# The Legal Implications of Blockchain Technology

**Waseem Irfan**
Faculty of Computer Science, Sukkur IBA University, Sukkur, Sindh, Pakistan
**Muhammad Furqan**
Faculty of Computer Science, Sukkur IBA University, Sukkur, Sindh, Pakistan

## Abstract

This paper explores the legal implications of blockchain technology, emphasizing its transformative potential across various sectors, including finance, healthcare, and supply chain management. It discusses the foundational aspects of blockchain as a decentralized and secure distributed ledger technology, highlighting its ability to facilitate transactions without intermediaries. The paper examines the unique legal challenges posed by blockchain, particularly concerning data privacy, smart contracts, and regulatory compliance. It addresses the tension between the immutability of blockchain records and the requirements of data protection laws, such as the EU's General Data Protection Regulation. Additionally, the paper analyzes the current regulatory landscape, noting the fragmented approaches across jurisdictions and the need for harmonization to foster innovation while protecting users. Case studies are presented to illustrate real-world applications of blockchain and the associated legal complexities. Ultimately, the study calls for a balanced regulatory framework that encourages technological advancement while safeguarding individual rights and promoting accountability. As blockchain technology rapidly evolves, it is essential for legal scholars and policymakers to engage with its implications to ensure effective governance in this emerging field.

## Keywords

Blockchain technology, legal implications, data privacy, smart contracts, regulatory compliance, decentralized ledger, General Data Protection Regulation, case studies

## 1. Introduction

The digital economy of today continues to evolve, with the arrival of blockchain technology as part of digitalization. The increasing adoption of blockchain technology is occurring in a wide variety of sectors, including agriculture, healthcare, finance, the Internet of Things, and smart contracts. Blockchain technology is, however, often

neglected by legal scholars. Thus, the legal implications of this technology, as the least developed area, shall be thoroughly researched.

Blockchain is a version of distributed ledger technology, based on cryptography. The technology ensures secure verification and authentication without a centralized intermediary. Blockchain is divided into three types, based on their control in the system: public blockchain, private blockchain, and consortium blockchain. The development of this technology has attracted the attention of researchers from multiple disciplines ranging from computer science to philosophical, legal, and business issues. Technically, blockchain technology creates new opportunities for social utility and economic benefit, but it also poses substantial challenges. The need to utilize the transparency, security, and redundancy that the method offers would warrant a thorough legal analysis of the technology (Dhar et al.2024)

This scientific study is designed to provide a comprehensive overview of blockchain technology, with a detailed evaluation of the distinctive features of this technology and consideration of legal requirements and contractual aspects impacting the blockchain. Tracing the trajectory of technological revolution, the study asks, “How does the law respond to the evolution of the technology?” and “How does the law deal with the digital revolution?” The difficulty lies in reconciling two divergent bodies of knowledge and discipline: law, a humanistic and normative discipline, and digital technology, a field of science that is empirical. The legal issues of blockchain technology deserve to be analyzed. This study is structured in the following way: it is divided into three main sections followed by a conclusion. A brief presentation of blockchain technology will be considered in the first part. In the second part, the distinctive features, implications, and standard requirements for blockchain technology will be evaluated. Also, in the same part, the legal framework for blockchain technology will be discussed. The third section discusses whether blockchain should be contractually regulated. The conclusion follows in the final part.

**2. Foundations of Blockchain Technology**

Blockchain technology is a unique information system because it is based on a data structure that is decentralized, transparent, and distributed to create a consensus across multiple users. Technically speaking, the term "blockchain" describes a form of distributed ledger technology that is often used as the foundation for the operation of

digital currencies. The principles that underpin distributed ledger technology and the blockchain represent a radical departure from central, top-down systems. Legal implications start with these decentralized networks. Every assertion or agreement submitted to the blockchain can be validated by an indefinite number of users, not subordinated to a central enforcer that decides what is valid (Liu et al., 2023)

Unsurprisingly, these core aspects, especially the principle of decentralization, generate considerable controversy. The "malleability" of the blockchain can lead to unwelcome changes in the consensus protocol. These controversial issues are pervasive and underline the need for a deeper understanding of the basic foundations of the blockchain and distributed ledger technology. The blockchain and distributed ledger technology are datasets that are shared among individual users. These assets may be highly dynamic and could be exchanged in a legal transaction, used as the basis for financial investment, represent a share in a company, or other rights and obligations. Data structure refers to the way that information is organized within an information system. The blockchain, technically speaking, is a data structure that stores and shares pieces or blocks of information across an Internet-based system. Once entered, the information in any given block cannot be deleted. Each block of data contains both a series of entries concerning transactions and the users who have the authority to enter new data into the system. Blockchains are often "chained" to each verifiable block of transactions and contain a record of when each transaction was entered. Each piece of information can stand independently and thus form a singular chain. Systems that rely on blockchain technology to verify, store, and spread information are known as distributed ledgers.

**2.1. Decentralization and Distributed Ledger Technology**

Decentralization is a core feature of blockchain technology. In a blockchain, data is stored in a way that allows it to be publicly verified but not tampered with, eliminating the need for a central authority to oversee the system. Decentralized systems enable information to be spread across participants, helping to promote trust and transparency among users. Distributed ledger technology is a decentralized database system that stores data across a network of interconnected computers. The operations of a distributed ledger are not controlled by a central authority, but rather distributed across all nodes in the system. This means that multiple parties have

simultaneous access to the database, providing secure and transparent storage and verification of public records.

Legal implications regarding the deployment of distributed ledger technology and decentralized technologies apply to multiple aspects of the technology. Technological features, namely offering a distributed and decentralized way in which to process, store, and access data at the global level, create jurisdictional challenges. Multiple parties can share the same set of data being accessed through different jurisdictions or countries, presenting difficulty if disputes over that same data would require legal resolution. To date, there is no global dispute resolution institution. Moreover, there are many current issues relating to the sharing of data between countries, typically referred to as governance, and they create adverse implications for the business intelligence value promised by distributed ledger systems. The potential for a dispute going beyond the use of code and smart contracts to resolve it adds further implications for regulators. In the absence of a centralized third party that vouches for the authenticity of the information stored in the blockchain, the risk of fraud and data tampering can elevate. However, this does not mean that a fully decentralized or distributed system has no drawbacks from a management point of view. There may be challenges in allocating responsibility and enforcing adherence to rules, as prior undertakings by participants may be hard to trace back. Public interests may conflict with anonymous participation in networks, yet the ability to censor free speech and the free exchange of ideas may also be criticized, especially under authoritarian regimes. Lastly, the inbuilt proposition for anonymity of transactional data in public systems can elicit concerns from regulatory authorities interested in knowing the beneficial owners in transactions. Contact details of transactions within public, if not also in permissioned systems, should also continue to be investigated by regulators to promote accountability and transparency. Conflict with possible abuses.

**3. Legal Challenges and Opportunities**

The use of a blockchain poses numerous legal challenges across a wide array of sectors. The integration of a blockchain system poses numerous challenges to traditional legal concepts and regimes. Established and deeply ingrained technological infrastructures have been created on the basis of paradigms within the legal context, which have evolved over time and in accordance with various legal sources and

organizational structures. The two most immediate challenges arise in relation to data protection and the usage of smart contracts, whereas further opportunities have been identified in connection with the presented challenges. The effects of blockchain on national and institutional law are completely unknown at this stage, and related guidelines do not exist. This is because policymakers are in a phase of knowledge-intensive discovery (Ferrag & Shu, 2021).

The immutability of blockchain systems and the irreversible process of record-keeping of personal data poses a threat to EU General Data Protection Regulation compliance. In principle, personal data on a blockchain can only be processed if the user or data controller has provided consent to do so. In a blockchain network organized through proper rights management within the context of the protocol, the right to add a set of data is typically transferred within the network. As subsequent rights assert that the data cannot be changed, the immutable character of permissioned and public blockchains constitutes a logic that, in its essence, implies consent. Part of the principles of "privacy by design and default" therefore remains the fundamental necessity to guarantee the authenticity of consents and decisions among users within a blockchain network. If there is no other regulation to refer to, then data could be considered the property of the network nodes since the nodes, during the execution of consensus mechanisms, can state who can access the data and when. Evidence for the latter can be found in blockchain licensing agreements where the unconditional provision of personal data eliminates guarantees on exclusive customer data control rights for the data controller. Blockchain can enforce and enhance data security on the user side, but at the same time, it may pose certain privacy threats. Digital certificates, for instance, may be used to secure data using blockchain underpinning without revealing the actual personal data. It could possibly also offer privacy-enhancing techniques to replace conventional policies; public keys designed in blockchain could be used as an identity token instead of the actual personal data (Hao et al.2022).

In principle, a contract on blockchain can be considered a smart contract. When a program is stored on-chain, it is indeed immutable, but if subsequent bilateral relations are conducted off-chain, databases, for instance, can be entered or uploaded again unless it leads to enforceable obligations in another legal system. The legal challenge, therefore, with regard to smart contracts, relates to whether smart contracts

are indeed smart contracts or even legal to enforce in the digital or non-digital world. In case a dispute occurs between stakeholders, it would be another question worth considering: At which jurisdiction should this case be represented? At the jurisdiction of the arbitrator, the country where the web publishing organization has its registered office, or the country of the consumer protection authority where the consumer has its domicile? If the case gets resolved in one of the mentioned jurisdictions, then which law should be applicable?

**3.1. Data Privacy and Security**

The most immediately apparent legal issue raised by blockchain is the conflict between the public visibility and immutability of transcribed data and the need in some cases to ensure an individual's privacy with regard to personal data. Many public and private enterprises are concerned with ensuring compliance in their dealings with the public, maintaining the standards expected of a trusted third party. For our purposes, the two main areas of law dealing with these concerns are data protection and computer misuse.

Every major jurisdiction in the world has developed some body of law or regulation dealing with issues of data protection, which have evolved in response to the technology itself. In the European Union, the General Data Protection Regulation came into effect in May 2018. Unfortunately, case law is sparse, regulation is just emerging, and the result is an uncertain and rapidly changing field. The principal trade-off revolves around public interest, a value that in all jurisdictions can often be subsumed with digital privacy laws. The status of digital data and security could be of concern to lawmakers who should not just accept an all-encompassing jurisdictional model of freedom of information or access to public records that sees transparency as an inherent good. They must also take into account the cybersecurity perspective, which is centered on ensuring that employees are not involved in an attack either unintentionally or intentionally as insiders (Kohl, 2021).

There are major challenges in the arts of data management, which is in the regulation of user consent in blockchain, personal data deletion, and the required right to be forgotten. Finally, the blockchain concept may seem robust to external hacks yet is prone to liabilities or risks either internal or external, particularly from insiders. An enterprise like Facebook working with user data might face the challenge of securing

the system against insider threats, including people who may accidentally leak personal data stored within the system, as well as from those who steal authentication credentials. While technologies exist to help deal with these risks, the regulatory environment in this area is as yet uncertain, and lack of legal clarity is known to stymie technological development by rendering investors uncertain about the security of their investments. Public concern over loss of privacy is therefore likely to refocus attention on the development of a legal framework in this area so far dominated by trade associations and user groups. In brief, there are fundamental commonalities between data protection concerns and blockchain. Even though the latter possesses a decentralized architecture, which is uncontrolled by any single party, it is clear that the lawful processing of personal data within such a structure is doubtful in the current regulatory and legal settings. Controlling law has stringent requirements to ensure user data registration, screening, and systematic record keeping, which was not designed with the non-modifiable nature of any blockchain in mind.

**3.2. Smart Contracts and Legal Enforceability**

A smart contract, a particular form of code, has been defined as "a computerized transaction protocol that executes terms of a contract." Smart contracts can run on blockchains, allowing the spread of trust and providing a predictable outcome. In addition, smart contracts are capable of storing information and assets, such as digital currency. The main advantages of the use of smart contracts are their efficiency. Legal contracts are anything but efficient, and they are also expensive to conclude and execute. Since smart contracts eliminate intermediaries and the need for them, they lead mainly to the reduction in transaction costs (Ramzan et al.2022).

However, smart contracts add concern to the analysis of their legal enforceability. Especially with the increase in the spread of legal technology, the question arises concerning whether smart contracts obtain the status of traditional contracts and can therefore be enforced in court. This is fundamental, particularly, to protect the member states and, more specifically, the competition authorities. This requires a definition of a smart contract to be included in legislation, especially concerning the consumer's definitions. The lack of the ex ante definition of a smart contract has led to the existence of a multiplicity of different definitions. In addition to the criticisms concerning smart contracts' definition, their enforceability is not always clear due to

their unique characteristics. Regarding their relationship with current legislation, given the difference in question with traditional contracts, recommendations have been put forward to avoid this conflict with intermediaries and convenience, the passage of time, and arbitrations.

This suggestion comes each time that the usage of technology emerges. Most of it feels the need for definitions that are not always needed, as case law and regulatory interpretation of the term can define its boundaries. In this sense, case law has also posed inquiries about various concerns attributed to smart contracts, especially about the distribution liability. However, it is true that smart contracts could pose some challenges attributed to their conflict with applying laws, especially if there is any requirement for licensure or qualifications. In the final analysis, smart contracts have not only been regarded as creating a legal headache due to the conflicts they reach with existing laws.

**4. Regulatory Frameworks**

There is already a considerable volume of law that affects the implementation of blockchain technology at international, European Union, and domestic levels. Whether any of these apply will depend on the specifics of each use case. Detailed analysis of each of these laws is provided throughout the text. In short, many pre-existing regulations relevant to blockchain have been drafted to apply to specific functionalities rather than reflecting the combination of features facilitated by blockchain. In particular, data protection, international sanctions, counter-terrorist financing, anti-money laundering, copyright, consumer, and competition law will apply, although the precise requirements are not clear-cut and need to be determined on a case-by-case basis. It is widely believed across all jurisdictions that as laws were not conceived with this disruptive technology in mind, there is significant room for interpretation, making compliance equally difficult to ascertain (Khettry et al., 2021).

This suggests that regulators have a key role in ensuring oversight of the disruptive applications of blockchain technology in finance. Equally, given the potential for widespread impact, firms and individuals that will benefit from these innovations may also need to be consulted in the balancing act between innovation and risk management. At present, regulators are grappling with an emerging technology with potential for immense impact in their fields of concern. The complexity of analysis

typically leads to more than one approach and leaves these parties in a state of ongoing debate. Those attempting to better appreciate the regulatory implications regarding bitcoin or blockchain technology invent a slew of terms that are hurdles to human understanding, not least of all to the underfunded legislators. Most assume that international law will primarily derive from the stance of the United States, as blockchain originated in the United States.

**4.1. Current Regulations and Compliance Issues**

The legality and compliance of blockchain technology have been investigated by a wide range of regulatory authorities around the world and are subject to oversight by various national and international organizations. Stringent compliance on behalf of organizations is imperative, given the variety of regulatory responses. Numerous regulatory endeavors have a direct or indirect effect on the development and operation of blockchain technology—primarily in the areas of digital currencies, financial services, and international trade. However, the refusal or inability of these stakeholders to put in place a clear, coherent, and contiguous regulatory framework results in—or stems from—several important issues that must be resolved if blockchain is to reach its full potential.

One of the most immediate threats lies in the lack of agreement across jurisdictions, which can lead to substantial obstacles for stakeholders working in the industry. The divergent regulatory approaches of states and international organizations, sometimes evident even within a single regulatory authority, can cause considerable legal confusion that, in effect, restricts blockchain operations. This restriction amounts to a restriction on blockchain innovation since firms may decide against developing any particular application if it is too uncertain and costly to operate. Compliance appears particularly challenging both due to confusing or vague regulatory guidelines and due to the often international nature of blockchain operations. From a global regulatory perspective, the current state of blockchain law is, therefore, fragmented and far from uniform, which does little to dispel one of the great fears for firms dealing with a new technology: changing domestic regulation and its potential impact on business. To that end, the further harmonization of domestic blockchain regulation is most likely to foster technological advances (Lehmann, 2021).

How can this technological progress be attained from a regulatory point of view? Ideally, regulators should strive to adhere to a relatively confined policy program: protecting the legal system and the blockchain community from bad actors; preserving individual rights and freedoms; sustaining competition in the marketplace. A step closer to attaining this regulatory objective could be the supervisory and informative participation of neglected stakeholders in blockchain policymaking.

**5. Case Studies**

In this chapter, we turn our attention to the real-world implications of the technology. We offer a range of case studies, examining the legal challenges and benefits arising from different blockchain implementations across various sectors. While we do not claim to cover every application of blockchain or every legal issue raised by it, our selection demonstrates the potential value that blockchain can offer societies while also helping us to identify some of the possible legal hazards and challenges that arise. Our case studies focus on the financial sector, given that it has historically been the domain of banks and financial services, thus facilitating a better understanding of this sector. Nonetheless, we also look at use cases from other sectors to demonstrate the wider implications of blockchain (Qin et al., 2021).

Our cases involve the following applications: blockchain in the clearing and settlement of securities; blockchain in last-mile voting; digital currencies and anti-money laundering compliance; blockchain in the use of smart contracts; and blockchain in the energy sector. Each of these case studies shows a blockchain application that has had real-world benefits. It also reveals some of the legal realities of blockchain, including the complications that arise when immutability ensures that mistakes are extremely difficult to correct. We also see that legal pitfalls are not simply technical or distant problems resulting from blockchain implementations; rather, they are ever-present, practical issues that need to be addressed as part of the development and implementation of blockchain systems. We shall tackle each of the technologies in turn, providing an analysis of the legal and practical implications of using blockchain.

**5.1. Impacts of Blockchain in the Financial Sector**

Blockchain technology has evolved to be one of the most impactful advancements in the financial sector. Blockchain has two main characteristics. It acts as a digital and

distributed ledger to facilitate fast, secure processing and verification, and as a cryptocurrency unit, independent of government control. This subsection provides in-depth explanations of blockchain's transformative impacts on the financial sector. It narrows the focus invariably to complex financial instruments and services, such as payment systems, various transactions in the trading process, trading of assets and securities under subsectors of financial markets, and record-keeping via accounting, along with their summary uses. It argues that once a transaction is in the blockchain ledger, there is a real-world need for intergenerational connections via law to the blockchain. (Blaszczyk, 2022)

In this capability, the risks to bank safety and the payments system arising from the operation of privately issued digital currencies based on blockchain are relatively limited. On a more strategic level, distributed ledger technology may have a number of applications that benefit the payments system. At this stage, opportunities are being explored to understand more about how the technology might support efficiency gains in processing payments and may eventually also inform decision-making on the implementation of new legislation or regulation in this area. DeFi is slowly but subtly aligning and reshaping the financial market system, albeit with concerns over institutional risks, data privacy including personal data, and security. The established legal links with the blockchain will protect those identified interests. Furthermore, the use of blockchain has been identified as the simplest way to allow financial institutions to send money and confirm finality with potentially instant transfer times and reduced costs. The operational costs of financial institutions could also decrease when payments are made on their blockchain solutions, enhancing internal efficiency and expediting final settlement times and transaction speed. Collaboration in a cash equity clearing and settlement proof of concept through the use of a public blockchain was established. To establish the interconnection and legal implications of every cross-border payment model, including a use case of sending local currency into a system, going through a payment system, and eventually ending up in a recipient account, was identified. A financial institution is under regulatory scrutiny after it completed a distributed ledger technology replacement model of its existing system for cash equity clearing and settlement for instant finality of payment.

## 6. Future Trends and Implications

The legal implications of blockchain cannot be regarded as fixed. Indeed, the evolution of the technology is so rapid that regulatory responses currently seem unlikely to keep pace with it. Accordingly, immediately predicting the legal implications of blockchain would seem rather foolhardy. Nevertheless, it is possible to speculate on what developments may occur in relation to the blockchain. First of all, digitizing business processes such as the execution of contracts is a dominant trend. Another possibility is the full integration of blockchain with the Internet of Things. Interestingly, it has also been predicted that existing data sources may be prioritized over blockchain databases owing to governance or data security concerns. The technology has, not least, the potential to be employed in a broad market range, including finance, manufacturing, supply management, and governmental services. These trends, however, would in themselves complicate the current regulatory landscape (Ferreira, 2021).

A key challenge for regulators, therefore, is to anticipate the different applications of the blockchain and the potential impacts for incumbent industries. More generally, ongoing innovation gives rise to ethical concerns related to, inter alia, identity theft and privacy invasion. Obviously, any transaction or personal details stored on a blockchain, if hacked, could have serious implications. Finally, a further complication for lawmakers is the increasing integration of emerging technologies. Predictions indicate that by the time blockchain becomes established, the integration of artificial intelligence and the Internet of Things will be so extensive that it will be impossible to discuss the 'blockchain' without reference to the two. For all these reasons, international cooperation on regulation will be vital to limiting the risks and ensuring the worldwide mimetic effects of good international standards. Taking these into account, it is important to stress here the balance between encouraging innovation and protecting customers in designing laws that cover blockchain; indeed, over-regulating the sector at an embryonic stage, involving complicated structures, would likely inhibit growth.

## References

Blaszczyk, M. (2022). Blockchain and Private Law. Available at SSRN 4319649.

Dhar Dwivedi, A., Singh, R., Kaushik, K., Rao Mukkamala, R., & Alnumay, W. S. (2022). Blockchain and artificial intelligence for 5G-enabled Internet of Things: Challenges, opportunities, and solutions. Transactions on Emerging Telecommunications Technologies, 35(4), e4329. dtu.dk

Ferrag, M. A. & Shu, L. (2021). The performance evaluation of blockchain-based security and privacy systems for the Internet of Things: A tutorial. IEEE Internet of Things Journal. [HTML]

Ferreira, A. (2021). Regulating smart contracts: Legal revolution or simply evolution?. Telecommunications Policy. [HTML]

Hao, X., Ren, W., Fei, Y., Zhu, T., & Choo, K. K. R. (2022). A blockchain-based cross-domain and autonomous access control scheme for internet of things. IEEE Transactions on Services Computing, 16(2), 773-786. [HTML]

Khettry, A. R., Patil, K. R., & Basavaraju, A. C. (2021). A detailed review on blockchain and its applications. SN Computer Science. [HTML]

Kohl, U. (2021). Blockchain utopia and its governance shortfalls. Blockchain and Public Law. ssrn.com

Lehmann, M. (2021). National Blockchain laws as a threat to capital markets integration. Uniform law review. oup.com

Liu, Y., Wang, J., Yan, Z., Wan, Z., & Jäntti, R. (2022). A survey on blockchain-based trust management for Internet of Things. IEEE internet of Things Journal, 10(7), 5898-5922. ieee.org

Poncibò, C. (n.d.). Blockchain and comparative law. Blockchain. unito.it

Qin, X., Huang, Y., Yang, Z., & Li, X. (2021). A blockchain-based access control scheme with multiple attribute authorities for secure cloud data sharing. Journal of Systems Architecture. [HTML]

Ramzan, S., Aqdus, A., Ravi, V., Koundal, D., Amin, R., & Al Ghamdi, M. A. (2022). Healthcare applications using blockchain technology: Motivations and challenges. IEEE Transactions on Engineering Management, 70(8), 2874-2890. researchgate.net