Bardhan, A. & Banerjee, S. (2026). Privacy in Blockchain Communication: A Meta-Analytic Review. Communication, 3(1), 298-312

Communication
Volume 3, Issue 1, Feb-Jul 2026, pp. 298-312

Privacy in Blockchain Communication: A Meta-Analytic Review

Aniket Bardhan[1], Sudeepa Banerjee[2]
[1]Research Scholar, University of Calcutta, Email ID : bardhananiket13@gmail.com
[2]Professor, University of Calcutta

Received on: May 21, 2026 | Accepted on: June 9, 2026 | Published on: July 15, 2026

Abstract
Amidst the rising concerns over communication surveillance and data breaches, in the present digital communication sphere, this study is motivated to analyse the role of blockchain in establishing privacy-enhanced communication. This study systematically synthesises the literature available at reputable databases, published between 2018-2023, from a qualitative perspective. The PRISMA framework was used for an effective data extraction process. Meticulous inclusion and exclusion criteria were set to ensure studies with empirical relevance. This study focuses on three critical dimensions: (a) communication data encryption facilitated by blockchain; (b) access and permissions control over digital communication leveraged by blockchain; & (c) blockchain efficiency in anonymising communication participants. The findings revealed that the asymmetric encryption methods dominate over symmetric methods to facilitate more privacy-enhanced communication through blockchain. Decentralisation of the communication system, facilitated by Blockchain, provides users with more control through empowering the participants to determine access rights to communication data. In the domain of 'anonymity', the blockchain inherently makes room for pseudonymous participation, but it is not absolute in nature. As the communication horizon evolves, the integration of blockchain technology in the digital communication system may offer more user-centric, transparent, and privacy-enhanced communication. Nonetheless, the blockchain technology is evolving every second, and the majority of the studies are simulation-based. Thus, this study limits the ability to generalise findings on a large scale – i.e., real-world implications.

Keywords: *Blockchain Communication, Privacy, Encryption, Access Control, Anonymity.*

1. Introduction

Data breaches are a major threat to online communication privacy (Talesh, 2018). When a data breach occurs, hackers can gain access to sensitive personal information, such as names, addresses, phone numbers, email addresses, and passwords. This information can then be used to commit identity theft, fraud, and other crimes (Talesh, 2018). On the other hand, governments around the world are increasingly surveilling their citizens' online communications. This surveillance can include monitoring internet traffic, reading emails, and tracking social media activity. Government surveillance can be used to suppress dissent and monitor political activity (Yang & Xu, 2018). Parallelly, Corporations also collect a vast amount of data about their customers' online activities. This data is often used to target advertising, but it can also be used to track people's movements, monitor their social circles, and even predict their behaviour (Pence, 2014). In addition to these general threats, there are also several specific privacy threats associated

ISSN(Online): 3108-0081

with different online communication platforms. For example, social media platforms are known for collecting a large amount of data about their users, which can then be used for targeted advertising or even sold to third-party companies. Messaging platforms can also be vulnerable to eavesdropping and surveillance (Khan & Salah, 2018).

2. Background Knowledge

2.1 Communication

Communication is the exchange of information, thoughts, and ideas between individuals or groups of individuals. It is two-way communication, i.e., the recipient and the sender of the message. Communication takes many forms, such as speech, nonverbal communication, and written communication (McQuail, 1987).

Fundamentals of communication

When it comes to communication, there are two main types of people involved: the sender, and the receiver. The sender is the one who starts the conversation, the receiver is the one who gets the message, and the recipient is the one who responds (McQuail, 1987). Messages are the information, opinions, or ideas that are sent and received, while channels are the mediums used to send and receive messages. For example, people can talk to each other in person, over the phone, through email, or on social media. Feedback can come in the form of a written, verbal, or nonverbal response (McQuail, 1987). Context is the environment in which communication takes place, and includes things like the sender's relationship with the receiver, the culture of the people involved, and what the communication is about (McQuail, 1987).

2.2 Privacy

Privacy is the right to be free from unwanted intrusion or observation. It is a fundamental human right that is essential for the protection of individual autonomy, dignity, and freedom (Messetti & Dallari, 2018). Privacy allows us to develop our thoughts and beliefs, and to make our own choices about our lives. The right to privacy is recognized in international law. The Universal Declaration of Human Rights (1948) states that "no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor unlawful attacks upon his honour and reputation. E-Privacy is a right, not a privilege (Puaschunder, 2018). We all have the right to privacy, regardless of our race, gender, nationality, or socio-economic status.

According to Gutierrez et al. (2019), privacy is not absolute. There are times when our privacy may be limited to protect other important interests, such as public safety or national security. However, any limitations on our privacy must be justified and proportionate. Everyone has the right to control their personal information. Control over who collects, uses, and stores our data.

Fundamentals of Privacy

Confidentiality means when anyone’s data is kept private and not shared with third parties without your permission. Privacy calls for personal information to be secure from unauthorized access, usage, disclosure, alteration, or destruction (Perwej, 2021). Any individual has a right to know what information is collected about you; how it is used; and who is sharing it with you; i.e. transparency (Akremi & Rouached, 2021). One may not use their identity in a communication process. Ensuring that identity is

ISSN(Online): 3108-0081

not known to others; then the identity is said to be masked behind a pseudonym, like a username or an avatar i.e. anonymity (Garg et al., 2020). These fundamental principles are important for preserving privacy and catering to the ability to control personal information.

2.3 Blockchain Technology

Blockchain technology is a decentralised database that is shared among computer network nodes (Sarmah, 2018). A blockchain, like a database, stores information electronically in a digital format. According to Min (2019), a peer-to-peer (P2P) computer network typically manages blockchains, for use as a publicly distributed ledger, with nodes collectively adhering to a consensus algorithm protocol to add and validate new transaction blocks. Once recorded, data in any given block cannot be changed retroactively without affecting all subsequent blocks and requiring network consensus (Wang et al., 2019). As a result, blockchains can be used to record events and track the ownership of assets. Blockchains are best known for their critical role in cryptocurrency systems like Bitcoin, where they keep a secure and decentralised record of transactions. The blockchain's innovation is that it ensures the fidelity and security of a data record and generates trust without the need for a trusted third party (Sarmah, 2018).

In recent years, there has been growing interest in the use of blockchain technology for enhancing communication privacy. Several researchers have proposed blockchain-based architectures that aim to maintain data privacy by leveraging the features of immutability and anonymity. For instance, Hossein et al. (2019), proposed a blockchain-based architecture for e-health applications, where users' data privacy is protected through features such as immutability and anonymity. Furthermore, the integration of blockchain technology with data-based strategies has been studied as a potential approach to reinforce data privacy.

These efforts have resulted in the development of protocols, communication schemes, and incentive methods that offer efficient and resilient solutions to data privacy challenges across communication and data processing. These advancements in blockchain technology have enabled the secure and private transmission of sensitive information even in multimedia data format (Khan et al., 2022). The integration of blockchain technology with communication privacy strategies has the potential to enhance data privacy in various applications, including healthcare platforms (Alqudaihi et al., 2021). Blockchain technology provides a distributed computing method that allows for secure and decentralized communication without the need for a central authority (Charpentier et al., 2019).

Fundamentals of Blockchain Technology

Blockchains are *decentralised*, which means that they are not controlled by a single entity (Sarmah, 2018). All blockchain transactions are *transparent* and publicly visible. *Immutability* entails the fact that once a transaction is recorded on a blockchain, it cannot be changed or deleted. *Cryptography* and consensus algorithms are used in blockchains (Wang et al., 2019). By providing a single, shared source of truth, blockchains can help to improve data *accuracy*. Blockchains are easily *traceable*, they are ideal for a secure online communication process (Min, 2019). Blockchains can aid in the automation and streamlining of communication processes, making them more efficient and cost-effective.

3. Research Methodology

ISSN(Online): 3108-0081

To conduct this study, a qualitative approach of research methodology is used. Two research tools are used to provide holistic knowledge – a) Systematic Literature Review (SLR) and b) Meta-Analysis. An in-depth review of SLR has fostered iteration in the planning, execution, and reporting phases of the review. The following sections explain the systematic literature review approach and an overview of blockchain technology and communication privacy.

3.1Systematic Literature Review

A systematic literature review is a comprehensive review of the literature on the fundamental concepts related to this paper. The purpose of a systematic literature review is to identify and evaluate all relevant literature available to understand the concepts of a) communication, b) privacy and c) blockchain technology. This catered to provide a comprehensive and current summary of the available literature (Petticrew & Roberts, 2008).

A systematic literature review (SLR) is a secondary research approach that follows a pre-defined methodology to identify, analyze, and review published literature related to a particular subject, issue, or phenomenon (Kitchenham & Charters, 2007)

The systematic literature review is also used to identify gaps related to the concept of the concepts of the study and the areas where future research needs to be conducted (Petticrew & Roberts, 2008). After reviewing all the relevant literature on a particular topic, the need for this study is ascertained.

In addition to the reasons mentioned above, there are specific reasons for using systematic literature reviews in this paper. The systematic literature review hopes to justify the need for this research study and provide a theoretical basis for this study. The research questions and the identification of the appropriate methodological approach for this research are also ascertained after a systematic literature review. Without a systematic literature review, a research study cannot stand (Petticrew & Roberts, 2008).

3.2Meta-Analysis

Meta-analysis is a method that combines the results of multiple studies to produce more precise and reliable knowledge about a specific study. It is often used in medical research to synthesize the results of clinical trials, but it can also be used in other fields such as psychology, education, and social science (Card, 2015).

Meta-analysis is a systematic approach that follows a set of predefined steps: 1. Identify and select relevant studies 2. Search for studies that meet specific criteria (e.g., similar design, outcome measure) 3. Coding the data 4. Extracting the relevant data from each study 5. Combining the results and 6. Analyzing the results for qualitative social science studies (Schmid, Stijnen & White, 2020).

The field of blockchain-facilitated communication and privacy issues is still in its early stages and there are only a few studies available. As a result, meta-research is necessary to synthesize existing literature and to identify trends and patterns in the field. Meta-research can also be used to identify gaps in existing literature and areas of research to be conducted in the future. As blockchain technology continues to develop, it is expected that it will have a significant impact on the way data is stored and shared in the future. However, there are privacy issues that need to be addressed before blockchain adoption becomes widespread.

CC BY-NC-ND 4.0

©COMMUNICATION

ISSN(Online): 3108-0081

3.3Research Question

After the screening of the existing literature, this article tends to throw light on the most relevant issues related to privacy in blockchain-facilitated communication. The questions are mapped in the table below:

ID	Question	Description
RQ 1	How is blockchain more efficient in encrypting communication data?	This question tries to find out the process of encryption of communication messages in blockchain technology.
RQ 2	How can blockchain manage communications access and permissions?	Access to the communication process and control of the participants over their communication process over communication through blockchain technology is likely to be answered through this question. This will help to ascertain the degree of decentralisation of the communication process.
RQ 3	How can blockchain anonymise communications participants?	Participants' degree of anonymity in the communication process facilitated by blockchain technology. This will help in analysing the secrecy related to participant identity.

Table 1: Research Question Table

Based on the findings, this study tried to interpret the literature and determine if it is relevant, feasible, interesting, new, ethical and pertinent. During the literature review, this study verified that the questions posed were sufficient to support their relevance and that the analytical methods used were appropriate.

3.4Selection of Primary Study

To emphasize the importance of fundamental research, certain keywords were categorised into a journal or a search engine search function. The keywords were chosen to make it easier to find study results that would help answer the fundamental research questions. In addition, only the operators "AND" and "OR" were used to restrict this research.

Serial No	Query Strings
1	(“blockchain” OR “block-chain” OR “distributed ledger”) AND “privacy”
2	(“blockchain” OR “block-chain” OR “distributed ledger”) AND (“privacy” AND “access” AND “control” AND “communication”
3	(“blockchain” OR “block-chain” OR “distributed ledger”) AND (“privacy”) AND (“encryption” OR “decryption”) AND (“communication”) AND “right to privacy”

Table 2: Query Strings Table

ISSN(Online): 3108-0081

We used various search terms in this research to get the data. As a result, we didn't miss any important articles because some writers used different word variants to distinguish their work. This research aims to collect and filter all necessary data for data collection. The platforms used in this research were:

a) HINDAWI;
b) IEEE Xplore Digital Library;
c) SpringerLink;
d) ScienceDirect;
e) MDPI.

The search platforms were based on the title, keywords or abstract. The search platforms or databases relied on the search platforms. From August 1, 2023, to August 31, 2023, we performed the searches and analyzed all the research published up to that date. The searches yielded filtered results based on the inclusion/exclusion criteria as described in section 3.5. The criteria allowed us to generate a set of findings which we could then put through the snowballing process (Wohlin, 2014). Snowballing iterations took place until there were no longer any articles that met the inclusion criteria.

3.5Inclusion & Exclusion

To filter the database search results, we have created a set of inclusion and exclusion criteria (IC) in Table 4 and a comprehensive list in Table 3. The studies that can be included in this Standard Library Report (SLR) include: Case studies Utilizing cutting-edge technology based on Blockchain technology, discussions on the evolution of existing security processes through Blockchain were integrated from peer-reviewed articles. Publishing was in the English language. As Google Scholar may generate lower-quality reports, any results that appear in Google Scholar were cross-verified to meet these standards. This SLR has the latest findings from the research

ID	Inclusion Criteria (IC)
IC 1	This survey requires complete studies with a minimum of five pages. The study must be peer-reviewed and published in a conference proceedings or journal.
IC 2	The included studies must have been published within the past 5 years.
IC 3	Research answers a research question or suggests an appropriate solution to privacy in blockchain technology.
IC 4	The study must include empirical data from applications of Blockchain technology in addressing issues related to privacy on the web.

Table 3: Inclusion Criteria for this study

ID	Exclusion Criteria (EC)
EC 1	Non-English-Language Studies
EC 2	Studies that were published before (01.08.2018) and after (31.08.2023)
EC 3	Studies that are not relevant to the subject matter of the study because they do not relate to the research questions.

ISSN(Online): 3108-0081

EC 4	Studies that duplicated.

Table 4: Exclusion Criteria for this study

3.6Data Extraction

The search string for the databases resulted in 40 papers. This research was conducted by PRISMA (preferred reporting items for systematic reviews and meta-analyses). These papers went through a filtering process that was divided into four stages:

a) The initial investigation, during which the majority of the relevant texts were gathered.
b) Duplication removal, where the duplicate papers are removed.
c) The final selection was based on the title and abstract, and the inclusion and exclusion criteria were applied to the results.

After a thorough reading, all chosen papers were subjected to inclusion and exclusion criteria.

Field	**Description**
Authors	List of authors
Year	Year of publication
Title	Title of the journal and the article
Source	HINDAWI; IEEE Xplore Digital Library; SpringerLink; ScienceDirect; MDPI
Type	Journals and Conference Proceedings
Research Question 1	How blockchain is more efficient in encrypting communication data?
Research Question 2	How blockchain can manage communications access and permissions?
Research Question 3	How blockchain can anonymize communications participants?

Table 5: Data Extraction

3.7Data Analysis

Following the selection methodology, a framework was defined for data collection and analysis. After implementation, data was collected and analyzed from 40 articles. The form and content of the dataset are shown in Table 5.

3.8Quality Assessment Criteria

The studies included in this paper were chosen based on five quality assessment (QAC) criteria listed in Table 6. The QACs are used to improve and analyze the data collected. The presented paper met the criteria to validate the data collected for this study.

ID	**Quality Assessment Criteria (QAC)**
QAC 1	Does the research contribute to the field of Blockchain-based communication and privacy issues?
QAC 2	Are the research methods and tools outlined in those papers being applied in practice today?

ISSN(Online): 3108-0081

QAC 3	Is the scope of the study sufficiently elucidated?
QAC 4	Is the scope and objectives of the study clear enough?
QAC 5	Is the research accompanied by presentations of related papers?

Table 6: Quality Assessment Criteria

3.9Compilation of Results

There are several issues with the validity of the research. First, not all of the relevant sources were found. The search was conducted across multiple databases using the most generic search query possible to counter this. Therefore, a significant amount of research was required. Secondly, the search was conducted to avoid discrimination and to ensure internal validity. Thirdly, the use of well-known databases and the total exclusion of grey literature ensures that the external validity of the study is maintained. Fourthly, as mentioned earlier, the full search query was conducted to collect the most pertinent information from the database search engines. When conducting a systematic mapping study there are many threats to consider. It is impossible to search for all relevant research and information in one place. Therefore, this study defined several search parameters and examined multiple databases to eliminate this threat. By using multiple criteria and logical operators it is possible to expand the coverage. In this study, all relevant documents were found using different keyword combinations. The missing paper review on this subject has too little effect on these conclusions. This research encircles the articles according to the designation criteria.

4. Communication, Privacy and Blockchain – Findings

While blockchain is still a work in progress, it has the power to transform communication. By tackling security, privacy and censorship issues, blockchain can create a more transparent and fair communication environment. Blockchain could be used to create decentralized identity systems in a communication process that would give participants of the communication process greater control over their own identities. These identity systems could be used to authenticate users across different platforms and services, without the need to rely on third-party intermediaries. Elaborative and in-depth findings are categorised according to the notions of the research question below:

4.1Encryption of Communication Messages in BlockChain and Privacy {RQ1}

Encryption of communications in blockchain is one of the most important ways to protect users' privacy and security. Blockchain is a type of distributed ledger technology that enables secure, open, and auditable transactions. This type of technology is perfect for storing and controlling encrypted communications.

There are two primary types of encryption used to encrypt messages in blockchain: symmetric encryption and asymmetric encryption. Symmetric encryption uses the same public key for encrypting and decrypting messages, which is relatively fast and efficient. However, it also means that in the event of a key compromise, all encrypted messages will be decrypted. Asymmetric encryption, on the other hand, uses two different keys: the public key to encrypt messages and the private key to decrypt them, which makes it much harder to compromise encrypted messages, even with the public key being known. The majority

ISSN(Online): 3108-0081

of communication systems based on blockchain use asymmetric encryption for their encryption. To illustrate how asymmetric encryption works, consider the following example: Sender generates a public / private key pair Public key is published to the blockchain Sender encrypts the message Sender sends it to the recipient Receives the message using the recipient's private key. Once the recipient decrypts the message, only the recipient can read the message. This is because the recipient holds the private key that decrypts the message.

4.2 Access and Control of Communication Process and Privacy {RQ2}

There are several ways in which blockchain technology can improve access to, and control over, communication and privacy.

Access- blockchain has the potential to create decentralized communications networks that are open to everyone. This is due to the fact that blockchain is not centralized, which can be especially useful for people who live in countries with oppressive governments or who have limited access to the internet. For instance, a blockchain social network could enable people to communicate without worrying about censorship, or a blockchain messaging app could enable people to send or receive messages without relying on centralized servers.

Control - Blockchain also gives users more control over their communications. For instance, users can use blockchain to establish their own digital identity and control who can access their data. For instance, a blockchain identity system could enable users to verify their identity across multiple platforms and services, eliminating the need for third-party middlemen. Another example is a blockchain data marketplace, where users can buy and sell data based on their usage.

4.3 The degree of anonymity in Blockchain facilitated the communication process and privacy {RQ3}

Depending on the blockchain platform and the communication protocol, the level of anonymity can vary. However, generally speaking, blockchain provides users with a high level of anonymity. This is because blockchain transactions are usually recorded using a pseudonymous address, so users do not have to disclose their real identities. The high level of anonymity can also be due to the fact that communication protocols are designed to protect users' privacy. For instance, some blockchain based messaging apps use encryption to prevent third parties from intercepting messages.Blockchain allows users to communicate anonymously, which can be beneficial for those living in countries with oppressive governments or those involved in sensitive information. On the other hand, blockchain isn't completely anonymous. For example, if a user's pseudonymous address is connected to their real identity, it is possible for them to become de-anonymous. However, this can happen if the user makes an error, such as disclosing their real identity through a public transaction, or if the user is targeted by a malicious actor. Still, the level of anonymity offered by blockchain can provide users with a number of advantages. As blockchain continues to evolve, we can look forward to even more exciting and transformative uses for anonymous communication.

5. Analysis and Discussion

Blockchain also helps protect users' privacy. This is due to the fact that blockchain is a "tamper-proof" ledger. In other words, once data is on the blockchain, it can't be changed or removed without consensus on the network. For instance, a messaging app built on blockchain would use encryption to keep users'

ISSN(Online): 3108-0081

messages safe. Another example is a data marketplace built on blockchain that uses smart contracts to make sure that users' data is only sent to authorized third parties. All in all, blockchain technology can help improve access to and control over the communication process, as well as privacy. By empowering users to control their data and communications, blockchain can create an open and more equitable communication environment.

Blockchain-based communications systems offer several key advantages over traditional communications systems, such as - a) Enhanced security: blockchain communications are encrypted with cryptography, making it much harder for malicious actors to intercept or decrypt communications. b) Enhanced privacy: blockchain communications systems provide users with greater privacy options, such as the ability to keep an anonymous identity and only share a public key with trusted people. c) Decreased censorship risk: blockchain communications systems are decentralized, meaning there is no centralized point of failure to censor or shut down communications.

All in all, blockchain communication systems offer increased security, increased privacy, and decreased censorship risk compared to traditional communication systems. With the development of blockchain technology, the adoption of blockchain communication systems is expected to increase.

Blockchain is revolutionizing the way we communicate and give us more control over our data. We can use it to create secure messaging apps that use blockchain to encrypt and verify messages, as well as data marketplaces that let us buy and sell our data securely and transparently. All of this is just the tip of the iceberg of what blockchain can do for us. As it continues to evolve, we can look forward to even more amazing use cases.

One of the most important benefits of blockchain is that it can support freedom of expression. This means that users can communicate without worrying about censorship since blockchain-based communications protocols are usually censorship-resistant.

6. Conclusion

Blockchain technology promises to revolutionise communication by tackling issues such as security, privacy and censorship. It can help create encrypted and decrypted communication systems that are more secure and decentralised. It can also provide users with more control over their data and communications. Blockchain can help users maintain their anonymity in a communication by helping them create a decentralized communication network that is resistant to censorship. It can also help create a new basis for being anonymous, as blockchain is a proof-of-stake (PoS) ledger that can't be changed or deleted without a consensus of the entire network. There is still research that needs to be done before a secure blockchain can be created, as blockchain is still developing. n terms of scalability, blockchain networks tend to be slow and costly to operate. This is due to the fact that all transactions must be verified by every node on the blockchain. Privacy: Blockchain can be used to ensure user privacy, but it is important to keep in mind that blockchain is not 100% anonymous. Users can de-anonymize if their pseudonymous address is linked to their real identity. Addressing security, privacy and censorship issues, blockchain can help create a more transparent and fair communication environment. As blockchain technology advances, we can look forward to more innovative and transformative uses cases for communication privacy.

CC BY-NC-ND 4.0

©COMMUNICATION

ISSN(Online): 3108-0081

References

- Abualsauod, EH (2022). A hybrid blockchain method in internet of things for privacy and security in unmanned aerial vehicles network. Computers and Electrical Engineering, Elsevier, https://www.sciencedirect.com/science/article/pii/S0045790622001392
- Akhter, AFMS, Ahmed, M, Shah, AFMS, Anwar, A (2021). A secured privacy-preserving multi-level blockchain framework for cluster based VANET. Sustainability, mdpi.com, https://www.mdpi.com/2071-1050/13/1/400
- Akremi, A., & Rouached, M. (2021). A comprehensive and holistic knowledge model for cloud privacy protection. *The Journal of Supercomputing*, 1-33.
- Alfandi, O, Khanji, S, Ahmad, L, & Khattak, A (2021). A survey on boosting IoT security and privacy through blockchain: Exploration, requirements, and open issues. Cluster Computing, Springer, https://doi.org/10.1007/s10586-020-03137-8
- Algarni, S, Eassa, F, Almarhabi, K, Almalaise, A, & ... (2021). Blockchain-based secured access control in an IoT system. Applied Sciences, mdpi.com, https://www.mdpi.com/2076-3417/11/4/1772
- Ali, A, Rahim, HA, Pasha, MF, Dowsley, R, Masud, M, Ali, J, & ... (2021). Security, privacy, and reliability in digital healthcare systems using blockchain. Electronics, mdpi.com, https://www.mdpi.com/2079-9292/10/16/2034
- Alqudaihi, K S., Aslam, N., Khan, I U., Almuhaideb, A M., Alsunaidi, S J., Ibrahim, N S., Alhaidari, F., Shaikh, F., Alsenbel, Y M., Alalharith, D M., Alharthi, H M., Alghamdi, W M., & Alshahrani, M. (2021, January 1). Cough Sound Detection and Diagnosis Using Artificial Intelligence Techniques: Challenges and Opportunities. https://scite.ai/reports/10.1109/access.2021.3097559
- Alzoubi, YI, Al-Ahmad, A, & Kahtan, H (2022). Blockchain technology as a Fog computing security and privacy solution: An overview. Computer Communications, Elsevier, https://www.sciencedirect.com/science/article/pii/S0140366421004321
- Atlam, HF, Azad, MA, Altamimi, M, & Fadhel, N (2022). Role of Blockchain and AI in Security and Privacy of 6G. … Blockchain Technology in 6G, Springer, https://doi.org/10.1007/978-981-19-2868-0_5
- Azzaoui, A El, Chen, H, Kim, SH, Pan, Y, & Park, JH (2022). Blockchain-based distributed information hiding framework for data privacy preserving in medical supply chain systems. Sensors, mdpi.com, https://www.mdpi.com/1424-8220/22/4/1371
- Babu, ES, Yadav, BVRN, Nikhath, AK, Nayak (2023). MediBlocks: secure exchanging of electronic health records (EHRs) using trust-based blockchain network with privacy concerns. Cluster, Springer, https://doi.org/10.1007/s10586-022-03652-w
- Bernabe, JB, Canovas, JL, Hernandez-Ramos, JL, & ... (2019). Privacy-preserving solutions for blockchain: Review and challenges. IEEE, ieeexplore.ieee.org, https://ieeexplore.ieee.org/abstract/document/8888155
- Card, N. A. (2015). *Applied meta-analysis for social science research*. Guilford Publications.
- Ch, R, Srivastava, G, Gadekallu, TR, & ... (2020). Security and privacy of UAV data using blockchain technology. Journal of Information, Elsevier, https://www.sciencedirect.com/science/article/pii/S221421262030822X

ISSN(Online): 3108-0081

- Charpentier, A., Flachaire, E., & Ly, A. (2019, April 11). Econometrics and Machine Learning. https://scite.ai/reports/10.24187/ecostat.2018.505d.1970
- Garg, L., Chukwu, E., Nasser, N., Chakraborty, C., & Garg, G. (2020). Anonymity preserving IoT-based COVID-19 and other infectious disease contact tracing models. *Ieee Access*, *8*, 159402-159414.
- Ghazal, TM, Hasan, MK, Abdullah, SNHS, & ... (2022). Private blockchain-based encryption framework using computational intelligence approach. Egyptian Informatics, Elsevier, https://www.sciencedirect.com/science/article/pii/S1110866522000494
- Guan, Z, Lu, X, Yang, W, Wu, L, Wang, N, & ... (2021). Achieving efficient and Privacy-preserving energy trading based on blockchain and ABE in smart grid. Journal of Parallel, Elsevier, https://www.sciencedirect.com/science/article/pii/S0743731520303609
- Guo, S, Hu, X, Zhou, Z, Wang, X, Qi, F, & ... (2019). Trust access authentication in vehicular network based on blockchain Communications, ieeexplore.ieee.org, https://ieeexplore.ieee.org/abstract/document/8753460
- Guo, S, Zhang, K, Gong, B, Chen, L, & ... (2022). Sandbox computing: A data privacy trusted sharing paradigm via blockchain and federated learning. IEEE Transactions, ieeexplore.ieee.org, https://ieeexplore.ieee.org/abstract/document/9791849
- Gutierrez, A., O'Leary, S., Rana, N. P., Dwivedi, Y. K., & Calle, T. (2019). Using privacy calculus theory to explore entrepreneurial directions in mobile location-based advertising: Identifying intrusiveness as the critical risk factor. *Computers in Human Behavior*, *95*, 295-306.
- Haro-Olmo, FJ de, Varela-Vaca, ÁJ, & Álvarez-Bermejo, JA (2020). Blockchain from the perspective of privacy and anonymisation: A systematic literature review. Sensors, mdpi.com, https://www.mdpi.com/1424-8220/20/24/7171
- Hossein, K. M., Esmaeili, M. E., & Dargahi, T. (2019, May). Blockchain-based privacy-preserving healthcare architecture. In *2019 IEEE Canadian Conference of Electrical and Computer Engineering (CCECE)* (pp. 1-4). IEEE.
- Jia, X, Luo, M, Wang, H, Shen, J, & ... (2022). A blockchain-assisted privacy-aware authentication scheme for Internet of Medical Things. IEEE Internet of Things, ieeexplore.ieee.org, https://ieeexplore.ieee.org/abstract/document/9792262
- Joshi, S, Pise, AA, Shrivastava, M, Revathy, C, & ... (2022). Adoption of blockchain technology for privacy and security in the context of industry 4.0. Communications, hindawi.com, https://www.hindawi.com/journals/wcmc/2022/4079781
- Khacef, K, & Pujolle, G (2019). Secure Peer-to-Peer communication based on Blockchain. Web, Artificial Intelligence and Network Applications, Springer, https://doi.org/10.1007/978-3-030-15035-8_64
- Khan, A. A., Laghari, A. A., Shaikh, A. A., Dootio, M. A., Estrela, V. V., & Lopes, R. T. (2022). A blockchain security module for brain-computer interface (BCI) with multimedia life cycle framework (MLCF). *Neuroscience Informatics*, *2*(1), 100030.
- Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. *Future generation computer systems*, *82*, 395-411.
- Kitchenham, B.; Charters, S. (2007). *Guidelines for Performing Systematic Literature Reviews in Software Engineering*; Keele University: Keele, UK.

ISSN(Online): 3108-0081

- Kumar, R, & Tripathi, R (2021). Towards design and implementation of security and privacy framework for internet of medical things (iomt) by leveraging blockchain and ipfs technology. the Journal of Supercomputing, Springer, https://doi.org/10.1007/s11227-020-03570-x
- Liang, W, & Ji, N (2022). Privacy challenges of IoT-based blockchain: a systematic review. Cluster Computing, Springer, https://doi.org/10.1007/s10586-021-03260-0
- Lin, C, Huang, X, & He, D (2022). EBCPA: Efficient blockchain-based conditional privacy-preserving authentication for VANETs. IEEE Transactions on Dependable, ieeexplore.ieee.org, https://ieeexplore.ieee.org/abstract/document/9749919
- Liu, X, Huang, H, Xiao, F, & Ma, Z (2019). A blockchain-based trust management with conditional privacy-preserving announcement scheme for VANETs. IEEE Internet of Things Journal, ieeexplore.ieee.org, https://ieeexplore.ieee.org/abstract/document/8920075
- Makhdoom, I, Zhou, I, Abolhasan, M, Lipman, J, & Ni, W (2020). PrivySharing: A blockchain-based framework for privacy-preserving and secure data sharing in smart cities. Computers & Security, Elsevier, https://www.sciencedirect.com/science/article/pii/S016740481930197X
- McQuail, D. (1987). Mass communication theory: An introduction. Sage Publications, Inc.
- Messetti, P. A. S., & Dallari, D. D. A. (2018). Human dignity in the light of the Constitution, human rights and bioethics. *Journal of Human Growth and Development*, *28*(3), 283-289.
- Min, H. (2019). Blockchain technology for enhancing supply chain resilience. *Business Horizons*, *62*(1), 35-45.
- Mundhe, P, Phad, P, Yuvaraj, R, Verma, S, & ... (2023). Blockchain-based conditional privacy-preserving authentication scheme in VANETs. Multimedia Tools, Springer, https://doi.org/10.1007/s11042-022-14288-8
- Nguyen, LD, Hoang, J, Wang, Q, Lu, Q, & ... (2023). Bdsp: A fair blockchain-enabled framework for privacy-enhanced enterprise data sharing. … and Cryptocurrency …, ieeexplore.ieee.org, https://ieeexplore.ieee.org/abstract/document/10174943
- Patil, P, Sangeetha, M, & Bhaskar, V (2021). Blockchain for IoT access control, security and privacy: a review. Wireless Personal Communications, Springer, https://doi.org/10.1007/s11277-020-07947-2
- Pence, H. E. (2014). What is big data and why is it important?. Journal of Educational Technology Systems, 43(2), 159-171.
- Perwej, Y., Abbas, S. Q., Dixit, J. P., Akhtar, N., & Jaiswal, A. K. (2021). A systematic literature review on cyber security. *International Journal of scientific research and management*, *9*(12), 669-710.
- Petticrew, M., & Roberts, H. (2008). Systematic reviews in the social sciences: A practical guide. John Wiley & Sons.
- Puaschunder, J. M. (2018). Dignity and utility of privacy and information sharing in the digital big data age. *International Journal of Commerce and Management Research*, *5*(4), 62-70.
- Qammar, A, Karim, A, Ning, H, & Ding, J (2023). Securing federated learning with blockchain: a systematic literature review. Artificial Intelligence Review, Springer, https://doi.org/10.1007/s10462-022-10271-9
- Rashid, A, Masood, A, & Khan, AR (2023). Zone of trust: blockchain assisted IoT authentication to support cross-communication between bubbles of trusted IoTs. Cluster Computing, Springer, https://doi.org/10.1007/s10586-022-03583-6

ISSN(Online): 3108-0081

- Sarmah, S. S. (2018). Understanding blockchain technology. *Computer Science and Engineering*, *8*(2), 23-29.
- Schmid, C. H., Stijnen, T., & White, I. (Eds.). (2020). Handbook of meta-analysis. CRC Press
- Shi, K, Zhu, L, Zhang, C, Xu, L, & Gao, F (2020). Blockchain-based multimedia sharing in vehicular social networks with privacy protection. Multimedia Tools and Applications, Springer, https://doi.org/10.1007/s11042-019-08284-8
- Singh, P, Masud, M, Hossain, MS, & Kaur, A (2021). Blockchain and homomorphic encryption-based privacy-preserving data aggregation model in smart grid. Computers & Electrical, Elsevier, https://www.sciencedirect.com/science/article/pii/S0045790621002032
- Singh, S, Pankaj, B, Nagarajan, K, Singh, NP (2022). Blockchain with cloud for handling healthcare data: A privacy-friendly platform. Materials Today …, Elsevier, https://www.sciencedirect.com/science/article/pii/S221478532203098X
- Suryavanshi, A, Apoorva, G, TN, MB (2023). The integration of Blockchain and AI for Web 3.0: A security Perspective on Innovative Trends, ieeexplore.ieee.org, https://ieeexplore.ieee.org/abstract/document/10068672/
- Talesh, S. A. (2018). Data breach, privacy, and cyber insurance: How insurance companies act as "compliance managers" for businesses. *Law & Social Inquiry*, *43*(2), 417-440.
- Valadares, DCG, Perkusich, A, Martins, AF, Kamel, MBM, & ... (2023). Privacy-Preserving Blockchain Technologies. Sensors, mdpi.com, https://www.mdpi.com/1424-8220/23/16/7172
- Wan, Y, Qu, Y, Gao, L, & Xiang, Y (2022). Privacy-preserving blockchain-enabled federated learning for B5G-Driven edge computing. Computer Networks, Elsevier, https://www.sciencedirect.com/science/article/pii/S1389128621005454
- Wang, H, Gan, J, Feng, Y, Li, Y, & Fu, X (2021). A privacy enhancement scheme based on blockchain and blind signature for Internet of vehicles. Blockchain and Trustworthy Systems, Springer, https://doi.org/10.1007/978-981-16-7993-3_28
- Wang, W., Hoang, D. T., Hu, P., Xiong, Z., Niyato, D., Wang, P., ... & Kim, D. I. (2019). A survey on consensus mechanisms and mining strategy management in blockchain networks. *Ieee Access*, *7*, 22328-22370.
- William, P, Yogeesh, N, Vimala, S, & ... (2022). Blockchain technology for data privacy using contract mechanism for 5G networks. 2022 3rd International …, ieeexplore.ieee.org, https://ieeexplore.ieee.org/abstract/document/9853118
- Wohlin, C. (2014) Guidelines for snowballing in systematic literature studies and a replication in software engineering. In Proceedings of the 18th International Conference on Evaluation and Assessment in Software Engineering, London.
- Xu, M, Zou, Z, Cheng, Y, Hu, Q, Yu, D, & ... (2022). Spdl: A blockchain-enabled secure and privacy-preserving decentralized learning system. IEEE Transactions on …, ieeexplore.ieee.org, https://ieeexplore.ieee.org/abstract/document/9761745
- Yang, F., & Xu, J. (2018). Privacy concerns in China's smart city campaign: The deficit of China's Cybersecurity Law. *Asia & the Pacific Policy Studies*, *5*(3), 533-543.
- Zaghloul, E, Li, T, Mutka, MW, & ... (2020). Bitcoin and blockchain: Security and privacy. IEEE Internet of Things, ieeexplore.ieee.org, https://ieeexplore.ieee.org/iel7/6488907/9219268/09122595.pdf

ISSN(Online): 3108-0081

- Zhang, C, Zhao, M, Zhu, L, Zhang, W, & ... (2022). FRUIT: A blockchain-based efficient and privacy-preserving quality-aware incentive scheme. … in Communications, ieeexplore.ieee.org, https://ieeexplore.ieee.org/abstract/document/9915368

ISSN(Online): 3108-0081