Review Article

International Journal of Advanced Technology and Engineering Exploration, Vol 10(109)
ISSN (Print): 2394-5443 ISSN (Online): 2394-7454
http://dx.doi.org/10.19101/IJATEE.2023.10101498

A systematic literature review on endpoint vulnerabilities of blockchain applications

Mohd Azeem Faizi Noor[1*] and Khurram Mustafa[2]
Research Scholar, Department of Computer Science, Jamia Millia Islamia, New Delhi– 110025, India[1]
Professor, Department of Computer Science, Jamia Millia Islamia, New Delhi– 110025, India[2]

Received: 08-February-2023; Revised: 12-November-2023; Accepted: 14-November-2023

Abstract
Blockchain technology is a publicly accessible decentralized and immutable transaction log that significantly simplifies the recording of transactions and asset management in a corporate network. An asset can be tangible like a house, car, cash, or land, or intangible like intellectual property, patents, copyrights, or branding. It may considered as a unique identifier for every data, with each block in the ledger having its own hash and containing the previous block's hash. It is one of the most emerging technologies with added built-in flexibility that has changed the world. Because of its all-encompassing nature, it is being accepted and endorsed as a promising technology by financial and non-financial transaction platforms. However, like any other developing technology, it too has its own set of concerns, bottlenecks and obstacles including scalability, privacy, regulation, and security issues. Recent heists and hacks have raised serious questions about its existence and security. Endpoint vulnerabilities are one such crucial and inherently particular security concern that must be addressed. Thus, this study systematically reviews the literature to bring about the state-of-the-art to determine the possible factors, aspects, and causes of the endpoint vulnerabilities with some mitigation countermeasures. Several recent studies were selected to mine the endpoint vulnerability information and focus on the pertinent issues. The major revelation is the lack of user knowledge, insufficient security mechanism, no security layer other than authentication, keylogger malware behind endpoint vulnerability exploitation. It explains the various factors and root causes of endpoint vulnerabilities and provides a relation between the endpoint and its attribute/components. Lacking adequate mechanisms to counteract endpoint vulnerability attacks, users are more likely to make technical and behavioral blunders. Moreover, it fulfills the lack of any systematic literature review (SLR) on endpoint vulnerabilities. It aims to raise security awareness among users, enhance security measures for developers, and provide valuable insights for further investigation by researchers. This study is a step towards understanding and improving the security posture at the endpoints of blockchain networks.

Keywords
Endpoint vulnerabilities, Blockchain, Key, Wallet, Cryptojacking.

1.Introduction
In networking, an endpoint is a device or location that is used to access a network. It includes computers, laptops, servers, smartphones, and other devices connected to the network [1]. Endpoints are typically used to access network resources and services, such as the internet or internal network resources. Endpoints are often the target of attackers, as they can be used to gain access to a network and its resources [2]. So, endpoint protection is exigency. The experts suggest many standards policies, practices and guidelines to in tune with security [3, 4].

Organizations implemented various security measures to protect endpoints, including antivirus and firewall software, strong password policies, and regular updates to security protocols and software to keep attackers at bay.

These security measures were up to mark against a distributed or centralised technique. However, blockchain, the latest technique, is fully decentralised [5]. So, these security measures are inadequate to protect endpoints in the blockchain. A few papers were published on endpoint vulnerabilities in blockchain, but none notice and addressed them properly. This study aims to investigate and find the endpoint vulnerabilities in existing blockchain, its root causes and mitigation techniques and fulfil the

*Author for correspondence

research gap. In decentralisation, there are no standard parameters, security measures, or organizations. Therefore, it is hard to implement policies, strategies, decisions, guidance etc. in such a network [6]. It creates security concerns at the application level and an open invitation to attackers. Consequently, numerous exchanges and users have experienced losses at the endpoint in blockchain applications countless times [2, 7]. This systematic study concerns all these issues. Though many studies were done in the past but lacked endpoint concepts and mitigation techniques.

The blockchain concept was first introduced in 2008 through a white paper by an unknown person or group of people using the pseudonym Nakamoto and Bitcoin [8]. This technology is in its early stages of development, mainly used for the creation of cryptocurrencies such as Bitcoin. Additionally, it has been implemented in many areas including finance, non-financial, supply chain management, and even voting systems despite the fact that no standard or certified framework exists [9]. The technology is in its embryonic stage and is far from providing a qualitatively assured system [10].

1.1Motivation and target audience

The motivation of this work is to initiate, discuss and guide the audience towards the endpoint security of blockchain via a systematic, critical and exhaustive review. Recently, blockchain has gained considerable attention for its remarkable services and characteristics [11]. Blockchain has built trust among enthusiast stakeholders by removing the very overheads of central dependency [12]. Since users from various fields are interested in using blockchain services in financial and non-financial activities [9], it is intuitive to gain a deeper knowledge and better understanding of the security of blockchain, especially endpoint protection. It protects users from online fraud, attacks and many other malicious traps [13]. As a result, users will be able to save their crypto money, wallet and control it. Additionally, users can enjoy blockchain services without any discomposure.

1.2Contributions

The primary goal was to explore, find, collect, and analyse relevant research on the topic before compiling it into a coherent share-worthy summary to make a case for additional research. However, the following are a few notable contributions:

- It emphasises the critical background knowledge needed for the private key, wallet, elliptic curve digital signature algorithm (ECDSA), and so on. These may be required to understand the working methodology, vulnerabilities, and challenges associated with the use of blockchain applications.
- There is lack of direct literature studies on endpoints. Therefore, most relevant literature review papers were selected and compared. Of the 19 studies identified, only one focused on the endpoint (refer *Table 2 in section 3*).
- It analytically reports on endpoint security vulnerabilities, layers, and heists that have occurred over time. At various levels, this study investigate the possibilities and types of potential attacks, as well as the financial and non-financial risks associated with blockchain applications.
- It prompts a debate and responses to research questions that explain the various factors and root causes that lead to endpoint vulnerabilities and the research gap.
- Finally, it identifies probable and feasible solutions to endpoint vulnerabilities in blockchain applications. The goal is to provide a fundamental understanding of endpoint vulnerabilities in blockchain applications.

The remainder of this paper is structured as follows. The remaining part of this section presents a preamble on blockchain technology, application, endpoint and introduction of research questions. Section 2 deals with the review methodology in detail. Next, section 3 deals with the literature review and presents two tables regarding the selected studies. Section 4 answers the research questions by analysing and discussion. Section 5 highlights the key finding and limitations as well. Finally, the paper is concluded in section 6 with pertinent trends and indications.

1.3Blockchain

Distributed ledger technology (DLT) is an automated system that records transactions along with their details in a distributed manner across multiple sites [14]. The various properties of DLT are enlisted in *Figure 1*. Unlike traditional databases, DLTs have no central authority [15]. Different types of DLT exists depending on the utility, like directed acyclic graph (DAG), Tempo, Holochain etc. [16]. Alkhodair et al. [17] has provided an extensive analysis of the categorization of DLT. The most well-known among them is blockchain as shown in *Figure 2*.

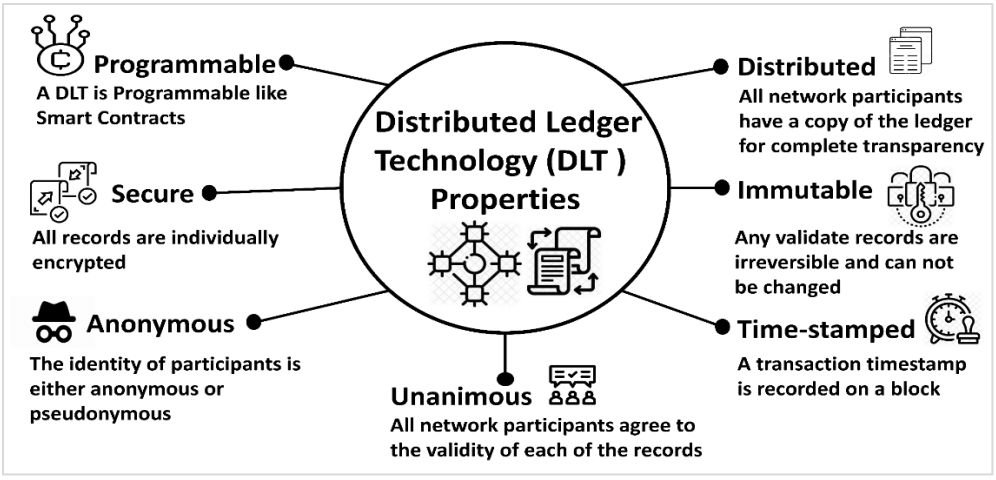

Figure 1 Properties of DLT

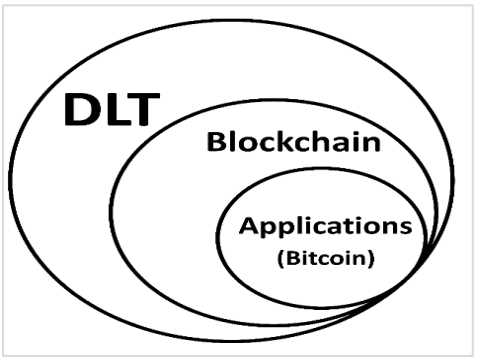

Figure 2 DLT and blockchain relation

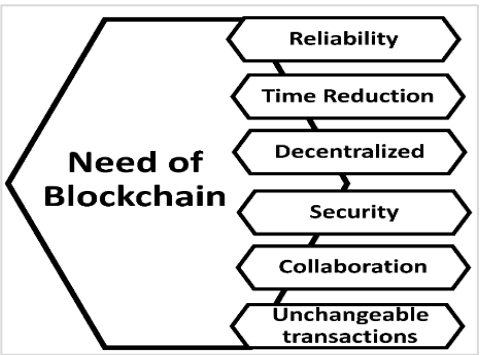

Figure 3 Need of blockchain

The blockchain concept was first presented as a research project in 1991[18] before its first popular use in use, Bitcoin [19, 20], in 2009. The creation of numerous cryptocurrencies, decentralised finance (DeFi) applications [17], non-fungible tokens (NFTs) [21] and smart contracts [22, 23] has skyrocketed the use of blockchain in the years thereafter. It eliminates the need for third-party verification and related expenditures which is much-need in the current era [8]. This is where, the need for a decentralised technology emerges (*Figure 3*). Blockchain Technology is a cryptographic-based, peer-to-peer [24], distributed ledger [25] that enables trust among untrusted participants in the network. This term was coined by a pseudonym person named Nakamoto and Nakamoto and Bitcoin in his white paper [8]. Blockchain, by its natural virtue, nullifies the role of mediator and ratifies the transactions between end-users [26]. These transactions are publicly available but immutable and indelible. With the increment in the value of Bitcoin and Ethereum (1st and 2nd applications of blockchain), more invaders are joining illegal activities [27]. A heist at the Mt Gox exchange happened and stole 740000 Bitcoins (BTC) ($450 million) through a loophole in the exchange [24]. In 2018, hackers compromised hot wallets and transferred $534 million worth of NEM cryptocurrency, popularly known as Coincheck Hacking. In 2016, a hacker compromised the BitFinex cryptocurrency exchange for 120000 BTC due to wallet vulnerability [28, 29]. Each threat is a curse for blockchain technology. Many investors invest their fiat currency to buy cryptocurrency like Bitcoin, Ethereum on an exchange service. Such exchange services shield customers' accounts through their safety precautions or lend safety technology from 3rd parties. Such precautions are suitable for safety but not immune to hacks.

1.3.1Blockchain applications

The properties of blockchain make it versatile and prominent [30]. This technology was initially preponderant in the financial sector. But, stakeholders and entrepreneurs have pushed its limit by implementing it in applications other than cryptocurrency [31]. Alqahtani and Algarni [32] have provided many applications of blockchain

technology. So, it has significantly impacted well financial and non-financial sectors, including banking, healthcare, supply chain, government, smart property, cybersecurity, tendering social media, etc. [33–35] (*Figure 4*). Moreover, it has influenced world currency markets, illegal activities (ransomware) [36], cyber heists etc. [9]. These applications encompass decentralization, immunity and transparency that make blockchain unparalleled from other technologies.

Many nations like Switzerland. United Arab Emirates, United Kingdom, Denmark, Honduras, Japan, China, and many others have stepped foot to unleash blockchain technology's hidden capabilities. Estonia is the first nation to use blockchain-based electronic voting [37]. The Swiss worldwide project Health bank is a milestone [38]. In a similar vein, the United States has Gem [39]; Estonia has Guardtime [40]; as a blockchain-based healthcare project. Experts call Malta 'Mecca' because of their unrestricted and open rules for blockchain and cryptocurrencies [9]. The UAE is strongly embracing blockchain technology and has launched the Dubai Blockchain Strategy to make transactions completely transparent and transform the public sector [32, 41]. Many other countries have invested a huge amount of money in their economy, data management security, transparency and instilling trust within their countrymen.

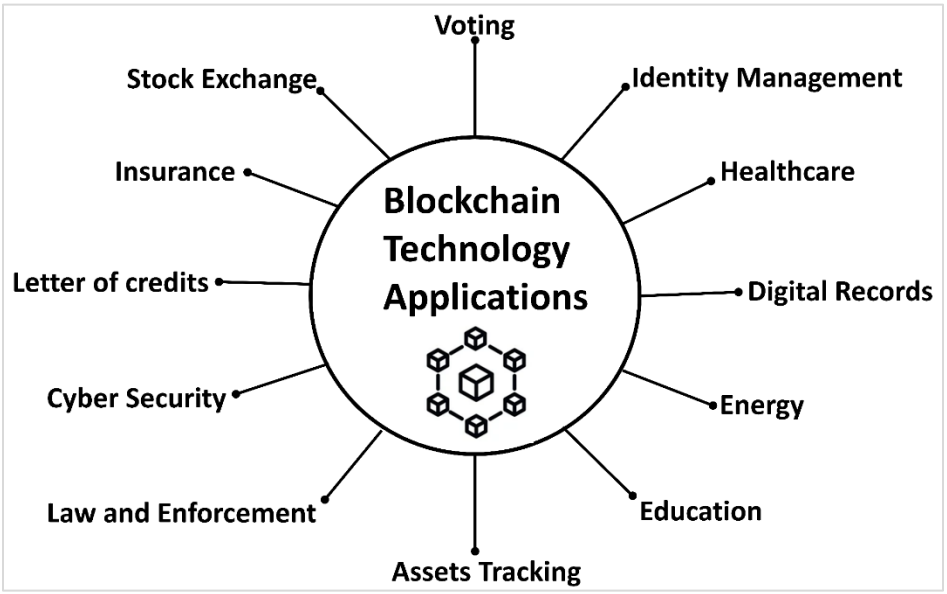

Figure 4 Various applications of blockchain technology

1.3.2 Endpoint

In a blockchain application, an endpoint is a network address that allows a user or device to connect to the blockchain network and access its features and functions [2]. This can include sending and receiving transactions and querying the blockchain for information. Endpoints are the spaces shared by humans and the blockchain, i.e., human interaction with the machine [42]. Human uses computers to enter data and access blockchain-based services [43]. During access to the blockchain, the data on the chain is vulnerable. As a result, the system, mobile devices, and personal computers are the most vulnerable components [44]. Thus, keeping the endpoint safe and secure is imperative to avoid stealing the blockchain keys [43, 45, 46].

Blockchain applications are not free from endpoint security concerns [47]. Consequently, it is vital to identify what current research exists specifically with the blockchain endpoint vulnerabilities and what research has already been done. A rigorous literature assessment of endpoint vulnerabilities in blockchain applications is required to find the answer.

1.3.3Prior research

These studies uncover a plethora of articles addressing blockchain applications and security challenges, but only a few appear to have undergone a systematic literature review (SLR). Among them, a handful appears to focus on endpoint vulnerabilities and related security concerns. One of the most closely-related research is done by Lee [24], which discusses vulnerabilities and analyses security in detail. In this study, the author highlighted numerous

cyberattacks due to endpoint-related compromises, security compromises, platform breaches, access point attacks, etc. Another related research was conducted by Conti et al. [48] which presents a survey on the security and privacy issue of Bitcoin with countermeasures. Though these studies attempt to elaborate on each topic nicely but lack the very idea of 'systematic review and coverage' to acclaim adequately feasible comprehensiveness and rigour. Taylor et al. [49], Zamani et al. [50], Zhang et al. [51], Hasanova et al. [52] are the other recent studies around blockchain and covered various topics. But, none of them elaborates on endpoint vulnerabilities in a depth and systematic ways.

Generally, the intent of attackers to attack the endpoint is to get the security key, cryptocurrency, wallet control and resource abuse [53]. To achieve these, attackers tried to penetrate the system security via numerous techniques like authentication breaches, phishing, malware, brute force, cryptojacking, taking advantage of human errors etc. Initially, the core wallet was not encrypted but after MtGox (1st) incidents, the encryption layer was added [54]. To enhance the security use of two wallets – a hot and cold wallet was suggested [55]. In fact, 2-factor authentication (2FA) was also suggested [56]. However, in 2012, the Bifloor exchange was compromised due to wallet insecurity [57]. Later, in 2013, inputs.io was exploited by the attacker through a bypass of 2FA [58]. McCorry et al. [59] introduced Multi-Signature (MultiSig) in blockchain applications but it was breached in 2016 at the Bitfinex exchange [54]. Exchanges and companies have been rolling out some security updates and patches to reduce thefts and heists activities but these measures are not proving the final nail in caffeine. *Figure 5* and *Figure 6* represent the above summaries.

Generally, a user interacts with the blockchain in three ways, which include 'third party exchanges, decentralized applications (dApps) and online web-based services [24]. The security of endpoint devices falls out of the blockchain area. While accessing through these methods, often security is compromised at the user side [42]. And, only the security of system data within the blockchain boundary is guaranteed against external threats by blockchain technology. Therefore, strong authentication procedures by themselves cannot guarantee sufficient security for the entire system, regardless of how secure your data is within blockchain. As a result, users have seen phishing, security breaches, fake emails, malware, cryptojacking, server compromise, 2FA etc, at the endpoint to steal wallet coins and control.

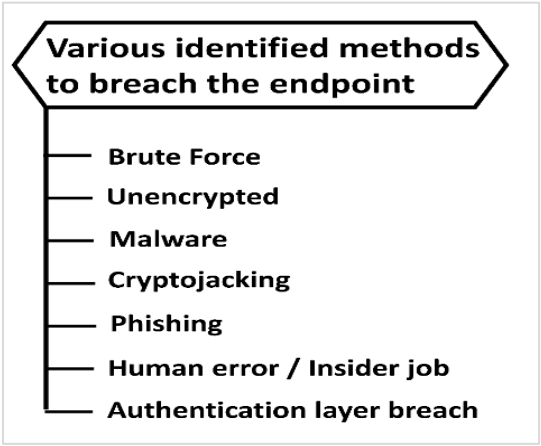

Figure 5 Various identified methods to breach the endpoint

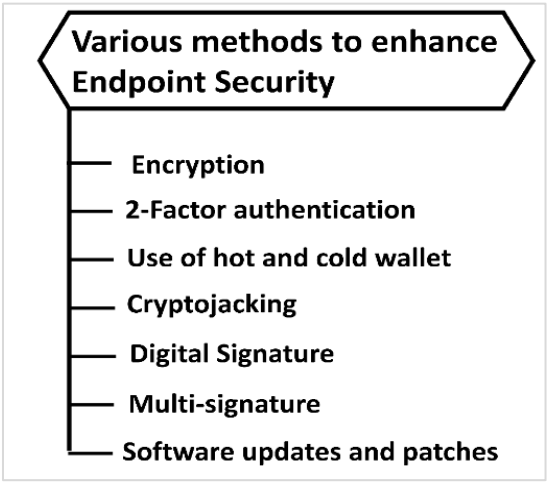

Figure 6 Various methods to enhance Endpoint Security

In fact, studies related to endpoint are very limited and terminology discussion is also very restricted and limited. Its mentioned or described within a few lines and in a generalized way by the researchers except the Lee's study [24] which was in systematic. Major approaches were survey/review/classification style without systematic in selected studies.

1.3.4Major current challenges

During the literature review, several research challenges were post by researchers in their studies. Lee [24] suggested the thin layer of authentication security. Levis [6] mentioned the lack of standard rules, parameter and policies. The technology is in its initial stages and has not developed fully yet, so,

most users don't trust on it [9]. In [24, 27] have investigated and reported various hacking and heist incidents targeting the endpoints of blockchain applications, leading to users losing their cryptocurrencies. Subsequently, [38, 40, 42] emphasized the importance of keeping endpoints secure and safe to prevent such unpleasant incidents. Rafi et al. [60] raised concerns about the security of wallet keys, control over wallets, and the potential for resource abuse by attackers. Conclusively, attackers try hard to the control over endpoint of the users to control the system, abuse the system, get the security get, steal the cryptocurrencies through phishing, cryptojacking, security breaches, bypass 2FA, and many more. The challenge is providing the security to minimize the underlying threat.

1.3.5Major current challenges faced by the researchers

- Blockchain is a complex technology, and it can be difficult to identify and understand all of the potential vulnerabilities.
- There are a limited number of researchers working on blockchain security, and they often lack the resources they need to conduct comprehensive research.
- As blockchain technology continues to develop, new threats are emerging, requiring researchers to constantly stay up-to-date on the latest security risks.
- The blockchain trilemma is a theoretical problem in blockchain technology that states that it is impossible to achieve all three properties (security, scalability, decentralization) at the same time.
- Blockchain applications are difficult to test and debug for security vulnerabilities.

1.3.6Research questions

R1.Are endpoint vulnerabilities a threat to the blockchain application/user?
R1.What specific factors cause endpoint vulnerabilities in blockchain applications?
R2.What are the root causes of existing endpoint vulnerabilities?
R3.Whether and how miners are related to endpoint vulnerabilities?
R4.What are the current research gaps in the endpoint vulnerabilities and their mitigation, particularly?
R5.What measures might be useful in mitigating endpoint vulnerabilities, resulting in improved security assurance?

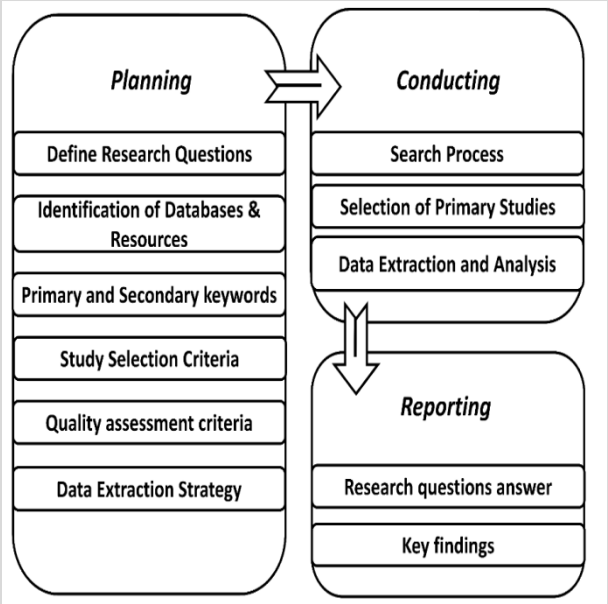

Figure 7 The SLR phases

2.Review methodology

Research methodology is the specific procedures or techniques accustomed to 'identifying, selecting, processing, and analysing' during the course of a study. A rigorous methodology lends the research validity and scientifically sound conclusions by keeping it on track with a clear strategy, making the approach seamless, effective, and manageable. To undertake the SLR methodically, the well-accepted guidelines suggested by Keele [61] for Software Engineering were adopted. *Figure 7* also depicts the same process.

2.1Study of the selection process

This study aims to search and figure out the related existing literature throughout the e-library, including IEEE, ACM, Science Direct etc. Which, in turn, lent the schema and scope of the research design during the pursuance of SLR, revealing the general strategic details as follows:
(a) Initially, 9159 papers were returned after executing search strategy, i.e., search string combinations of keywords. Later, filter out the papers based on title, abstract, and conclusion. Finally, to avoid confusion, read the paper thoroughly whether it is related/relevant or not.
(b) Further, process proceeded and selected 109 primary papers after filtering out all unrelated and duplicate papers.

(c) Finally, total 41 quality papers were selected based on quality assessment criteria and forward/backwards snowballing to acknowledge the research questions. *Figure 8 (a), (b)* and *(c)* depicts all the processes.

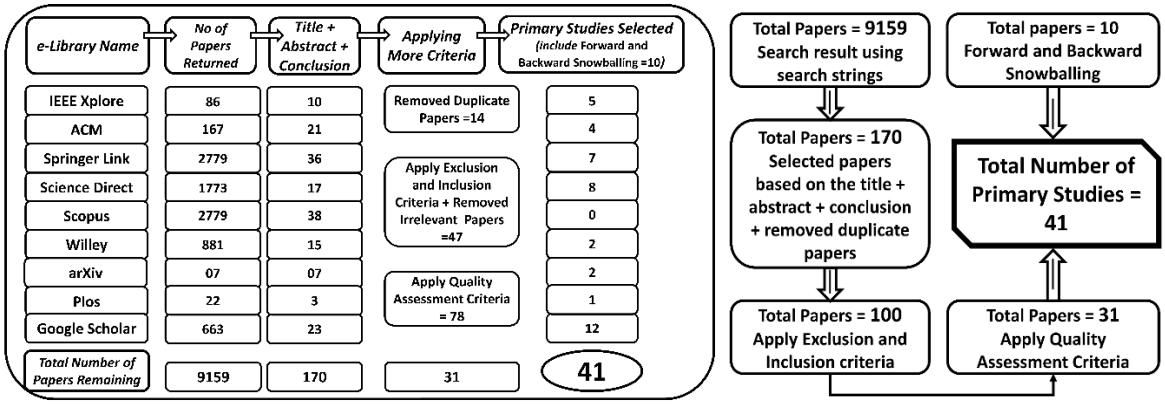

Figure 8 (a) Process of selection of studies

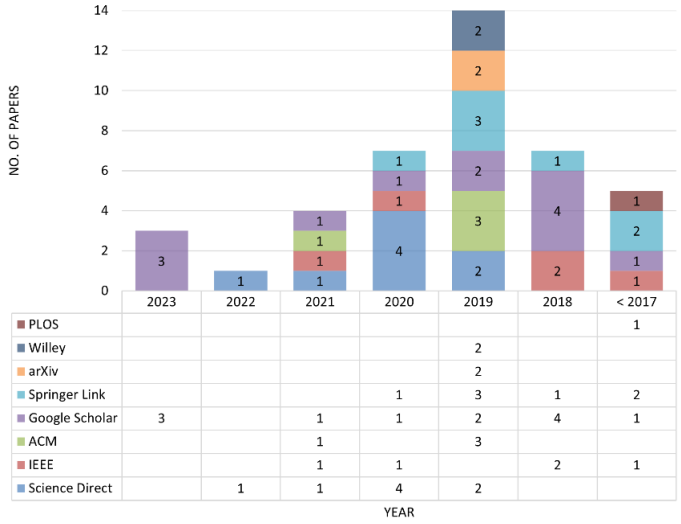

Figure 8 (b) Number of journal studies per year

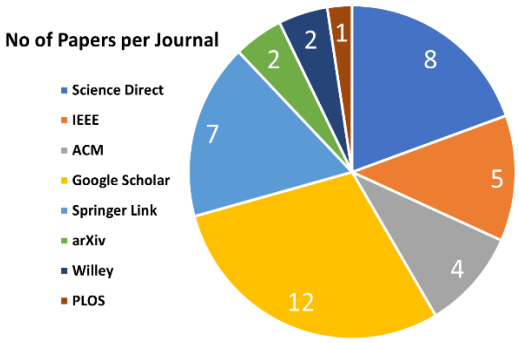

Figure 8 (c) No of papers per journal

2.2Selection of primary studies

Primarily, a synonym table (*Table 1*) was made for the title 'mitigating endpoint vulnerabilities in blockchain applications' by separating each word except the word 'Blockchain'. Word 'Blockchain' was fixed as the essential pivot and then conducted a search around it. The initial step was to search the primary and secondary keywords of the topic 'endpoint vulnerabilities in blockchain application'. Also, synonyms of the primary key were taken as the secondary keywords , as described in *Table 1*.

Table 1 The synonym table

Word	Synonyms
Mitigate	Reduce, Remove, Alleviate, Ease, Diminish, Decrease, Abate, Minimise, Minimize
Endpoint	Terminal, End-point
Vulnerability	Weakness, Exposure, Susceptible, Threat, Pitfall, Openness, Problem, Issue, Challenge, Threat
Application	Utilisation, Exercise, Practice, Usage, Function, Implementation, Operation

2.3Search strategy

The search strategy was divided into four parts S1, S2, S3 and S4. S1 is a string made up of keywords related to the main research topics such as 'reduce terminal weaknesses in blockchain application'. Every combination of the keywords were used by replacing them with their synonyms words and not adding any extra aid of 'OR' or 'AND' operators.

S2 is the string made up of keywords with the aid of OR & AND operator that gives a good number of papers. It made different strings with the use of operators. Each keyword returned a different set of papers, including a few common papers. While including the endpoint or its synonym word, it returned zero or a very less number of papers and these papers were irrelevant too. While searching, it was learnt that the number of keywords is inversely proportional to the number of papers. With the reduction of keywords, a greater number of papers were obtained. However, in search of getting some papers, the term 'vulnerability' was omitted. The same process was repeated with 'mitigate' and 'application' keywords to get some more papers. The search string was composed in the database manually based on the search functionality offered by the database.

S3 is the 'Level wise search'. In this method, firstly, keywords were searched and some papers were got, say set C1. Later, in C1, another keyword was searched to get more filtered papers. For instance, initially, keyword 'blockchain application' searched and 952 papers were got. Later, further restrictions with the word endpoint or terminal or vulnerability were added and even fewer papers were got.

S4 is the miscellaneous type string. It's like a free search where any keyword can be searched like 'Bitcoin vulnerabilities', 'Bitcoin Blockchain', 'Bitcoin wallet', 'Blockchain wallet', etc. *Figure 9* summarizes all the search strategies. *Figure 10* summarizes the searched platform and selection strategies.

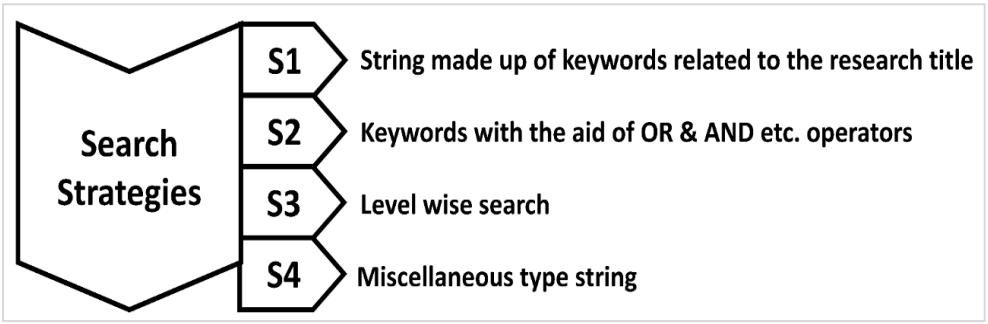

Figure 9 Search strategies summary

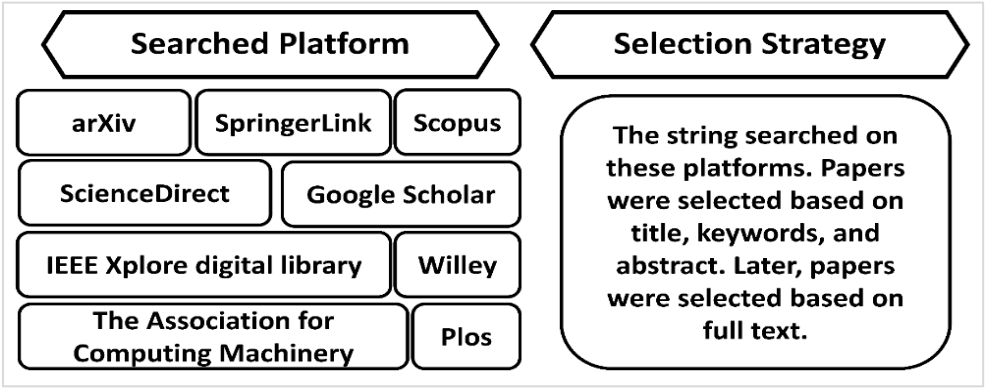

Figure 10 Searched platform with Selection strategies

Different permutation and combination with the search string were used using boolean operators AND and OR. Additionally, wildcards '?', '*' etc were used. The Wildcard '*' replaces or represents one or more characters. For example, *math** will match *math, maths, and mathematics*. The search strings were:

(mitigate OR minimise OR remove OR alleviate OR ease) AND (endpoint OR terminal) AND (vulnerability OR weakness OR issue OR challenge OR problem) AND (application OR usage OR practice OR Operation OR implementation OR function OR utilisation).

2.4Elimination of duplicate paper

While searching, manual precautions were taken to avoid duplicate documents. Since databases return a huge number of papers it was difficult to remember all selected papers by title. As a result, there may be some duplicate papers by false positives. To remove these papers, 'Easy Duplicate Finder' tool was used and manual checking was done to improve accuracy.

2.5Inclusion-exclusion criteria

Inclusion and exclusion criteria are used to define the scope of the systematic review and keep it on track. These are determined directly or indirectly by posing research questions. Conventionally, an SLR requires explicit inclusion and exclusion criteria to get valuable studies. Thus, the framed research questions encompass both criteria, as in *Figure 11*:-

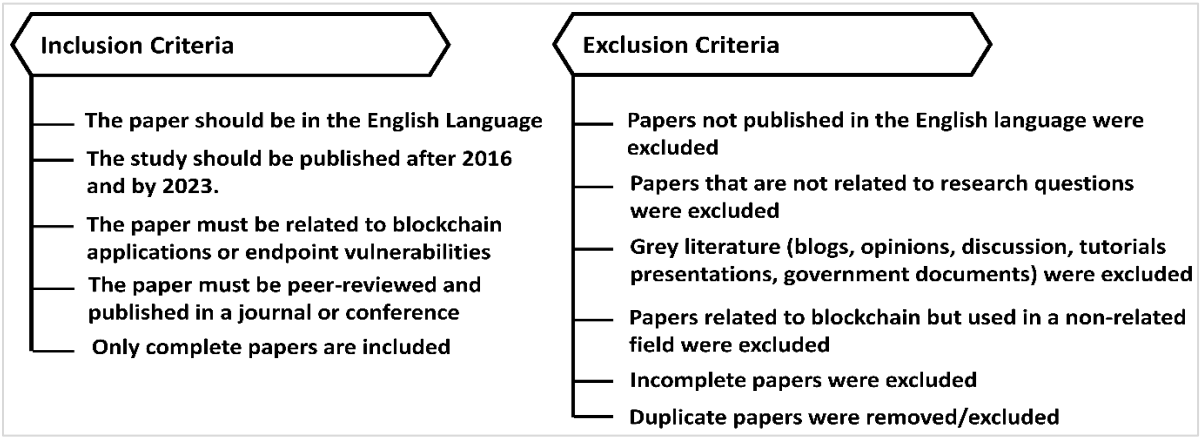

Figure 11 Inclusion and exclusion criteria

2.6Quality assessment criteria

Quality assessment is the final step in filtering the studies. It provides more quality control over the study than inclusion-exclusion criteria. It gives more relevant studies pertinent to the research questions [61]. It removes biases [60]. Some quality assessment tips are formulated to assess the selected studies' authenticity, credibility, and relevance, as in *Figure 12*.

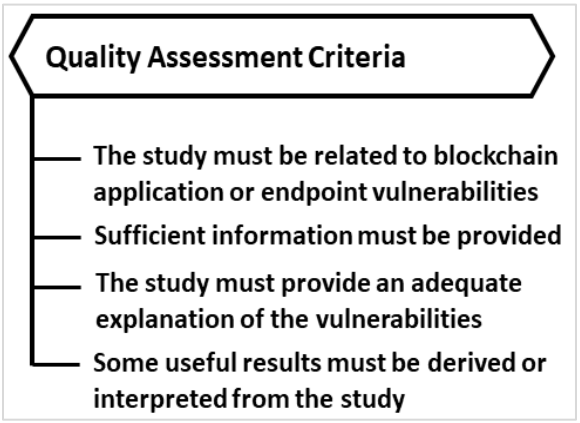

Figure 12 Quality assessment criteria

3.Literature review

Several recent studies were taken into account when searching for relevant articles. These studies are related to various blockchain research topics, but very few of them have touched on endpoint issues. Moreover, several studies touched on endpoints but they did not provide a concrete platform for endpoint issues. *Table 2* accumulates several literature review studies describing various aspects of blockchain. None of them focuses on endpoint issues except Guo and Yu [62] study. However, many of them describe private keys, wallets, and malicious code. On the basis of these attributes, 13 studies were selected for the final study out of the given 19 studies in *Table 2*.

Currently, barely any literature review exists on the endpoint. Therefore, most relevant literature review papers were selected and compared in *Table 2*. In *Table 2*, the tick mark (✓) indicates that the particular attribute has been discussed in detail or briefly. If an attribute was not discussed well or did not play a tiny role then the attribute in that particular study was not considered and marked it as (x).

These survey studies talk about blockchain technology's basic structure, concept, consensus and working. The discussion focused on the various shortcomings and attacks on blockchain technology and applications. Most of the studies lacked a systematic review. A trend was noticed that ECDSA were discussed with the breaches of private keys. Malicious code/keylogger is less discussed than other attributes. Moreover, In these studies, many security breaches and heists were mentioned. [24, 29, 48, 63] etc are the studies that discussed various challenges and issues of blockchain. Mt.Gox is the most discussed heist among them. Only [64] gave Intel software guard extensions (SGX) as the solution to mitigate endpoint vulnerabilities in the e-Health sector. Except for him, other researchers suggested mitigating it like Yli-Huumo et al. [65] suggests BlueWallet, Brengel and Rossow [66] suggest knowledge awareness, Pal et al. [67] suggests group key management (GKM) mechanism, Kiktenko et al. [68] suggest two methods against brute force attack on private key etc.

Table 2 Comparison among the most relevant literature reviews studies on blockchain and its challenges to show endpoint status

Serial No	Paper Title	Year	Basic Theory	Focus on attributes				Limitations	Other attributes
				Endpoint	Private Key	Wallet	Malicious code		
1.	A survey on blockchain technology and its security [62]	2022	comprehensive examination of consensus, smart contracts, cryptography, and research problems	✓	✓	✓	✓	Not a systematic review.	Quantum Computing, open-source distributed ledger (IOTA), Privacy-preserving, Supply chains
2.	Blockchain Security Attacks, Challenges, and Solutions for the Future Distributed IoT Network [69]	2021	- An analysis of potential security attacks with its countermeasures - Shed on open issues and blockchain-IoT system	x	✓	x	✓	Authors include different literature survey papers but left some important studies like Conti et al. paper [48].	Criminal activities through blockchain, Smart contract vulnerabilities
3.	A survey on the security of blockchain systems [70]	2020	Security issues of blockchain technology	x	✓	✓	x	No systematic review. No discussion of blockchain 3.0	Criminal activity, Vulnerability in smart contract, Oyente
4.	On the security risks of the blockchain [50]	2020	analysed 38 blockchain (categorized them into 7) incidents to determine the vulnerabilities	x	x	✓	✓	Brief information about category number 6.	Some security recommendations to reduce cyber security risks
5.	Security and Privacy on Blockchain [51]	2019	Overview of the security and privacy of blockchain with respect to properties and techniques	x	✓	✓	x	No Systematic Literature, e-library Database name missing	Consensus, UTXO
6.	The Blockchain: State-of-the-Art and Research Challenges [71]	2019	Focus on the integration of blockchain with IoT, cloud and data mining along with some applications	x	x	x	x	Lack of SLR, Brief introduction about many topics.	Healthcare, blockchain in 5G network
7.	A SLR of Blockchain cyber	2019	Blockchain solutions to enhance	x	x	x	✓	Limited to some e-library,	SLR, IoT, Data storage and sharing

Serial No	Paper Title	Year	Basic Theory	Focus on attributes				Limitations	Other attributes
				Endpoint Private Key		Wallet	Malicious code		
	security [49]		cybersecurity					Some more findings can be derived from paper studies.	
8.	A survey of blockchain from security perspective [29]	2019	Various blockchain vulnerabilities are classified into 8 groups	x	✓	✓	✓	Lack of systematic review, lack of literature work for many attacks	Privacy issues, Some blockchain challenges
9.	A survey on blockchain cybersecurity vulnerabilities and possible countermeasures [52]	2019	Vulnerabilities in Blockchain 1.0, 2.0 & 3.0 with possible countermeasures	x	✓	✓	x	Laconic information about some attacks and tools	Casper protocol, Tendermint
10.	Exploring the attack surface of blockchain- a systematic overview [12]	2019	Various Blockchain peer to peer attacks and blockchain applications attacks	x	x	✓	✓	No SLR	Private blockchain, Consensus
11.	A SLR of blockchain-based applications: current status, classification and open issues [72]	2019	Various applications of blockchain and its challenges/issues	x	✓	x	x	Less information about many latest technologies. The selection and analysis of studies took up a lot of space.	Big Data, Artificial Intelligence, Systematic review
12.	A Survey of Blockchain Frameworks and Applications [73]	2018	Blockchain frameworks for IoT, academic, healthcare etc	x	x	x	x	Need some more research on blockchain frameworks	Blockchain applications and challenges
13.	Cryptocurrency in Digital Wallet: Pros and Cons [74]	2018	Pros and Cons of cryptocurrencies with some statistics	x	x	✓	x	Selected a few cryptocurrencies for the study.	Decision-making scheme for investment
14.	Consensus Algorithms in Blockchain: Comparative Analysis, Challenges and Opportunities [75]	2018	Different consensus algorithm	x	x	x	✓	No SLR, Lack of experiment	Bitcoin, Sharding, Byzantine
15.	Blockchain Challenges and Security Schemes: A Survey [76]	2018	Blockchain application, consensus and types	x	x	x	x	No Quality. Very general information.	Smart Contract
16.	On Blockchain Security and Relevant Attacks [77]	2018	DLT security challenges like mining pools, wallet, DDoS etc	x	x	✓	✓	No systematic review, a lack of related literature	Smart Contract, Lightweight client
17.	A survey on	2018	A plethora of attacks	x	✓	✓	x	- No systematic	The adverse effect

Serial No	Paper Title	Year	Basic Theory	Focus on attributes				Limitations	Other attributes
				Endpoint	Private Key	Wallet	Malicious code		
	security and privacy issues of bitcoin [48]		on bitcoin are mentioned					review. - Discussed several attacks but Endpoint vulnerability is missing.	of major attacks and misbehaviour attacks.
18.	Blockchain-bitcoin wallet cryptography security, challenges and countermeasures [28]	2017	Focus on each aspect of bitcoin wallet	x	✓	✓	x	Some easy spelling mistakes. Categorization of different wallets	Anonymity attack, ECDSA
19.	Where Is Current Research on Blockchain Technology? —A Systematic Review [65]	2016	Literature review on the security and privacy of blockchain	x	✓	✓	x	Need research on endpoint or wallet. Absence of privacy techniques	Blockchain Botnet networks, Usability

Abbreviation used in Table 2: ✓= Mentioned and considered, ✗= Not mentioned and not considered

From *Table 2*, it is acknowledged that the endpoint was discussed only once in these respective survey studies. The selected studies shows most of the e-libraries are not covered. Many studies are lack of systematic review. However, other attributes related to an endpoint like private key, wallet and malicious code were discussed 10, 12 and 8 times respectively, out of 19 studies (*Figure 13).* It can easily be observed that the endpoint was touched in these reviews rarely. In a report, MtGox (2643 BTC) [54, 78], Bitfloor (24000 BTC) [62], Picostocks (6000 BTC) [58], Bitstamp (19000 BTC) [24], BTER (7170 BTC) [78] etc. and many more such incidents are the losses due to the endpoint breaches. As a result, it demands rigorous work and attention to mitigate the endpoint problem in blockchain applications.

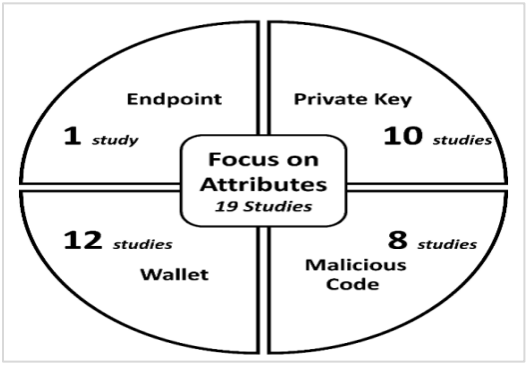

Figure 13 No of discussion of attributes in selected survey papers

To validate the findings regarding the lack of research papers, a tool VOSviewer [79] was used which is a software tool used for creating and visualizing bibliometric maps and networks. It used the references as input and constructed three maps. *Figure14* is the cooccurrences map based on text data and it shows the very less emphasis is given on the endpoint security. Similarly, *Figure 15* and *Figure 16* are the co-authorship map that shows few authors have discussed it very briefly.

Table 3 is the analysis of all final selected studies 41 with their title, basic concept, endpoint discussion, other topics than basic theory and limitations in terms of the endpoint. 8 out of 41 studies, though insufficiently, noted endpoint vulnerabilities. Only one study, i.e. done by Guo and Yu [62], has described the endpoint well. Finally, there exist only seven studies that touched the endpoint issues. The rest are selected studies through quality assessment criteria. Some studies do not qualify for all quality assessment criteria but are selected because of the interpretation of important results. From the study of *Table 3*, it can be stated that a SLR on endpoint vulnerabilities is lacking and no countermeasures exist or have been revealed now. More than 1/3 of the studies focused on the wallet and related concepts, smart contracts and blockchain general problems like scaling, throughput, various attacks and malleability attacks. About 20% studies discuss about quantum, ECDSA and weak randomness explicitly. Some of

the papers discussed criminal activities, Oyente, IOTA, open-source intelligence platform (OSINT) etc. However, about half of the studies discuss general issues of blockchain and smart contracts such as scalability, throughput, various attacks.

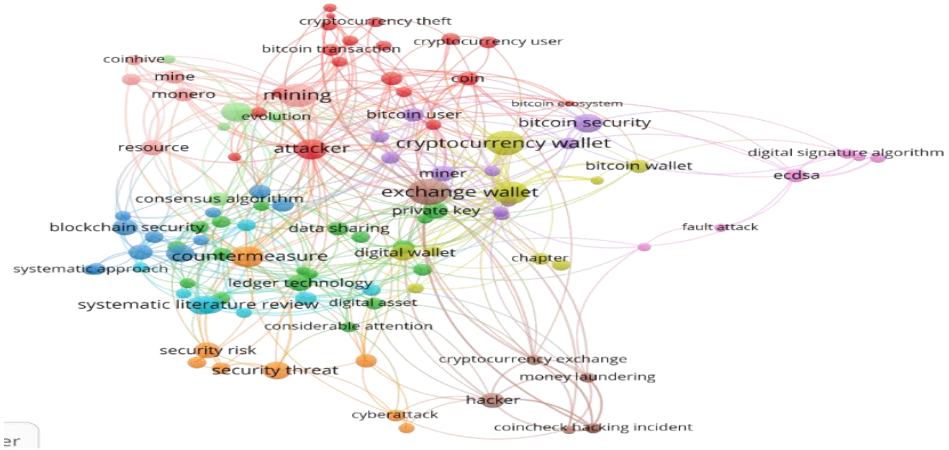

Figure 14 Co-occurrence map based on text data [Minimum occurrence 3], 20 linked clusters

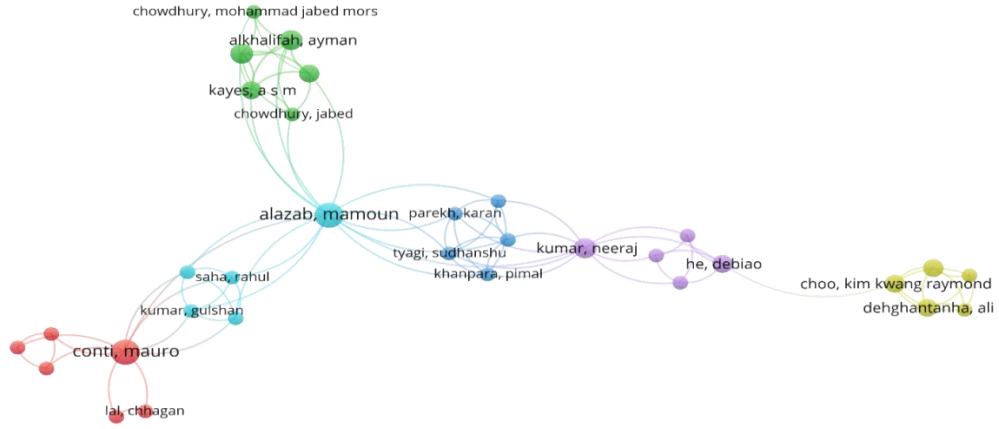

Figure 15 Co-authorship map based on bibliographic data [Minimum no of documents per author -2], 6 linked clusters

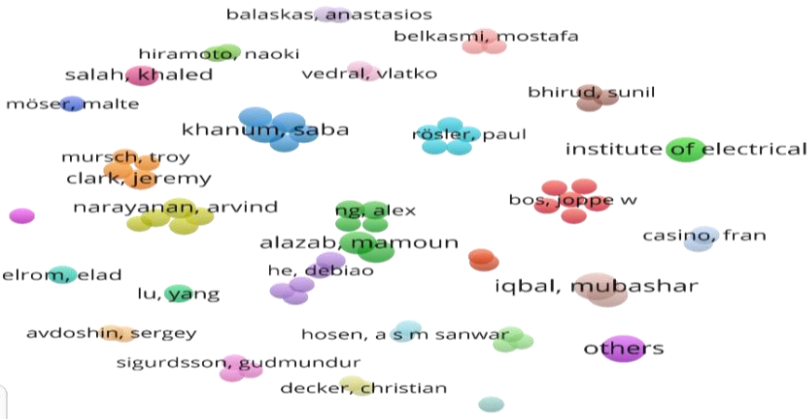

Figure 16 Co-authorship map based on bibliographic data [Minimum no of documents per author -3], 28 broken clusters

Table 3 An intense analysis of selected studies through quality assessment criteria. In addition, it points to endpoint discussion and comments on studies in terms of endpoint limitations

Serial No	Paper title & reference	Year	Basic Theory	Discuss on Endpoint	Other Attributes	Limitations in term of endpoint
S1.	A Survey on Blockchain Technology Concepts, Applications and Security [32]	2023	General introduction of blockchain and limited discussion of various security issues	Yes	Consensus algorithm and cryptography	Only few lines were mentioned. Lacking detailed discussion
S2.	Protocols and Guidelines to Enhance the Endpoint Security of Blockchain at User's End [2]	2023	Guidelines and protocols to secure the endpoint.	Yes	Attacks due to insecure endpoint and user unawareness	Lack of framework and implementation
S3.	Blockchain Technology: Security Issues, Healthcare Applications, Challenges and Future Trends [80]	2023	Blockchain and healthcare security issues are elaborated	Yes	Security risk at each layer of the blockchain architectural layers	Lacking details about endpoint
S4.	A survey on blockchain technology and its security [62]	2022	comprehensive examination of consensus, smart contracts, cryptography, and research problems	Yes	Quantum Computing, IOTA, Privacy preserving, Supply chains	……
S5.	Blockchain Security Attacks, Challenges, and Solutions for the Future Distributed IoT Network [69]	2021	- Inscribe security attacks with countermeasures and enhancement - discusses IoT related issues and challenges.	No	Criminal activities, Security tools	None of them addressing endpoint directly
S6.	Blockchain Vulnerabilities in Practice [81]	2021	Core blockchain and Smart contract vulnerabilities	No	Cryptocurrency exchanges	Lacking details about wallet
S7.	Facing the Blockchain Endpoint Vulnerability, an SGX-based Solution for Secure eHealth Auditing [64]	2021	Endpoint vulnerability solution through Intel SGX	No	Trusted Execution Environment(TEE)	---
S8.	Key management for blockchain technology [67]	2021	Key management for blockchain wallet	No	Bitcoin wallet types	---
S9.	A SLR of Blockchain cyber security [49]	2020	Impact of blockchain technology on cyber security in each aspect	No	Blockchain in IoT security, Sidechain	Wallet breaches rarely addressed
S10.	On the security risks of the blockchain [50]	2020	Six major blockchain incidents root causes and preventions	No	Some security recommendations to reduce cyber security risks	Lacks clarification on Wallet
S11.	The Disruptive Blockchain Security Threats and threat categorization [51]	2020	49 major security threats are categorised into six headings	No	Language and Quantum related threats	Any solutions or suggestions is missing.
S12.	Vulnerabilities and security breaches in cryptocurrencies [82]	2020	Cryptocurrencies vulnerabilities and related security cracks	No	Social Engineering, DAO	Lacking on any suggestions or solutions
S13.	ECDSA weak randomness in bitcon[83]	2020	An investigation of weak randomness in ECDSA	No	Bitcoin wallets, RFC 6979	---
S14.	A decentralised approach to privacy preserving trajectory mining [84]	2020	Trajectory data can reveal the sensitive information about users	No	Trajectory data mining	Absence of relation of trajectory data with endpoint

Serial No	Paper title & reference	Year	Basic Theory	Discuss on Endpoint	Other Attributes	Limitations in term of endpoint
S15.	A survey on the security of blockchain systems [70]	2020	Security issues of blockchain technology	No	Criminal activities, Vulnerabilities in smart contract, Oyente	Limited details on private key security
S16.	Risks and opportunities of blockchain based on e-voting Systems [42]	2019	Highlight risks and opportunities in e-voting system based blockchain	Yes	TEE, Biometric, Sharding, Lightning network	No detailed information about malware and keylogger
S17.	Systematic Approach to Analyzing Security and Vulnerabilities of Blockchain Systems [24]	2019	An intense investigation and study of blockchain vulnerabilities	Yes	Heists case study, threat modelling	---
S18.	A survey of blockchain from security perspective [29]	2019	Blockchain security threats	No	Malware attack, privacy, quantum threat, bigdata	Insufficient literature coverage
S19.	Blockchain private key storage algorithm based on image information hiding [85]	2019	Use of image steganography to hide security keys	No	Watermark embedding	Missing consideration of different image formats
S20.	Exploratory analysis of block chain security vulnerabilities [86]	2019	Different blockchain platforms and vulnerabilities	Yes	Smart contract	Lacking details about endpoint and wallet theft
S21.	Private key encryption and recovery in blockchain [87]	2019	Use of biometric to secure private key	No	Fingerprint, Reed-Solomon Error Correction	---
S22.	Research challenges and opportunities in blockchain and cryptocurrencies [88]	2019	The research challenges in blockchain and its applications	No	Scalability, privacy, security, consensus	Limited to hardware and paper wallet
S23.	Exploring the attack surface of blockchain- a systematic overview [12]	2019	Various attacks and security of blockchain	No	Web cryptojacking, DDoS, ECDSA	Lacking details on wallet theft
S24.	Detecting brute force attacks on cryptocurrency wallet [68]	2019	Brute force attack on bitcoin wallet	No	Smart contract, collision detection	Absence of related work
S25.	Pitfalls of open architecture-how friends can exploit your cryptocurrency wallet [89]	2019	Security of RPC interface of wallets	No	Defence mechanisms	No experimental work
S26.	Security and privacy on blockchain [51]	2019	A Comprehensive review of the security and privacy of blockchain	No	UTXO, CAP properties, security and privacy techniques	TEE based smart contract is limited
S27.	A survey on blockchain cybersecurity vulnerabilities and possible countermeasures [52]	2019	Blockchain 1.0, 2.0 and 3.0 vulnerabilities with countermeasures	No	Major attacks on blockchain using POW & PoS, ECDSA	Lacking on Wallet solutions
S28.	A SLR of blockchain-based applications: current status, classification and open issues [72]	2019	Systematic review of blockchain applications and issues	No	Supply chain management, healthcare management, voting	Lacking emphasis on countermeasures
S29.	A survey on privacy protection in blockchain system[90]	2019	Review the privacy issues and cryptographic protection	No	Anonymity, Privacy, Cryptography	Fails to link privacy leakage with endpoint

Serial No	Paper title & reference	Year	Basic Theory	Discuss on Endpoint	Other Attributes	Limitations in term of endpoint
S30.	Blockchain Technology: a new domain for Cyber Forensics [44]	2018	Systematic study about the vulnerabilities of blockchain system	Yes	Forensic aspect of blockchain	Lacking explanation
S31.	A survey on security and privacy issues of bitcoin [48]	2018	Overview on security and privacy of Bitcoin	No	Client-side security threat. anonymity	Missing endpoint vulnerabilities
S32.	Identifying key leakage of Bitcoin users [66]	2018	Explicit and implicit key leakage of bitcoin	No	OSINT, ECDSA	---
S33.	Blockchain - future of decentralized systems [45]	2018	Overview of blockchain	Yes	Steem, security issues	Absence of literature work for endpoint vulnerability
S34.	Mcafee blockchain threat report [91]	2018	Cover security problems, incidents and techniques used for attacks in blockchain	Yes	Phishing, Malware, Endpoint miners	---
S35.	Security threats classification in blockchains [92]	2018	systematic survey of the security threats and reviewed the existing vulnerabilities in the Blockchain	No	Wallet threats, Security thread taxonomies	---
S36.	A blockchain-based public key infrastructure (PKI) management framework [93]	2018	Design and develop a blockchain based PKI management framework	No	Smart contract, certificate authorities (CA)	---
S37.	Chainguard — a firewall for blockchain applications using SDN with OpenFlow [94]	2017	A firewall for blockchain to enhance security	No	SDN, node	---
S38.	Blockchain-bitcoin wallet cryptography security, challenges and countermeasures [28]	2017	Security of bitcoin system and mitigations to enhance security	No	Wallet theft, client-side attacks	---
S39.	The Bitcoin Brain Drain: Examining the Use and Abuse of Bitcoin Brain Wallets [95]	2016	Use of brain wallets in bitcoin	No	Brain wallet	---
S40.	Where is current research on blockchain technology? -a systematic review [65]	2016	Blockchain technology recent gaps study	No	Scalability, privacy, usability Botnet networks	Missing details on endpoint exploitation
S41.	Bitcoin transaction malleability and Mt. Gox [96]	2014	Malleability attack	No	ECDSA, Mt. Gox	N.A.

From *Table 3*, the major issues that an endpoint is suffering from are cryptojacking, ECDSA, private keys, wallets and user lazy behaviour. These are the some factors that are troubling users more. The authors described the role of weak randomness of ECDSA in private keys revealing. Also, they claimed quantum computing is an emerging threat to blockchain Technology/ private keys. Compared to quantum, the Brute force method is a classical and time-consuming method. But, many attacks have been done by brute force method. Thus, Blockchain technology is still susceptible and not immune to breaches, but being decentralized gives blockchain a better line of defence. These studies share various suggestions/ solutions, including 2FA, multi-sig, hardware wallet, etc. TEE was suggested as a solution by Zhang et al. [51] and Abuidris et al. [42]. Other possible solutions discussed are biometric [42], request for comments (RFC) 6979 [83] and steganography [85].

4.Revisiting the research question-analysis and discussion

This SLR on the topic reveals several trends and indications and throws light on the research questions. The most general comment appears in the form that 'there is a lack of an adequate set of focused studies on mitigation of endpoint vulnerabilities and the field stills remain to be well attended'. Moreover, apropos of the review, a brief, summative and interpretative response appears imminent as follows.

R1.Are endpoint vulnerabilities a threat to the blockchain application/user?

Blockchain technology is widely accepted and adopted across the globe in all basic applications, whether financial or non-financial, due to its salient characteristics. The blockchain features to facilitate a number of tremendous outcomes such as inflation control, double spending avoidance, ensuring decentralization, low fee transactions across the globe, etc. Blockchain has plenty of use cases. However, it suffers due to its limitations. These include scalability, high power consumption, not fully secure, still not mature, etc. One such vulnerability that arises at the end-user is called an endpoint vulnerability.

Initially, the endpoint was compromised when one of the MtGox auditor systems was compromised. MtGox claimed that the core wallet was not encrypted. This case was named system compromised. Later, users witnessed other crypto hacks such as Bitfloor, input.io, Bitpay, Localbitcoins, Bitfinex etc. These hacks were targeted through interface access, phishing email, structured query language (SQL) injections etc. But none of the experts called it endpoint exploitation. Lee [24] collected all blockchain incidents and termed them as an endpoint domain. He also added the endpoint includes terminals, computers and mobile devices and these are the devices through which a user interacts with blockchain services and usage. Attackers target these devices to steal sensitive information. They use various techniques malware attacks, cross-site scripting, forgery attacks etc. During the same time period Raziel [47], Strom [97] and Martin [43] also tried to explain the endpoint vulnerability and its causes.

Zamani et al. [50] explore and analyze 38 blockchain incidents. Out of those, they review six incidents in detail. Half of them were related to server or application-based. Dasgupta et al. [29] explain the weakest link in the blockchain is third-party applications like exchanges, wallets, and dApps. Later on, Shrivas et al. [63] categorised blockchain threats into six categories and mentioned 'endpoint vulnerabilities' in their categorization. Guo and Yu [62] extended all earlier work on endpoint vulnerabilities by describing its types as: 51% vulnerability, Sybil attacks, personal key security, mining malware, and cryptojacking Attacks. *Figure 17* shows a brief timeline of the above discussion.

Consequently, the users suffered and lost crypto coins and sensitive information due to endpoint breaches. Besides this, the problem of private key management in blockchain applications is still unresolved. According to general data protection regulation (GDPR), blockchain lacks in maintaining the end user's privacy. Finally, all this evidence proves endpoint vulnerability is a threat and needs to be addressed properly with some mitigation techniques.

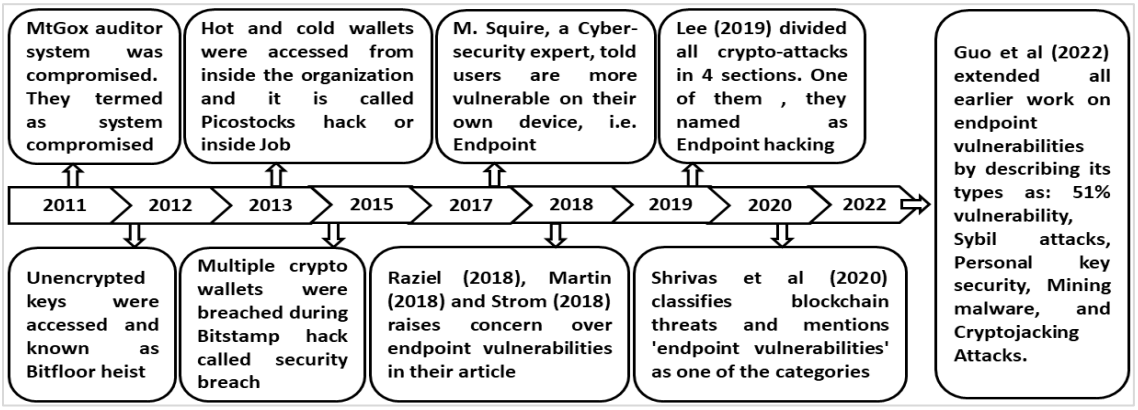

Figure 17 A Timeline of endpoint vulnerabilities

R2:What are the root causes of the existing endpoint vulnerabilities?

In the case of endpoint vulnerabilities in blockchain, this study shows various root factors that cause crypto-loss, wallet loss, control loss etc while using blockchain applications.

Thin security layer

Generally, a user interacts with blockchain in three ways, including '3rd party exchange, dApps and online web-based services'. These ways have a thin layer of authentication [24, 89]. There is a lack of extra data security or security controls. If an invader breaches this thin layer of authentication, there is no data safety mechanism. The security layers in blockchain-based decentralized architecture are not defined clearly and fail to provide enough security, making an increment in the number of attack and exploitation attempts (*Table 4*). It makes the system more vulnerable and is likely to become a victim of cyberattacks [24]. Blockchain is a decentralised technology whose security mechanism is entirely different from a distributed or centralised system [98, 99]. The centralised system has a firewall, an intrusion detection system, and network monitoring. In contrast, decentralised technology does not have such a security layer, which makes it more vulnerable and can be easily exploited if an invader invades the authentication process [24].

Table 4 List of some attacks at security layer

Incident name	Date	Amount	Equivalent amount ($)	Reason	Description
Inputs.io	Oct 2013	4100 BTC	813,891	Security Breach	Using a very old email address, a hacker hacked the hosting account. Then, bypassed 2FA due to a server host side flaw
Bitsmap	Jan 2015	19,000 BTC	5,200,000	Security Breach	The attackers gained access to two servers belonging to Hot Wallet and the password file of Bitstamp's account
Bitfinex	Aug 2016	119756 BTC	72,000,000	Security Breach	Hackers stole BTC. Hacker was able to exploit the Bitfinex system and obtain a private key of Bitgo API. Then attacker broke the multi-sig function of Bitgo's authentication
2gether	July 2020	--	1390000	Security Breach	Hackers compromised 2gether's servers. So, user passwords have been compromised.
Crypto. com	Jan 2022	4,836.26 ETH+ 43.93 BTC	34000000	Security Breach	Initially, the company said no coin loss but finally confirmed that the attacker stole cryptocurrencies. The attacker bypassed 2FA authentication to approve the transaction

Users' unusual behaviour

Another reason is the lazy behaviour of users that opens the gate for invaders [80]. Brengel & Rossow [66] explain that most users use Pastebin for personal use and are unaware that its entries are publicly available. On this platform, many users share crypto-coin-related sensitive information intentionally or unintentionally. When cryptojacking [62] happens with a system for mining the coin or stealing private keys, the users are ignorantly caught 'unaware of recognizing, detecting, or avoiding' it. So, they become victims very quickly (*Table 5*). The users' unusual behaviour and activity generally reveal the privacy, internet protocol (IP) addresses, and much sensitive information loopholes that an invader badly needs to break the system security [84].

Table 5 List of some attacks due to user's unawareness

Incident name	Date	Amount	Equivalent amount ($)	Reason	Description
Bitfloor	Sept 2012	24,000 BTC	250,000	Unencrypted wallet keys	Bitfloor servers were hacked to obtain unencrypted backups of wallet keys
Picostocks	Nov 2013	6000 BTC	5,681,520	Human Error/ Insider Job	The attacker transferred funds from the company's hot and cold wallets by accessing the non-terminated and dormant private key
BTER	Aug 2015	7,170 BTC	1,750,000	Human error/ insider	Attackers access the private key from a cold wallet
Bithumb (1st)	July 2017	340 BTC	870,000	Human error and Brute force	Hackers hacked customer data, including their names, mobile phone numbers, and email addresses. Then they launched a brute

Incident name	Date	Amount	Equivalent amount ($)	Reason	Description
					force attack with voice phishing.
CASHAA	July 2020	336+ BTC	3000000	Human error	Cashaa assumes that malware was inserted into the employee's laptop

ECDSA weak randomness

Bitcoin's private key heavily depends on ECDSA to sign and validate the user. ECDSA used in Bitcoin serves as a digital signature authenticator for signing transactions. Secp256k1 128 bits define standard for efficiency cryptography (SEC) that refers to ECDSA parameters of the curve used in Bitcoin [51]. The elliptic curve secp256k1 has a 256-bit private key and is based on the Koblitz curve. The Koblitz curve [100] is an elliptic curve that is not considered standard. As a result, it can be regarded as less secure [28]. Sometimes faulty use of ECDSA creates a weakness in a wallet that make private key susceptible [28,101]. Mt. Gox was breached by an attacker that cost $450 million [66]. This attack was possible due to poor security shields and mismanagement. As a result, the attacker accessed the private key stored in an online wallet. Decker and Wattenhofer [96] explained Mt Gox defraud more clearly. It was done through a Malleability attack where signature authenticity and ownership were changed. This process was derived from ECDSA.

As it is known, a nonce value is used with a private key to generate the signature. The nonce value must differ for each signature generation [102]. Due to insufficient randomness in ECDSA, the report found that there was 158 such public address that used a nonce for more than one sign generation [48]. Wang et al. [83] analysed bitcoin transactions from the start date to July 2017. They noticed 0.48 per cent of transactions involve the reuse of nonce more than once. Consequently, 1331 private keys were revealed. They added another flaw: some addresses have a common pattern in their transactions, which attackers could exploit. In fact, the ECDSA weak randomness problem originated in 2013. At that time, it was addressed but not completely. Still, user experience the ECDSA weak randomness problem very often. Because of observing the pattern, it is predicted that the user may experience the same problem in the future. Analysis over it shows an awful pattern: the number of ECDSA reuse nonce values in transactions increases over time [66, 70, 83]. Wuille [103] identifies many ways to modify the signature and then exploit malleability attacks in his bitcoin improvement proposal (BIP). Some of them are ECDSA signature malleability; only data pushes are permitted in scriptSig, Inherent ECDSA signature malleability etc.

RFC 6979 proposed to use the output of HMAC-SHA256(private_key, message) instead of the random data, which eliminates the risk. Therefore, an update of RFC 6979 is necessary. RFC 6979 plays a vital role in Bitcoin wallet security. Since Bitcoin is decentralized in nature, it is difficult to follow the update by all Bitcoin users and developers [83,104]. Also, Mollajafari talks about two preventive techniques for weak randomness but remains an issue that can lead to centralisation risks [105]. Interested users can refer to the work of Ulla and Sakkari on ECDSA [106] for more knowledge.

It is also acknowledged that computer, mobile device, cross-site scripting attacks, cryptojacking, inadequate security, computer noob, wallet exposure [107], storing blockchain keys in a word or text or unencrypted way [45], using general email instead of using email feature of blockchain wallet for sharing either keys, human lazy behaviour on the internet, user's unawareness of the keys' security [42] are some main reasons that cause the endpoint vulnerability [46] (*Figure 18*). Businesses that allow employees to bring your own devices (BYOD), laptops, or smartphones to work often face endpoint security issues. There are numerous reasons for endpoint device compromise. Everything is possible, from a Brute Force attack to user laziness.

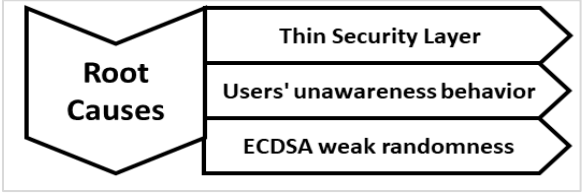

Figure 18 A summary of root causes of endpoint vulnerabilities

R3:What specific factors cause endpoint vulnerabilities in blockchain applications?

Initially, blockchain was considered a revolutionary technology due to its immutability, cryptography mechanism and other characteristics. However, the 51% attack was mentioned by Satoshi itself, which makes blockchain susceptible. The reward halving

structure, biasing in the distribution of transaction fees, blockchain low throughput, blockchain difficulty readjustment after every 2016 blocks are some important flaws that leave the world ununanswered. These factors are the invitation of the hacking and attackers/miners taking advantage of them. Critically analysing endpoint attacks found that wallet and exchange attacks were the the most common attacks due to private key infrastructure.

Public-private keys

Taylor et al. [49] find data privacy and public key infrastructure (PKI) are the 4th most common theme in the attack. Pal et al. [67] showed that keys could be tracked by several attacks (like side channel, replay), physical access to the system, weak encryption and brute force. To make things easier, Brengel and Rossow [66] divided the key leakage as explicit and implicit. The explicit key leakage happens on an OSINT where an attacker scans publicly available information and finds out sensitive data. To experience this, they chose Pastebin as OSINT, where users accidentally shared crypto-coin-related sensitive information and were unaware that Pastebin entries were publicly visible. The researchers identified 21,464 secret keys that makeup 42,936 addresses. However, most of them were unused. They conclude that those addresses hold 327 BTC. In contrast, explicit leakage defines the wrong usage of cryptographic primitives and the reusing of a nonce value.

Another study by Pal et al. [67] indicates that the keys can be exposed via replay attack, side channel, weak encryption, brute force, and so on. In their study, Patel et al. [45] suggested using such private keys that are very hard to brute force [108]. Kiktenko et al. [68] successfully considered the Brute Force attack on Private keys with a probability close to 1. They also suggested two methods for dealing with potential brute-force attacks. The first method suggests amending the current consensus and freezing the stolen transfer funds. The second method suggests creating a special reward transaction. Patel et al. [45] suggest that users should use anti-malware to check for any unknown or unintentional program or script that monitors user activities. Pal et al. [67] suggest the GKM mechanism to minimise the breach's possibility.

The user has started different services and techniques to protect the wallet from attackers. Multisig [109] is one of them. They used parity multisig to save their wallet but the attacker cracked it in 2017 and stole 150000 ethers [64]. Interestingly, experts are concerned over the security of the private key of blockchain; Yakubov et al. [93] developed a blockchain-based framework to manage the PKI as a solution to avoid breaches of certificate authorities (CA).

Phishing

Phishing is a way of social engineering to get users' sensitive information, including users' names, private keys, passwords etc [110,111]. The most common methods are Fake Airdrops and Punycode. In the latter method, the attacker sends an email to the users that links with a fraudulent or fake website that looks completely the same as the official website but with a different web address like facebook.com and facébook.com [80]. The former method is another way of phishing that emerges alongside the explosion of cryptocurrency/ NFT popularity. It makes users fraudulently share their sensitive and personal information by email or on social media [112]. *Table 6* lists some phishing attacks at the endpoint.

To solve this, several solutions have been proposed to mitigate the risk of breaches. The notable proposals include using the cold wallet to keep private keys safe [55,113], mounting hardware security modules to shield the hot wallet, introducing multiple-signature concepts [59] etc. These measures were a success but partially. As a result, users witnessed BTER heist [78], parity multisig wallet attack [52] etc.

Table 6 List of some Phishing attacks at the endpoint

Incident name	Date	Amount	Equivalent amount ($)	Reason	Description
Bitcash .cz	Nov 2013	485 BTC	1000,000	Phishing email	Web interface/ system compromised.
Bitpay	Dec 2014	5000 BTC	1,800,000.	Phishing Attack	The attacker sent spoofed emails from Bitpay's Chief Financial Officer (CFO) to the Chief Executive Officer (CEO) asking for 5000 BTC in three separate transactions.
Local Bitcoins	Jan 2015	17 BTC	5,336.	Phishing	The attacker injected a key logger through a live chat program
IOTA	Jan		3940000	Phishing + malware	A phishing attack to gather the client's private

Incident name	Date	Amount	Equivalent amount ($)	Reason	Description
	2019				key
Axie Infinity	Mar 2022		620000000	Phishing	The attacker successfully executed social engineering attack on Axie Infinity

Cryptojacking

Cryptojacking attack is an endpoint attack [114]. Currently, many cryptojacking tools exist and hackers prefer to use browser-based cryptojacking [29]. In 2017, a cryptojacking was a plugin in the Chrome browser to mine the Monero coins without the user's consent. The cryptocurrency mining service Coinhive is one of the biggest dangers for Monero as it is the most popular platform for cryptojacking [115]. This issue can be identified with reading/monitoring of high central processing unit (CPU) usage [91].

In Jan 2011, a malware Infostealer.Coinbit, known as Coinbit, was discovered to steal users' Bitcoin wallets [28]. This trojan attracts Windows users to use it [116]. The trojan scans the Bitcoin wallet and emails it to the attacker during running conditions. This trojan and other such malicious programs are reported in the crypto world. Saad et al. [12] explain the cryptojacking process in a more convenient and detailed way. PoW requires a high processor to solve a difficult puzzle, including finding a target hash value. As the aggregate hash power of mining increases, the associated possibility of mining a block also increases. To fulfil the difficulty requirements, dedicated hardware, like graphics processing unit (GPUs) and application-specific integrated circuit (ASIC) chips, is used by miners [117]. The mining pool increases its hash power by inviting other miners to join their pool and share the resources [118]. Saad et al. [12] also elucidate that the attackers inject malicious JavaScipt code into the web browser. When a user use browser, it executes JavaScipt code that set-up a WebSocket connection with a remote dropzone server. Dropzone [119] is a lightweight javascript library that turns any hypertext markup language (HTML) element into a dropzone. It means a user can drag and drop a file onto the area of the page, uploading it to a server. The server then sends puzzles to the user. The user computes hashes for those puzzles and sends them back to the server.

After the Windows operating system, Mac was also attacked by DevilRobber trojan horse [28]. It spreaded its piracy copy and was enticing for the users [116]. Very often, when software packages are offered at no cost, some malicious programs are injected with them. Miner-D was embedded with a GraphicConverter tool, an editing program on Mac systems. It generates the counterfeit certificate of the wallet info. When a user does a transaction, the counterfeit wallet info is transferred to the receiver [120]. *Table 7* lists some malware attack.

Table 7 List of some malicious code attack

Incident name	Date	Amount	Equivalent amount ($)	Reason	Description
Allinvain	Jun 2011	25000	500,000	Malware	Not bitcoin service but a member of the forum. The first person to suffer crypto loss. Hackers compromised the windows computer and stole the bitcoins from his hard drive
Cryptsy	Jul 2014	13000 BTC	7500000	Malware	breached due to exploiting an intentionally placed backdoor in an open-source software dependency.
BTC-E (2^{nd})	Oct 2014	70000 BTC	26,000000	SQL injection	A SQL injection was injected.
Coincheck	Jan 2018	523,000,000 NEM	534,000,000	Virus	A hot wallet connected to the external internet was exploited via an email containing viruses because its endpoint security was not obligated with a cold wallet, 2-FA, smart contracts or multi-sig technology as recommended by the developers. To make matters worse, the organization kept all coins in the same hot wallet.

Wallet

A blockchain wallet is a digital wallet storing and managing Bitcoin, Ether, and other cryptocurrencies. It is a service provided by blockchain, which is a typical software for the ownership and exchange of cryptocurrencies rather than a tangible thing. It is a data file stored in the user's file system. Such Wallets store the public and private keys of the investors.

Both keys are used to perform transactions [89]. The public key is similar to a bank account number and is shareable with the recipients. The private key is identical to a bank pin code or signature that must keep secret and used to create a digital signature for the transaction [44]. The signature confirms the transaction has come from a particular user and ensures that the signature will be invalid if the transaction gets changed [28]. Mainly, there are two types of wallets: cold and hot [50].

Hot wallet

A software wallet is a hot wallet [50]. A hot wallet is an online tool that stores tokens or crypto coins and allows users to send and receive tokens. It needs an active internet connection to use the facilities [121]. Hot wallets are more user-friendly and provide an easy interface for online transactions. Because hot wallets are internet-connected, they are considered less secure and highly accessible [121] Consequently, they are more prone to security threats and attacks [29]. The protection and security of a hot wallet largely depend on the user's actions and behaviour.

Cold wallet

The cold wallet, also known as hardware or offline wallet, stores the user's address and private key and communicates with the computer's relevant software. These wallets cannot be hacked since they are not connected to the Internet and are considered safer than hot wallets [122]. Such wallets are used to hold crypto-tokens offline [123]. It protects from unauthorized access, cybercrime, and other possible threats. Offline crypto tokens are kept on a paper, hard disk, universal serial bus (USB), hardware wallet or offline computer [88]. As a result, transferring assets to a cold wallet is no longer an option; it is a need. It extends complete control and security over private keys and encryptions protects from third-party liabilities, making it the most secure solution for keeping crypto assets [113]. Apart from hot and cold, the wallets can be divided into custodial/ non- custodial, hardware/software/ paper wallets etc [124].

Erinle et al. has provided a detailed overview of signifiicant attacks and vulnerabilities on wallets and exchanges [125]. So, it is imperative to secure the crypto token online or offline. Once a crypto token is stolen, it will be lost forever [44]. The blockchain is independent of any third party, organization, centralized bank etc. So, if the user's private keys are compromised once, it cannot be restored or recovered [28]. It is difficult to track the attacker's behaviour or activities [70]. There is no dedicated organization or method to recover it. So, login credentials need to be kept very safe [82]. Hackers invest a good time in capturing the credentials that can be exposed through security fragility at the endpoint by the users [126].

To secure the endpoint, one needs to secure the wallet [62]. The increase in popularity of Bitcoin encourages Hackers to steal wallet information through various mechanisms like system hacking, bugs, malware threats, and flawed key generation through ECDSA etc. [92]. The main objective of the securing endpoint is the safety of a wallet and providing a mechanism that escapes from private key theft. Wallet attacks are another way to obtain private keys [127]. *Figure 19* represents a summary of the above discussion.

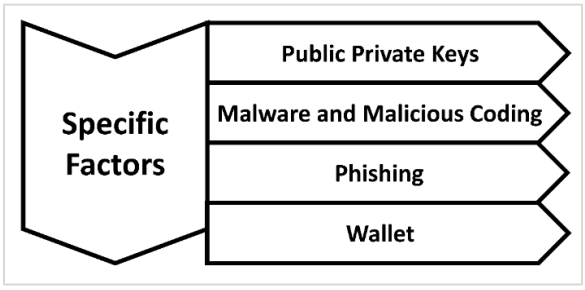

Figure 19 A summary of specific reasons for endpoint vulnerabilities

R4:Whether and how miners are related to endpoint vulnerabilities?

The miners are mainly responsible for the mining of new crypto-coin. The malicious behaviour of miners originates from many vulnerabilities and attacks. Some of the major attacks are Selfish mining, Block withholding attacks, Bribery attacks, Fork after withhold, Finney attack, Vector 76, Time jacking etc. [48,63]. None of the attacks was related to the endpoint attack. Thus, a miner does not relate to endpoint vulnerabilities. When any malicious user or invader attacks an endpoint, she is responsible. She may or may not be a miner, as to attack an endpoint, one need not be a miner.

R5:What are the current research gaps in the endpoint vulnerabilities?

The endpoints have been breached multiple times in the past, and many heists have successfully wiped out the crypto-coin. In 2013, a cryptocurrency exchange Picostocks [58] was compromised when an attacker used an old access key. Later in 2014, blockchain witnessed Mt. Gox heist [28]. Cryptsy [78] exchange was exploited by malware. Jaxx heist happened when the attacker targeted a rooted android phone. Bithumb [91] heist happens when an employee stored

userIDs and sensitive information without encryption. CoinCheck was breached through the hot wallet exploitation [24]. Since the data on chains are most vulnerable. Therefore, it needs a safe environment to access blockchain services. Accessing the private key in any possible way is the main objective of the invaders [63]. Therefore, they target endpoint devices [44].

Mahmoud et al. [88] state that the Hardware wallet keeps a private key in an integrated circuit that never transmits to other devices. When a user uses a private key on a hardware wallet, then the user sends an unsigned transaction to the hardware wallet. The transaction gets verified if the user approves. They also mentioned that Hardware wallets and paper wallets [88] are the safest mode but are vulnerable. For example, the paper wallet can be compromised if the associated network printer is compromised or the attacker compromises the hardware wallet if she compromises firmware repositories. A study by Vasek et al. [95] identified 881 brain wallets but 21 wallets were drained, indicating a high-risk potential. Yli-Huumo et al. [65] address the authentication issue in Bitcoin. The BlueWallet [107], a Bitcoin hardware token, communicates using Bitcoin low energy and provides secure sign-in. They also figure out the Mt. Gox incident with more explanation. The attacker attacks the Bitcoin wallet company and steals the customers' private keys. This incident has motivated developers to strengthen the authentication process in Bitcoin. The elliptic curve cryptography (ECC) [101], which is used to generate Bitcoin addresses for users, has weak randomness and is insufficient to provide reliable security [65]. Hasanova et al. [52] suggested that Wallet theft uses phishing, such as system hacking, buggy software and the incorrect use of wallets.

Bui et al. [89] show concern over desktop cryptocurrency wallets. Most cryptocurrency wallet services provide their services through a remote procedure call (RPC) interface for other blockchain-based applications. In some cases, malicious processes were attached that masquerade the RPC channel's communication endpoint, and the outcome ended with stealing crypto coins. One such incident happened when authentication was not properly configured and the attacker exploited the remotely accessible RPC interface and stole the coins [89].

To keep them away, it is necessary to secure the key. Still, researchers don't have sufficient mechanisms to stop or mitigate the endpoint vulnerability attack [126]. This must be addressed before any other heist. The crypto-coin must be safe for every user, whether savvy or noob. This problem needs to be addressed.

R6:Measurements to mitigate the endpoint vulnerabilities.

Various suggestions, mitigation techniques, countermeasures and other ideas were noticed to reduce the endpoint vulnerabilities in blockchain applications. Steichen et al. [94] discussed private and consortium blockchain security issues. They framed a framework called ChainGuard to filter network traffic and implemented it as a firewall for blockchain applications. Requests from illegitimate users are intercepted and attackers cannot target the users' endpoint. Later, they discussed the security issues of private and consortium blockchains. Recently, Talat et al. [84] proposed a privacy-preserving trajectory mining framework and they execute code on Hyperledger Iroha as a blockchain platform. It preserves the privacy of the users. The proprietary of the data rests with the user and not with the enterprise. The reveal of privacy often leads to guessing the private key and many hackers try to get the private key from activities, addresses, IP, trajectory data etc. The trajectory data is a kind of mobility information that tells the location and temporal information of the moving object. It can reveal users' sensitive data [128].

Li et al. [70] and Coppolino et al. [64] used Intel Software Guard Xtension to create a safe environment that protects the application from attacks. They remark that many hardware-assisted trusted execution environment (HTEE) implementations, including the eHealth sector, are widely adopted. Intel SGX, AMD secure encrypted virtualization (SEV), ARM TrustZone are the various HTEE-released versions and Intel SGX draws more attention. Remote browser isolation (RBI) is a protective measure that isolates users' devices from web browsing. It relocates the execution of all browsing activities from the user's device to the remote server (secure environment). At the end of each browsing session, it destroys the browsing environment automatically. This method may be handy for the users but till now, there does not exist any link between RBI and blockchain. These are some procedures that can formulate valuable results for blockchain users. It's important to stick with the approaches and methods for useful outcomes.

5.Key findings

As a result of summarizing, synthesizing, integrating, or critically evaluating previous knowledge to learn more about the similarities and differences between different types of reviews, the following seems to be the typically generic findings:

- The economy of a country depends on a set of policies and regulations. Regulatory services for blockchain technology vary by country. Scams, tampering and market manipulation have become commonplace in the crypto world due to the lack of standard rules and regulations. The users don't have reliable, legalized protocols or frameworks to lodge their grievances. So, there is a strong need for an authentic, legalized framework that provides endpoint security to the users.
- The end user adds new data while accessing the blockchain services. This data is more vulnerable to an attacker. This phase lies outside the scope of the security of blockchain. A safe and secure environment should be provided to access the blockchain services safely.
- Hackers observe users' behaviour and action carefully. Then, target end devices to steal private keys or sensitive information. Thus, users should not save their blockchain keys on their devices unencrypted. Also, they should educate themselves regarding security and adhere to it by action.
- Hot wallets are more vulnerable to attackers compared to Cold wallets. Cold wallets are more secure and should be used with some hardware wallets. It will enhance the security of blockchain applications.
- Some lazy users often reveal their sensitive information and location unknowingly. Also, the attacker looks for some pattern during the transaction and, sometimes, aggregates enough information to attack. In such a scenario, Zero Knowledge Algorithm may be proved handy.
- The single layer of authentication is one of the limitations of blockchain applications. If an invader bypasses this layer, the invader can control the account and resources. The authentication service was enhanced by multisig. Users' data were breached despite the security being laced with multisig. So, users need a healthy and safe environment.
- ECDSA's weak randomness causes nonce reusable. It reduces the security of the wallet, which makes private keys vulnerable. Quantum computing is also a threat to ECDSA. It needs Quantum computing and blockchain to merge to give users a more reliable and secure platform.
- Phishing, social engineering to get sensitive information, has been quite successful for attackers. Email phishing, Voice phishing, spoofed mail etc. worked in the attacker's favour. More technical knowledge and security enhancement are needed to avoid this trap.
- Cryptojacking has done more damage than other methods since its arrival. It is reported that more than 26 million crypto tokens are mined. Attackers install malicious code into the user's system without permission. This code will do mining for attackers and provide sensitive information as well. It can be prevented by updating the intrusion system, monitoring CPU usage etc.
- The endpoint security breach has nothing to do with the miners. It can be any person or group, irrespective of miners.
- Some notable works have been done to avoid endpoint breaches. Steichen et al. [94] framed a framework named ChainGuard to intercept illegitimate requests. In another work done by Coppolino et al. [64], they used Intel Software Guard Xtension to create a safe environment for accessing blockchain services. There exist other TEE tools that can be studied and used. TEE is discussed by fewer authors but can be quite useful in providing a secure environment.
- *Table 8* show the significant contributions with the reasons.

Table 8 Significant performances with reasons

Advantage	Description
Reduced risk of data breaches	Blockchain applications often store sensitive data, such as financial information, medical records, and intellectual property. By securing endpoint vulnerabilities, organizations can reduce the risk of this data being stolen by attackers.
Improved network security	Endpoint vulnerabilities can also be used to gain access to a blockchain network and launch attacks against other systems. By securing endpoint vulnerabilities, organizations can improve the overall security of their blockchain networks.
Compliance with regulations	Many regulations, such as the GDPR, require organizations to take steps to secure endpoint vulnerabilities. By complying with these regulations, organizations can protect themselves from legal liability and financial penalties.
Preventing Malware Attacks	Secured endpoints protect against malware that can compromise blockchain nodes and clients, minimizing the risk of attacks that can undermine the entire network.

Advantage	Description
Enhancing User Trust and Adoption	A secure blockchain application instills trust in users, as they know their data is protected, transactions are valid, and the overall system is resilient against malicious activities.
Long-Term Viability	A blockchain with secured endpoints is more likely to have a longer lifespan, as it can withstand evolving cybersecurity threats and vulnerabilities over time.
Reduced Financial Loss	Preventing security breaches through secured endpoints saves costs associated with data breaches, legal liabilities, and potential disruptions to business operations.

5.1Limitations

The sample size of the related study is low due to the unavailability of research articles on the topic of endpoint vulnerabilities in blockchain applications. Thus, the findings are based on and limited by these papers. Also, a greater number of research studies are needed to generalize the concept more precisely, clearly, and empirically.

A complete list of abbreviations is shown in *Appendix I.*

6.Conclusion

Blockchain technology runs many cryptocurrencies like Bitcoin, Ethereum, Tether, Ripple, Monero etc. It is a decentralized, immutable, distributed ledger that publicly records all transactions. The blockchain's objective is to provide users free from dependency, security, anonymity and transparency. Most of the facts about blockchain are misinterpreted, exaggerated, little known or still unknown. So, while using blockchain services, users are making technical and behavioural mistakes. Ndri [129] has listed almost all the barriers to blockchain adoption in a taxonomic form. These challenges need to be addressed. One of those challenges is endpoint vulnerabilities that originate outside the blockchain. When humans and machines interact, the human end becomes susceptible and prone to the attacker. The attacker observes human action and behaviour while accessing the blockchain services and tries to get sensitive information and control. User wtinesses 20+ heists and attacks at endpoint of blockchain applications. The major factors that work in the attacker's favour are a single authentication layer, malicious code, user negligence behaviour, weak randomness in ECDSA, wallet exposure etc. Due to anonymity, the attackers cannot be tracked, identified or punished. So, the attackers are trying hard to get into the system through the vulnerabilities and openness of blockchain to steal the crypto-coin. The expert advises using a cold wallet along with a hot wallet, 2-FA, multi-sig, and encryption to control endpoint breaches. To overcome this issue, TEE, RBI, steganography, biometric etc. were suggested as a solution. In fact, a secure and hack-proof environment is needed to access the blockchain services.

Overall, this study provides a detailed and SLR of endpoint vulnerabilities. During the review, the research questions were set and then extracted and analyzed all belonging papers from all related digital libraries. Later, a discussion was done in all possible ways. Currently, no permanent solution exists to mitigate the endpoint vulnerabilities, which invites serious attention to the issue. The questions were raised and set the future research direction for all enthusiast researchers. It is hoped that this study will motivate the researchers and help in tackling the problem.

Acknowledgment

None.

Conflicts of interest

The authors have no conflicts of interest to declare.

Author's contribution statement

Mohd Azeem Faizi Noor: Conceptualization, methodology, data curation, original draft preparation, visualization, investigation, analysis and writing. **Prof Khurram Mustafa:** Conceptualization, methodology, visualization, supervision, writing- reviewing and editing.

References

[1] Khan MA, Salah K. IoT security: review, blockchain solutions, and open challenges. Future Generation Computer Systems. 2018; 82:395-411.

[2] Noor MA, Mustafa K. Protocols and guidelines to enhance the endpoint security of blockchain at user's end. In proceedings of the 3rd international conference on ICT for digital, smart, and sustainable development 2023 (pp. 231-41). European Alliance for Innovation.

[3] https://learn.microsoft.com/en-us/mem/intune/protect/endpoint-security. Accessed 04 November 2023.

[4] https://www.selecthub.com/endpoint-security/endpoint-security-software-requirements/. Accessed 04 November 2023.

[5] Khanum S, Mustafa K. A systematic literature review on sensitive data protection in blockchain applications. Concurrency and Computation: Practice and Experience. 2023; 35(1):e7422.

[6] Levis D, Fontana F, Ughetto E. A look into the future of blockchain technology. Plos One. 2021; 16(11):1-20.
[7] Houy S, Schmid P, Bartel A. Security aspects of cryptocurrency wallets—a systematic literature review. ACM Computing Surveys. 2023; 56(1):1-31.
[8] Nakamoto S. A peer-to-peer electronic cash system. Bitcoin. 2008: 1-24.
[9] Noor MA, Khanum S, Anwar T, Ansari M. A holistic view on blockchain and its issues. In blockchain applications in IoT security 2021 (pp. 21-44). IGI Global.
[10] Zheng XR, Lu Y. Blockchain technology–recent research and future trend. Enterprise Information Systems. 2022; 16(12):1939895.
[11] Baygin N, Baygin M, Karakose M. Blockchain technology: applications, benefits and challenges. In 1st international informatics and software engineering conference 2019 (pp. 1-5). IEEE.
[12] Saad M, Spaulding J, Njilla L, Kamhoua C, Shetty S, Nyang D, et al. Exploring the attack surface of blockchain: a comprehensive survey. IEEE Communications Surveys & Tutorials. 2020; 22(3):1977-2008.
[13] Laroiya C, Saxena D, Komalavalli C. Applications of blockchain technology. In Handbook of Research on Blockchain Technology 2020 (pp. 213-43). Academic Press.
[14] Sunyaev A, Sunyaev A. Distributed ledger technology. Internet Computing: Principles of Distributed Systems and Emerging Internet-Based Technologies. 2020:265-99.
[15] Gugueoth V, Safavat S, Shetty S, Rawat D. A review of IoT security and privacy using decentralized blockchain techniques. Computer Science Review. 2023; 50:100585.
[16] Panwar A, Bhatnagar V. Distributed ledger technology (DLT): the beginning of a technological revolution for blockchain. In 2nd international conference on data, engineering and applications 2020 (pp. 1-5). IEEE.
[17] Alkhodair AJ, Mohanty SP, Kougianos E. Consensus algorithms of distributed ledger technology--a comprehensive analysis. arXiv preprint arXiv:2309.13498. 2023.
[18] Yermack D, Fingerhut A. Blockchain technology's potential in the financial system. In proceedings of the financial market's conference 2019 (pp.1-20).
[19] Firdaus A, Razak MF, Feizollah A, Hashem IA, Hazim M, Anuar NB. The rise of "blockchain": bibliometric analysis of blockchain study. Scientometrics. 2019; 120:1289-331.
[20] Garriga M, Dalla PS, Arias M, De RA, Pareschi R, Andrew TD. Blockchain and cryptocurrencies: a classification and comparison of architecture drivers. Concurrency and Computation: Practice and Experience. 2021; 33(8):e5992.
[21] Chohan UW. Non-fungible tokens: blockchains, scarcity, and value. Critical Blockchain Research Initiative (CBRI) Working Papers. 2021: 1-14.
[22] Auer R, Haslhofer B, Kitzler S, Saggese P, Victor F. The technology of decentralized finance (DeFi). Bank for International Settlements, Monetary and Economic Department; 2023:1-37.
[23] Wang S, Yuan Y, Wang X, Li J, Qin R, Wang FY. An overview of smart contract: architecture, applications, and future trends. In intelligent vehicles symposium (IV) 2018 (pp. 108-13). IEEE.
[24] Lee JH. Systematic approach to analyzing security and vulnerabilities of blockchain systems (Doctoral Dissertation, Massachusetts Institute of Technology). 2019:119-49.
[25] Kim H, Kim D. A taxonomic hierarchy of blockchain consensus algorithms: an evolutionary phylogeny approach. Sensors. 2023; 23(5):1-27.
[26] Dhanya D, Jha B, Jha D. Moderated mediation model of the factors influencing intention to invest in cryptocurrency among millennials and generation Z. Scope. 2023; 13(3):201-13.
[27] Al-hashedi KG, Magalingam P, Maarop N, Samy GN, Manaf AA. A conceptual model to identify illegal activities on the bitcoin system. In international conference on advances in cyber security 2021 (pp. 18-34). Singapore: Springer Singapore.
[28] Latifa ER, Omar A. Blockchain: bitcoin wallet cryptography security, challenges and countermeasures. Journal of Internet Banking and Commerce. 2017; 22(3):1-29.
[29] Dasgupta D, Shrein JM, Gupta KD. A survey of blockchain from security perspective. Journal of Banking and Financial Technology. 2019; 3:1-7.
[30] Halaburda H. Blockchain revolution without the blockchain? Communications of the ACM. 2018; 61(7):27-9.
[31] Frizzo-barker J, Chow-white PA, Adams PR, Mentanko J, Ha D, Green S. Blockchain as a disruptive technology for business: a systematic review. International Journal of Information Management. 2020; 51:102029.
[32] Alqahtani AM, Algarni A. A survey on blockchain technology concepts, applications and security. International Journal of Advanced Computer Science and Applications. 2023; 14(2):841-44.
[33] Mustafa MK, Waheed S. A governance framework with permissioned blockchain for the transparency in e-tendering process. International Journal of Advanced Technology and Engineering Exploration. 2019; 6(61):274-80.
[34] Kombe C, Dida M, Sam A. A review on healthcare information systems and consensus protocols in blockchain technology. International Journal of Advanced Technology and Engineering Exploration. 2019; 5(49):473-83
[35] Crosby M, Pattanayak P, Verma S, Kalyanaraman V. Blockchain technology: beyond bitcoin. Applied Innovation. 2016; 2(6-10):1-19.
[36] Adlaon JK. A systematic literature review of Ransomware attacks in healthcare. Electronic Theses, Projects, and Dissertations. 2023.

[37] Fatrah A, El KS, Haqiq A, Salah K. Proof of concept blockchain-based voting system. In proceedings of the 4th international conference on big data and internet of things 2019 (pp. 1-5).
[38] Agbo CC, Mahmoud QH, Eklund JM. Blockchain technology in healthcare: a systematic review. Healthcare. 2019; 7(2):1-30.
[39] Farouk A, Alahmadi A, Ghose S, Mashatan A. Blockchain platform for industrial healthcare: vision and future opportunities. Computer Communications. 2020; 154:223-35.
[40] Heston T. A case study in blockchain healthcare innovation. SSRN Journal. 2017: 1-3.
[41] Iqtait A. Blockchain technology in MENA: sociopolitical impacts. Available at SSRN 4475898. 2023: 1-18.
[42] Abuidris Y, Hassan A, Hadabi A, Elfadul I. Risks and opportunities of blockchain based on e-voting systems. In 16th international computer conference on wavelet active media technology and information processing 2019 (pp. 365-8). IEEE.
[43] https://igniteoutsourcing.com/blockchain/blockchain-security-vulnerabilities-risks/. Accessed 04 November 2023.
[44] Rasool MA, Muhammad SH. Blockchain technology: a new domain for cyber forensics. Master Thesis, Halmstad University. 2018.
[45] Patel R, Sethia A, Patil S. Blockchain–future of decentralized systems. In international conference on computing, power and communication technologies 2018 (pp. 369-74). IEEE.
[46] https://www.cloudcodes.com/blog/endpoint-security-risks-due-to-blockchain.html. Accessed 04 November 2023.
[47] https://www.darkreading.com/endpoint/the-good-bad-news-about-blockchain-security. Accessed 04 November 2023.
[48] Conti M, Kumar ES, Lal C, Ruj S. A survey on security and privacy issues of bitcoin. IEEE Communications Surveys & Tutorials. 2018; 20(4):3416-52.
[49] Taylor PJ, Dargahi T, Dehghantanha A, Parizi RM, Choo KK. A systematic literature review of blockchain cyber security. Digital Communications and Networks. 2020; 6(2):147-56.
[50] Zamani E, He Y, Phillips M. On the security risks of the blockchain. Journal of Computer Information Systems. 2020; 60(6):495-506.
[51] Zhang R, Xue R, Liu L. Security and privacy on blockchain. ACM Computing Surveys. 2019; 52(3):1-34.
[52] Hasanova H, Baek UJ, Shin MG, Cho K, Kim MS. A survey on blockchain cybersecurity vulnerabilities and possible countermeasures. International Journal of Network Management. 2019; 29(2):e2060.
[53] https://blockchaintrainingalliance.com/blogs/news/blockchain-security-vs-standard-cybersecurity. Accessed 04 November 2023.
[54] Charoenwong B, Bernardi M. A decade of cryptocurrency 'hacks': 2011–2021. Available at SSRN 3944435. 2021.
[55] Eskandari S, Clark J, Barrera D, Stobert E. A first look at the usability of bitcoin key management. arXiv preprint arXiv:1802.04351. 2018.
[56] Atiquzzaman M, Yen N, Xu Z. Big data analytics for cyber-physical system in smart city: BDCPS 2019 (pp.28-9), Shenyang, China. Springer Nature.
[57] Marella V, Kokabha MR, Merikivi J, Tuunainen V. Rebuilding trust in cryptocurrency exchanges after cyber-attacks. In Hawaii international conference on system sciences 2021 (pp. 5636-46).
[58] Lazarenko A, Avdoshin S. Financial risks of the blockchain industry: a survey of cyberattacks. In proceedings of the future technologies conference 2019 (pp. 368-84). Springer International Publishing.
[59] Mccorry P, Möser M, Ali ST. Why preventing a cryptocurrency exchange heist isn't good enough. In security protocols XXVI: 26th international workshop, Cambridge, UK, 2018 (pp. 225-33). Springer International Publishing.
[60] Rafi S, Yu W, Akbar MA, Mahmood S, Alsanad A, Gumaei A. Readiness model for DevOps implementation in software organizations. Journal of Software: Evolution and Process. 2021; 33(4):e2323.
[61] Keele S. Guidelines for performing systematic literature reviews in software engineering. EBSE Technical Report. 2007.
[62] Guo H, Yu X. A survey on blockchain technology and its security. Blockchain: Research and Applications. 2022; 3(2):100067.
[63] Shrivas MK, Dean TY, Brunda SS. The disruptive blockchain security threats and threat categorization. In first international conference on power, control and computing technologies 2020 (pp. 327-38). IEEE.
[64] Coppolino L, D'antonio S, Mazzeo G, Romano L, Campegiani P. Facing the blockchain endpoint vulnerability, an SGX-based solution for secure eHealth auditing. In ITASEC 2021 (pp. 298-308).
[65] Yli-huumo J, Ko D, Choi S, Park S, Smolander K. Where is current research on blockchain technology?—a systematic review. PloS One. 2016; 11(10):1-27.
[66] Brengel M, Rossow C. Identifying key leakage of bitcoin users. In research in attacks, intrusions, and defenses: 21st international symposium, RAID 2018, Heraklion, Crete, Greece, 2018 (pp. 623-43). Springer International Publishing.
[67] Pal O, Alam B, Thakur V, Singh S. Key management for blockchain technology. ICT Express. 2021; 7(1):76-80.
[68] Kiktenko EO, Kudinov MA, Fedorov AK. Detecting brute-force attacks on cryptocurrency wallets. In international conference on business information systems 2019 (pp. 232-42). Cham: Springer International Publishing.
[69] Singh S, Hosen AS, Yoon B. Blockchain security attacks, challenges, and solutions for the future

distributed IoT network. IEEE Access. 2021; 9:13938-59.
[70] Li X, Jiang P, Chen T, Luo X, Wen Q. A survey on the security of blockchain systems. Future Generation Computer Systems. 2020; 107:841-53.
[71] Lu Y. The blockchain: state-of-the-art and research challenges. Journal of Industrial Information Integration. 2019; 15:80-90.
[72] Casino F, Dasaklis TK, Patsakis C. A systematic literature review of blockchain-based applications: current status, classification and open issues. Telematics and Informatics. 2019; 36:55-81.
[73] Tavares B, Correia FF, Restivo A, Faria JP, Aguiar A. A survey of blockchain frameworks and applications. In international conference on soft computing and pattern recognition 2018 (pp. 308-17). Cham: Springer International Publishing.
[74] Antipova T, Emelyanova I. Cryptocurrency in digital wallet: pros and cons. In international conference on digital science 2018 (pp. 313-22). Cham: Springer International Publishing.
[75] Chaudhry N, Yousaf MM. Consensus algorithms in blockchain: comparative analysis, challenges and opportunities. In 12th international conference on open source systems and technologies 2018 (pp. 54-63). IEEE.
[76] Sayadi S, Rejeb SB, Choukair Z. Blockchain challenges and security schemes: a survey. In seventh international conference on communications and networking 2018 (pp. 1-7). IEEE.
[77] Moubarak J, Filiol E, Chamoun M. On blockchain security and relevant attacks. In middle East and North Africa communications conference 2018 (pp. 1-6). IEEE.
[78] Oosthoek K, Doerr C. From hodl to heist: analysis of cyber security threats to bitcoin exchanges. In international conference on blockchain and cryptocurrency 2020 (pp. 1-9). IEEE.
[79] Van ENJ, Waltman L. VOS viewer manual. Manual for VOS viewer version. 2011; 1:1-27.
[80] Wenhua Z, Qamar F, Abdali TA, Hassan R, Jafri ST, Nguyen QN. Blockchain technology: security issues, healthcare applications, challenges and future trends. Electronics. 2023; 12(3):1-28.
[81] Amiet N. Blockchain vulnerabilities in practice. Digital Threats: Research and Practice. 2021; 2(2):1-7.
[82] Sigurdsson G, Giaretta A, Dragoni N. Vulnerabilities and security breaches in cryptocurrencies. In proceedings of 6th international conference in software engineering for defence applications: SEDA 2018 (pp. 288-99). Springer International Publishing.
[83] Wang Z, Yu H, Zhang Z, Piao J, Liu J. ECDSA weak randomness in Bitcoin. Future Generation Computer Systems. 2020; 102:507-13.
[84] Talat R, Obaidat MS, Muzammal M, Sodhro AH, Luo Z, Pirbhulal S. A decentralised approach to privacy preserving trajectory mining. Future Generation Computer Systems. 2020; 102:382-92.
[85] Wang N, Chen Y, Yang Y, Fang Z, Sun Y. Blockchain private key storage algorithm based on image information hiding. In artificial intelligence and security: 5th international conference, 2019 (pp. 542-52). Springer International Publishing.
[86] Shah P, Manjunath P, Mishra S, Sudarsanan H. Exploratory analysis of block chain security vulnerabilities. Australian Journal of Wireless Technologies, Mobility and Security. 2019; 1-5.
[87] Aydar M, Cetin SC, Ayvaz S, Aygun B. Private key encryption and recovery in blockchain. arXiv preprint arXiv:1907.04156. 2019.
[88] Mahmoud QH, Lescisin M, Altaei M. Research challenges and opportunities in blockchain and cryptocurrencies. Internet Technology Letters. 2019; 2(2):e93.
[89] Bui T, Rao SP, Antikainen M, Aura T. Pitfalls of open architecture: how friends can exploit your cryptocurrency wallet. In proceedings of the 12th European workshop on systems security 2019 (pp. 1-6). ACM.
[90] Feng Q, He D, Zeadally S, Khan MK, Kumar N. A survey on privacy protection in blockchain system. Journal of Network and Computer Applications. 2019; 126:45-58.
[91] https://www.mcafee.com/enterprise/en-us/assets/reports/rp-blockchain-security-risks.pdf. Accessed 04 November 2023.
[92] Mosakheil JH. Security threats classification in blockchains. Culminating Projects in Information Assurance, *St. Cloud State University*. 2018.
[93] Yakubov A, Shbair W, Wallbom A, Sanda D. A blockchain-based PKI management framework. In the first international workshop on managing and managed by blockchain 2018 (pp. 1-6). IEEE
[94] Steichen M, Hommes S, State R. ChainGuard—a firewall for blockchain applications using SDN with open flow. In principles, systems and applications of IP telecommunications 2017 (pp. 1-8). IEEE.
[95] Vasek M, Bonneau J, Castellucci R, Keith C, Moore T. The bitcoin brain drain: examining the use and abuse of bitcoin brain wallets. In financial cryptography and data security: 20th international conference, 2017 (pp. 609-18). Springer Berlin Heidelberg.
[96] Decker C, Wattenhofer R. Bitcoin transaction malleability and MtGox. In computer security-ESORICS 2014: 19th European symposium on research in computer security, Wroclaw, Poland, 2014. Proceedings, Part II 2014 (pp. 313-26). Springer International Publishing.
[97] https://securityintelligence.com/blockchain-exploits-and-mining-attacks-on-the-rise-as-cryptocurrency-prices-skyrocket/. Accessed 04 November 2023.
[98] Alkurdi F, Elgendi I, Munasinghe KS, Sharma D, Jamalipour A. Blockchain in IoT security: a survey. In 28th international telecommunication networks and applications conference 2018 (pp. 1-4). IEEE.
[99] Bergman S, Asplund M, Nadjm-tehrani S. Permissioned blockchains and distributed databases: a performance study. Concurrency and Computation: Practice and Experience. 2020; 32(12):e5227.

[100]Semmouni MC, Nitaj A, Belkasmi M. Bitcoin security with a twisted Edwards curve. Journal of Discrete Mathematical Sciences and Cryptography. 2022; 25(2):353-71.
[101]Bos JW, Halderman JA, Heninger N, Moore J, Naehrig M, Wustrow E. Elliptic curve cryptography in practice. In financial cryptography and data security: 18th international conference, 2014 (pp. 157-75). Springer Berlin Heidelberg.
[102]Poddebniak D, Somorovsky J, Schinzel S, Lochter M, Rösler P. Attacking deterministic signature schemes using fault attacks. In European symposium on security and privacy 2018 (pp. 338-52). IEEE.
[103]https://github.com/bitcoin/bips/blob/master/bip-0062.mediawiki. Accessed 04 November 2023.
[104]Pornin T. Deterministic usage of the digital signature algorithm (DSA) and elliptic curve digital signature algorithm (ECDSA). 2013.
[105]Mollajafari S, Bechkoum K. Blockchain technology and related security risks: towards a seven-layer perspective and taxonomy. Sustainability. 2023; 15(18):1-24.
[106]Ulla MM, Sakkari DS. Research on elliptic curve crypto system with bitcoin curves–SECP256k1, NIST256p, NIST521p and LLL. Journal of Cyber Security and Mobility. 2023:103-28.
[107]Bamert T, Decker C, Wattenhofer R, Welten S. Bluewallet: the secure bitcoin wallet. In security and trust management: 10th international workshop, 2014 (pp. 65-80). Springer International Publishing.
[108]Kaushik A, Choudhary A, Ektare C, Thomas D, Akram S. Blockchain—literature survey. In 2nd international conference on recent trends in electronics, information & communication technology 2017 (pp. 2145-8). IEEE.
[109]Maxwell G, Poelstra A, Seurin Y, Wuille P. Simple schnorr multi-signatures with applications to bitcoin. Designs, Codes and Cryptography. 2019; 87(9):2139-64.
[110]Weber K, Schütz AE, Fertig T, Müller NH. Exploiting the human factor: social engineering attacks on cryptocurrency users. In learning and collaboration technologies. human and technology ecosystems: 7th international conference, LCT 2020, Held as Part of the 22nd HCI international conference, HCII, Copenhagen, Denmark, Proceedings, Part II 2020 (pp. 650-68). Springer International Publishing.
[111]Chanti S, Chithralekha T. A literature review on classification of phishing attacks. International Journal of Advanced Technology and Engineering Exploration. 2022; 9(89):446-76.
[112]Astrakhantseva I, Astrakhantsev R, Los A. Cryptocurrency fraud schemes analysis. In SHS web of conferences 2021 (pp. 1-7). EDP Sciences.
[113]Elrom E, Elrom E. Security and compliance. The blockchain developer: a practical guide for designing, implementing, publishing, testing, and securing Distributed Blockchain-based Projects. 2019:419-66.
[114]Wijesekara PA, Gunawardena S. A review of blockchain technology in knowledge-defined networking, its application, benefits, and challenges. Network. 2023; 3(3):343-421.
[115]Aziz AB, Ngah SB, Dun YT, Bee TF. Coinhive's monero drive-by crypto-jacking. In IOP conference series: materials science and engineering 2020 (pp. 1-9). IOP Publishing.
[116]Pallas R. Bitcoin security. [Unpublished Master Dissertation]. Tallin University of Technology. 2012.
[117]Eskandari S, Leoutsarakos A, Mursch T, Clark J. A first look at browser-based cryptojacking. In European symposium on security and privacy workshops (EuroS&PW) 2018 (pp. 58-66). IEEE.
[118]Kim S, Kim J. POSTER: mining with proof-of-probability in blockchain. In proceedings of the 2018 on Asia conference on computer and communications security 2018 (pp. 841-3). ACM.
[119]https://www.dropzone.dev/. Accessed 04 November 2023.
[120]https://www.cnet.com/tech/computing/devilrobber-trojan-steals-bitcoins-and-data/. Accessed 04 November 2023.
[121]Franco P. Understanding bitcoin: cryptography, engineering and economics. John Wiley & Sons; 2014.
[122]Cohen S, Rosenthal A, Zohar A. Reasoning about the future in blockchain databases. In 36th international conference on data engineering 2020 (pp. 1930-3). IEEE.
[123]Furneaux N. Investigating cryptocurrencies: understanding, extracting, and analyzing blockchain evidence. John Wiley & Sons; 2018.
[124]Nowroozi E, Seyedshoari S, Mekdad Y, Savaş E, Conti M. Cryptocurrency wallets: assessment and security. In blockchain for cybersecurity in cyber-physical systems 2022 (pp. 1-19). Cham: Springer International Publishing.
[125]Erinle Y, Kethepalli Y, Feng Y, Xu J. SoK: design, vulnerabilities and defense of cryptocurrency wallets. arXiv preprint arXiv:2307.12874. 2023.
[126]Mills DC, Wang K, Malone B, Ravi A, Marquardt J, Badev AI, et al. Distributed ledger technology in payments, clearing, and settlement. Finance and Economics Discussion Series 2016-095. Washington: Board of Governors of the Federal Reserve System.2016:1-36.
[127]Davenport A, Shetty S. Air gapped wallet schemes and private key leakage in permissioned blockchain platforms. In international conference on blockchain (Blockchain) 2019 (pp. 541-5). IEEE.
[128]Yin LH, Liu H. Searching activity trajectories with semantics. Journal of Computer Science and Technology. 2019; 34:775-94.
[129]Ndri A. The applications of blockchain to cybersecurity. Culminating Projects in Information Assurance, *St. Cloud State University*. 2013.

Mohd Azeem Faizi Noor is a Senior Research Fellow at the Department of Computer Science in Jamia Millia Islamia (a central university) in New Delhi, India. He holds dual post-graduate degrees, MCA and MTech, from Pondicherry Central University. His research interests focus on Steganography and Blockchain technologies.
Email: azeemfaizif@gmail.com

Dr Khurram Mustafa is an IIT Delhi alumnus, who is currently the seniormost professor in the Department of Computer Science at Jamia Millia Islamia (a central university) in New Delhi, India. Despite having completed his PhD on a topic related to eLearning, he continues to supervise students and write/speak on information security, e-learning, and research methods. During his five-year hiatus, he worked as a professor/associate professor at universities in Saudi Arabia, Yemen, and Jordan. In addition to authoring Scientific Research Primer (Ane Books, 2021) and co-authoring two other books, Software Quality: Concepts and Practices and Software Testing: Concepts and Practices (both published by Narosa, India, and Alpha Science, UK), he has mentored over a dozen PhD candidates. The latter's Chinese edition has also been released. Aside from these, he has co-authored more than a dozen book chapters and over 100 research papers published in international journals/proceedings. He was also the principal investigator for a three-year government-funded information security project and delivered more than 60 invited talks, including several keynote addresses. He is also a member of several professional scientific societies, including ISTE, ICST, CSI, EAI, ACM-CSTA, eLearning Guild, and InfoPier, as well as several academic committees and editorial review boards.
Email: kmfarooki@gmail.com

Appendix I

S. No.	Abbreviation	Description
1	2FA	2-Factor Authentication
2	ASIC	Application-Specific Integrated Circuit
3	BIP	Bitcoin Improvement Proposal
4	BTC	Bitcoin
5	BYOD	Bring Your Own Devices
6	CA	Certificate Authorities
7	CEO	Chief Executive Officer
8	CFO	Chief Financial Officer
9	CPU	Central Processing Unit
10	dApps	Decentralized Applications
11	DAG	Directed Acyclic Graph
12	DeFi	Decentralised Finance
13	DLT	Distributed Ledger Technology
14	ECC	Elliptic Curve Cryptography
15	ECDSA	Elliptic Curve Digital Signature Algorithm
16	HTEE	Hardware-assisted Trusted Execution Environment
17	HTML	HyperText Markup Language
18	IP	Internet Protocol
19	IOTA	Open-Source Distributed Ledger
20	GDPR	General Data Protection Regulation
21	GKM	Group Key Management
22	GPU	Graphics Processing Unit
23	MultiSig	Multi-Signature
24	NFT	Non-Fungible Token
25	OSINT	Open-Source Intelligence Platform
26	PKI	Public Key Infrastructure
27	RBI	Remote Browser Isolation
28	RFC	Request for Comments
29	RPC	Remote Procedure Call
30	SEC	Standard for Efficiency Cryptography
31	SGX	Software Guard Extensions
32	SLR	Systematic Literature Review
33	SQL	Structured Query Language
34	TEE	Trusted Execution Environment
35	USB	Universal Serial Bus