Journal of Posthumanism
2025
Volume: 5, No: 2, pp. 1557–1575
ISSN: 2634-3576 (Print) | ISSN 2634-3584 (Online)
posthumanism.co.uk

DOI: https://doi.org/10.63332/joph.v5i2.538

A Systematic Approach to Selecting the Right Blockchain for a Given Application

Shahnawaz Khan[1], Sultan Alamri[2], Abdullah Alourani[3], Ajlan Al-Ajlan[4], Mohammad Subhi Al-Batah[5], Philippe Pringuet[6]

Abstract

Blockchain and Industry 4.0 are two of the most transformative technologies in the present time. Integrating both technologies can be disruptive in many industries such as supply chain management, healthcare, data sharing, energy trading, and finance, etc. Since the invention of Bitcoin, the use of Blockchain for consensus-based transactions in multiple application areas has been growing exponentially. All the major technology giants have blockchain-based solutions, ready to be used in the public domain. However, applying blockchain technology in every distributed application is not well suited. Various blockchain-based solutions have been proposed in different application areas to address the challenges emphasizing their efficiency and security. But the question of the hour is whether Blockchain is really required to be used in all such cases. Can it really solve all the security-related issues that often occur in distributed systems? The answer may be both yes and no. Of course, blockchain technology helps to create information transparency as well as manage it well and provides a safeguard against fraudulent mutation, etc. This paper discusses the challenges applying blockchain technologies and issues related to blockchain technology itself. It also investigates the promises which blockchain-based applications make in supporting consensus-based as well as transparent transactions in spite of the inherent risks available in such application scenarios. Conclusively, it proposes a blockchain recommendation algorithm that takes the primary constraints of using blockchain and features of the application into account and recommends which type of blockchain should be applied in a particular use case. A case study for the algorithm-based recommendation along with human expert recommendation has also been discussed. Several application scenarios have been discussed and tested with algorithm for blockchain type recommendation.

Keywords: *blockchain; internet of things; artificial intelligence; algorithm; security; supply chain management.*

Introduction

The first major and successful application of Blockchain has been Bitcoin (Nakamoto, 2008). Though, in past, there have been several attempts by several researchers in developing something similar. For example, research (Haber & Stornetta, 2007) proposed a technique for securing the creation and last amendment information of the digital contents using a series of linked records protected by encryption. With the recent advancements in blockchain technology, the application

[1] Faculty of Engineering, Design and Information & Communications Technology, Bahrain Polytechnic, Bahrain; shahnawaz.khan@polytechnic.bh
[2] College of Computing and Informatics, Saudi Electronic University, Saudi Arabia; salamri@seu.edu.sa
[3] Department of Management Information Systems, College of Business and Economics, Qassim University, Buraydah 51452, Saudi Arabia; ab.alourani@qu.edu.sa
[4] Department of Management Information Systems, College of Business and Economics, Qassim University, Buraydah 51452, Saudi Arabia; aajlan@qu.edu.sa,
[5] Jadara University, Faculty of Information Technology, Department of Computer Science, Irbid, Jordan; albatah@jadara.edu.jo
[6] Faculty of Engineering, Design and Information & Communications Technology, Bahrain Polytechnic, Bahrain; philippe.pringuet@polytechnic.bh

of blockchain has reached beyond cryptocurrencies. The application of blockchain technology has been growing in almost every sector, such as industry 4.0, healthcare, the internet of things, logistics, supply chain, accounting, finance, banking, agriculture, education, and many more. Blockchain provides security, transparency, immutability (or data incorruptibility), decentralized storage (that is independency on cloud or centralized servers), failsafe transactions, and consensus for decision-making on the network. Thus, blockchain provides great security, trust, and efficiency. These features and benefits of the blockchain attract researchers and businesses to opt for blockchain for various solutions (Sharma et al., 2022). Blockchain is a shared digital record system that makes it possible to carry out transactions in a secure, clear, and unchangeable way (Kosba et al., 2022).

Industry 4.0 or fourth Industrial revolution is defined as the combination of smart technology, Internet of Things, artificial intelligence, big data, and automation into various traditional manufacturing, and other industrial practices. Industry 4.0 is changing how products are created, built, and brought to customers. It is a complex and ongoing evolving process (Bai et al., 2020). It is still in its infancy, but it has the potential to revolutionize the global industry. Industry 4.0 includes a broad spectrum of technologies such as cyber-physical systems, cognitive computing, cloud computing, advanced robotics, automated machines, smart algorithms, internet of things, massive data sets and analytics, etc. (Frank et al., 2019; Khan & Kannapiran, 2019) It introduces a new level of automation using smart modern technologies. The goal is to build intelligent factories that are more flexible, effective and responsive to the needs of the customers. Industry 4.0 does not only affect the manufacturing but also several other industries such as healthcare, transportation, and energy (Ghobakhloo, 2019). A research study by (Borowski, 2021) highlights the importance of innovative strategies, digitization, and Industry 4.0 technologies in the energy sector's efforts toward environmental sustainability and a low-carbon economy.

There have been several blockchain-based solutions proposed by several researchers to address the issues faced in different application areas. A research study (Tanwar et al., 2019) explores several solutions and suggests that blockchain technology-based solutions are more efficient and secure. However, there are several challenges as well. These issues might cause several other issues as well in the long term. Therefore, it is crucial for the businesses to understand the potential impact of industry 4.0 (Alonso et al., 2019; Alrubaiei et al., 2021). Several attempts are being made in this direction by integrating blockchain into various application scenarios such as supply chain management, healthcare record management (Cao et al., 2019), intellectual property management, energy trading, etc.

The paper has been organized into the following sections. The next section briefly discusses the literature related to the blockchain application in industry 4.0. Then, section three discusses general types of blockchain along with the differentiating characteristics and challenges, and disadvantages of using each type of blockchain. Section four focuses on the blockchain issues in general. Section five proposes the blockchain recommendation algorithm. Section six provides a brief discussion of the research study outcomes, and the last section concludes the research study and presents future research directions.

Related Work

Blockchain and Industry 4.0 are two of the most transformative technologies. Integrating both technologies can be disruptive in many industries such as supply chain management, healthcare, data sharing, energy trading, and finance, etc. Blockchain has the potential to revolutionize many industries. However, there are several challenges such as lack of understanding and awareness,

technological complexity, security and privacy concerns, etc. This section provides a brief review of how blockchain can be adopted in different industry 4.0 applications and the implications of it.

Research by (Bodkhe et al., 2020) studies the application of blockchain technology in various smart domains. It addresses challenges in Industry 4.0, and supports its arguments with case studies, indicating the potential and feasibility of blockchain for industry 4.0. The research study (Javaid et al., 2021) discusses the potential integration of blockchain technology in Industry 4.0. It emphasizes the potential benefits of using blockchain in terms of security, privacy, data transparency, and identity protection, etc. Blockchain can introduce automation through smart contracts to various industrial fields within the industry 4.0 paradigm (Fernandez-Carames & Fraga-Lamas, 2019).

The research study (Liu et al., 2019) proposes a blockchain-driven system for managing a product's entire lifecycle in the industrial sector. The proposed framework aims to address the challenges of data sharing and collaborating with other stakeholders in the product lifecycle. It uses smart contracts to automate carrying out transactions and sending notifications throughout the product's life cycle. Research by (Mohamed & Al-Jaroodi, 2019) discusses how blockchain could be utilized to support intelligent manufacturing applications. It proposes a middleware method to make use of blockchain tools and functions, aiming to support smarter manufacturing that's safer, more dependable, transparent, consistent, and able to run on its own.

A research study (Leng et al., 2020) highlights that there are many potential benefits of blockchain technology for sustainable manufacturing. However, there are a number of obstacles that need to be addressed. For example, the study indicates that the blockchain technology is not proper for all sustainable manufacturing modes. It is crucial to consider the costs and benefits of implementing blockchain carefully before making a decision. It also emphasizes to ensure that blockchain-empowered sustainable manufacturing systems are achieving the desired energy-saving and energy-conserving benefits. Therefore, it can be concluded that blockchain-empowered transformation of sustainable manufacturing yet has several challenges to overcome.

The research study (Mushtaq & Haq, 2019) describes the blockchain technology's potential of playing a transformative role in Industry 4.0. The applications of blockchain can include from such as product counterfeiting, maintenance, and IP theft to improved efficiency, reduced costs, and increased flexibility in Industry 4.0. A research study (Kayikci et al., 2020) discusses the potential of applying blockchain technology in food supply chain by improving traceability, trust, and accountability. Blockchain can be used to track food products from farm to fork. It can be helpful in ensuring that consumers receive the right quality of food and that food loss is minimized. A research study (Benzidia et al., 2021) develops a model of how blockchain technology and relational social capital can be used to enhance buyers' innovation potential in industry 4.0. It identifies that blockchain can help buyers to exploit their internal capabilities and achieve their innovation targets. However, the managers and sponsors should consider investing in tools and collaborative frameworks to enable the implementation of smart technologies in industry 4.0.

Based on the above discussion, it is obvious that blockchain technology has a chance to revolutionize the industry 4.0. However, at the same time, there are several challenges in usage of blockchain technology. For example, interoperability issues between diverse manufacturing systems pose a significant barrier to the effective implementation of blockchain (Leng et al, 2020). The concept of decentralized manufacturing through Blockchain encounters challenges

related to production coordination and resource optimization (Zhao et al., 2020). Moreover, implementing smart contracts can be complex in some industry 4.0 scenarios (Fernandez-Carames & Fraga-Lamas, 2019; Liu et al., 2019). Like other networks, blockchain networks are vulnerable to cyberattacks, and it is essential to assure that sensitive data is protected. There is always a security threat to decentralized networks of potential vulnerabilities and cyber-attacks. The ownership and privacy of data in industry 4.0 environments present ethical and legal challenges. There is no clear regulatory framework for blockchain-based applications in many jurisdictions. Therefore, establishing a regulatory framework and standards for Blockchain is an ongoing challenge. Addressing these obstacles is imperative for recognizing the entire potential of Blockchain in Industry 4.0. Therefore, as much as blockchain can revolutionize industry 4.0, it is also important to consider the appropriate environment for applying blockchain. Awareness about blockchain technology is crucial among the managers, users and the sponsors. The following sections discusses the about different types of the blockchain technologies, issues and challenges in using blockchain technology.

Blockchain, the Good, and the Bad Characteristics

Blockchain has been introduced by Satoshi Nakamoto (Nakamoto, 2008) as a solution to the problem of double-spending using cryptocurrency or digital currency (Bitcoin). Since then, blockchain has been evolving and has been implemented in several application domains. Blockchain has been implemented in several application areas from cryptocurrency to smart contracts, from agriculture to healthcare, and so on, since its inception. Blockchain has given a new direction to how trade and transactions can take place. It has given the opportunity to perform a transaction (or online payment), even between the mutually mistrusting parties without involving any central third party while still offering integrity-protected data storage and transparency (Nakamoto, 2008).

Blockchain is a constantly increasing chain of blocks that are connected with each other by storing cryptographic code from their predecessor block. Blockchain is a distributed decentralized database on a computer network. Different nodes can connect and perform, access, and store the transactional information on the blockchain anonymously. Blocks in the blockchain collect a set of transactional information based on the capacity of the block, and once the block is filled, it is connected to its previous node by satisfying the cryptographical solution. The cryptographical code is calculated using the information stored in blocks, therefore, if there is any change in the block's information the code will change and hence the next block will not be consistent with the new code. Therefore, to make any update in the block's information 51% of the nodes should provide consensus which makes the blockchain transactions irreversible and immutable. It also provides the flexibility and transparency to access the blockchain data by anyone without any security threat.

Blockchains can be broadly classified into public, private and consortium blockchain based on the participation and consensus. Sometimes the public and private blockchains are combined to built a new variant called hybrid blockchain. This section briefly describes the public, private and consortium blockchains and their challenges.

Public Blockchain

Public Blockchain can be used arbitrarily by anyone as per their requirement. Third-party validator/s are not required in the use of Public Blockchain. Any user, who is the part of the Blockchain, is authorized to access all the records. Some instances of public blockchains are

Bitcoin, Litecoin, and Ethereum. Public blockchains are trustable because it is fully distributed and all the users are potentially unknown, it is a trustworthy system. The process of proof-of-work ensures a fraud-less transaction. Public Blockchain is a truly distributed network of nodes/records, making it hard to hack. Every participant plays an essential role in every transaction verification to make it a legitimate transaction. Due to these characteristics and working philosophy, a public blockchain is safer than other types of Blockchains.

However, the primary challenge for public blockchains is speed. Due to its distributed framework and working philosophy (each participant will verify each transaction) the throughput of public Blockchain is very slow; for instance, Bitcoin could process seven transactions per second (TPS) that is very less than Visa (24,000 TPS). Public blockchains also experience scalability Issues. The public Blockchain has a slow rate of processing which introduces the scalability issues. Because as network size increase size, the TPS will slow down gradually. Public blockchains cause high energy consumption. The proof-of-work is a compute-intensive process that requires high energy consumption. Therefore, it raises issues from both a sustainability and financial perspective. Another key issue public blockchains encounter is privacy. Public blockchain provides little privacy for transactions.

Private Blockchain

Only chosen entities can access and participate in block mining in Private Blockchain. One authoritative person can only choose participants and revoke permission from an existing participant. Private Blockchains are mainly used in private organizations to protect sensitive information from outside entities. The application of Private Blockchain can be used in elections, tracking goods in supply chains, verifying digital identities, managing ownership of assets, and more. A few well-known private blockchain platforms include Sawtooth, Hyperledger Fabric, and Corda. The private blockchains have speed and are scalable. The rate of transactions is more significant than Public blockchains. It is also scalable, and one could choose the size of the Blockchain as per the need.

Trust-building is paramount in Private Blockchain to transmit confidential information in a network, which is sometimes very dangerous. For example, any outside can extract the information by using behavioral phishing attacks on the participants. Private blockchains usually are less secure. In a private blockchain network, only few participants participate in proof-of-work, which makes it prone to security breaches. It needs a trusted central Identity and Access Management (IAM) system to function correctly. Private blockchains contradict the idea of decentralization which is an essential founding pillar of blockchain technology.

Consortium Blockchain

It is a partly public and partly private type of system. In this system, different nodes share the Blockchain, and only a few participants are allowed to access this Blockchain. Banks, government organizations, etc., typically use consortium blockchains. Some examples for consortium blockchains include R3, Energy Web Foundation, etc.

Hybrid Blockchain

A hybrid blockchain mixes elements of public and private blockchains. In such a network, users can control the access at the granular data level. It means that the participants of public blockchains can access a specific set of data and keep the rest confidential within the private network. It’s flexible, enabling users simply link a private blockchain to several public ones. A

transaction in a private network is verified inside that network but can also allow outsiders to verify them in the public Blockchain. Dragonchain is an instance of hybrid blockchain.

Blockchain Challenges

Using blockchain technology can bring various advantages to the application. But, it also introduces several challenges as well. Using blockchain is generally considered as a secure solution, but there have been different kinds of attacks by hackers on blockchain in the last decade. Because of these attacks, users have lost billions of dollars, there have been privacy issues and therefore, sensitive data protection can also not be guaranteed. Scalability is also an important concern, an increment in the number of participants can increase the transaction latency. Some of such these challenges are discussed in this section.

Security

Security is one of the strong points of Blockchain. However, there have been several security-related issues and attacks on blockchain-based systems. A research study (Li et al., 2017) analyses the security aspects of blockchain systems. The study links different kinds of security risks to the various components of blockchain such as consensus mechanism, smart contract applications, transaction verification process, public-key encryption scheme, blockchain application development related flaws, etc. (Li et al., 2017). Though there is a very low likelihood of most of these vulnerabilities, these vulnerabilities have been exploited by attackers oftentimes in the past and might cause a bigger financial risk in the case of Fintech application of Blockchain or in the exploitation of smart contracts, etc. Research by Luu et al. (Luu et al., 2016) identified that 8833 out of 19366 (which is around 46%) Ethereum contracts are vulnerable to attacks. The vulnerable smart contracts may cause big challenges and financial losses. The publicly reported financial losses, linked to blockchain-related security issues, account for worth billions of dollars. Therefore, it is worth considering if cryptocurrencies and other blockchain-based Fintech are worth the risk or not.

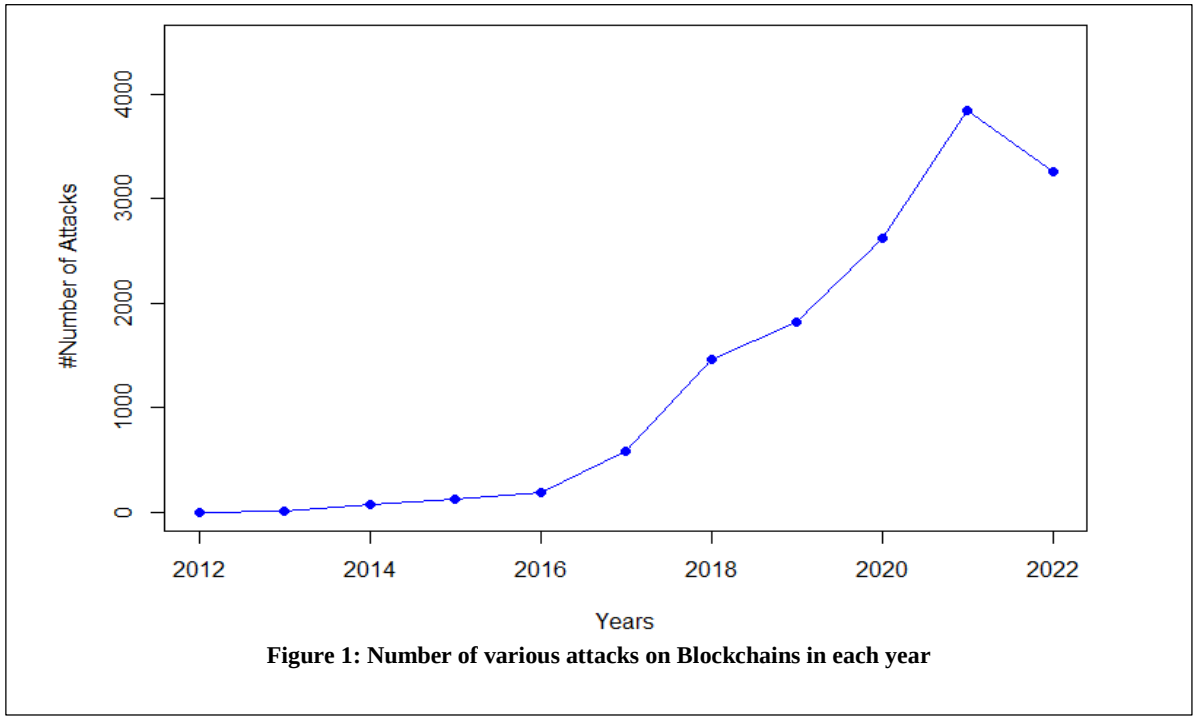

Figure 1: Number of various attacks on Blockchains in each year

This research study has collected data from various sources such as Chainalysis, TheBlock,

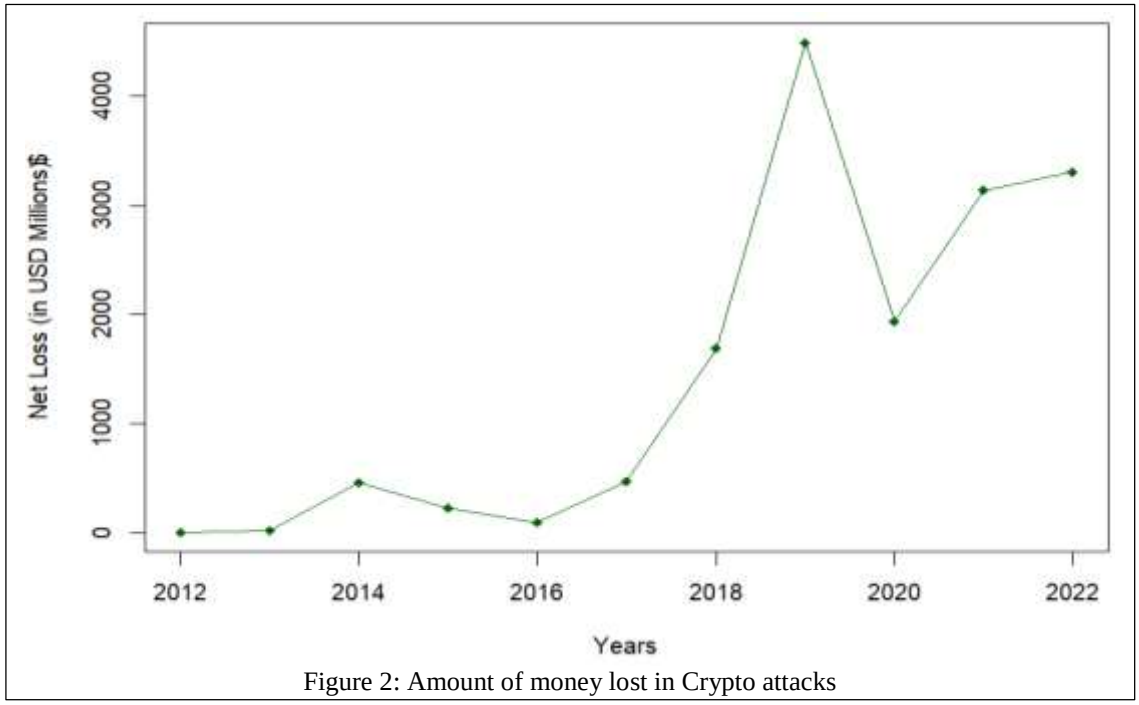

Figure 2: Amount of money lost in Crypto attacks

CoinMarketCap, and TheHackerNews. The figure 1 illustrates the numbers of various kinds of attacks on different blockchain implementations in each year. The most common types of attacks are 51% attack, malware attack, phishing attack, distributed denial-of-service attack," and social engineering attack. There have been various other types of attacks but these have been most common. The crypto market has lost millions of dollars each year since 2013. The figure 2 demonstrates the net loss in each year in different crypto attacks. The following table 1 represents the amount lost in each year and how little of that loss was recovered. The data has been collected from various sources as mentioned above and merely represents an approximate amount.

Table 1: Number of Attacks and Amount of money lost in Crypto attacks

Year	Number of Attacks	Lost	Recovered	Net Loss
2012	0	$0	$0	$0
2013	1	$11.8 million	$0	$11.8 million
2014	74	$450 million	$0	$450 million
2015	121	$223 million	$0	$223 million
2016	189	$92 million	$0	$92 million
2017	586	$462 million	$2.2 million	$460 million
2018	1,456	$1.7 billion	$200,000	$1.68 billion
2019	1,824	$4.5 billion	$13 million	$4.48 billion
2020	2,624	$1.97 billion	$40 million	$1.93 billion
2021	3,845	$3.2 billion	$62 million	$3.13 billion
2022	3,259	$3.6 billion	$300 million	$3.3 billion
2023 (Up to August)	2,168	$656 million	$215 million	$441 million

Privacy

The principal factor of cryptocurrencies' popularity has been the privacy of the identity of the users. Users can generate multiple addresses to address the information leakage issue. However, research studies (Meiklejohn et al., 201; Kosba et al., 2016) have illustrated that transactional privacy cannot be guaranteed by the blockchain. Since the transactional information and the balances related to a public key are accessible by the public, therefore, they can be linked to the users, and reveal users' private information. A research study by (Biryukov et al., 2014) demonstrated that blockchain users could be uniquely identified based on the group of nodes a user connects to. Several researchers have attempted to provide the solution in different ways such as by using an intermediary mixing service that maps the multiple senders to the multiple receivers. But, using the mixing service will create the issue of the centralized mixing service which can further lead to encrypting the data sent to the service and hence, will increase the transaction processing time.

Private Branching

In blockchain mining, it is possible that a selfish miner mines the block but does not broadcast until some requirements are satisfied for the miner. When the selfish miner's requirements are satisfied, the miner broadcasts all the mined blocks resulting in a separate branch of the blockchain. Such branches are known as private branches. As per the general notion, the blockchain cannot be exploited until 51% of the nodes agrees. However, researchers have proved otherwise (Eyal & Sirer, 2014). A lesser amount than 51% of hashing power can be used to exploit the blockchain. For example, if the private branch becomes longer than the public blockchain branch at any point in time, then this branch would be agreed by all the miners as the primary blockchain branch. Now, as the private branch will be considered the main blockchain branch, so more and more miners would join it and hence, the selfish minor's branch would get more than 51% of the hashing power and the main blockchain will have lesser nodes. There are other similar related attacks possible on blockchains such as stubborn mining in which miners attack the blockchain with a network-level eclipse attack.

Blockchain Scalability

The scalability of the blockchain is another key challenge. As the number of transactions increases, the size of the blockchain also grows. Bitcoin blockchain is one of well-known blockchain based cryptocurrency. Therefore, this research study considers the case of Bitcoin blockchain. As of September 2023, the Bitcoin blockchain storage size is over 510 gigabytes, the average size of each block is around 1.6 megabytes. The Bitcoin blockchain size has grown almost double from around 250 gigabytes in Jan 2020 to 500 gigabytes in July 2023. On an average 5 transactions are added to the Bitcoin mempool per second. While, the current average duration for a transaction with miner fees to become part of a mined block and get recorded in the public ledger is around 10 minutes. As the size of the blockchain grows, the transaction processing time will increase and the practicality of implementing Bitcoin as a real-time payment

alternative will diminish. The figure 3 demonstrates the how the size of the bitcoin blockchain has increased over the years.

The figure 4 demonstrates the time-series data of average number of transactions per block for Bitcoin blockchain. It has been observed that the average number of transactions per bitcoin block has an upward trend. If the block size is big, it may cause an issue of delayed propagation which may cause blockchain branches. The transactions are in millions and are required to be

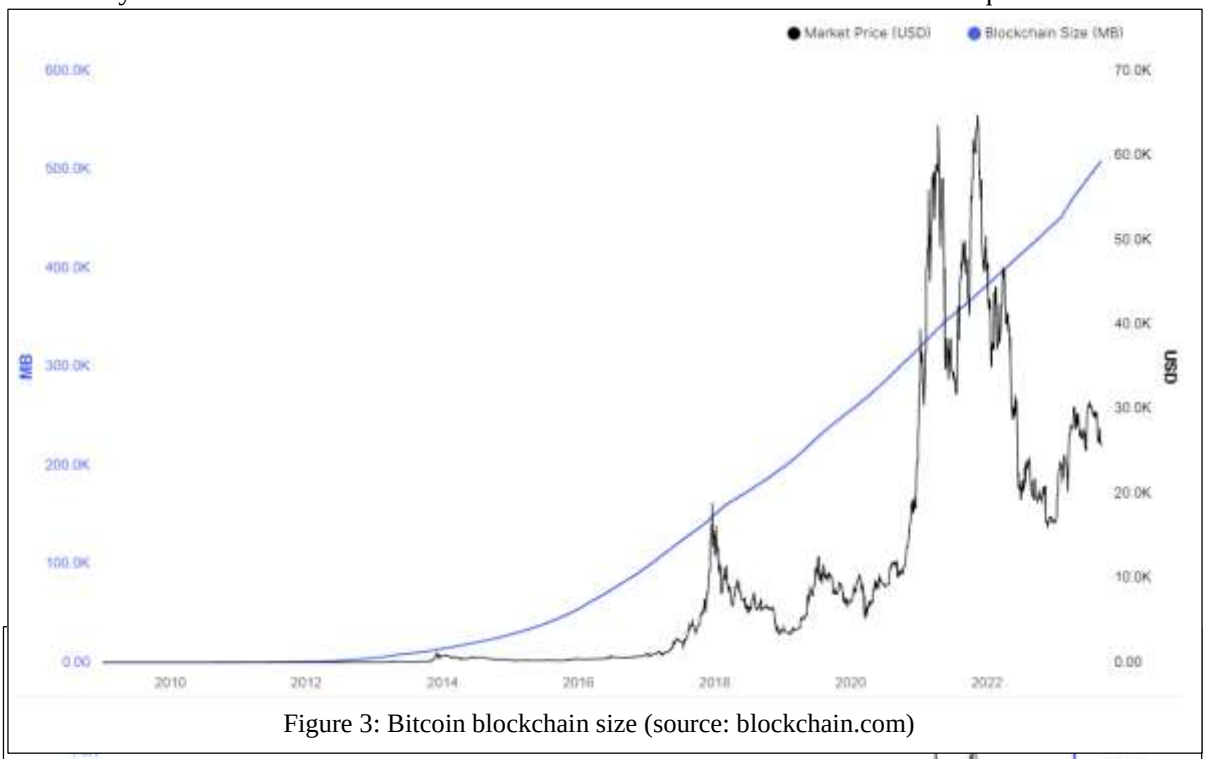

Figure 3: Bitcoin blockchain size (source: blockchain.com)

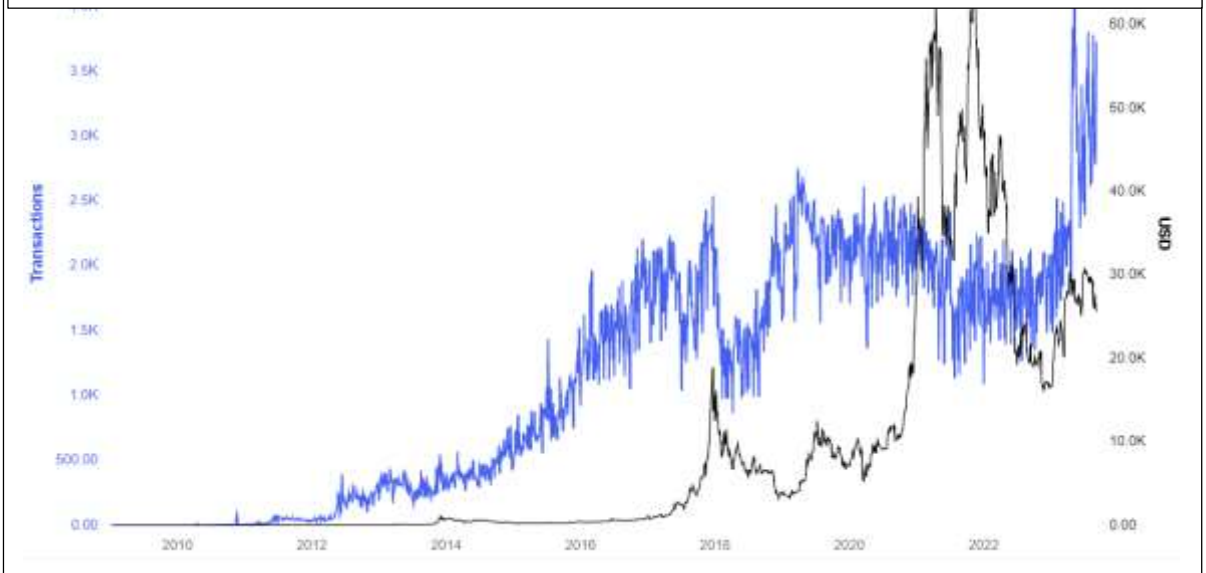

Figure 4: Bitcoin blockchain Average Transactions Per Block time-series (Blockchain.com, 2022)

stored for validating new transactions. Therefore, the size of the blockchain keeps growing exponentially (based on the lifetime data of the Bitcoin blockchain). Based on the above discussion, it is evident that as the blockchain grows, the size of the blockchain grows dramatically. Therefore, scalability is quite a challenging issue for blockchain.

Several researchers (Bruce, 2014; van den Hooff et al., 2014) have analyzed scalability and attempts have been made to resolve the issue of growing storage requirements. In these attempts, the concept of lightweight clients and the removal of old transactions from the network have been proposed. In another attempt (Eyal & Sirer, 2014), the underlying concept has been revamped to decouple the blockchain block into micro-block for transactions and key-block for elections. These attempts provide a significant step in the direction of addressing the issue of scalability. However, they have not been adopted by any of the blockchain systems for practical applications.

Therefore, based on the above discussion, it can be stated that there are several issues associated with blockchain. Consequently, applying blockchain in each scenario might not be an ideal solution specially where there is a requirement for scalability, information sharing and security. Each type of blockchain has certain requirements and certain limitations (or other associated constraints). The following section proposes a blockchain recommendation algorithm considering the key primary requirements for the application and recommends where and which type of blockchain should be applied.

Blockchain Recommendation Algorithm

This section discusses the approach for selecting an appropriate blockchain for different application use cases. As discussed in the previous sections, there are several challenges in using the blockchain technology in different domains. Moreover, there are several types of blockchain and each type has its own challenges. However, since the inception of Bitcoin, the usage of blockchain have been observed in several application areas. There have been several interesting applications of blockchain such as in industry 4.0, healthcare, supply chain, internet of things, logistics, finance, banking, education, accounting, agriculture, and many more (Kosba et al., 2022; Sharma et al., 2022; Alrubaiei et al., 2021; Khan & Rabbani, 2020). The application of blockchain is increasing day by day but as discussed in the previous sections, there are several challenges associated with it. It suggests that there might be overuse of blockchain.

The proposed blockchain recommendation algorithm considers the various features of the application and recommends a most appropriate type of blockchain based on the features of the application. The key features that the proposed algorithm takes into account are multi-party participation, decentralized authority, immutable storage, data generation frequency and latency, transparency, and participation type. It is a decision tree-based algorithm that asks several yes-no questions related to the requirements and features of the applications and recommends if blockchain should be used or not for the given application. It also recommends the type of blockchain that should be used in the given scenario. Hence, the proposed blockchain recommendation algorithm aids in decision making process about where the blockchain should be used, and where it should not be used. Furthermore, it also assists in deciding what type of blockchain should be used. The following figure 5 presents the flowchart of the proposed blockchain recommendation algorithm.

The steps for proposed blockchain recommendation algorithm are given in the following figure

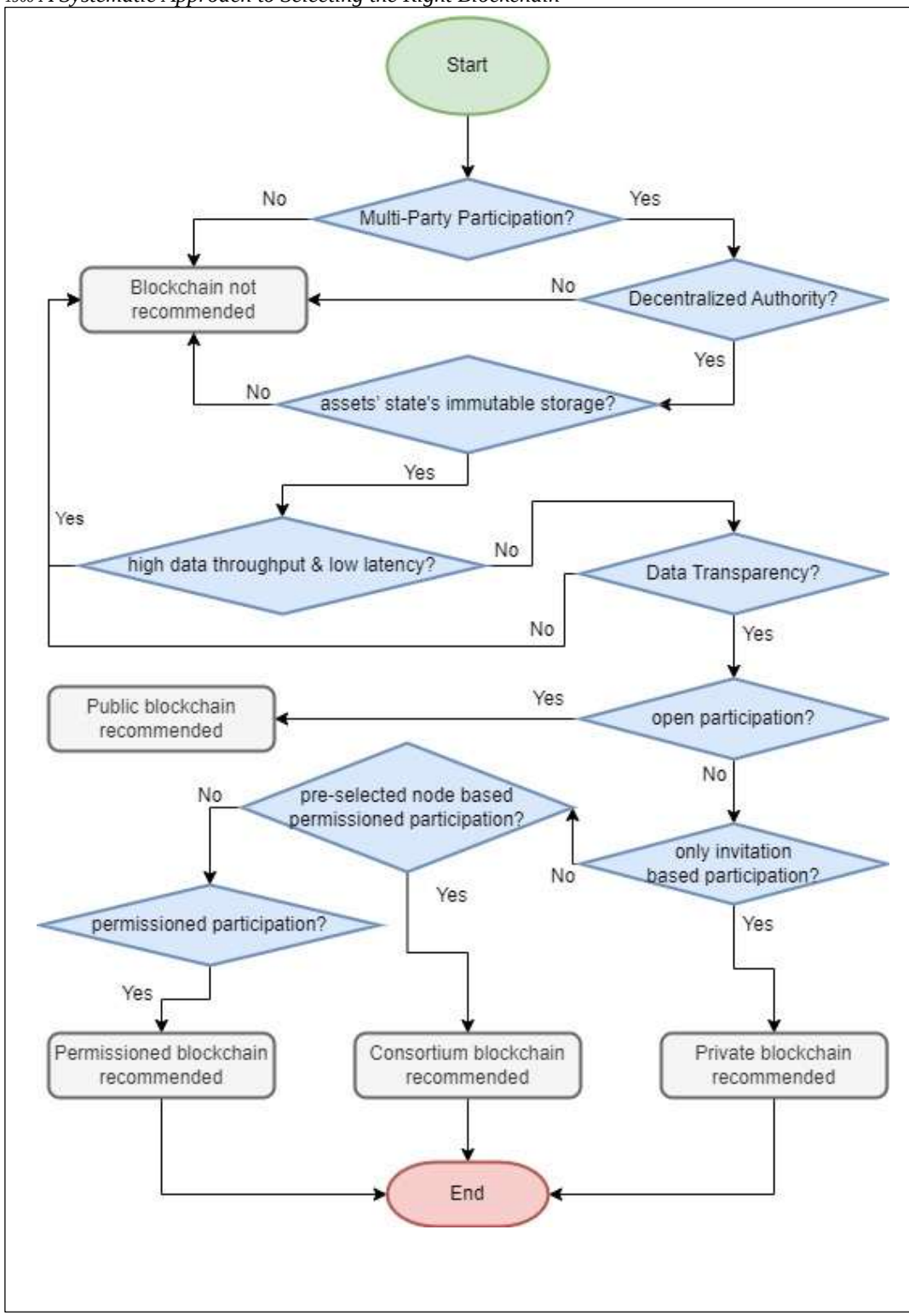

Figure 5: Flowchart for the Blockchain Recommendation Algorithm

type of participation. Because without participation by multiple parties, the use of blockchain is not recommended because blockchain is a distributed ledger technology. If multiple parties or nodes are participating in the transaction storage or transaction management then blockchain can be used and the algorithm moves to the next step for further analysis. The next step identifies the authority of the transaction management and storage. If the transaction management and storage require a decentralized authority then the likelihood of using the blockchain increases and the algorithm moves to the next step. Next step is to confirm if the immutability of the stored information about the asset's state is required or not. If there is a requirement that states the information state of the asset must be immutable then the algorithm considers the frequency of the data generation. The frequency of the data generation plays a vital role in the selection of the blockchain. If the frequency of the data generation is high, for example, time-series data such as health records, we should avoid the use of blockchain because the generation of frequent blocks incurred an unnecessary burden on the system. If the frequency of data generation is very then blockchain should not be used and some other solution such as distributed ledger technology, etc. should be considered. Because, blockchain transactions are typically slow and expensive. However, the blockchain can also be used in a scenario when it has high latency (here, latency signifies the time required to process and confirm a blockchain transaction) but, it can be a crucial issue where real-time data updates are required.

```
If multi-party participation is required
        If there is a requirement of a decentralized authority
                If there is a requirement for the immutable storage of the asset's state
                        If the data generation is having very high frequency and low latency is
required
                                Blockchain is not recommended
                        else if there is a transparency requirement for the stored data
                                If the participation is open for all (unrestricted)
                                        Public Blockchain is recommended
                                else if the participation requires an invitation from the member
                                        Private Blockchain is recommended
                                else if the participation requires from pre-selected permission
nodes
                                        Consortium Blockchain is recommended
                                else if the participation requires permission
                                        Permissioned Blockchain is recommended
                        else
                                Blockchain is not recommended
                else
                        Blockchain is not recommended
        else
                Blockchain is not recommended
else
        Blockchain is not recommended
```

Figure 6: Blockchain Recommendation Algorithm

If the data generation frequency is not very high and there is a requirement that there should be

transparency for the stored data. Then blockchain technology should be considered. Reaching and satisfying the condition for this step approves that blockchain is necessary for the given application. The next step identifies the type of blockchain that should be used for the given application. The next steps determine the blockchain type based on the type of participation. If the participations are open for everyone without any restrictions, then a public blockchain should be used. If participation is based on the invitation from the existing members, then a private blockchain should be used. if permission is required but the consensus is not controlled by a predefined group of nodes and all the nodes of the blockchain network can participate in consensus for permission then a permissioned blockchain should be used. However, in some use cases, the participation has to be approved by a pre-selected set of nodes, in these cases, a consortium blockchain should be used.

Discussion

In recent years, the application of blockchain has extended across a variety of domains. The finance domain, due to cryptocurrencies, has witnessed a great number of innovations and applications of blockchain. However, several blockchain applications can be seen in many other domains such as the healthcare industry, the internet of things (IoT), public and social services, security and privacy, etc. The primary reasons for using blockchain technology are the assurance of data integrity and decentralized trust. However, one of the important considerations is to understand the various aspect of the problem and identify why and which type of blockchain should be considered for the problem. The flowchart (see figure 5) represents the process that supports making decisions for applying blockchain solutions to different kinds of problems. The following subsection applies the proposed algorithm to a sample scenario.

Problem: Let's say you are working on a project to develop a new supply chain management system. The system will need to trace the movement of goods from the factory to the customer. You need to decide whether to use blockchain for this project and to decide whether to use a public or private blockchain or consortium blockchain. The key requirements for this system are summarized as following:

The system will need to be used by multiple parties to track the movement of goods, including suppliers, manufacturers, distributors, and retailers.

The system would need to be decentralized so that there should be fault-tolerant in the system and no single party has control over the data.

The data in the system must be secure and tamper-proof. The system needs to store the state of the supply chain immutably so that it cannot be tampered with.

The system must be scalable to handle a large number of transactions. Although, the system will need to handle a large volume of data, but the data generation frequency is not very high.

The data stored in the system should be transparent to all participants so that all parties involved in the supply chain can see it and verify it.

The cost of using the system must be affordable.

Human Expert Recommendation

Public blockchains are more secure than private blockchains, but they are also less scalable and more expensive. Private blockchains are less secure than public blockchains, and they are more scalable and less expensive. In this case, the best type of blockchain for the supply chain

management application would be a private blockchain. This is because the application requires a high level of security, but it does not need to be as scalable as a public blockchain. The cost of using a private blockchain is also more affordable than the cost of using a public blockchain. In addition to the key requirements of the problem, there are other factors that can be considered when choosing a type of blockchain. These factors include the level of trust required, regulatory landscape, and future plans. If the application requires a high level of trust between the participants, then a public blockchain may not be the best choice. In this case, a private blockchain or a consortium blockchain may be a better option. The regulatory landscape in the region where the application will be used can also affect the choice of blockchain type. For example, in some regions, public blockchains are not allowed. If the application is likely to grow in the future, then a scalable blockchain may be a better choice. As per these recommendations, a likely choice for the above problem will be a private or consortium blockchain.

While considering the regulatory factors, those are applicable for both scenarios whether the decision is made using the algorithm or by a human expert. Therefore, the algorithm described above can be used to help choose the right type of blockchain for the given problem. However, it is important to consider all of the factors involved before making a decision such as future plans and regulatory landscape. Apart from these factors, the decision made by the algorithm is more clear and faster.

Algorithmic decision-making process:

1. Input: Problem description
2. Output: Type of blockchain
3. Steps:
    - Identify the key requirements of the problem.
    - Evaluate the different types of blockchains in terms of their ability to meet the key requirements.
    - Select the type of blockchain that best meets the key requirements.

The following function provide the pseudocode to decide if there is a requirement to use blockchain to best meet the requirements of the problem.

```
def decide_blockchain_usage(multi_party, decentralized, immutable_storage,
high_frequency_low_latency, transparency_requirement, participation_type):
    if multi_party:
        if decentralized:
            if immutable_storage:
                if high_frequency_low_latency:
                    print("Blockchain is not recommended")
                else:
                    if transparency_requirement:
                        if participation_type == "unrestricted":
                            print("Public Blockchain is recommended")
                        elif participation_type == "invitation":
                            print("Private Blockchain is recommended")
                        elif participation_type == "pre-selected nodes":
                            print("Consortium Blockchain is recommended")
                        elif participation_type == "permission":
                            print("Permissioned Blockchain is
recommended")
                        else:
                            print("Blockchain is not recommended")
                    else:
                        print("Blockchain is not recommended")
            else:
                print("Blockchain is not recommended")
        else:
            print("Blockchain is not recommended")
    else:
        print("Blockchain is not recommended")

#Usage on the given application:
```

The above function takes six arguments such as multi_party_participation, decentralized_authority, immutable_storage, high_frequency_data_generation, transparency_requirement, and participation_type. First five arguments carry boolean values (yes/no or true/false). The arguments represent various features of the application. The function recommends to use consortium blockchain. The consortium blockchain meets all the key requirements of the system as described in the problem description. The system developed using consortium blockchain will meet all the requirements of the application such as being used by multiple parties to track the movement of goods, including suppliers, manufacturers, distributors, and retailers. The system would be decentralized, so there would be no single point of failure. The data in the system would be secure, tamper-proof, transparent, and scalable to handle a large number of transactions. The decision-making using the proposed algorithm is faster and clearer than the decision provided by the human expert.

This section provides just one example of the proposed algorithm. It is quite possible that the

specific requirements for a particular application may vary, so there might be some amendments required, however, the general principal algorithm will remain same across different problem application scenarios. For example, to record financial activities in a protected and clear way, to track the ownership of intellectual property assets, to store and share medical records in a secure and private manner, to create a more secure and transparent voting system, etc. The following table 2 provides recommendation to different applications.

Table 2: Algorithm recommendation for different applications

Application	Application Features	Recommendation
Supply Chain Management	Multiple stakeholders, decentralized authority, ensuring product data integrity, end-to-end transparency, participation is open for all stakeholders and consumers	Public blockchain is recommended
Healthcare record management	Multiple stakeholders such as healthcare providers, patients, and insurers, data integrity, transparency in treatment and billing, controlled access	Permissioned blockchain
Voting System	Multi-party participation (such as voters, election authorities, and auditors), preventing manipulation of election results, ensuring the integrity of votes, publicly verifiable election results, open participation.	Public blockchain
Intellectual Property Management	Multi-party participation (creators, licensors, and consumers), managing IP without a centralized entity, proving the ownership and history of IP rights, transparency in licensing and usage, participation for creators and licensees	Permissioned blockchain
Cross-Border Payments	Multiple parties (banks, financial institutions, and individuals), reducing the need for intermediaries, ensuring transaction history cannot be altered, transparent cross-border transactions, participation for banks and financial institutions.	Permissioned blockchain
Food Safety Tracking	Multiple parties (producers, distributors, retailers, and consumers), ensuring the integrity of food supply chain data, tracking the origin and handling of food products, transparency in food sourcing and safety, participation for industry stakeholders.	Consortium blockchain
Property Transactions	Various sides (such as buyers, sellers, brokers, and government agencies), reducing reliance on intermediaries, ensuring transparent property history, transparent property ownership and transaction history, participation for real estate professionals	Permissioned blockchain
Energy Trading	Multiple parties (producers, consumers, and grid operators),	Consortium blockchain

	enabling peer-to-peer energy trading, recording energy production and consumption accurately, transparent energy transactions and pricing, participation for energy market stakeholders.	
Smart Contracts for Legal Agreements	Multiple parties (contracting parties, lawyers, and arbitrators), ensuring contract execution without intermediaries, recording contract terms and execution, transparent contract performance, participation for contract parties and legal professionals	Permissioned blockchain
Identity Verification	Multiple parties (users, service providers, and government entities, user-controlled identity verification, storing verified identity data securely, transparent identity verification process, participation for identity providers and service platforms.	Permissioned blockchain

The algorithm can be applied to a variety of the problem areas where there is a decision required about the selection of the blockchain type and to decide whether there is a requirement of using the blockchain. However, there are certain limitations associated with it. The proposed algorithm provides the general guiding principles and consider the technical features primarily. It does not take the financial (i.e., the cost of implementation) and post implementation maintenance into account. There certain other points to be considered in general such as, if the size of the network is very small or application requires to store large amount of data into blocks, or there are some regulatory compliance requirements then blockchain might not be well-suited solution and some other solutions should be sought for.

Conclusion and Future work

This research study discusses the applicability of the blockchain in different scenarios and where it should be considered and where it should be avoided. The research study primarily analyzes the difficulties in applying blockchain to build solutions for the industry 4.0 era. It discusses about the problems and obstacles of blockchain technology overall. In the light of this discussion, it has proposed a blockchain recommendation algorithm that takes the primary constraints of using blockchain into account and recommends which type of blockchain should be applied in a particular use case. The proposed algorithm covers all types of blockchain except the hybrid blockchain. Because in the hybrid blockchain, the type of ratio of hybridization will be the primary deciding factor after following the rules for a public blockchain. In future work, the algorithm could be updated to recommend alternate solutions such as distributed ledger technology, etc. in place of blockchain. The algorithm may also include recommended usage for hybrid blockchain.

Generally, it is assumed that the blockchain is invincible, cannot be attacked, and all the information stored on the blockchain is secure. However, as discussed in the blockchain challenges section that there are several possibilities where blockchain can be attacked and the participants can be tricked to participate in the private branches of the selfish miners. Therefore, applying blockchain for the sake of application, merely complicate the problem and adds a layer of technical complexity. The use case of blockchain should be selected after considering all the

constraints and taking the blockchain challenges into account.

References

Alonso, S. G., Arambarri, J., López-Coronado, M., & De La Torre Díez, I. (2019). Proposing new blockchain challenges in eHealth. Journal of Medical Systems, 43(3). https://doi.org/10.1007/s10916-019-1195-7

Alrubaiei, M. H., Al-Saadi, M. H., Shaker, H., Sharef, B., & Khan, S. (2021). Internet of Things in cyber security scope. In Advances in computer and electrical engineering book series (pp. 146–187). https://doi.org/10.4018/978-1-7998-8382-1.ch008

Bai, C., Dallasega, P., Orzes, G., & Sarkis, J. (2020). Industry 4.0 technologies assessment: A sustainability perspective. International Journal of Production Economics, 229, 107776. https://doi.org/10.1016/j.ijpe.2020.107776

Benzidia, S., Makaoui, N., & Subramanian, N. (2021). Impact of ambidexterity of blockchain technology and social factors on new product development: A supply chain and Industry 4.0 perspective. Technological Forecasting and Social Change, 169, 120819. https://doi.org/10.1016/j.techfore.2021.120819

Biryukov, A., Khovratovich, D., & Pustogarov, I. (2014). Deanonymisation of clients in Bitcoin P2P network. Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security. https://doi.org/10.1145/2660267.2660379

Blockchain.com | Charts - Average Transactions per block. (2022). Retrieved March 25, 2025, from https://www.blockchain.com/charts/n-transactions-per-block

Bodkhe, U., Tanwar, S., Parekh, K., Khanpara, P., Tyagi, S., Kumar, N., & Alazab, M. (2020). Blockchain for Industry 4.0: A Comprehensive Review. IEEE Access, 8, 79764–79800. https://doi.org/10.1109/access.2020.2988579

Borowski, P. (2021). Digitization, digital twins, blockchain, and industry 4.0 as elements of management process in enterprises in the energy sector. Energies, 14(7), 1885. https://doi.org/10.3390/en14071885

Bruce, J. D. (2014). The mini-blockchain scheme, 2014. URL: http://cryptonite. info.

Cao, S., Zhang, G., Liu, P., Zhang, X., & Neri, F. (2019). Cloud-assisted secure eHealth systems for tamper-proofing EHR via blockchain. Information Sciences, 485, 427–440. https://doi.org/10.1016/j.ins.2019.02.038

Eyal, I., & Sirer, E. G. (2014). Majority is not enough: Bitcoin mining is vulnerable. In Lecture notes in computer science (pp. 436–454). https://doi.org/10.1007/978-3-662-45472-5_28

Fernandez-Carames, T. M., & Fraga-Lamas, P. (2019). A review on the application of blockchain to the next generation of cybersecure industry 4.0 smart factories. IEEE Access, 7, 45201–45218. https://doi.org/10.1109/access.2019.2908780

Frank, A. G., Dalenogare, L. S., & Ayala, N. F. (2019). Industry 4.0 technologies: Implementation patterns in manufacturing companies. International Journal of Production Economics, 210, 15–26. https://doi.org/10.1016/j.ijpe.2019.01.004

Ghobakhloo, M. (2019). Industry 4.0, digitization, and opportunities for sustainability. Journal of Cleaner Production, 252, 119869. https://doi.org/10.1016/j.jclepro.2019.119869

Haber, S., & Stornetta, W. S. (2007). How to Time-Stamp a digital Document. In Springer eBooks (pp. 437–455). https://doi.org/10.1007/3-540-38424-3_32

Javaid, M., Haleem, A., Singh, R. P., Khan, S., & Suman, R. (2021). Blockchain technology applications for Industry 4.0: A literature-based review. Blockchain Research and Applications, 2(4), 100027. https://doi.org/10.1016/j.bcra.2021.100027

Kayikci, Y., Subramanian, N., Dora, M., & Bhatia, M. S. (2020). Food supply chain in the era of Industry 4.0: blockchain technology implementation opportunities and impediments from the perspective of

people, process, performance, and technology. Production Planning & Control, 33(2–3), 301–321. https://doi.org/10.1080/09537287.2020.1810757

Khan, S., & Kannapiran, T. (2019). Indexing issues in spatial big data management. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3387792

Khan, S., & Rabbani, M. R. (2020). In depth analysis of blockchain, cryptocurrency and sharia compliance. International Journal of Business Innovation and Research, 1(1), 1. https://doi.org/10.1504/ijbir.2020.10033066

Khan, S., Syed, M. H., Hammad, R., & Bushager, A. F. (Eds.). (2022). Blockchain technology and computational excellence for society 5.0. IGI Global.

Kosba, A., Miller, A., Shi, E., Wen, Z., & Papamanthou, C. (2016). HAWK: The blockchain model of Cryptography and Privacy-Preserving smart Contracts. 2022 IEEE Symposium on Security and Privacy (SP). https://doi.org/10.1109/sp.2016.55

Leng, J., Ruan, G., Jiang, P., Xu, K., Liu, Q., Zhou, X., & Liu, C. (2020). Blockchain-empowered sustainable manufacturing and product lifecycle management in industry 4.0: A survey. Renewable and Sustainable Energy Reviews, 132, 110112. https://doi.org/10.1016/j.rser.2020.110112

Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2017). A survey on the security of blockchain systems. Future Generation Computer Systems, 107, 841–853. https://doi.org/10.1016/j.future.2017.08.020

Liu, X., Wang, W., Guo, H., Barenji, A. V., Li, Z., & Huang, G. Q. (2019). Industrial blockchain based framework for product lifecycle management in industry 4.0. Robotics and Computer-Integrated Manufacturing, 63, 101897. https://doi.org/10.1016/j.rcim.2019.101897

Luu, L., Chu, D., Olickel, H., Saxena, P., & Hobor, A. (2016). Making smart contracts smarter. Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security, 254–269. https://doi.org/10.1145/2976749.2978309

Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G. M., & Savage, S. (2013). A fistful of bitcoins. In Proceedings of the 2013 Conference on Internet Measurement Conference. https://doi.org/10.1145/2504730.2504747

Mohamed, N., & Al-Jaroodi, J. (2019). Applying Blockchain in Industry 4.0 applications. 2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC), 0852–0858. https://doi.org/10.1109/ccwc.2019.8666558

Mushtaq, A., & Haq, I. U. (2019). Implications of Blockchain in Industry 4.O. 2021 International Conference on Engineering and Emerging Technologies (ICEET), 1–5. https://doi.org/10.1109/ceet1.2019.8711819

Nakamoto, S. (2021). Bitcoin: A peer-to-peer electronic cash system, Decentralized Business Review, Bitcoin. org, 2008. URL: https://bitcoin. org/bitcoin. pdf.(Accessed 24 February 2021), 21260.

Sharma, S., Syed, M. H., & Khan, S. (2022). Blockchain Technology in Ecosystems. In Blockchain Technology and Computational Excellence for Society 5.0 (pp. 1-15). IGI Global Scientific Publishing.

Tanwar, S., Parekh, K., & Evans, R. (2019). Blockchain-based electronic healthcare record system for healthcare 4.0 applications. Journal of Information Security and Applications, 50, 102407. https://doi.org/10.1016/j.jisa.2019.102407

van den Hooff, J., Kaashoek, M. F., & Zeldovich, N. (2014, November). Versum: Verifiable computations over large public logs. In Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security (pp. 1304-1316).

Zhao, H., Chen, P., Khan, S., & Khalafe, O. I. (2020). Research on the optimization of the management process on internet of things (Iot) for electronic market. The Electronic Library, 39(4), 526–538. https://doi.org/10.1108/el-07-2020-0206