# Blockchain and GDPR – A Study on Compatibility Issues of the Distributed Ledger Technology with GDPR Data Processing

**Mani Karthik Suhas Suripeddi and Pradnya Purandare***
Symbiosis Centre for Information Technology, Symbiosis International (Deemed University), Pune, Mahaarashtra, India
Email: pradnya@scit.edu*

**Abstract.** This research work aims to investigate Blockchain technology and GDPR compliance studies. This will analyze the data privacy perspective with respect to distributed ledger technology. Blockchain has become one of the most frequently discussed technologies for its ability to allow for peer-to-peer transactions without a centralized intermediary. The GDPR was implemented in May 2018 for EU member states to maintain data privacy. DLT, the underlying technology of blockchain as is a decentralized system without any monetary authority. This research conducted a thorough literature review on prior conducted research to investigate the problems and determine the gaps of GDPR compliance with blockchain technologies and discuss the technical, use-case designs or solutions that make blockchain more compliant GDPR in terms of privacy. This systematic literature review addresses the gaps, feasibility, efficiency, and data privacy issues on compatibility problems that are primarily concerned with how a distributed ledger technology system in which recorded data or transaction cannot be changed or erased is challenging the GDPR data subject access rights (DSAR), where every data subject's personal data which is compliant to GDPR has a right to exercise their Rights to rectify, delete or limit the processing of your personal data at any time if necessary.
**Keywords:** Blockchain, GDPR, Distributed Ledger Technology, De-Centralized System, Data Privacy, Data Subject.

## 1. Introduction

Recently, major improvements have been made in the way businesses collect and manage personal data. The dependence on data to drive routine businesses and utilizing it for innovation has raised potential threats and risks to individuals' privacy. Privacy is an individual's right to monitor how personal data is collected, with whom it is shared, and how it is processed, retained, or deleted. GDPR is one of its kinds of regulation in protecting user data. Blockchain is considered to be shared and immutable for recording or registering transactions in a decentralized, shared storage system in a free and transparent manner. Such properties allow for the complete distribution of blockchain without a central authority and yet in terms of user privacy. This raises a question to find the gap: Will GDPR and Blockchain comply with the data


Content from this work may be used under the terms of the Creative Commons Attribution 3.0 licence. Any further distribution of this work must maintain attribution to the author(s) and the title of the work, journal citation and DOI.
Published under licence by IOP Publishing Ltd

protection issues enough? In the event that Blockchain and the GDPR are compliant to the degree the open distributed. As in blockchain, stored data cannot be modified and removed. This paper provides detailed attention to how distributed ledger can be complied with and adapted to GDPR regulations and laws and how it can be beneficial for data subjects.

*1.1 GDPR*

It is stated that EU GDPR is considered one among the modern regulatory frameworks providing guidelines for personal data processing from European Union (EU) residents and ensuring data subjects' privacy [6]. Under the GDPR, organizations must be compliant with personal data processing and comply with limiting collection purposes and protect the same from misuse [5]. As stated in GDPR, Personal data is defined as means to any information concerning an identified or identifiable individual data subject [7].

Here, Data processing in GDPR is interpreted as an operation or collective operations performed on personal data, such as gathering, storing, saving, modifying, retrieving, publishing, rendering available, erasing, or destroying such data. As per Article 32 of the GDPR: Data controllers are known to be the principal owners and are accountable for the fair and reasonable processing of the information by means of measures and procedures [17]. At the same time, data processors are liable to data controllers and notify the controller of any data breaches.

*1.2 Blockchains*

In simpler terms, blockchain is a chain of blocks that could define blockchain as a database that ensures security, transparency, and decentralization of transactions [8]. A larger group of technologies together combined are known as "Distributed Ledger Technology," which is connected to "Blockchain," which is protected by using reliable, public, private key signature technology [4] is shown in Figure 1. For businesses that need a database, required shared access amongst parties that may not be known or trusted or may have competing interests, and it is not practically possible for a third party to be trusted to manage the database, then blockchain comes into play as the distributed architecture of the blockchain is more resilient, reducing the ability for hacks to happen. Blockchain transactions are verifiable, traceable, and auditable, creating transparency [26].

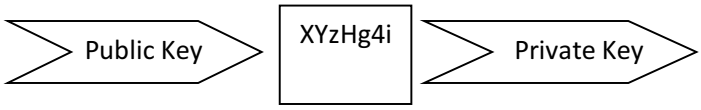


**Figure 1:** Blockchain Public and Private Key Signature

Next to bitcoin, there were many other Cryptocurrencies introduced in the market. Some of them are Ethereum, XRP, Tether, Litecoin, and EOS. They leverage blockchain technology to gain transparency, decentralization, and immutability (Politou et al., 2019). Blockchain has properties such as: i) All transactions are open, and any participant in the blockchain can see any user's information. ii) Transactions are in the nature of shared and decentralized form, which makes many duplicates of the blockchain co-exist together. iii) Also, transactions in blockchain are considered permanent in nature, which implies that any transaction information stored or documented cannot be changed or erased easily [1].

As the transaction is decentralized and data is encrypted and stored on multiple storage devices, a public blockchain is considered a transparent ledger, making it almost impossible to hack it [9]. Besides, permissioned blockchains are considered open and transparent to everyone or bounded, depending on the case-to-case basis. A private blockchain is considered to be less secure when compared to a public

blockchain as it mostly works on the basis of access controls that restrict the participants who can participate in the network [24].

*1.3 Blockchain and GDPR Compliance*

However, while blockchain has been touted as a fail-safe technology for securing personal data and privacy, there are concerns that it could potentially impinge. Most notably, blockchain poses lawful enforcement issues when storing information. It is said that any data which is written in the blockchain is considered to be permanent. This property of blockchain technology is why we hear that a blockchain is referred to as being immutable in nature [19].

Due to blockchain's immutable nature, the transactions in each block of the blockchain have the previous or predecessor block hash, which results in the formation of a cryptographically secure chain, and this property makes altering the chain practically impossible, as any change would invalidate all subsequent blocks [20]. If we consider the requirements of European Union GDPR regulation, therefore, the very nature of blockchain's protection lies with the privacy needed to protect personal data. Blockchain also opposes the Data Minimization principle of GDPR, which means collecting only the data which is required to fulfill a specific purpose [28]. Notably, conflicts between GDPR and Blockchain continue to exist between data subjects' rights to rectify, alter, remove data and Data controllers, Data processor's distinctive proof, and obligations on the blockchain [10].

*1.4 Conceptual Model for Research*

Figure 2 discusses the phase by phase approach followed for this systematic literature review.


**Figure 2:** Conceptual Model

## 2. Research Objective and Prior Research

The idea behind this research is to chalk out the previous research papers, their results, reviewing the efforts of GDPR-compatible Blockchain research. Explicitly focused on data subjects entitled rights to rectify transaction data and delete data whenever data is processed excessively. For this purpose, we have created 2 research questions to perform the research work more progressively is shown in Table 1.

**Table 1:** Research Questions

| Research Questions | Discussion |
|---|---|
| RQ 1: In which areas, blockchain technology is not aligned with the privileges of the data subject in GDPR? | The transactions between participants are permanent, immutable, open, and visible in nature to every participant in Blockchain technology. In addition, the basic principle of this blockchain technology is to distribute data. But these discussed properties of blockchain make it difficult for the GDPR data subjects to utilize personal data privacy rights and the wide distribution of data in blockchain contradicts the principle of data minimization. |
| RQ 2: Which methods or techniques are available for blockchain to exercise the GDPR data subject rights capacity on the right to erase, right to rectify the processed personal data? | A few articles addressed approaches on Self-sovereignty, Hashing techniques, Encryption, Decentralized identities, and Zero-knowledge proofs methods that help the data subject to utilize their rights. This question revolves around those papers which discussed the use-cases, applications, and types of techniques used to address data privacy issues of blockchain in concern to GDPR. |

### *2.1 Literature Review of Primary Studies*

In relation to compliance design between Blockchain technology and GDPR, so far as we might reasonably learn, Systematic Literature Reviews (SLRs) tend to be particularly limited on this topic. One of the very recent articles covered GDPR and Blockchain technology compliant design [25]. In [15], existential resolutions for self-sovereign distinctiveness on blockchain also investigate the problems associated with GDPR. However, there seems a requirement for the case through case analysis to understand the authorized uncertainties and privacy-enhancing technologies. When it comes to technologies, it cites a comprehensive review of technical and advanced cryptographic techniques to resolve conflicts when applied in permissioned and permissionless blockchains. Given sluggish adoption into real-life applications through blockchain, scientist's approach towards researching methods is remarkable [29].

Consent from the user is one of the major responsibilities of the Data controller when collecting personal data; the user here in terms of GDPR means data subject [30]. A decentralized model guarantees access to user data only by approved parties on the basis of user consent. This discusses the correctness, completeness mechanisms for user consent [3]. It discusses a comprehensive analysis of the current cutting-edge technologies in the field of privacy that retains research approaches and processes in blockchain privacy issues. There is still a need to be discussed about the main problems resulting from the

applicability of techniques to protect privacy due to cryptographic operations. Further, there is a need to focus on exploring current threats to next-generation DFS technologies which are yet to be fully exploited.

In [13] discussed the information precise to be disremembered in concern with the right to erase the data if they believe that their personal data is no longer needed to be stored by the data controller. This paper expresses the intent of presenting digital information lawfully, which obliges others to obscure personal information about others at the data subject request. There are several questions and problems that have arisen in relation to the effect of GDPR on information security operations [11]. This work has given researchers [12] clear discussion in support of exchanging data in cybersecurity [27].

The studies explained the role of technologies such as Jolocom, Decentralized identities, Hashing techniques, and Encryption techniques and how those help data subjects to perform the secured transactions. A need for potential research in further to design-based solutions, use-cases, and reduced latency is much more required from the researchers in the nearby future. This helps to address the problem with increased accuracy and maintain the conduct of data privacy. Therefore, more researches need to be performed, as this is a newly developed concept, and there is a lot of areas for future researchers to explore more in this area and find out more feasible concepts and architectural solutions [26].

## 3. Research Methodology

We followed the Systematic Literature Review to build this paper according to the direction of [14] paper to achieve the aim of the research questions.

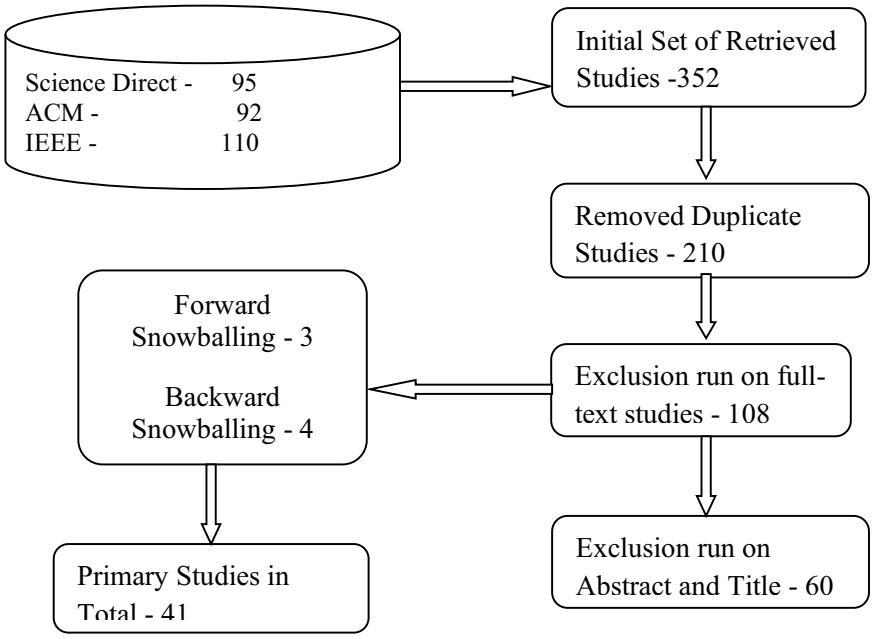


**Figure 3:** Process for Selection of Primary Studies

### *3.1 Primary studies*

Research project studies were conducted by performing a search on particular keywords in respective search engine databases. Search engine databases that were used for searching research papers are mentioned below in Figure 3.

*3.2 Quality Assessment Criteria*

Criteria for inclusion and exclusion impose restrictions for the literature review. They are usually determined before the search is conducted after the research questions are set. However, scoping searches may need to be undertaken to determine appropriate criteria. Information about the requirements for inclusion and exclusion is generally reported as a paragraph.

This Systematic review addresses the necessities for inclusion and exclusion, which report observational findings dependent on the idea of the papers tending to the new territories of blockchain. Other than this, it talks about fortifying data protection issues with effective methodologies for use-cases.

The total number of studies found for the respective platforms for the initial keyword searches was 352. Then a search was done to remove the duplicates, and it was reduced to 210 articles. This SLR selected inclusion and exclusion criteria to set the boundaries for the systematic review. After following this criterion, the papers were reduced to a total of 60. Those 60 articles were interpreted in articles containing full-text and a remainder of 34 papers included. Using the Forward and Back snowballing method, 7 articles were identified, totaling the final number to 41 research studies.

*3.3 Inclusion criteria*

- The article ought to contain a clarification of sorts of blockchain transactions, their attributes, and concerns of privacy.
- The article should be focused on the GDPR access rights of data subjects and whether distributed ledger technology is legitimate with consumer privileges to exercise their rights based on this paper research questions a) The subject data rights for processing of data. b) Compliance concerns of distributed ledger and GDPR.
- The article ought to examine the use-cases that offer powerful and potential advancements that follow blockchain and information security, strategies for structure protection, self-sovereignty, and encryption.

*3.4 Exclusion Criteria*

- The articles are focusing solely on blockchain cryptocurrencies like Bitcoins, Ethereum, Libra, Litecoin, etc.
- The papers were offering non-peer-reviewed literature, including technical reports, editorials.
- The articles are non-English and focus on different advances like IoT, programming, etc.

*3.5 Data Analysis*

Table 2 interprets the excluded studies, which are run on full-text analysis. We have found a total of 7 primary studies to be excluded after performing the quality assessment process suggested in [23]. Figure 4 demonstrates the Primary studies published over time.

**Table 2:** Criterion for Excluded Studies

| **Criteria Stages for exclusion** | **Excluded Studies** |
|---|---|
| Stage 1: Related to Blockchain | [19], [8], [9] |
| Stage 2: Context | [31], [33] |
| Stage 3: IoT | [34] , [30] |

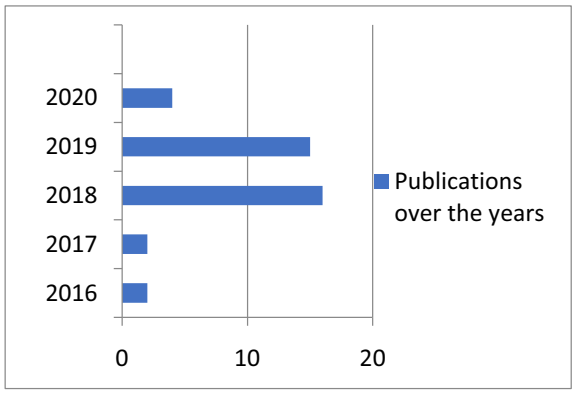


**Figure 4:** Primary studies published over the time

## 4. Research Findings

All the primary studies were read and evaluated, both qualitative and quantitative, in the full specification. The research focused on irreversible blockchain existence, the permanence of blockchain-written data, and incorrigible transactions. Studies based on self-sovereignty, collective identification, hashing techniques, etc.

The trends found in the primary studies highlight that due to its free and transparent nature of transactions, nearly half of all studies on blockchain and its data privacy issues concerned. Privacy techniques are the second most common theme, with 20%. The studies provide potential technological approaches for a self-sovereign individuality on blockchains also examine the problems that occur in concern to the European Union GDPR. This also speaks about how blockchain can get around these issues. ZKP applications hold great promise in terms of data protection through design and self-sovereign control. Each block contains the hash of the predecessor one, which means the block is connected linearly back to the original block of genesis. The challenge of modifying one block and finding correct hashes for all the following blocks is what makes the blockchain almost incorruptible or immutable. Some research papers discussed the data security strategies that need to be placed in place and how to rectify the data, although few papers discussed how data controllers can play a role for a data subject itself and manage the transactions in the blockchain.

In the blockchain, bitcoin is the most famous application of blockchain technology so far. Other cryptocurrencies such as Ethereum, Libra, Litecoin, and Zcash are also considered to be familiar [21]. In fact, Ethereum is considered to be the second-largest cryptocurrency. To show details of transaction nodes in the blockchain, we have taken bitcoin transactions as an example. Bitcoin blocks generally contain around 1500-2000 transactions. Blocks are limited to 1MB in size. A timestamp is a nonce, a hash list of predecessor blocks in a transaction chain as shown in Figure 5. Transactions records are historical, verifiable, incorruptible in mature. Each record adds to the chain of blocks.

## 5. Research Discussion

The initial keyword searches indicate a good amount of blockchain-related papers exist. But here, in this research paper, the only blockchain is not the consideration. Besides, it also deals with GDPR. So research keyword searches were mostly focused on blockchain and GDPR combined instead of solely searching on blockchain technology and GDPR separately. Though we have considerable papers on Blockchain and GDPR[31] if segregated separately, there are fewer amounts of papers that discuss qualitatively on the combination of data privacy GDPR and blockchain technology. The scope for research has been slowly

seen a spike in the past 2 years. This shows how researchers were interested in exploring the data privacy issues of transparent blockchain transactions when it comes to protecting the data subject privacy [32].

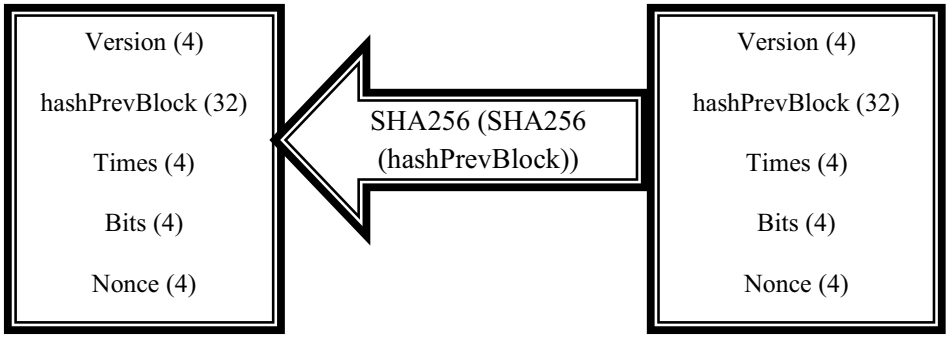


**Figure 5:** Bitcoins linked block headers

*5.1 Research Question 1: How is blockchain technology non-aligned with the privileges of the data subject in GDPR?*

Blockchain has compliance issues in handling GDPR personal data processing. Supposedly, it is because of the permanence nature of blockchain with respect to the GDPR principle of storage limitation. Besides this, it is also noted that blockchains can be effective in providing solutions and meet the necessities imposed by GDPR regulation. For instance, the permanence of activities completed on blockchains can empower arrangements that successfully follow the consent of data subject [1] . As a data privacy law, GDPR speaks to advancement instead of a revolution. The decentralized model used by blockchain brings about a large number of actors engaged with the processing. This adds a layer of unpredictability to compliance with a legitimate structure that was not planned in light of blockchain[33].

Participants should carefully select the type of blockchain that aligns with their design to the data protection processing principles under GDPR and always try to minimize the personal data stored in a chain. In a blockchain:

a) Participants with the right to make entry can act as data controllers;
b) Miners who validate the transaction containing personal data on a blockchain can act as processors; and
c) Accessors may be acting either as processors or controllers.

Data subject access rights, right to access personal data and right to data portability are not, from the outset, but especially risky on the blockchain. Actualizing the rights to delete, object, and rectify can be challenging; however, there are few technical solutions that were talked about by some research papers prior in their studies which will help to exercise those rights that can draw nearer towards compliance with GDPR [16], [2]. As a data controller and data processor, an enterprise must be able to show compliance with the GDPR requirements, or at most, record how the implementation is progressing by performing risk assessments, data protection impact assessments company-wide.

*5.2 Research Question 2: Which methods or techniques are available for blockchain to exercise the GDPR data subject rights capacity on the right to erase, right to rectify the processed personal data?*

In GDPR, controllers or processors are organizations handling personal data. The test for deciding who is acting as a controller is focused on reality. The controller's job is to define the data processing means and ends. This is also unique to the processing carried out: an individual may behave as a controller in respect of a specific process related to a specific set of personal data and simultaneously as a processor in respect

of a different process related to the same set of personal data. Here entity means the transaction initiator, i.e., the data subject, maybe someone who is processing the data.

Article 17 of GDPR states data subjects reserve the option to have individual information that is required no longer with the end goal of legitimate preparing to be erased. As discussed, permission blockchain is one of the answers for the option to restrict the processing; there are studies about the self-sovereignty method explained by researchers. The Sovereign or Decentralized Network is the first public permission blockchain as a global public utility to support self-sovereign identity and verifiable statements exclusively. Recent advances in blockchain technology now allow each public key to have its own address, known as a decentralized identifier (DID). A DID store on the public ledger along with a DID essay which includes the identification key for the DID, all other sensitive authorizations that the identity owner chooses to reveal to the identification, also the network statements for communication. A large no. of studies indicate that the identity owner manages the DID record using the Sovrin network by accessing the corresponding private key[34].

Jolocom framework helps in the storage of DID's on the public permission less blockchains. Sovereign, Jolocom does not store the authorizations on a blockchain. The authorizations are mutual with an agent, a cloud provider. The supervisor could be the distributing organization, some agent. Frequently authorizations can only be provided at the data subject request so that a credential is revoked under their control, while the distributing organization may only enhance notice of the revocation. A data subject is itself deemed to be responsible for the personal data processing; the GDPR may not extend to them. However, it might be applied to computers on behalf of the data subject [15].

To understand how to categorize the controller, the processor, we need to understand the transaction procedure in the blockchain. DIDs are deposited on a blockchain. On blockchains, we have to differentiate among the levels of supervisor on the blockchain level, transaction-level, besides - if applicable - the controller on the clever contract level. A real solution would be to simply store the personal data somewhere else, somewhere where we have read and write access. Let’s say a secure server or cloud server. Then we can store a reference to that data on our blockchain [22]. Almost like a shortcut or pointer. To create this link, we make a digital fingerprint of our data using a hash function, and then we store that hash on the blockchain as shown in Figure 6 a. Hash has two interesting properties:

- Hashes work in one way, meaning participants can create a hash of some data but cannot take the hash and turn it back into data.
- The hash function allows us to verify that the files on the central server haven't been tampered with. The hash stored inside the blockchain is just a string of random letters and numbers, but it qualifies as personal data [35] because it can be linked to the data on the server is shown in Figure 6 b. In order to exercise the right to erase a data subject, they just remove actual data from the central server. In that case, the hash in our blockchain becomes useless and no longer considered personal data because it points towards nothing.

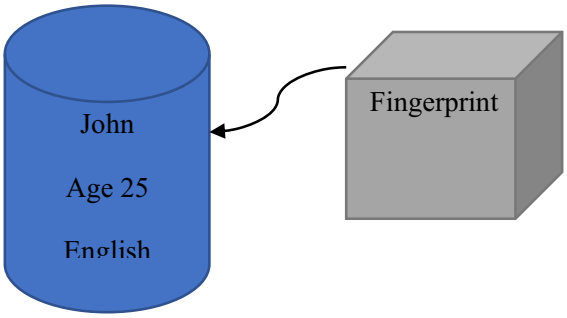


**Figure 6 a:** Hashing link with a digital fingerprint

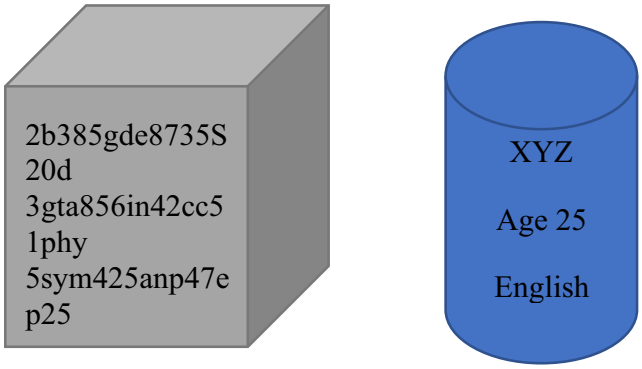


**Figure 6 b:** Hashing link to personal data

## 6. Conclusion

Regardless of the fact that blockchain technology provides the upsides of transparency and immutability, but these properties of blockchain cause significant conflicts with GDPR data protection regulation. Blockchain developer's tasks ought to, in this way, cautiously investigate the information proposed for capacity in blockchain and weigh up its favorable circumstances and disservices of the sort on how blockchain to be utilized.

The beneficial thing about this topic is that blockchain is at a phase where the establishments are yet being constructed, and a portion of these establishments will have the option to consolidate the spirit and the letter of the GDPR over time.

## 7. Future Scope

Blockchain is a newer technology and EU GDPR is a new data privacy law, a further research scope is large to understand more about these two, as it build on it gives the opportunities to researchers to find the different approaches which would be feasible to maintain compliance with respect to personal data protection. We need to remember that data protection is a journey, but not a destination. The deeper the technologies get developed, the more there will be scope of understanding and resolving the issues with respect to the data privacy laws. There's needed to be a thorough research done on the following:

- How Blockchain customers can rely on its transparency and be assured of the confidentiality and integrity of data using newly developed technologies?
- What are all of blockchain's cybersecurity issues that need to be discussed to prevent attacks?

**Acknowledgement**

The authors wish to acknowledge Symbiosis Centre for Information Technology for providing the library facilities.

**Conflict of Interest:** There is no conflict of interest among the authors

**Funding:** Self-funded

**Ethical approval:** Not applicable

**References**

[1]. Casino, F., Politou, E., Alepis, E., & Patsakis, C. (2020). Immutability and Decentralized Storage: An Analysis of Emerging Threats. IEEE Access, 8, 4737–4744. https://doi.org/10.1109/ACCESS.2019.2962017
[2]. Compert, C. M. L. (@MauLui) B. P. (@lebertrand). (2018). Blockchain and GDPR. 1(1), 8–23. https://doi.org/10.3868/s050-004-015-0003-8
[3]. Davari, M., & Bertino, E. (2019). Access Control Model Extensions to Support Data Privacy Protection based on GDPR. Proceedings - 2019 IEEE International Conference on Big Data, Big Data 2019, 4017–4024. https://doi.org/10.1109/BigData47090.2019.9006455
[4]. Distributed, C., & Union, E. (n.d.). Distributed Ledger Technologies and Data Protection in the European Union. 1–57.
[5]. Farshid, S., Reitz, A., & Roßbach, P. (2019). Design of a Forgetting Blockchain: A Possible Way to Accomplish GDPR Compatibility. Proceedings of the 52nd Hawaii International Conference on System Sciences, 6, 7087–7095. https://doi.org/10.24251/hicss.2019.850
[6]. Finck, M. (2018). Blockchains and Data Protection in the European Union. European Data Protection Law Review, 4(1), 17–35. https://doi.org/10.21552/edpl/2018/1/6
[7]. Finck, Michèle., & European Parliament. European Parliamentary Research Service. Scientific Foresight Unit. (2019). Blockchain and the General Data Protection Regulation : can distributed ledgers be squared with European data protection law? : study. In European Parliament (Issue July).
[8]. Gu, J., Sun, B., Du, X., Wang, J., Zhuang, Y., & Wang, Z. (2018). Consortium blockchain-based malware detection in mobile devices. IEEE Access, 6, 12118–12128. https://doi.org/10.1109/ACCESS.2018.2805783
[9]. He, Y., Li, H., Cheng, X., Liu, Y., Yang, C., & Sun, L. (2018). A Blockchain Based Truthful Incentive Mechanism for Distributed P2P Applications. IEEE Access, 6, 27324–27335. https://doi.org/10.1109/ACCESS.2018.2821705
[10]. Horák, M., Stupka, V., & Husák, M. (2019). GDPR compliance in cybersecurity software: A case study of DPIA in information sharing platform. ACM International Conference Proceeding Series. https://doi.org/10.1145/3339252.3340516
[11]. Hristov, P., & Dimitrov, W. (2019). The blockchain as a backbone of GDPR compliant frameworks. Quality - Access to Success, 20(October), 305–310.
[12]. Ibáñez, L., O'Hara, K., & Simperl, E. (2018). On Blockchains and the General Data Protection Regulation Brief introduction to Blockchain technologies. 1–13.
[13]. Jones, M. L., Zeide, E., Mai, J.-E., Jones, E., Dupre, J., & Richards, N. (n.d.). THE RIGHT TO BE FORGOTTEN. http://www.forbes.com/sites/homaycotte/2014/09/30/ame
[14]. Keele, S. (2007). Guidelines for performing systematic literature reviews in software engineering. Technical Report, Ver. 2.3 EBSE Technical Report. EBSE.
[15]. Kondova, G. (2020). Self-Sovereign Identity on Public Blockchains and the GDPR. 342–345. https://doi.org/10.1145/3341105.3374066
[16]. Lima, C. (2018). Blockchain-GDPR Privacy by Design. IEEE Blockchain, June, 1–5.
[17]. Lyons, T., Courcelas, L., & Timsit, K. (2018). Blockchain and the GDPR. 4–31. https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf
[18]. Malgieri, G. (2020). The concept of Fairness in the GDPR. Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency, 154–166. https://doi.org/10.1145/3351095.3372868
[19]. Mann, S., Potdar, V., Gajavilli, R. S., & Chandan, A. (2018). Blockchain technology for supply chain traceability, transparency and data provenance. ACM International Conference Proceeding

Series, 22–25. https://doi.org/10.1145/3301403.3301408
[20]. Melin, K., & Melin, K. (2019). The GDPR Compliance of Blockchain technology study on regulating innovative technology.
[21]. Moinet, A., Darties, B., & Baril, J.-L. (2017). Blockchain based trust & authentication for decentralized sensor networks. 1–6. http://arxiv.org/abs/1706.01730
[22]. Muma, S., Kappos, D., & Sumroy, R. (2012). The Right to Be Forgotten Meets the Immutable - A Practical Guide to GDPR-Compliant Blockchain Solutions. 1. https://www.cravath.com/files/Uploads/Documents/Publications/3898415_1.pdf
[23]. Nuseibeh, B. (2010). IEEE Transactions on Software Engineering: Editorial. IEEE Transactions on Software Engineering, 36(6), 735. https://doi.org/10.1109/TSE.2010.104
[24]. Ouaddah, A., Abou Elkalam, A., & Ait Ouahman, A. (2016). FairAccess: a new Blockchain-based access control framework for the Internet of Things. Security and Communication Networks, 9(18), 5943–5964. https://doi.org/10.1002/sec.1748
[25]. Biruk, Z., & Muleta, D. (2019). IoT based lawn cutter. International Journal of MC Square Scientific Research, 11(2).
[26]. Sirur, S., Nurse, J. R. C., & Webb, H. (2018). Are we there yet? Understanding the challenges faced in complying with the General Data Protection Regulation (GDPR). Proceedings of the ACM Conference on Computer and Communications Security, iii, 88–95. https://doi.org/10.1145/3267357.3267368
[27]. Taylor, P. J., Dargahi, T., Dehghantanha, A., Parizi, R. M., & Choo, K. K. R. (2019). A systematic literature review of blockchain cybersecurity. Digital Communications and Networks, June 2018. https://doi.org/10.1016/j.dcan.2019.01.005
[28]. Truong, N. B., Sun, K., Member, S., Lee, G. M., & Member, S. (2019). GDPR-Compliant Personal Data Management : A. 15(March), 1–13.
[29]. Manie, N., & Pattanaik, B. (2019). Zeta DC-DC converter based on MPPT technique for BLDC application. International Journal of MC Square Scientific Research, 11(2), 1-12.
[30]. Wu, Z., Williams, A. B., & Perouli, D. (2019). Dependable public ledger for policy compliance, a blockchain based approach. Proceedings - International Conference on Distributed Computing Systems, 2019-July, 1891–1900. https://doi.org/10.1109/ICDCS.2019.00187
[31]. Yu, Z., Xue, D., Fan, J., & Guo, C. (2020). DNSTSM: DNS Cache Resources Trusted Sharing Model Based on Consortium Blockchain. IEEE Access, 8, 13640–13650. https://doi.org/10.1109/ACCESS.2020.2966428
[32]. Zhang, R., Xue, R., & Liu, L. (2019). Security and privacy on blockchain. ACM Computing Surveys, 52(3). https://doi.org/10.1145/3316481
[33]. Zhang, Y., Deng, R. H., Shu, J., Yang, K., & Zheng, D. (2018). TKS: Trustworthy keyword search over encrypted data with two-side verifiability via blockchain. IEEE Access, 6, 31077–31087. https://doi.org/10.1109/ACCESS.2018.2844400
[34]. Zhao, Y., Li, Y., Mu, Q., Yang, B., & Yu, Y. (2018). Secure Pub-Sub: Blockchain-Based Fair Payment with Reputation for Reliable Cyber-Physical Systems. IEEE Access, 6, 12295–12303. https://doi.org/10.1109/ACCESS.2018.2799205
[35]. Zyskind, G., Nathan, O., & Pentland, A. S. (2015). Decentralizing Privacy: Using blockchain to protect personal data. Proceedings - 2015 IEEE Security and Privacy Workshops, SPW 2015, 180–184. https://doi.org/10.1109/SPW.2015.27