Data Privacy and Blockchain in the Corporate Context: Striking a Balance between Transparency and Data Protection

Parth Sharma

Assistant Professor of Law at Seedling School of Law and Governance, JNU, Jaipur

Abstract

In the digital era, companies face the dual challenges of safeguarding data privacy while ensuring transparency. Blockchain technology, known for its decentralized and unchangeable characteristics, presents potential solutions to improve data security and reliability. Nonetheless, its built-in transparency may clash with data protection laws such as the General Data Protection Regulation (GDPR), which highlights user rights including data deletion and consent administration. This paper examines the complex equilibrium between utilizing blockchain's transparency and maintaining strict data privacy regulations in corporate environments. It explores the difficulties presented by blockchain's unchangeable ledger regarding data deletion requests and investigates possible solutions, such as off-chain data storage, permissioned blockchains, and privacy-enhancing technologies like zero-knowledge proofs. Through the examination of existing regulatory structures and technological progress, the research seeks to offer an in-depth insight into how businesses can manage the challenges of incorporating blockchain technology while adhering to data privacy regulations.

Keywords: Blockchain, Privacy, Corporate, GDPR and Data Protection

Introduction

India was placed sixth in terms of the biggest amount of data breaches among countries. According to research by cybersecurity startup Surfshark, 18% of Indians have experienced data breaches since 2004. The relationship between data privacy and blockchain technology has become an emerging field of study in the changing digital transformation scenario. Blockchain, first designed as the supporting technology for Bitcoin, has expanded into a decentralised ledger system with the potential to transform multiple industries, including finance, supply chain management, and healthcare. It is known for its immutable, transparent, and tamper-resistant record-keeping features that have gained substantial attention from companies looking to streamline operations, boost trust, and optimise efficiency. This research explores the complex relationship between transparency and data protection in the corporate world, a balance that is becoming more crucial in the digital era. Corporations are facing the challenge of balancing transparency to preserve trust and compliance with demanding worldwide data protection rules, while still safeguarding sensitive data. Blockchain technology in this scenario can become a possible path to achieve this equilibrium. Yet, incorporating it into business data privacy strategy is filled with intricacies and possible drawbacks.

The major purpose of this research paper is to explore the subtle interplay between blockchain's promise to promote transparency and the requirement of data privacy. This paper aims to delves into the conceptual underpinnings of blockchain technology concerning data privacy and assesses its actual implementations and the issues encountered by companies currently. The authors tried to provide insights on how organisations might use blockchain technology to create a transparent and safe data environment through the analysis of legal frameworks, and regulatory landscapes. Besides, the paper provides a detailed examination that adds to the current discussion on digital ethics, presenting a sophisticated view on how blockchain might improve data privacy and transparency in company operations. Through this research, the authors intend to create a path for effectively applying blockchain technology in line with global data protection requirements by connecting theoretical knowledge with actual application.

Understanding Key Concepts

1. *Blockchain*

Blockchain technology aims to boost trust among users by safeguarding transactions on its network using Distributed Ledger Technology (DLT). DLT functions through a network of interconnected nodes that authenticate transactions when prompted. Once a transaction is verified, it is contained within a new block, which is then chronologically added to a series of existing blocks, building a blockchain.[1] This blockchain is immutable, meaning once a block is added, its data cannot be altered. Attempts by any single node to modify information on the blockchain would be invalidated by the rest of the network, guaranteeing the integrity of the ledger. Essentially, blockchain functions as a continuously growing ledger that timestamps and records data securely after each transaction. Any attempt to amend or reverse transactions would require a new transaction, which must also be confirmed and uploaded to the blockchain as a new block.

One of the primary characteristics of blockchain is its peer-to-peer network structure, which eliminates the need for centralised authority or intermediaries to oversee activities. Instead, all nodes in the network hold collective responsibility for verifying and producing new blocks through consensus procedures. Transactions, including payments made using digital currencies like bitcoin, are recorded on the blockchain following certification by the network. Blockchains can be either public, allowing anybody to watch and participate, or private, confined to certain individuals. Public blockchains keep their records across a distributed network of nodes, boosting security and transparency since no single node may unilaterally alter the blockchain without consensus from the others, leaving the ledger tamper-proof.

2. *Smart contracts*

Nick Szabo, an American computer scientist and cryptographer, developed the concept of smart contracts in 1994[2]. Szabo defined smart contracts as transaction protocols that run on computers to autonomously enforce contract requirements. He compared smart contracts to a vending machine, explaining that smart contracts function similarly to a vending machine by executing a certain action

[1] Jean Bacon, Johan David Michels, Christopher Millard and Jatinder Singh, *'BlockchainDemystified'* (2017) 31, Queen Mary School of Law Legal Studies. 268.

[2] Nick Szabo, *'Smart Contracts'* (1994).

once certain conditions are met. Smart contracts gained significant attention only after the introduction of Bitcoin in 2008 by the pseudonymous creator Satoshi Nakamoto[3], following Szabo's initial work.[4] Smart contracts are digital representations of conventional contracts that operate based on a conditional logic of “if this, then that.” These contracts are integrated into a blockchain, which is a decentralised ledger that is resistant to tampering and spans a network of peers. The decentralised structure prevents any single party from making changes, eliminating the need to trust that the other party would meet their responsibilities. A smart contract programmed to release payments to a child upon reaching a specified age will only activate if that condition is met, safely enforcing the agreement without manual intervention.So far there is no judicial pronouncement in this nascent field, but court recognises that contract do not become unenforceable just because it is in digital format.[5]

Data Privacy Issues in Corporate Sector

In the corporate sector, data privacy exceeds basic regulatory compliance to become a crucial component of trust, reputation, and financial stability. At the centre of any customer-corporate relationship is trust, a fragile commodity that, once damaged, is difficult to rebuild. Customers entrust firms with their personal data under the assumption of security and privacy. A breach or exploitation of this trust can lead to immediate and significant loss of confidence, making recovery a challenging effort.

The importance of preserving a flawless reputation in today's digital age cannot be emphasised much. A company's goodwill is one of its most precious assets, and data privacy errors can ruin this image in seconds. The quick spreading of information online means that news of a data breach can spread globally in a matter of hours, leading to broad reaction from customers, partners, and the public. This not only undermines client loyalty but may also lead to severe financial losses when stakeholders remove themselves from the organisation.

Moreover, the legal and financial penalties of failing to respect data privacy legislation such as “Information Technology Act” 2000, the CICRA “Credit Information Companies Regulation Act”, 2005 and the latest “The Digital Personal Data ProtectionAct”, 2023 (DPDP) at national level EU’s GDPR and CCPA at international level are severe. These rules are designed to enforce ethical data management methods, and non-compliance can result in large penalties and legal challenges. Beyond the financial penalties, the process of navigating legal disputes and addressing compliance concerns can take resources and focus away from a company's core operations, further hurting its performance and growth.

Moreover, in an era where data breaches are all too common, exhibiting a strong commitment to data privacy might act as a competitive advantage. Consumers are more aware of and concerned about their privacy, making it a significant aspect in their decision-making process. Companies that can ensure clients of their data's safety are more likely to recruit and retain those that promote privacy.

Lastly, the influence of data privacy on internal stakeholders, notably employees, cannot be underestimated. A culture that cherishes and protects personal information generates a sense of security among the workforce. This not only boosts morale and productivity but also confirms the company's overall commitment to privacy, generating a positive feedback loop that benefits all sides of the organisation.

[3] Satoshi Nakamoto, “*Bitcoin: A Peer-to-Peer Electronic Cash System*” (2008) 1.
[4] Nick Szabo, “*Smart Contracts: Building Blocks for Digital Markets*” (1996).
[5] Tamil Nadu Organic Private Ltd. and Ors. v. State Bank ofIndia(2014) Mad AIR 103.

Therefore, data privacy in the corporate sector is a complicated issue that affects not just legal compliance but also trust, reputation, financial health, competitive posture, and internal morale. Companies that value data privacy are better positioned to negotiate the complexity of the modern business landscape, developing stronger, more resilient connections with both customers and staff.

Challenges

Companies hoard data that can drive innovations and sharpen competitive edges. But with great data comes great responsibility and this is where things get tricky.

- Risks related to third party- Companies rely on third parties, outsource vendors or providers for operating, processing and storage of data. However, entrusting sensitive data to third parties introduces additional privacy risks, particularly if these providers lack adequate security measures.[6] They may fail to adhere to compliances or standards.
- Regulatory compliances- Companies are subjected to various municipal laws and international regulations including EU's GDPR and various industry specific laws. There is a need to ensure compliance with these laws and this needs meticulous data governance practices. Failure to comply with these regulations can expose enterprises to significant legal and financial consequences.
- Data Breaches- Entities store vast amounts of personal and sensitive data, which can vary from basic information of customers to proprietary business information. Data breaches due to cyberattacks, financial fraud, identity theft and other malicious activities may not only compromise individual data privacy but also undermine corporate integrity and trust.[7]
- Cross border transactions of data: In a globalised business era, big entities often deal across multiple jurisdictions. This can complicate cross border data transfer due to differences in their legal framework and cultural norms. Ensuring compliance with data requirements and implementing adequate measures, such as data encryption and contractual protections, can be proved very essential for mitigating the risks associated with cross border data transactions.
- Budding Technologies: The advent of new technologies, such as AI, IOT and blockchain gives new challenges for corporate data protection These technologies can develop vast amounts of data and introduce privacy risks such as algorithmic bias, unauthorised access to data and various risks associated.[8]

Blockchain Technology: A Saviour Tool

Blockchain technology is causing a stir in the business world with its many potential advantages that might change a number of areas of how companies run their operations. Here are some significant domains in which blockchain is influencing the corporate environment:

1. *Logistics and Supply Chain:*

[6] Alexander Savelyev, "*Contract Law 2.0: Smart Contracts as the Beginning of the End of Classic Contract Law*".

[7] Accenture, *'Editing the Uneditable Blockchain: Why Distributed Ledger Technology Must Adapt to an Imperfect World'* (2017)

[8] Vinod Joseph, "*Deeya Ray and Protiti Basu, 'Fintech Laws in India A Primer*", (Mondaq2020)

Blockchain technology enables real-time tracking of the origin, location, and condition of resources and items as they travel through the supply chain. This openness can guarantee ethical sourcing methods, enhance food safety, and fight counterfeiting.Blockchain can simplify supply chain operations and lower administrative expenses by automating tedious processes and doing away with the need for middlemen. In order to achieve the objectives of supply chain visibility and transparency, blockchain increases the number of suppliers and buyers as well as helps to ensure the integrity of data moving through the supply chain. One instance is Walmart's use of the blockchain network IBM Food Trust to track leafy greens since 2018.[9]

2. *Safe and Effective Transactions:*

Transaction records are guaranteed to be secure and unchangeable by blockchain's distributed ledger technology, making them resistant to fraud and tampering. This can be especially helpful in high-value or sensitive information-related transactions. Blockchain has the potential to greatly expedite transaction settlement, saving money and time compared to more conventional approaches. Ripple aims to lower chargebacks in transactions involving digital asset exchanges, banks, businesses, and payment processors. It allows for cross-border transactions with the virtual currency known as "Ripple," which is currently one of the most popular cryptocurrencies along with ether and bitcoin.[10]

3. *Enhancing Corporate Governance:*

Blockchain technology can be used to make company actions transparent and auditable, improving accountability and lowering the possibility of misbehaviour or fraud.It can promote trust and enhance investor relations by giving investors transparent, safe access to company data. Odra is a state-of-the-art blockchain network that lets companies interact directly using smart contracts. Data on the entire network can only be accessed by registered users via the approved blockchain of Corda. It has no cryptocurrency or built-in tokens. Its authoritative operation provides precise control over access to digital information while bolstering anonymity.[11]

4. *Novel Business Structures:*

Blockchain technology enables the creation of virtual tokens that stand in for tangible assets like stocks, patents, or even tangible commodities. This creates new opportunities for finance and asset trading.D apps, or decentralised apps, are programs that operate on a decentralised network and are not governed by a single party. They can be created using blockchain technology. The two main categories of blockchain applications in finance are decentralised finance, or DeFi, and cryptocurrencies. Even with the recent setbacks, cryptocurrency is becoming more and more accepted as a substitute for traditional payment methods in the global financial system, which is mostly controlled by huge payment processors like Mastercard and Visa as well as government central banks.DeFi is also starting to show promise as a

[9] Yiannas, Frank. "*A new era of food transparency powered by blockchain." Innovations: Technology, Governance, Globalization*" (2018): 46-56.

[10] George C. Dumitrescu, "*Bitcoin – A Brief Analysis of the Advantages and Disadvantages*", (5(2) Glob. Econ. Obs. 63 2017)

[11] Shafi Mohamad et al., "*Blockchain Technology: Implications for Accountants*", Int'l J. Innov. Creativity Chang. 101 (2020).

possible substitute for other procedures that banks and other financial service providers have historically managed, including credit, insurance, banking, and investing.

5. *Additional Uses:*

- Financial services firms are incorporating decentralised finance technology into their conventional centralised finance systems. Additionally, they are utilising blockchain technology to expedite payment processing on private networks by doing away with the need for traditional clearinghouses, which might take a day or longer
- In order to facilitate pharmaceutical research and facilitate the transmission of electronic medical records, new applications of genetic data and personal medical records are being made possible by blockchain's security, privacy, data integrity, and anonymity.
- Blockchain technology has the potential to simplify and legalise the process of obtaining a passport, voting online, transmitting personal identification electronically, and preparing legal and regulatory filings like financial reports and mortgage deeds.

Legal and Regulatory Framework

A. India

As of now, India does not have a single comprehensive law designed especially for blockchain technology. As the government and pertinent agencies weigh the possible advantages and disadvantages of blockchain technology and its applications, the regulatory environment is constantly changing. Depending on the particular blockchain use case, the below mentioned existing statutes apply to varied degrees.

1. *Information Technology Act, 2000*

Section 3 of Information Technology (IT) Act of 2000 acknowledges digital signatures as a legitimate method of electronic record authentication. [12]Chapter III of IT Act, that is electronic governance, makes it easier to employ digital signatures and electronic records in official correspondence and governance. S.11 of IT Act addresses how to identify the owner of an electronic record and assign credit to them.[13]Section 15 addresses the security of digital signatures and electronic records.[14]Section 13 of IT Act addresses how to ascertain the time and location of electronic record dispatch and receipt.[15]Section 10A of IT Act authenticates agreements created electronically, reaffirming their lawful validity.[16]

2. *Indian Evidence Act, 1872*

The admissibility of electronic records as evidence in court is covered under Section 65B of the IEA. It describes the requirements, such as the need for a certificate identifying the electronic record, for the admission of electronic evidence.[17]Section 65C describes the way in which electronic evidence is admitted, and Section 65D lays out the requirements for computer-generated electronic evidence to be admissible. Section 65B of the Indian Evidence Act, which is a part of the Information Technology

[12]Information Technology Act, S.2
[13]Information Technology Act, S11.
[14]Information Technology Act, S.15
[15]Information Technology Act, S.13
[16]Information Technology Act, S.10A
[17]Indian Evidence Act, 1872, S.65B

Act,(IT Act) 2000 , addresses the admissibility of electronic records.[18] This is essential for establishing the legitimacy of blockchain-based documents in court. Under Sections 3, 3A, 5 of the IT Act, digital signatures are recognized by the Act and are necessary for non-repudiation and authentication on blockchain networks.[19]

3. *Indian Contract Act,1872*

Although blockchain is not mentioned explicitly in the Indian Contract Act, its principles nevertheless apply to contracts created with the use of these technologies.If properly constructed, blockchain smart contracts might be accepted as legitimate contracts under Indian law.Blockchain contracts will fall under the purview of the Indian Contract Act's offer, acceptance, and consideration principles.In this context there are certain sections of the Indian Contract Act, 1872 that are likely to be relevant. Some of the key sections that could be applicable to blockchain transactions include:

Section 10 defines the elements of a valid contract, including the offer, acceptance, and intention to create legal relations. Section17 deals with the definition of fraud which is an important element in the context of blockchain transactions to ensure the validity of contracts. Section 23 provides an outline for the necessity of a lawful consideration for a valid contract. This can be important in the context of smart contracts and blockchain-based transactions. Section24 specifies that if the consideration or object of an agreement is unlawful, the contract becomes void. Section 56 states that agreements to do impossible acts are void. In the context of blockchain, this may relate to the technical feasibility of smart contract execution. Section 73 provides remedies for breaches of contract, which could be applicable if a smart contract on the blockchain is not executed as agreed.

4. *Companies Act of 2013*

The Companies Act, 2013 does not explicitly mention blockchain technology. Although there isn't a clear reference, several sections may become indirectly applicable depending on how blockchain is specifically used within a corporation.

I. Debentures and Capital Issued in Chapter IX:The process of raising money through different channels, such as initial public offerings, is covered in this chapter. Section 62: Any issuance of securities is subject to shareholder approval under this clause, which may also apply to token offerings if the relevant regulations consider them to be securities.[20]

II. Registrations and Returns: Chapter XII The several registrations and returns that businesses must keep up to date and submit to the Registrar of Companies (ROC) are described in this chapter. Sections128–138: The information that must be included in the company's filings is outlined in these provisions. Depending on how blockchain is used specifically, businesses may need to decide whether any disclosures fall under these categories.[21]

[18] Indian Evidence Act, S.65C and 65D.
[19] Information Technology Act ,S.3, 3A, 5.
[20] Companies ActS.62.
[21] Companies Act,Sections 128–138.

III. The Balance Sheet, Schedule III:The format for a company's balance sheet is specified in this schedule. By notification dated 24.03.2021, the Ministry of Corporate Affairs (MCA) amended Schedule III to the Companies Act, 2013 to require certain disclosures from companies in their financial statements, with effect from April 1, 2021, in an effort to increase transparency in the reporting of financial statements. If the company made any trading or investment in virtual or cryptocurrency during the fiscal year, the information related to profit or loss on transactions involving virtual or cryptocurrency currency, the total amount of money held as of the reporting date, and any advances or deposits made by anybody with the intention of trading or investing in virtual or cryptocurrency currency must be revealed.[22]

5. *Digital Personal Data Protection (DPDP) Act,2023*

The Digital Personal Data Protection (DPDP) Act and blockchain have a complex and growing relationship. While the DPDP Act strives to protect the privacy of individuals' data, blockchain technology inherently maintains data on a public and distributed ledger. Section 7(a) requires the data fiduciary to erase personal data after its purpose is accomplished. Blockchain data is immutable, making deletion difficult.[23]

Under section 16, the central government can prohibit personal data transfer to third countries under this section. Cross-border data transfer blockchain applications may be affected.[24] The DPDP Act guarantees individuals the right to ownership of their personal data. How this right relates to blockchain-based systems, where data is spread over a network, is still being disputed.Blockchain offers high security characteristics due to its decentralised nature. However, the DPDP Act also demands specific data security procedures, and it's vital to maintain compliance with both sets of requirements.

6. *Prevention of Money Laundering Act, 2002*

In March 2023, the Prevention of Money Laundering Act, 2002 (PMLA) was revised in India to include Virtual Digital Assets (VDAs), also including cryptocurrencies, within its purview. The sections of PMLA relevant to blockchain technology are as follows:

Section 2(g) defines a "virtual digital asset" to mean "any information or code recorded on a distributed ledger, cryptographically secured, which can be transferred, stored, or traded electronically for payment or investment purposes, with or without an underlying asset."[25] This effectively places all bitcoin transactions within the jurisdiction of the PMLA.Section 5 requires reporting entities, such as cryptocurrency exchanges and Virtual Digital Asset Service Providers (VDASPs), to keep transaction records on file for at least 10 years.[26] Section 6 mandates that, like banks and other financial organisations, VDASPs adhere to Know Your Customer (KYC) standards.[27] Section 11 gives authorities the authority to look into questionable transactions and confiscate or freeze assets that may be used in

[22] Companies Act, Schedule III
[23] DPDP Act, S.7(a)
[24] DPDP Act, S.16.
[25] Prevention of Money Laundering Act, 2002 S.2(g).
[26] Prevention of Money Laundering Act, 2002 S.5.
[27] Prevention of Money Laundering Act, 2002 S.6

money laundering schemes.[28] Section 13 Gives the Financial Intelligence Unit-India (FIU-IND) the authority to fine and issue show-cause notices to VDASPs that violate PMLA guidelines.[29]

7. *Reserve Bank of India Act of 1934*

The Reserve Bank of India as per the RBI Act of 1934 has a big say in how people approach cryptocurrency and other blockchain-related applications. RBI guidelines and advisories are vital to take into account even though there isn't a specific statute on blockchain. There are no sections of the Reserve Bank of India Act, 1934 that specifically address blockchain technology. It has, however, been amended to allow for the possible blockchain-based issue of a Central Bank Digital Currency (CBDC):
Section 2(2) states that in order to include both physical and digital versions, the definition of "bank note" was expanded in this section in 2017.[30] This makes it possible for RBI to introduce a blockchain-based digital rupee. Although there aren't any explicit mentions of blockchain, the RBI has acknowledged the technology's potential impact on financial systems in the future with this update. Consequently, even while the RBI Act has been modified to perhaps accept blockchain for CBDC, it does not yet contain any particular rules or directives for its wider use outside of this particular use case. The RBI's Regulatory Sandbox Framework takes a cautious stance toward blockchain applications by excluding from its purview any actions pertaining to cryptocurrencies and initial coin offerings (ICOs).

8. *Income Tax Act, 1961*

The term "blockchain" is not specifically included in the Income Tax Act of 1961 because it was passed before blockchain technology was widely used. Nonetheless, when it comes to revenue from blockchain applications, such as cryptocurrency, two important aspects apply:

I. Section 115BBH was introduced in 2022 It specifically addresses the taxation of virtual digital assets (VDAs), such as cryptocurrencies, non-fungible tokens (NFTs), and other digital assets exchanged on a blockchain. It specifies that profits from the transfer of VDAs are subject to a 30% flat tax plus an extra 4% cess, with the acquisition cost being the only allowable deductible.[31]

II. Section 194S: This provision, which was also added in 2022, requires 1% Tax Deducted at Source (TDS) to be applied to payments made for purchasing VDAs. This TDS must be paid if the transactions surpass a specific threshold in a given fiscal year. The goal of this is to increase tax compliance inside the bitcoin ecosystem and collect taxes at the source.[32]

In India, case law addressing blockchain in particular is still in its infancy.

Internet and Mobile Association of India v. Reserve Bank of India (2020)[33]: The RBI's prohibition on banks engaging with cryptocurrencies was overturned by the Supreme Court, however the RBI is still warning about the risks involved. One popular use of blockchain technology is the regulation of

[28] Prevention of Money Laundering Act, 2002 S.11
[29] Prevention of Money Laundering Act, 2002 S.13
[30] Reserve Bank of India S.2(2).
[31] Income Tax Act1961,Section 115BBH.
[32] Income Tax Act, S.194S.
[33] MANU/SC/0264/2020

cryptocurrencies, which is a major responsibility of the RBI. The RBI does not have a complete prohibition on cryptocurrencies, but it has issued recommendations warning against their risks. The possibility of a Central Bank Digital Currency (CBDC) is another thing they are investigating.

Ministry of Information and Electronic Technology(Meity) : The **"National Strategy on Blockchain,"** published by MeitY, provides a framework for integrating blockchain technology into government and aims to promote further study and advancement of the field.[34] "Blockchain technology uses technology to enable trust in the digital world." In order to build a shared blockchain infrastructure and provide blockchain as a service, MeitY has also started a project to design and develop a national blockchain framework. Additionally, according to the paper published by Meity current rules and guidelines will be updated as the National Blockchain Framework evolves and more experience is gained during the implementation.[35]

After a multi-institutional initiative funded by MeitY called the "Distributed Centre of Excellence in Blockchain Technology" conducted a great deal of research, a proof of concept solution for the application of Blockchain in multiple areas was created. One such instance is the blockchain-based property registration system that Telangana is testing. In a similar vein, a general Proof-of-Existence (PoE) architecture built on the Blockchain has been created to allow PoE for digital artefacts, such as ensuring the authenticity of sale deed documents and academic credentials.[36]

B. International

1. General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) is a comprehensive rule in the European Union (EU) that came into effect on May 25, 2018. Its purpose is to safeguard personally identifiable information and ensure privacy. The General Data Protection Regulation (GDPR) is intended to provide individuals with increased control over their personal data and to set stringent standards on how corporations approach and manage such data. There are a number of obstacles and factors to take into account when it comes to the incorporation of blockchain technology, which intrinsically supports openness and immutability, with the General Data Protection Regulation (GDPR). Although blockchain technology isn't specifically mentioned in the GDPR, the following articles are relevant:

I. Lawfulness of processing (Article 6): The legitimate interests, permission, and contract fulfilment are some of the legal bases for processing personal data that are established in this article. Businesses utilizing blockchain technology must determine the legal justification for data processing and make sure that the selected justification is followed.[37]

II. Article 5(1)(c): Data Minimization: The focus of this article is on gathering and using as little personal data as is required for the intended use. Because blockchain technology stores all historical data by default, it can be difficult to follow this principle. Therefore, data that is maintained on the blockchain must be carefully chosen.[38]

[34] National Strategy on Blockchain –MeitY, (2021)
[35] (https://blockchain.gov.in/)
[36] "*Blockchain & Cryptocurrency Laws and Regulations 2024", *Global Legal Insights (2024).
[37] General Data Protection Regulation 2018, Article. 6.
[38] General Data Protection Regulation 2018, Article 5(1)(c).

III. Articles 12–22 Concerning Data Subject Rights: These articles give people several rights about their personal data, such as the ability to access, correct, delete, and limit processing (sometimes known as the "right to be forgotten"). Certain blockchains' immutability puts these rights in jeopardy because it might not be possible to completely erase data.[39]

IV. Data Processor and Data Controller (Articles 4(7), 24):The duties and obligations of organisations managing personal data are outlined in these articles. In permissionless blockchains, where there is no central authority, identifying the data controller (the responsible party) and processor (the party working on the controller's behalf) can be difficult.[40]

V. Supplementary Articles: Other articles, such as those discussing data security (Article 32),[41] transfers of personal data (Articles 44–50),[42] and reporting data breaches (Article 33),[43] may also be pertinent when processing personal data with blockchain technology, depending on the particular use case.

In essence, the integration of blockchain with GDPR compliance demands a deliberate and thoughtful strategy. Organisations must be aware of the possible conflicts and investigate technological and procedural solutions to ensure that the benefits of blockchain may be utilised without compromising individuals' rights to data privacy and protection.

Recommendations

1. Improve Regulatory Frameworks: Promote the creation and application of strong regulatory frameworks tailored to blockchain technology in order to resolve concerns about data privacy. A balance between protecting user data and promoting innovation should be struck by regulations.
2. Implement Privacy-Centric Blockchain Solutions: Promote the adoption of blockchain privacy-centric technologies to improve data confidentiality, such as zero-knowledge proofs. Organisations ought to investigate and fund blockchain solutions that put users' privacy first.
3. Educate Stakeholders: Create educational initiatives to raise knowledge and comprehension of the relationship between blockchain technology and data privacy among stakeholders, such as developers, companies, and legislators. For blockchain technology to be used responsibly and ethically, a knowledgeable community is essential.
4. Interoperability Standards: Promote the creation of interoperability guidelines to guarantee smooth communication across various blockchain networks. This can improve data privacy by offering uniform security protocols across different systems.
5. Continuous Auditing and Monitoring: Create a framework for ongoing blockchain network auditing and monitoring in order to spot and fix any privacy issues. To keep up with changing security threats, evaluations and upgrades should be carried out on a regular basis.

Conclusion

In conclusion, the authors examined how blockchain technology and data privacy interact in a corporate setting. There are a number of benefits in implementing blockchain in corporate settings, including less

[39] General Data Protection Regulation 2018, Articles 12–22.
[40] General Data Protection Regulation2018, Articles 4(7), 24.
[41] General Data Protection Regulation2018,Article 32.
[42] General Data Protection Regulation2018,Articles 44-50.
[43] General Data Protection Regulation2018,Article 33.

dependence on middlemen, more data integrity, and the ability to conduct safe and effective transactions. Achieving a successful integration of blockchain technology into corporations requires careful consideration of issues like scalability, interoperability, and regulatory compliance. Furthermore, because blockchain technology is dynamic, it requires constant study and development to keep up with new threats and weaknesses. Notwithstanding these obstacles, blockchain's potential advantages in protecting data privacy in a corporate context is clear. The technology has the ability to completely change how corporations handle and safeguard sensitive data as it develops and becomes more widely accepted.

Bibliography

I. STATUTES

1. General Data Protection Regulation[2018]
2. Income Tax Act 1961 (Act 43 of 1961).
3. The Information Technology Act, 2000 (Act 21 of 2000).
4. Companies Act 2013 (Act 18 of 2013).
5. Contracts Act 1872 (Act 9 of 1872).
6. Prevention of Money Laundering Act, 2002 (Act 15 of 2002).
7. Reserve Bank of India Act1934 (Act 2 of 1934).
8. The Digital Personal Data Protection Act, 2023(Act 22 of 2023)
9. Indian Evidence Act 1872 (Act 1 of 1872)

II. BOOKS

1. Daniel Drescher,Blockchain Basics: A Non-Technical Introduction in 25 Steps,(Apress,2017)
2. Don Tapscott and Alex Tapscott,Blockchain Revolution: How the Technology Behind Bitcoin and Other Cryptocurrencies is Changing the World, (Penguin Business,2019)
3. Misra &Tyagi,Blockchain Applications in the Smart Era, (Springer International Publishing, 2022)
4. Bruce Schneier,Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World,(W.W. Norton & Company,2016)
5. Shoshana Zuboff, The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power, (PublicAffairs,2020)
6. Woodrow Hartzog,Privacy's Blueprint: The Battle to Control the Design of New Technologies, (Harvard University Press,2018)

III. ARTICLES

1. Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction. (2016). Princeton University Press.
2. Zohar, A.’Bitcoin: under the hood’(2015). Communications of the ACM, 58(9), 104-113.
3. Swan, M. ‘Blockchain: blueprint for a new economy’(2015).O'Reilly Media, Inc.
4. Tapscott, D. & Tapscott, A. How blockchain is changing finance.(2017). Harvard Business Review, 94(6), 110-121.

5. Mougayar, W.The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology.(2016) John Wiley & Sons.
6. George C. Dumitrescu, “Bitcoin – A Brief Analysis of the Advantages and Disadvantages”, (2017) Glob. Econ.Obs. 5(2) , 63
7. Shafi Mohamad et al., “Blockchain Technology: Implications for Accountants”, (2020). Int’l J. Innov. Creativity,Chang. 101
8. Jean Bacon, Johan David Michels, Christopher Millard and Jatinder Singh, 'BlockchainDemystified' (2017), Queen Mary School of Law Legal Studies.31, 268
9. Yiannas, Frank. "A new era of food transparency powered by blockchain.",2018,Innovations: Technology, Governance, Globalization,46-56.

IV. DATABASES

1. KLUWER ARBITRATION
2. LEXIS ADVANCE
3. HEINONLINE
4. JSTOR
5. sMANUPATRA