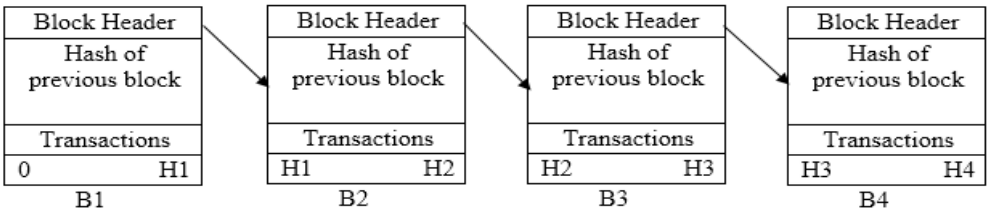


Figure 5: The performing this action for each block, the previous block is kept up to date

A web server is not sophisticated storage software when it comes to the data services (storage/processing/retrieval). A new method of separating the servers from the database servers was necessary because the data servicing, such as the above-mentioned services, complicated operations on data, performed by commercial websites and anyone else presenting lots of dynamic data, should be handled by a separate database mechanism. Repeating this will ensure that the previous block is retained operation for each bloc architecture is a classical model of web communication, there is a more advance version of this process was developed known as, Blockchain Detection Condition Model Process architecture. In which, eleven layers are being used for the overall communication process to detect the operation in blockchain technology. This leads to a complex architecture of communication model, figure 6 is showing the request generated the trusted protocol in Blockchain Technology.

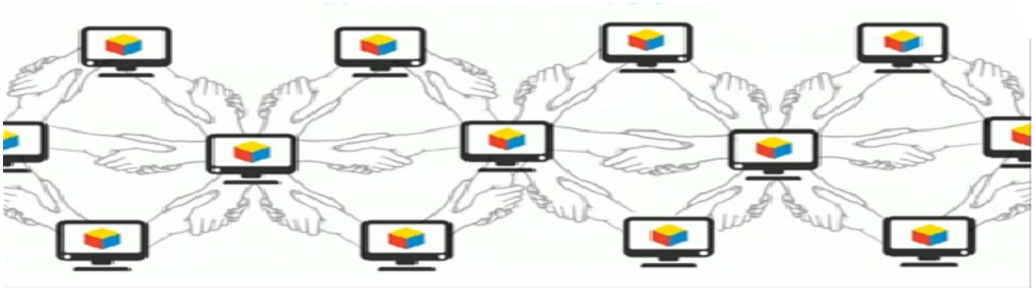


Figure 6: The trusted protocol in Blockchain Technology

Blockchain Detection Condition Model Process

In this modern era of the digital world calculating and the means of accomplishing it, that is software have developed a crucial component of daily systems on which millions of lives depend. The software offers

a safe environment where the system's performance, adaptability, and efficiency are the only things being tested [10]. But in modern times, security and safety are the main factors to be taken into account. When these crucial applications use software, the issue of security and safety becomes crucial since software failure has major consequences and could pose a grave risk to property and human life [14].

The blockchain technology provide at the time of message transfer, the blockchain technology gives both the sender and the receiver a hashing security key [11]. The communication key for the blockchain is used to hash messages in each block, and both parties can access the message. In terms of security, we need to create a process for identifying blockchain conditions that will provide a better and interactive security model for commercial web apps leveraging blockchain technology [12].

This kind of architecture is a conceptual form of any application model, the modern data intensive applications are having the same architectural phenomena for a better separation of the application logics to the storage mechanism. It organizes a structure of combining eleven logical or physical computing layers in an order. User interface is that deals with user actions and work as presentation layer, application layer that consists all the data processing activities and the data layer which contain all the data associated with particular application. Web based applications consist of different implementation versions to support with the Blockchain Detection Condition Model Process architecture. Most common architecture consists of the web server that works with scripting engine to process the scripts and produces the results of their execution and the blockchain process system. If the advanced hardware is used, this kind of application can manage multiple security requests in an hour. Figure 7 reflect that eleven components of blockchain technology that create a secure web security method through blockchain technology.

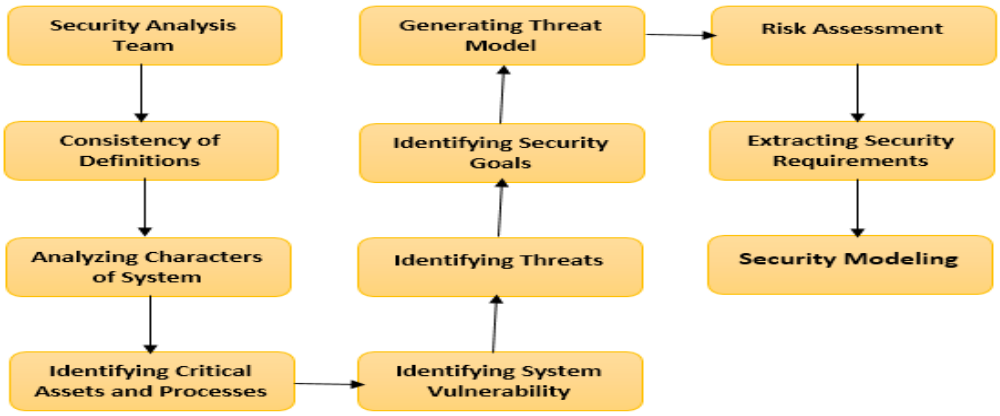


Figure 7: Blockchain Detection Condition Model Process

Implementing web applications with Blockchain Detection Condition Model Process architecture make the model more robust and fine-tuned in order to organizing the structures. We must investigate a crucial protocol that is being explained in the next one by one model in order to comprehend the use process: -

Team for Security Analysis

The properties of security analysis make it possible to evaluate the value of any product's securities as well as other instruments to determine a company's entire worth, which is important for investors when making decisions. The fundamental, technical, and quantitative analyses are the three techniques for determining the value of stocks.

Consistency of Definition

Consistency is defined as a state in which everything acts, breaks, or seems consistently. One way to explain consistency is the way a wall looks whenever paint is evenly applied from one side to the other. Blockchain technology offers the option to not decrypt messages that have been sent encrypted and then deleted by the sender. In some other situations, a third party or hackers may encrypt or decrypt data as it is being transferred.

Analyzing Characters of System

The process of acquiring information, comprehending it, detecting issues, and using advice to enhance the system is called system analysis. The system analyst's job is to examine the system's characters. System analysts' work involves examining the system's characters. The message is verifying by the sender through key components is related to that sender or not. Then message is transfer otherwise they save draught automatically through the sanded private key. This is analyzing by the system generating automatic process in blockchain technology.

Identifying Critical Assets and Processes

The blockchain provide that if data is transfer by the sender is encryption mode with there must be provided key component attached with them or not and the message is identifying in which component. This idea of recognizing significant assets and processes can be seen in the identification of Copyrights and patents, information on the company's finances, buyer income, human resources, branded tools, technical analysis, graphics, and internal manufacturing procedures.

Creating a Threat Model

Early on in the process of developing an application, you can identify security design issues by using a threat model. You may easily create a basic danger model for the results of your application using this technique. This threat model can then be used to support and enhance your apps, particularly in terms of design and team communication. For the purpose of evaluating application threats and vulnerabilities, a threat model is an organized activity.

Identifying Security Goals

Actions that are of high quality must be able to be stopped or detected by the system. As a form of security feature, security goals must concern confidentiality, integrity, or availability. The fundamental goal of security measures is to protect data from various threats while maintaining its security. In this module, we must identify the person who, although being prohibited from receiving data, yet makes an effort to gain it by abusing the system and employing a variety of tricks and methods to obtain accurate information.

Identifying Threats

The threat identification approach presents many viewpoints on the subject by utilizing the argument for damage, argument for entrance point, argument for risk, and argument for vulnerability. Organizations should begin by identifying the assets they need to safeguard, both material and intangible [2]. It's critical for businesses to comprehend the worth of their assets. The firm can then create a threat matrix for each asset to help identify dangers to each asset. A straightforward threat matrix will list the danger agent, the weakness the threat agent can exploit, and the threat that results from that vulnerability. The person who might take advantage of an asset's vulnerability, such as a hacker, a fire, a worker, or malware, is known as a threat agent. A system's vulnerability is a flaw that a threat agent could potentially use to their advantage [1]. The threat actor and the vulnerability work together to create the final threat [2].

Finding System Vulnerabilities

In order to measure and enhance programmed security by identifying system defects, security testing is intended to be a generally useful procedure. A flaw or weak spot in a computer system or network that can be used by an attacker to harm it or gain control of it in another way is known as a computer system vulnerability.

Risk Evaluation

Risk assessment identifies the overall method or approach for identifying threats and risk elements that have the potential to cause harm when identifying vulnerabilities. The risk connected to a vulnerability can be analyzed and evaluated using two different techniques: risk analysis and risk assessment.

Extracting Security Requirements

A serious privacy and confidentiality risk results from identifying the security standards that are the governing authority's security guidelines that are given the critical nature of these systems and the governing body's security regulations, which cover system behavior, user conduct, and emergency failures.

Security Model

At the time of message transfer, the blockchain technology gives both the sender and receiver a hashing security key. Each block on the blockchain has a communication key that allows both stockholders to view the communication that is provided. We need to create a process for identifying blockchain conditions in terms of security so that commercial web apps using blockchain technology can have an interactive and better security model. The blockchain provides the asymmetric key hashing algorithms of SHA256 bit for information security. In this have both have public and private key but the information is only one time encrypted. We are not decrypted the information, only system can do this work.

The most significant improvisation

According to the previously discussed developments in blockchain architecture and their influence on application modelling over time. The discussion itself depicting web security application modeling was the most impactful improvisation that forced/ applied various other required aspects to the application's building over the same. The main improvisation was security and privacy in real-time web based security applicative modeling that can be tossed like Confidentiality, Integrity, and Availability (CIA) [10].

V. CONCLUSION

Protection in the current and advanced blockchain modeling over Cloud-based environments can be measured in various aspects- User Authentications, Authentication of Authorized Applications and Access Control to Objects, Backup and Recovery Systems. The transactional modeling-based concurrency control that includes- timing limitations, integrity constraints, Authentication, Authorization, and Servicing, also needs to deal with security and privacy aspects. Web Security using Blockchain Technology(WSUBT), storage area networks, and distributed file systems for the real-time on-demand application building are the second face of most amazing improvisations that are much more efficient and be used for new paradigm modelling of the future online web-based applications.

References

[1] Shah, P. K., Pandey, R. P., & Kumar, R. (2016, Noveber). 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 Java point.
[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. In Workshop 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.