LGURJCSIT
Volume 06, Issue 04, Article ID 314, 6 pages
https://doi.org/10.54692/lgurjcsit.2022.06004314

A survey paper on blockchain and its implementation to reduce security risks in various domains

Ayesha Abubakar [1], Sidra Minhas [1]
[1]Forman Christian College, Lahore, Pakistan
Email: ayeshaabubakar412@gmail.com

(*Received 04 Aug 2022; Accepted 29 Sep 2022; Published 01 Oct 2022*)

Abstract— Every technology with its powerful uses has issues connected to it and security is at the top of it. As for the changing environment, the world has been shifting to Virtual Reality, the new coming world seems to be the internet and blockchain technology which is more powerful than others and has its applications in every field, be it quantum computing, internet of things, security or others. This survey paper covers the blockchain and its security in different fields of sciences and technology. We begin with the introduction of blockchain and then discuss its structure. After that security issues have been highlighted which include attacks and their behavior in quantum computing, internet of things, cloud computing. Furthermore, we have discussed the most common types of attacks and the SRM model of blockchain followed by the conclusion.

Keywords — Cryptocurrency, Blockchain, Sybil, Smart Contracts, Double Spending

1. INTRODUCTION

Blockchain technology is a database that carries information among the nodes of a computer network. It is a unique form of carrying data that is traceable, unalterable, distributed, decentralized, and has a time stamp. It is also commonly referred to as distributed ledger technology because it creates a chain of blocks one after the other, unlike other databases which have tables to carry data. This structure of blockchain presented itself as a viable, secure, and transparent mode of transactions excluding the need for a trusted third party, and resulted in the creation of cryptocurrency, decentralized finance (Defi) applications, and non-fungible tokens (NFTs) and smart contracts. Blockchain technology was invented in 1991 but its widespread application came into existence in 2009 with the creation of bitcoin – the best-known cryptocurrency. Bitcoin, the cryptocurrency, was created by some anonymous Japanese developers who in their research paper called it “A new electronic cash system that is fully peer to peer, with no third party involved” (Bhutta, 2021). The developer’s identity is still not known and has been given a pseudonym, Satoshi Nakamoto. All cryptographic forms of money are exchanged in the web-based digital currency platform. The cryptographic money market is like other trade markets like the securities, and stock exchange with different exchanging stages. Nonetheless, the digital money market is not controlled by an administration or office, and exchanging happens every minute of every day across the world. The idea of cryptocurrency permits exchanges to happen at speeds that cannot be achieved with government-issued money, like the United States dollar. These outcomes in a significantly more unpredictable market than other exchanging markets. Coin costs are persistentlyrising and dropping, and new digital forms of money reliably enter and leave the platform. Blockchain is the critical watchman in securing bitcoin exchanges from many known and hard security, protection, and trust issues (Zaghloul, 2020). For example, twofold spending, unapproved divulgence of private exchanges, dependence on a confided-in focal authority, and the dishonesty of decentralized registering. Over the past decade, the new technology cryptocurrency has been introduced in the world and has been doing wonders through it has applications changing the way our financial institutions work.

The study of the available literature by multiple researchers has been covered in this paper. In this short survey paper, first we describe the structure of a blockchain. Then, application of block chain in cloud computing using edge computing and cloud block chain hybrid technology is discussed. Next, security issues in different layers of Internet of things (IoT) and their solutions via block chain are detailed. Afterwards we discuss the application of block chain in quantum computing. In the end security risk model and common types of security attacks are mentioned.

2 Structure of blockchain

Zhang et al. (2020) presented the structure of blockchain and gives an overview of its architecture.

A block is the data structure of Blockchain which stores transaction records. As shown in the Figure1, it consists of two parts: Block Header and Block Body.

2.1 Block header

The block header contains the following fields:

1. Block Version: specifies the rules for block validation.
2. Merkle Tree Root Hash: it stores the hash value of all transactions in the block.
3. Time Stamp: stamps the current time in seconds according to universal time sinceJanuary1,1970.
4. nBits: threshold for a valid block hash.
5. Nonce: a mathematical value starts with 0 and increases with calculation of every hash.

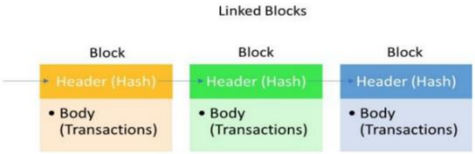


Figure 1: Structure of blockchain.

6. Parent Block Hash: points to the previous block.

2.2 Block body

The block body contains the transactions and transaction counter. The maximum capacity of block to store the transactions is determined by the block size and size of each transaction contained in it. In general, there are two types of nodes in the Blockchain network:

1) Full node
2) Lightweight node

To make any changes within blocks, a consensus is required between more than half of the users of the network. The Consensus is required to validate transactions and update the ledger. Also, Blockchain is very important in establishing a democratic, secure, and transparent fabric for many industries of the world. The consensus algorithm ensured the consistent operations of the Blockchain applications. Many cryptocurrencies are motivating Blockchain technology. Microsoft and Intel are also favoring the Blockchain. There are two challenges for the Blockchain in the future. First, is maintaining the privacy and security of the individual. This is because of Distributed Ledger Technology (DLT). Second, is addressing the security and privacy issues which were brought about by IoT. These issues include the right issues, lack of standards, legal challenges, regulatory issues, development issues, etc.

3. Implementations of Blockchain

Blockchain has its application in almost every field of sciences and technology. It has become an integral part of computing fields. Here we are going to discuss its application in Edge and Cloud computing, Internet of things, quantum computing. Internet is developing towards technology; this technology is an archetype. Archetype is grounded on smart systems. This technology relies on Artificial Intelligence, machine learning, a Blockchain platform, edge computing, and the Internet of Things.

3.1 Edge computing and blockchain, Cloud Computing (architecture not implementation)

The two major implementations of the blockchain rely on Edge Computing and Cloud Computing. Edge computing architecture naturally supports blockchain architecture which keeps processing units on edge devices. On the contrary, cloud computing architecture performs processing within clouds. Bhat et al. (2020) presents the security threats in the edge computing model of blockchain and provides defense solutions to the problem. If edge computing, the Internet of things and blockchain emerges, it will result in the empowerment of new automatic services and commercial models. This automatic service and commercial models of blockchain have various properties such as self-verifying, self-executing, immutability, and data reliability. This provides advancement in the blockchain. Cloud computing is also used for the processing of data. Arranging the data computing capabilities near the edge of the computer is known as edge computing. Here, data is generated and actions are performed to enhance the response time and bandwidth utilization. There are seven edge computing paradigms

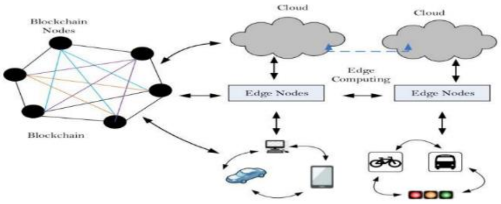


Figure 2: Cloud-blockchain hybrid architecture

These paradigms include programmability, the naming of edge devices, data abstraction, servicemanagement, Heterogeneous system integration, optimization matrices, and persistent qualityofservice and quality of experience. Blockchain, IoT, AI, and ML are very important in the constructionof a secure edge computing paradigm. The security and privacy issues faced due to edge computingcan be resolved by

Blockchain-based solutions. Cloud-blockchain hybrid architecture

A cloud-blockchain hybrid architecture, in which a maximum volume of IoT data is carried across the conventional IoT cloud-edge architecture, is one of the most recent ways for implementing block chains into IoT edge. The blockchain is a revolutionary technology at the application level. When public accountability is required, this method is used. The goal is to impact the low-latency data flow between the devices. Traditional cloud and edge architecture, as well as blockchains' immutable data storage capabilities, As a result, Bhat et al, (2020) proposed a hybrid cloud-blockchain architecture (Figure#2) that would reduce the need for all generated events to be stored in the blockchain. The architecture depicted in this diagram makes advantage of the blockchain's account ability features, but it does not impose service. The edge computing node and cloud server are connected at the same panel by an overlay network. In the communication layer, Blockchain converges with edge computing to preserve the privacy and security of IoT edge devices in radio spectrum management and ID management. In the network layer, it is used to protect security. To apply the solutions practically, convergence service is divided into different computing services. These services are distributed among the entire network. Cloud servers and data storage servers have high computing and storage abilities'. So, it stores the entire Blockchain and performs intensive tasks.

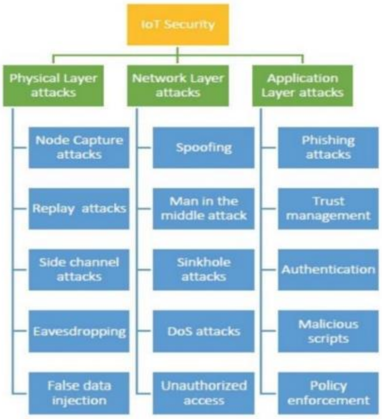


Figure 3: Types of attack

3.2. The Internet of Things

The Internet of Things (IoT) emerged a lot in the last decade. A lot of smart devices and associated technologies have been introduced from an industrial and research perspective. Many applications have been developed. These applications have been developed by IoT techniques. These smart things have low processing and storage capacity. This is the reason; smart things can be attacked. Existing security and cryptography techniques are not appropriate for this. Cyber Crimes on the internet are increasing day by day. Layers of IOT System

Bhutta et al, (2021) The IoT system contains three layers. These are the physical layer, network layer, and application layer. IoT is facing many privacy and security challenges. Blockchain, fog computing, and machine learning are used to resolve these issues. To get a connection these devices are connected with a wire or wirelessly. ZigBee, WIFI, or Bluetooth is used for connectivity purposes. The devices can be attacked in different ways. There are different attacks including the Node Capture attacks, Replay attacks, Side Channel attacks, Eavesdropping, False data injection, Spoofing, MITM attack, Sinkhole attacks, DoS attacks, unauthorized access, phishing attacks, trust management, Authentication, Malicious attack, and policy enforcement. Secondly, Blockchain technology provides some security solutions. Preservation Techniques

Preservation techniques should be made to keep the privacy of the users. Blockchain is used to overcome some of the security and privacy issues. Some consensus algorithms have been used by Blockchain technology. These consensus algorithms are Proof of Work, Proof of Burn, Proof of stake, Raft, and practical Byzantine Fault-tolerant, etc. " Bubble of Trust" is also proposed Bhutta et al,(2021) for the authentication of IoT devices. Many things are checked before using the Blockchain. These checks include centralized/ decentralized systems, whether nodes are trustworthy or not, and whether information can be shared with all participants or not. IoT techniques have been used for applying different applications. These applications involve the smart city, smart home and smart transportation. The invention of smart things that possess wireless connectivity, storage space, and processing power made use of these devices in real-time. However, there are some privacy and security issues faced by the IoT. Several devices are used to make an IoT smart environment. For testing purposes, some contracts are written on the Blockchain. Nodes are verified using the previous information that was stored on the Blockchain database. The purpose of smart contracts is broadcasting. This broadcasting on the network is done by using a digital signature and encryption. The function of nodes is doing verification and validation, as a result, a smart contract starts running on the Ethereum platform.

3.3 Quantum computing

Blockchain and other Distributed Ledger technologies were introduced in the last few years. These technologies are used for different applications when working with quantum computing. These technologies are important because they can provide transparency, redundancy, and accountability for the current state of the art on post-quantum cryptosystems and how they can be applied to blockchains and DLTs. The author Mohantana et al, (2021) provides the current state of the art on post-quantum crypto systems and how they can be applied to blockchains and DLTs. Quantum computing is progressing very fast, this fast progress makes it possible to perform attacks. These attacks are based on Grover's and Shor's algorithms. The risk of these attacks is very high soon. These algorithms are threatening the cryptography and hash functions. In such a situation, we need to design the Blockchain to make the cryptosystem stand against quantum attacks.

Blockchain is the technology that is created to provide secure communication and data privacy. The has the key to the Blockchain. A cryptosystem is designed to secure the data from quantum attacks. Also, Blockchain is used to secure the data that has been shared among persons who never trust each other. The piece of code which is stored on the Blockchain is known as a Smart Contract. A smart contract is used to automate the tasks. A lot of development has technologies such as quantum computing. As a result of these developments, researchers and developers started taking interest in DLTs like Blockchain. Here, public-key cryptography and hash functions are very important.

Post-quantum cryptosystem

Computing can attack the Blockchain and these attacks can be overcome by applying a post-quantum cryptosystem. Many post-quantum schemes have been introduced for this purpose. The applications of this post-quantum to Blockchain were also analyzed. In addition, their main challenges were also analyzed. Also, a lot of comparisons have been provided. These comparisons were on the performance and characteristics of the post-quantum public-key encryption and digital signature schemes. There are many cryptosystems which include codes-based cryptosystems, lattice-based cryptosystems, multivariate-based cryptosystems, hybrid schemes and hash-based digital signature cryptosystems.

Signature

We can enhance the security of the Blockchain by adding some features. These features include Aggregate signature and ring signature. Aggregate signatures allow the generation of unique signatures. This feature is very important in the Blockchain as it promotes faster verification and it reduces storage and bandwidth. On the other hand, the ring signature is used to specify the possible set of signatures. Ring signature does this without revealing who produced these signatures. Some developers suggest that we can secure ring signature by using a quantum-resistant lettuce-based scheme.

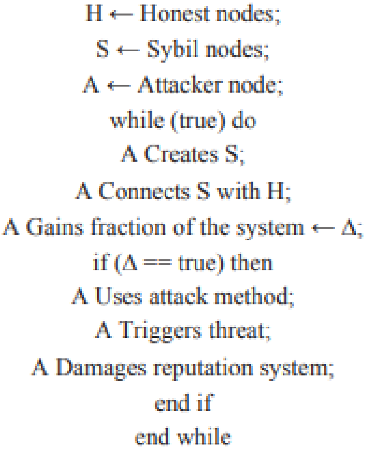
4. Security risk the (SRM) space model

A security risk in the (SRM) space model Yuet al, (2021) and foster a structure to investigate two security chances - Sybil and Double-spending - that are noticed and considered most concerning security risk inside blockchain frameworks. Concerning innovation, blockchain has demonstrated its legitimacy and solid arrangement of safety for facilities yet every new innovation has its upsides and down sides additionally there are dangers to the framework in every case regardless of areas of strength for how resistant the framework is. The turing complete language-based shrewd agreements in blockchain made an unmistakable commitment to the development of blockchain innovation. Shrewd agreements' definitive objectives are to wipe out confided-in go-betweens, less human mediation, decrease authorization costs and forestall deliberate or unexpected extortion and security gambles.

6.1 Sybil and Double-spending attacks

Sybil and Double-spending are the most unsettling security take a chance inside blockchain frameworks. The aggressor could take advantage of these security changes and influence the important resources and administrations of blockchain frameworks. Sybil assault is an organizational assault and notable with regards to P2P networks, where an assailant can produce or make various phony personalities to acquire an impressive effect on the network.

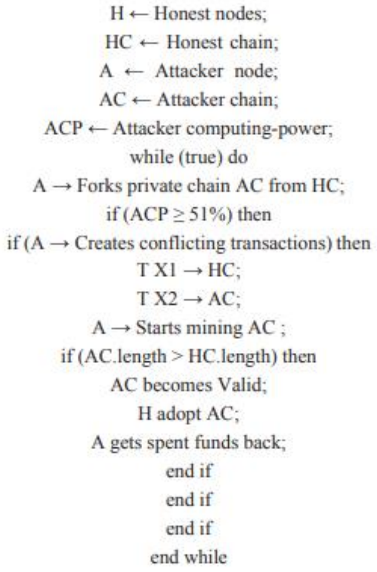
Algorithm 1: Sybil attack



```
H ← Honest nodes;
S ← Sybil nodes;
A ← Attacker node;
while (true) do
    A Creates S;
    A Connects S with H;
    A Gains fraction of the system ← Δ;
    if (Δ == true) then
        A Uses attack method;
        A Triggers threat;
        A Damages reputation system;
    end if
end while
```

Double-spending is an information consistency assault, and it happens while spending similar computerized cash (or computerized resource) two times. These days, different associations fabricate their redid blockchain frameworks to satisfy their particular requirements.

Algorithm 2: Double-spending by 51% attack



```
H ← Honest nodes;
HC ← Honest chain;
A ← Attacker node;
AC ← Attacker chain;
ACP ← Attacker computing-power;
while (true) do
    A → Forks private chain AC from HC;
    if (ACP ≥ 51%) then
        if (A → Creates conflicting transactions) then
            T X1 → HC;
            T X2 → AC;
            A → Starts mining AC ;
            if (AC.length > HC.length) then
                AC becomes Valid;
                H adopt AC;
                A gets spent funds back;
            end if
        end if
    end if
end while
```

Such frameworks are inclined to various security gambles, including Sybil and Double-spending chances. Douceur examined Yu, et al (2021) the Sybil assault on P2P frameworks. The P2Pframeworksdo not depend on a focal believed party chain of trust to check the character of every member hub, too moderately modest to create personalities on. Sybil assaults are difficult to forestall, in any case, there exist preventive measures to increment
assurance against Sybil assault. The creators present a standing-based plot 'GOLF' to distinguish Sybilhubs on BitTorrent DHT given designs in IP addresses. Numan et al. play out a literature survey and gather the cloned hub identification plans alongside their downsides and difficulties.

6.2 Safety Instruments

Moreover, the study classified three distinct instruments to safeguard P2P frameworks against Sybil
assaults:
(1) Trusted certificate (e.g., incorporated or appropriated certificate utilizing cryptographic natives),
(2) assets testing (e.g., IP testing, network facilitates, expecting clients to tackle puzzles), and
(3) informal community methods (e.g., Sybil Guard, Sybil Limit, Sybil Infer, vote collection, and Gate Keeper). Twofold spending is a gamble of computerized cash where the assailant can spend similar cash two times to acquire financial benefits. For example, the assailant changes the transaction state and spends a similar exchange two times. The hazard of Double-spending nullifies the trustworthiness of the record. A few dangers exist that can cause Double-spending, for model, Sybil-based Double-burning through, 51% assault, and so on. In segment III-B, these dangers are tended to exhaustively.

6.3 Comparative Analysis

Many applications of Blockchain have been discussed in this research paper. The applications discussed in this research paper include internet of things, quantum computing, SRM model of Blockchain and cloud computing but many this research paper missed many applications of Blockchain from which we are getting benefit in today’s world. These applications of Blockchain include money transfer, smart contracts, media, non-fungible tokens, logistics and government etc. Many security parameters and measures of Blockchain has been discussed in this research paper but it missed few of them. The safety instruments discussed in this paper include Trusted certificate, assets testing and informal community methods. In addition to these safety measures, another protection method is used in Blockchain and in this method every transaction is approved and network. The transactions are approved and verified on the Blockchain network using a proof of work consensus algorithm. Methods of Blockchain discussed in this research paper have various outcomes. Various outcomes of the cloud computing have been discussed in this research paper like it reduce security risks, process data etc. In addition to these outcomes, there are some more outlines of cloud computing like cloud computing provide a platform to the user through which user can trust each other. Cost of managing and maintaining IT system will also lowered by using Cloud Computing. If we discuss about the Internet of things, then many attacks on IoT and risks of IoT has been discussed in this paper but it missed the applications and benefits of Internet of Things. IoT is a smart home which use sensor in order to maintain lighting, resource management and security system. Industrial internet, Smart city, Farming and self-driving cars are the other applications of Internet of Things. If we discuss the outcomes of the quantum computing, then we can say that in this research paper only security threats of quantum computing have been discussed. In addition to threat to the security, quantum computing has many applications and benefits. Quantum Computing is very useful in data analytics. Quantum Computing can solve the problems at a large scale. Quantum Computing can solve the calculations seconds, these are the calculations for which supercomputers takes decades. Like Quantum Computing only risks of SRM are discussed in this research paper. SRM is very important because cost management can be improved by SRM. SRM cause reduction in the cost. In addition to managing cost, SRM is very important because it streamline operational efficiency, it increases your potential to outsource and it make the supplier relationships more stronger. Many advancements can be made in Blockchain like using it in the field of education. Also, the technology of Blockchain can be improved by dealing with security risks and threats. Experts need to take step in order to eradicate all the security risks. Software Engineers need make such kind of software through which no one can attack the network or no hacker can access your network. If all the security risks of the Blockchain can be removed than this technology can touch the heights of reputation and success.

Conclusions

Blockchain technology, with a wide range of applications in different aspects of life, is increasing its uses and helping the world change more securely and feasibly. This paper addresses the security and privacy issues present in our system. As Blockchain is the distributed network and security is maintained. In this study, Blockchain is integrated with quantum computing, IoT, and attacks on the system, their algorithms and behavior have been discussed. As the world is advancing new measures and solutions are being implemented to cope with such threats and attacks performed.

REFERENCE

[1] Bhat, S. (2020). Edge Computing and Its Convergence With Blockchain in 5GandBeyond: Security, Challenges, and Opportunities. IEEE Access, 8(1), 205340 - 205373. IEEE Access. 10.1109/ACCESS.2020.3037108. [2] Bhutta, N. (2021). A Survey on Blockchain Technology: Evolution, Architecture and Security. IEEE Access, 9(1), 61048 - 61073. IEEE Access. 10.1109/ACCESS.2021.3072849

[2] Choo, K. (2022). Blockchain Ecosystem—Technological and Management Opportunities and Challenges. IEEE TRANSACTIONS ON ENGINEERING MANAGEMENT, 69(3), 3. IEEE Access. 10.1109/TEM.2020.3003565. [3] Iqbal, M. (2021). Exploring Sybil and Double-Spending Risks in Blockchain Systems. IEEE Access, 9(1), 76153 - 76177. IEEE. 10.1109/ACCESS.2021.3081998

[5] Meng, T. (2021). On Consortium Blockchain Consistency: A Queueing Network Model Approach. IEEE Transactions on Parallel and Distributed Systems, 32(6), 1369 - 1382. IEEE Accesss. 10.1109/TPDS.2021.3049915

[6] Xu, L. D. (2021). Embedding Blockchain Technology Into IoT for Security: A Survey. Internet of Things Journal, 8(13), 10452 - 10473. IEEE Access. 10.1109/JIOT.2021.3060508

[7] Yu, X. (2021). BC-BLPM: A multi-level security access control model based on blockchaintechnology. China communications, 18(2), 110 - 135. IEEE Access. 10.23919/JCC.2021.02.008

[8] Zaghloul, E. (2020). Bitcoin and Blockchain: Security and Privacy. IEEE Internet of things Journal,7(10), 10288 - 10313. IEEE Access. 10.1109/JIOT.2020.3004273

[9] Zhang, R. (2020). Security and Privacy on Blockchain. ACM Computing Surveys, 52(3), 1-34. ACM Digital Library. https://doi.org/10.1145/3316481

A survey paper on blockchain and its implementation to reduce security risks in various domains Page[10] Mohantana, B. (2021). Addressing Security and Privacy Issues of IoT Using Blockchain