SN Social Sciences (2025) 5:11
https://doi.org/10.1007/s43545-024-01044-y

ORIGINAL ARTICLE

Beyond the blockchain hype: addressing legal and regulatory challenges

Alesia Zhuk[1]

Received: 16 June 2023 / Accepted: 24 December 2024

Abstract

Blockchain technology has gained widespread attention and adoption in various industries. However, despite its potential benefits, there are still numerous challenges and issues that need to be addressed. This paper provides an overview of the legal, regulatory, and technical challenges related to the use of blockchain technology. It explores the challenges associated with privacy, data protection, and data security, and analyses the regulatory challenges and implications. Additionally, it identifies future challenges and issues that may arise in the field of blockchain technology, including the integration with emerging technologies such as the Internet of Things (IoT), artificial intelligence (AI), and big data. The paper concludes by discussing the need for collaboration among stakeholders and the development of comprehensive legal and regulatory frameworks to address the challenges and ensure the successful implementation of blockchain technology in various sectors.

Keywords Cryptocurrency · Distributed ledger technology · Smart contracts · Data privacy · Cybersecurity · Digital identity

Introduction

In the current swiftly evolving landscape, the compelling nature of blockchain technology remains indisputable, driven by its extensive potential to reshape various industries, notably within the legal domain. However, as this study delves into the intricate interplay between blockchain and legal systems, its intention transcends mere exploration. Adopting a unique stance, this research aims to uncover the complex regulatory and data challenges arising from the application of blockchain within the legal system. To achieve this, the study systematically examines the challenges

✉ Alesia Zhuk
alesia.zhuk@ug.uchile.cl

[1] Law Department, Pompeu Fabra University, Barcelona, Spain

Published online: 21 January 2025

faced by legal systems in adapting to blockchain technology, offering both theoretical insights and practical suggestions for integrating blockchain in legal contexts. By thoroughly examining these intricate challenges and unraveling their implications, the primary objective is to illuminate their impact on the legal fabric. In turn, the study endeavors to provide a comprehensive understanding of the opportunities and hurdles emerging from the convergence of blockchain technology and legal frameworks.

This perspective shift enables the construction of a holistic comprehension of the challenges and opportunities stemming from the amalgamation of blockchain technology and legal frameworks. Through this distinctive approach, the aspiration of this study is to contribute not only to the ongoing discourse on blockchain but also to offer a fresh perspective that resonates with the evolving requisites of the legal realm. Furthermore, the paper seeks to identify specific challenges that will enrich the existing body of literature by highlighting gaps in the current legal frameworks and proposing actionable solutions.

This study will center its focus on two primary perspectives: firstly, examining the legal implications and challenges introduced by blockchain technology for the legal system in general. The potential significant issues include concerns related to privacy, data protection, and data security. Consequently, features of blockchain such as pseudonymity and decentralisation, which could be viewed as advantageous in legal systems, may simultaneously present vulnerabilities. By identifying these challenges, the paper aims to contribute to the field of law by enriching current understanding and offering practical guidance on navigating these issues.

Secondly, attention must be directed towards the regulatory challenges that arise when contemplating the regulation of a blockchain system. This paper proposes that addressing issues such as the enforceability of smart contracts, conflicts of laws, and the protection of rights could be proactively resolved through the implementation of corresponding regulations. The study aims to provide guidance to legal expert by suggesting regulatory frameworks that could mitigate these challenges, ensuring that blockchain's integration into legal systems is both effective and secure.

Hence, the principal contribution of this research lies in highlighting the potential challenges associated with blockchain application and suggesting preventive measures through the incorporation of appropriate regulations. The novelty of this approach is underscored by the limited integration of blockchain into the legal system, despite its potential benefits.

Addressing the legal and regulatory challenges associated with blockchain is imperative within the current academic discourse due to the rapid evolution of this transformative technology. As blockchain applications extend across diverse sectors, including finance, healthcare, and supply chain management, the development of robust legal frameworks becomes paramount. The dynamic and decentralised nature of blockchain necessitates swift adaptation of legal structures to govern its global impact, mitigating risks, protecting stakeholders' interests, and ensuring compliance with evolving data protection standards. Timely resolution of legal ambiguities surrounding smart contract enforceability and privacy concerns is crucial for fostering consumer confidence, encouraging economic growth, and guiding the responsible evolution of financial systems, such as the emergence of Central Bank Digital Cur-

rencies (CBDCs) and decentralised finance (DeFi) platforms. This paper's aim to provide guidance to legal systems on the necessity of regulating blockchain applications is aligned with the growing need for informed and strategic policymaking in the field. In academia, this pursuit aligns with the imperative to facilitate innovation while safeguarding ethical, secure, and compliant blockchain implementations.

Prior to delving into the main issues, it is pertinent to provide a comprehensive definition of blockchain based on the approach adopted by the European Union. The European Central Bank (2022) characterises blockchain as a distributed ledger technology (DLT) that orchestrates the validation and subsequent recording of transactions within interconnected blocks. This decentralised architecture, underpinned by cryptographic mechanisms, empowers participants to engage in transactions without traditional intermediaries. ENISA, the European Union Agency for Cybersecurity (n.d.), concurs, describing blockchain as a peer-to-peer network where transactions form linked blocks, composing an immutable, chronological chain. This decentralised ledger fosters transparency and security while eliminating the need for centralised oversight. Building upon these foundations, the European Investment Bank (2021) frames blockchain as a technology that unlocks consensus and transparent information recording without reliance on central authorities.

Blockchain, in its essence, represents an immutable digital ledger, redefining traditional data management, verification, and authentication methodologies. This transformative potential resonates profoundly in contexts like Central Bank Digital Ledger Technologies (CB-DLT), where blockchain's malleability manifests within intricate financial frameworks. Notably, the ascent of Central Bank Cryptos heightens the urgency of exploring the juncture between blockchain technology and legal systems, navigating opportunities intertwined with regulatory intricacies. For instance, the prospect of a Digital Euro necessitates a comprehensive risk assessment to address potential consequences such as shifts in monetary policy transmission and financial stability (European Central Bank 2020a, b).

Within this context, the implementation of Central Bank Digital Currency (CBDC) demands rigorous scrutiny, particularly at the state level. In addition to addressing the legal and regulatory challenges inherent in the assimilation of blockchain into the legal system, this study extends its gaze towards the future. It anticipates challenges that may arise in tandem with the growing prominence of AI, big data, and the Internet of Things (IoT) alongside the continued evolution of blockchain within legal frameworks. The examination will systematically initiate with an in-depth exploration of legal challenges, progressing towards an analysis of regulatory complexities, and ultimately culminating in the exploration of potential challenges on the horizon. This sequential and comprehensive approach aims to provide a nuanced understanding of the multifaceted landscape that encompasses blockchain technology, CBDC implementation, and the intricate interplay with emerging technologies within legal contexts.

This research employed a comprehensive and systematic literature review as its primary methodology, targeting scholarly databases such as Google Scholar, JSTOR, and HeinOnline. The selection of sources was guided by factors such as the citation index, ensuring the inclusion of references with significant impact in the academic community. Additionally, emphasis was placed on the publication year, preferring

sources between 2013 and 2023 to capture the latest developments in blockchain's intersection with the legal landscape. This temporal focus, especially on recent sources, aimed to align closely with evolving technological advancements.

The search strategy also adopted a nuanced approach, utilising both general and specific terms like "AML and KYC," "governance," and "IP rights," alongside broad terms such as "blockchain" and "law." The interdisciplinary search extended to incorporate technical papers when feasible, bridging the gap between legal and technological perspectives. The selection criteria for laws and reports were aimed at official agencies, with a preference given to official EU institutions like the European Bank and Monetary Fund to enhance the reliability and authority of information.

In addition, a qualitative content analysis was undertaken to identify key themes and pressing challenges associated with the legal and regulatory implications of blockchain technology. This method enabled a structured exploration of issues such as data protection, privacy, and enforceability—considerations that are pivotal to the successful integration of blockchain into legal frameworks. By adopting a mixed-methods approach that combines a systematic review with qualitative analysis, this study offers a nuanced perspective on the legal complexities and regulatory strategies essential for adapting blockchain applications to the demands of the legal sector. Through this methodological approach, the study contributes both to the identification of critical challenges and to providing actionable insights for legal experts.

Overview of legal issues and challenges related to the use of blockchain in the legal system

It is imperative to acknowledge that blockchain technology has not yet been extensively incorporated into contemporary legal systems. Its introduction as a novel feature inevitably poses challenges that require diligent consideration. Despite being recognised as an emerging technology, a substantial body of literature, primarily spanning the years 2017–2020, is dedicated to this evolving subject. This study aims to discern primary sources based on their credibility and citation indices. The entire literature can be categorised into two main types: general literature, which possesses a suggestive character, and more specific literature that delves into particular fields and applications of blockchain.

Within the general literature De Filippi and Wright (2018) delve into the fundamental interplay between code-driven decentralised systems and established legal frameworks. Significantly, their work underscores the imperative to adapt legal norms to accommodate the distinct challenges presented by blockchain, emphasising the rule of law within a code-driven environment. Complementing this Szostek (2019) provides a nuanced examination of governance, liability, and compliance challenges arising alongside decentralised technologies. This work augments De Filippi and Wright's foundational insights, contributing to a more comprehensive understanding of legal dynamics within blockchain applications. Additionally Werbach (2018b) advocates for a balanced approach, highlighting the symbiotic relationship between blockchain and legal structures. Proposing a framework ensuring transparency while

upholding established legal norms, Werbach provides a middle ground for the coexistence of blockchain and traditional legal principles.

Dimitropoulos (2020) further explores regulatory challenges and the evolving legal landscape, emphasising the necessity for legal adaptation to match the rapid advancements in blockchain technology. Fulmer's (2018) study underlines the imperative of nuanced legal understanding, particularly in areas such as smart contracts and data security. An edited volume by Lianos et al. (2019) contributes a multifaceted perspective, underscoring the interdisciplinary nature of the discourse—encompassing technological, societal, and legal dimensions.

Quintais et al.'s (2019) work critically assesses governance, privacy, and the evolving role of intermediaries in decentralised systems, encouraging a more nuanced understanding of legal challenges inherent in blockchain applications. Addressing sector-specific challenges Yeoh's (2017) exploration underscores the need for regulatory clarity to navigate the evolving landscape of blockchain applications. Further insights into sector-specific legal challenges are provided by Naves et al. (2019), highlighting the complexities of legal relationships within blockchain ecosystems.

Turning to more specific or sector-oriented literature, Garcia-Teruel (2020) navigates unique challenges in the real estate sector. Savelyev's (2018) focus on copyright challenges in the blockchain era anticipates disruptions and opportunities within the realm of intellectual property.

Sung (2019) provides an in-depth exploration of challenges within the copyright legal system. This examination sheds light on the transformative potential and challenges blockchain introduces to established copyright norms. Fabiano's (2017) examination offers a forward-looking perspective on privacy concerns at the intersection of the IoTh and blockchain, emphasising the need for a standardised privacy framework. Drummer and Neumann's (2020) work scrutinises the legal and technical adoption challenges associated with blockchain-enabled smart contracts, providing insights into addressing legal challenges intertwined with code-driven contracts.

The reviewed literature underscores crucial recommendations for adaptive legal frameworks amidst blockchain integration. Authors emphasize the significance of flexible legal norms, a balanced approach acknowledging the symbiotic relationship between blockchain and legal structures, and the necessity for regulatory clarity, transparency, and compliance. Interdisciplinary collaboration is considered vital, coupled with sector-specific adaptations to tackle nuanced challenges across different industries. In addition to these insights, this research aims to delineate specific categories where blockchain holds considerable potential for transformative impact in the legal domain—namely, blockchain-based evidence in courts, enforceability of smart contracts, jurisdictional and conflicts of laws issues, and the conceptualization of CBDCs.

Foremost among these concerns is the authentication and admissibility of blockchain-based evidence within legal proceedings. Despite its inherent potential, the admissibility of blockchain-based evidence in judicial settings remains a subject of contention, primarily attributed to the absence of well-defined legal precedents and standards governing the presentation of such evidence (Kshetri 2018).

Another substantial challenge linked to the use of blockchain in the legal system is the matter of smart contract enforceability. While smart contracts have the potential

to automate and streamline diverse legal processes, concerns arise regarding their legal enforceability. Given their self-executing nature, operating based on predefined rules and conditions, these contracts may not always align seamlessly with the traditional legal system and established legal concepts (Raskin 2016).

Furthermore, the decentralised nature of blockchain technology triggers concerns about jurisdiction and conflicts of laws. With blockchain-based transactions traversing borders devoid of intermediaries, determining the applicable legal jurisdiction becomes intricate. This complexity gives rise to conflicts of laws and a sense of legal uncertainty (Cumming et al. 2019).

Lastly, blockchain technology is also harnessed in the conceptualisation of CBDCs. While CBDCs are not inherently enmeshed within the legal system, a well-informed and adept implementation could potentially integrate them seamlessly into diverse financial transactions, encompassing even those within the judicial domain.

The ECB has been at the forefront of discussions regarding the intersection of blockchain technology and the evolution of digital currencies. Notably, two reports—"Stablecoins: Implications for monetary policy, financial stability, market infrastructure and payments, and banking supervision in the euro area" (2020) and "EU ECB Report on a digital euro" (2020)—illuminate the potential implications, challenges, and opportunities arising from the convergence of blockchain and digital currency.

The ECB's report on stablecoins underscores the transformative changes taking place within the financial ecosystem. Stablecoins, a type of digital currency designed to maintain a stable value by pegging to traditional currencies or commodities, have garnered attention due to their potential to reduce the volatility commonly associated with cryptocurrencies. A significant takeaway from this report is the consideration of stablecoins as potential alternative means of payment and value storage, which could potentially disrupt traditional financial intermediaries.

Stablecoins offer the potential for improved transparency, streamlined cross-border transactions, and potential cost reduction for users. However, the report also underscores that the widespread adoption of stablecoins could pose challenges to monetary policy and financial stability. The impact of stablecoins on traditional banking and financial infrastructure, as well as the potential risks of runs on stablecoin issuers, are areas of concern that regulators must address.

In its report on the digital euro, the ECB explores the possibility of introducing a CBDC to complement physical cash and existing digital forms of money. The emergence of CBDCs, including the digital euro, reflects central banks' recognition of the evolving payment landscape and the need to adapt to technological advancements.

A digital euro, if introduced, could leverage blockchain technology to offer secure, efficient, and instantaneous payments. This could reshape how individuals and businesses transact, reducing reliance on intermediaries and enhancing financial inclusion. However, the report acknowledges the complexities associated with designing a digital euro that balances the advantages of technological innovation with the need to ensure privacy, cybersecurity, and compliance with regulatory requirements.

Both reports underscore the pivotal role of blockchain in shaping the future of digital currency, ensuring transparency, security, and traceability for stablecoins and CBDCs through its distributed ledger capability. While highlighting advantages such as automation and streamlined cross-border transactions, they acknowledge

challenges, including scalability, regulatory compliance, privacy, and cybersecurity. Effective collaboration among central banks, regulators, financial institutions, and technology providers is crucial for maximising benefits and managing risks.

Nevertheless, blockchain introduces concerns, particularly in privacy and data protection. The technology's immutable nature, enhancing security, raises issues related to user privacy and compliance with regulations like General Data Protection Regulation (GDPR). The integration of blockchain into the legal system amplifies these concerns, as its distributed ledger and immutability may compromise the confidentiality of sensitive information. Striking a balance between technological potential and robust privacy controls is imperative for sustainable development in this dynamic digital landscape.

Given the escalating importance of privacy, data security, and data protection issues, the subsequent sections will shift the focus to the primary data-related challenges of blockchain in the legal system. This shift aims to provide a comprehensive exploration and discussion of the implications of these challenges for the legal industry.

Examination of privacy, data protection, and data security issues

The literature exploring privacy, data protection, and data security issues with blockchain extensively discusses both the significant benefits of blockchain in safeguarding privacy and data protection, as well as potential challenges that may arise. Consequently, the integration of blockchain into the legal system cannot be unequivocally deemed either entirely beneficial or detrimental.

A foundational survey conducted by Joshi et al. (2018) provides a comprehensive overview of security and privacy challenges in blockchain technology. This survey categorizes challenges into various dimensions, including consensus algorithms, privacy concerns, and smart contract vulnerabilities. Serving as a baseline for subsequent discussions, this work offers a holistic view of security issues in blockchain.

Wylde et al. (2022) further explores the intersection of cybersecurity, data privacy, and blockchain technology, emphasizing the evolving nature of this relationship. Building upon Joshi et al.'s survey, this review provides a more current analysis of the dynamic landscape, shedding light on how the relationship between blockchain, cybersecurity, and data privacy is evolving over time.

Contrary to the common belief that blockchain and data protection are inherently contradictory, Moerel (2018) argues that with careful design and legal considerations, these two can coexist. Her perspective challenges the notion of an inevitable clash between blockchain and data protection, introducing the idea that, with the right approach, they may not necessarily conflict.

Jiménez-Gómez (2019) delves into risks associated with blockchain concerning data protection, particularly from a European perspective. This work addresses regulatory challenges and potential implications on user data privacy, providing insights into how regional variations in legal frameworks might influence perceived risks associated with blockchain and data protection.

Feng et al.'s (2019) survey focuses specifically on privacy protection mechanisms within blockchain systems. Examining various methods and technologies deployed to enhance privacy in blockchain, it addresses anonymity, confidentiality, and consent, serving as a bridge connecting general security and privacy discussions with specific privacy protection mechanisms.

Wirth and Kolain (2018) propose a design-oriented approach to embed privacy features directly into blockchain systems, emphasizing the development of GDPR-compliant blockchain systems that prioritize user data protection. This proactive solution aligns with Moerel's notion of coexistence, offering a counterpoint to concerns raised by other authors regarding the clash between blockchain and data protection.

Giordano (2020) explores challenges posed by the GDPR concerning blockchain applications, adding legal depth by focusing on how regulatory frameworks, especially in the European context, interact with blockchain technology.

De Hert and Kumar (2021) contribute to the legal discourse on blockchain, emphasizing privacy and data protection. They explore the intersection of blockchain with fundamental rights and data protection regulations, contributing to the evolving understanding of how legal frameworks adapt to challenges posed by blockchain.

Yassein et al.'s (2019) comprehensive overview combines a broad examination of blockchain technology with a specific focus on security and privacy, acting as a bridge between fundamental technology aspects and intricate challenges associated with security and privacy.

This extended literature review captures diverse viewpoints, ranging from technical security concerns to legal considerations, providing a comprehensive understanding of the multifaceted relationship between blockchain, security, and privacy. See Fig. 1.

This research endeavors to scrutinise the nuanced data issues emanating from the decentralised architecture of blockchain and its core structure. The objective is to elucidate that, notwithstanding the prevalent portrayal of blockchain as a secure and

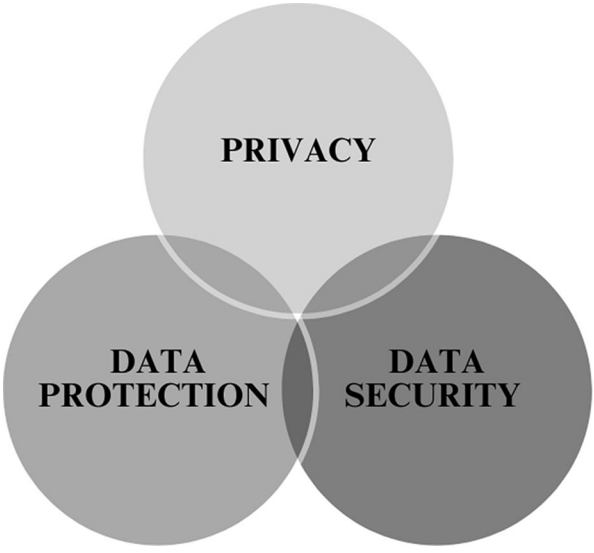

Fig. 1 Primary data-related challenges of blockchain in the legal system

transparent data management solution, it may not universally represent an infallible choice. Nonetheless, its utility may manifest in specific contextual scenarios.

Blockchain technology's inherent transparency and immutability offer promising solutions for various legal applications such as supply chain management, smart contracts, and digital identity. However, this transparency, whilst advantageous, also presents privacy challenges, particularly when dealing with sensitive data within the blockchain ecosystem. If protective measures are insufficient, the utilisation of blockchain in the legal realm could inadvertently jeopardise the privacy of individuals and entities involved in legal transactions (Jin et al. 2019).

Among the noteworthy privacy concerns associated with blockchain technology is the complexity in identifying the individuals or entities behind transactions. Blockchain transactions employ pseudonymity, whereby users are identified by public keys rather than real names or identities. While this provides some level of anonymity, it also engenders privacy risks, particularly when blockchain systems are utilised within legal contexts. Additionally, public keys and other identifying information often required by blockchain systems can compromise user privacy if not adequately safeguarded (Zohar 2015).

The deployment of smart contracts, characterised by their self-executing nature and encoded execution of predefined rules, also introduces privacy risks. The contents of these contracts, accessible to all parties on the blockchain, can jeopardise the privacy of individuals participating in legal transactions (Staples et al. 2017). See Fig. 2.

Beyond the realm of privacy, the integration of blockchain into legal systems necessitates a comprehensive evaluation of data security. Blockchain's reputation for security is rooted in cryptographic mechanisms and decentralisation. However, this veneer of security can be misleading, given that a single vulnerability can potentially lead to widespread consequences. In alignment with the multifaceted definitions examined earlier, these security concerns compel us to bridge the gap between blockchain's potential and the imperative of robust cybersecurity measures. Moreover, as legal documents and sensitive information become integral components of the blockchain infrastructure, safeguarding them against unauthorised access and breaches assumes paramount importance. See Fig. 3.

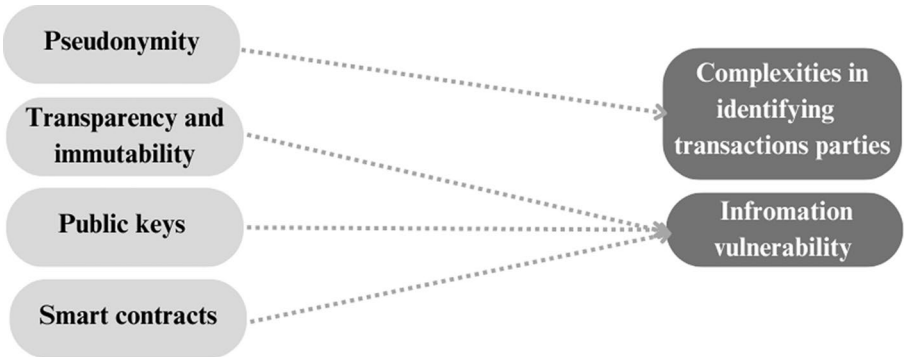

Fig. 2 Key privacy challenges of blockchain

Fig. 3 Data security issues of blockchain

Fig. 4 Data protection issues of blockchain

Applying blockchain technology within the legal domain has also raised apprehensions about data protection. The immutable and decentralised nature of blockchain systems introduces significant challenges in managing and safeguarding personal data. Using blockchain technology, especially in scenarios involving sensitive data, can pose data protection risks (Jin et al. 2019).

One of the primary challenges related to data protection in blockchain systems revolves around immutability. Data stored on the blockchain becomes immutable, and any attempt to alter or delete it results in invalidating the entire blockchain. This poses challenges when complying with data protection laws, such as the GDPR, which mandates the deletion of personal data upon request (Schellinger et al. 2022).

Another data protection concern pertains to the potential for data breaches. Despite blockchain's reputation for security, vulnerabilities persist, and a successful breach could lead to the compromise of sensitive data. Additionally, the transparent nature of blockchain transactions means that any individual with access to the blockchain can view its contents, thereby endangering the privacy of those involved in legal transactions (Jin et al. 2019). See Fig. 4.

Addressing the challenges of privacy and data protection necessitates the incorporation of privacy-enhancing technologies into blockchain systems. These technologies are engineered to anonymise transactions, shield user identities, and prevent sensitive information from being divulged on the blockchain. Techniques such as zero-knowledge proofs and ring signatures enhance anonymity and confidentiality, allowing users to engage in transactions without revealing their identities (Mahmood and Vacius 2020). Additionally, cryptographic methods like homomorphic encryption safeguard sensitive data within the blockchain, ensuring that only authorised parties can access such information (Jin et al. 2019).

The seamless and secure sharing of information is one of the cornerstones of blockchain's appeal. By employing cryptographic techniques like encryption, blockchain systems can ensure that only authorised parties can access and decipher the information they are entitled to view. This controlled approach to data sharing maintains the integrity and confidentiality of the data while still facilitating the transparent and traceable nature of blockchain transactions. (Narayanan et al. 2016)

It is worth noting that while encryption enhances privacy and security, it can potentially introduce certain challenges when it comes to maintaining the full transparency that blockchain systems are known for. Encryption can make data unreadable to anyone without the decryption key, which might limit the degree of openness that some blockchain implementations aim to achieve. (Kosba et al. 2016)

Furthermore, the use of blockchain technology amplifies the potential for cyberattacks and data breaches, which could result in the loss or theft of sensitive data (Jin et al. 2019). A significant data security challenge in blockchain technology is the risk of 51% attacks. In a blockchain network, a 51% attack occurs when a single entity or group controls over 50% of the network's computing power, enabling them to manipulate the network and potentially steal sensitive data. Although rare, such attacks pose a substantial risk to the security of blockchain networks (Nakamoto 2008).

Smart contracts also introduce data security concerns due to potential vulnerabilities. Since smart contracts contain sensitive information and execute automatically, vulnerabilities within them can be exploited, potentially leading to the compromise of sensitive data. The transparent nature of blockchain transactions means that vulnerabilities in smart contracts could be exploited by anyone with access to the blockchain, magnifying security risks (Jin et al. 2019).

Mitigating these data security challenges demands the implementation of appropriate measures to secure blockchain networks and smart contracts. Multi-factor authentication and encryption can bolster access protection, permitting only authorised parties to engage in transactions (Şahan et al. 2019). Additionally, conducting audits and tests on smart contracts can unearth and address vulnerabilities, thereby reducing the risk of attacks and data breaches (Jin et al. 2019).

Finally, it is essential to consider the legal implications of deploying blockchain technology within the framework of data security laws. Many jurisdictions stipulate data security regulations mandating organisations to undertake measures safeguarding sensitive data against unauthorised access or disclosure. Therefore, ensuring the presence of suitable measures to comply with data security laws becomes pivotal when employing blockchain technology for legal purposes (Daneshgar et al. 2019).

Overall, the escalating presence of blockchain technology within the legal landscape unfurls crucial inquiries concerning privacy, data protection, and data security. While the transparency and decentralisation innate to blockchain hold promise for diverse legal applications, they concurrently pose privacy risks when handling sensitive data. The immutable and decentralised nature of blockchain systems also ushers in formidable challenges for managing and preserving personal data. Addressing these issues necessitates not only fortifying personal data stored within the blockchain but also meticulously navigating the intricate landscape of data protection regulations and augmenting data security measures. In the ensuing chapter, we will delve deeper into the regulatory challenges emanating from the infusion of blockchain into legal

systems, underscoring the imperative of addressing these concerns to harness blockchain's transformative potential responsibly within the legal sphere.

While legal and data challenges are fundamental concerns for lawyers and other stakeholders in the legal field, specific attention must also be directed towards the regulatory challenges associated with the integration of blockchain into the legal system. The following section will delve into nine key challenges related to implementation, rights, and conflict of laws. As demonstrated, there is a dual nature to the coin; while certain blockchain features are beneficial from one perspective, particularly in legal terms, they may not perfectly align from another.

Analysis of regulatory challenges and implications

Regulatory challenges linked to the integration of blockchain in the legal domain revolve around the complexities stemming from the application of law to govern interactions among different entities. Unlike data breaches, the array of potential challenges is extensive, though not exhaustive, given the diverse range of legal issues at play. This study explicitly examines nine key regulatory challenges sourced from various literature, acknowledging the absence of a single comprehensive reference.

Regarding the literature review, it exhibits a fragmented structure, lacking the incorporation of all pertinent sources into a cohesive academic framework.

Lianos et al. (2019) delve into the techno-social and legal challenges associated with regulating blockchain, recognising the intricate task of adapting existing legal frameworks to accommodate its decentralised nature. This highlights the necessity for a comprehensive regulatory approach. Building on this, Yeoh's (2017) work specifically addresses regulatory challenges tied to blockchain technology, emphasising the evolving legal landscape and the critical need for regulatory clarity to effectively navigate the complexities arising from blockchain integration.

Expanding the regulatory perspective, Cumming et al. (2019) undertake a broader examination of regulatory issues within the crypto-economy. Their comprehensive analysis underscores the importance of managing risks and uncertainties, providing insights that extend beyond the immediate scope of blockchain technology. Guo's (2016) work focuses on patentability and admissibility concerns linked to blockchain receipts, exploring the intersection of intellectual property and blockchain and raising inquiries regarding the legal status of related innovations.

Spring's (2019) exploration of the blockchain paradox sheds light on the tension between reliability and admissibility in legal contexts, emphasising the challenges associated with integrating blockchain as evidence in court proceedings. Shifting focus to smart contracts, Durovic and Lech's (2019) contribution navigates the legal complexities surrounding the enforceability of self-executing contracts on blockchain platforms.

Dwivedi et al.'s (2021) systematic literature review synthesises existing knowledge, offering a comprehensive analysis of legally enforceable smart-contract languages. This work provides an exhaustive overview of the legal considerations intrinsic to smart-contract development. Möslein's (2018) exploration focuses on

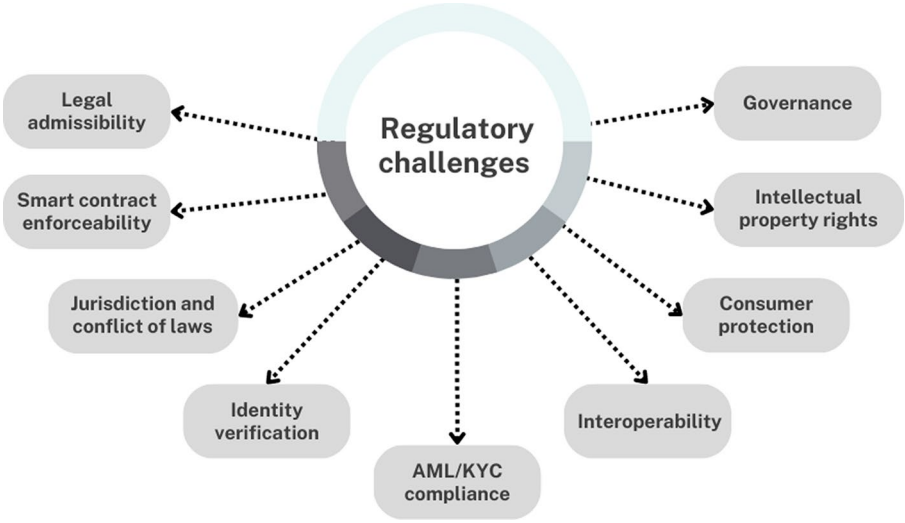

Fig. 5 The regulatory challenges of blockchain

conflicts of laws in digital jurisdictions, contributing to the understanding of the challenges posed by blockchain to traditional legal structures.

Examining the intersection of blockchain and identity verification, Jamal et al. (2019) illustrate the implementation of a blockchain-based identity verification system and its potential impact on legal and regulatory practices. Additionally, Aydar et al. (2019) propose a system for blockchain-based digital identity verification and record sharing, contributing to discussions on data protection and privacy.

Overall, this comparative literature review underscores the multidimensional nature of blockchain integration within regulatory contexts, with each study offering unique insights into the evolving landscape of legal considerations. Subsequent sections will delve deeper into the specific contributions of each work, providing a closer examination of their respective nuances and implications. See Fig. 5 and Table 1.

Legal admissibility

The legal admissibility of blockchain-based evidence in court is a crucial regulatory challenge that needs to be addressed. While blockchain technology offers a tamper-proof and secure method of storing and sharing data, the lack of established legal standards and precedents for the admissibility of blockchain-based evidence poses a significant challenge for its use in legal proceedings (Berto 2019). Without clear guidelines and standards, it can be challenging for judges to determine the authenticity and reliability of blockchain-based evidence, which could lead to legal disputes and delays in the legal process.

One possible solution to address this challenge is the establishment of legal standards and precedents for the admissibility of blockchain-based evidence. Several jurisdictions have already taken steps towards this goal. For example, in the United Kingdom, the LawTech Delivery Panel's Blockchain Legal and Regulatory Group

Table 1 Regulatory challenges, benefits, weaknesses, and proposed solutions of blockchain in the legal system's regulatory landscape

Exploring challenges	Benefits	Weaknesses	Solution
Legal admissibility	Tamper-proof data storage	Absence of legal standards for blockchain evidence	Establishment of legal standards and precedents
Smart contract enforceability	Contract terms defined in code	Relevance of traditional legal concepts	
Jurisdiction and conflict of laws	Global nature of blockchain	Jurisdiction ambiguity due to decentralisation	
Identity verification	Resistant blockchain-based identity	Protocols complying with legal standards	
AML/KYC compliance	Blockchain-based transaction monitoring	Balancing privacy and transparency	
		Identifying beneficial owners of assets	
Consumer protection	Blockchain-based IP protection	Clear legal framework and enforcement challenges	
Intellectual property rights	Critical governance mechanisms	Balancing decentralisation and centralisation	
Governance	Critical for coordination and decisions	Requires collaboration between legal and technical experts	
		Balancing decentralisation and centralisation tension	
Interoperability	Seamless communication between networks	Lack of common interoperability standard	
		Varied regulatory frameworks across jurisdictions	

has published a guidance note on the use of blockchain-based evidence in legal proceedings. The guidance note outlines several factors that should be considered when assessing the admissibility of blockchain-based evidence, including the reliability and integrity of the blockchain system, the accuracy of the data recorded on the blockchain, and the relevance of the evidence to the legal proceedings (Blockchain Legal and Regulatory Group 2023)

An example of a successful implementation of blockchain-based evidence in legal proceedings is the case of Everledger. Everledger is a blockchain-based platform that creates a digital certificate of authenticity for diamonds. In 2018, the platform provided blockchain-based evidence to the UK High Court in a case involving a dispute over the ownership of a $1.6 million diamond. The court recognised the admissibility of the evidence provided by Everledger and ruled in favor of the party that could prove ownership of the diamond through the blockchain record (Bal 2018).

Another example is the use of blockchain-based evidence in the criminal case against Ross Ulbricht, the founder of the Silk Road darknet marketplace. In 2015, the prosecution presented blockchain-based evidence in court, including the public ledger of the Bitcoin transactions used to purchase illegal goods on the Silk Road. The court recognised the admissibility of the evidence and sentenced Ulbricht to life in prison (Kethineni 2019).

In Canada, the National Institute of Standards and Technology (NIST) has published a document titled "Blockchain Technology Overview" which provides guidance on the use of blockchain technology in general, including its use in the context of digital forensics and evidence.

In summary, the legal admissibility of blockchain-based evidence is a critical regulatory challenge that needs to be addressed to ensure the effective integration of blockchain technology into the legal system. The establishment of legal standards and precedents for the admissibility of blockchain-based evidence is a crucial step towards addressing this challenge, and several jurisdictions have already taken steps towards this goal.

Smart contract enforceability

Smart contracts are self-executing contracts with the terms of the agreement directly written into lines of code. These contracts are based on blockchain technology, which ensures transparency, security, and immutability. However, one question that arises with the use of smart contracts is their enforceability in the legal system.

To be legally binding, a contract must meet certain requirements such as offer, acceptance, consideration, and intention to create legal relations (Suff 1997). With smart contracts, the terms of the contract are already defined in the code, and the contract is automatically executed when certain conditions are met. This raises the question of whether traditional legal concepts such as offer and acceptance are still relevant in the context of smart contracts.

To address this issue, legal frameworks and standards need to be developed to ensure the enforceability of smart contracts in the legal system. Some countries, such as the United States and the United Kingdom, have already started to recognise smart contracts as legally enforceable agreements.

The Uniform Law Commission in the US has proposed the Uniform Electronic Transactions Act (UETA) and the Uniform Commercial Code (UCC) as frameworks for the enforceability of smart contracts. These frameworks provide legal recognition for electronic records and electronic signatures, including those used in smart contracts (Uniform Law Commission n.d.a, b).

In the UK, the LawTech Delivery Panel has published a Legal Statement on the Status of Cryptoassets and Smart Contracts (LawTech Delivery Panel 2019), which sets out the legal position on smart contracts and provides guidance on how they can be used within the existing legal framework.

In Singapore, the Electronic Transactions Act (ETA) was first enacted in 1998 to provide a legal framework for electronic transactions. The ETA was amended in 2010 to recognise electronic records and signatures as legal equivalents of paper-based

records and signatures. In 2019, the ETA was further amended to explicitly recognise smart contracts as legally binding and enforceable contracts.

Under the amended ETA, a smart contract is defined as "a contract comprising computer programs that automatically execute all or some of its obligations or terms when certain conditions specified in the contract are satisfied" (Electronic Transactions (Amendment) Act 2019, s 2). The amendment also clarifies that a smart contract is not invalid simply because it is in electronic form, and that it is legally binding and enforceable in the same way as a traditional written contract.

The recognition of smart contracts in Singapore is part of the government's efforts to support the development and adoption of digital technologies in the country. Singapore's government has been proactive in promoting the use of blockchain technology and smart contracts in various industries, including finance, logistics, and real estate.

In The Abu Dhabi Global Market (ADGM), a financial free zone in the United Arab Emirates (UAE), has been at the forefront of recognising the legal validity of smart contracts. In November 2021, ADGM enacted the Electronic Transactions Regulations 2021, which established a legal framework for the recognition and enforcement of electronic records and contracts (ADGM 2021).

In Switzerland, the legal validity of smart contracts is recognised under a legal framework introduced by the Federal Council in 2019 (Swiss Federal Council 2019). Furthermore, in September 2020, the Swiss Parliament adopted the Federal Act on the Adaptation of Federal Law to Developments in Distributed Ledger Technology (DLT bill), which adjusts various federal laws to specifically address the legal framework for distributed ledger technology and smart contracts.

The amendments to the Code of Obligations, the Federal Intermediated Securities Act, and the Federal Act on International Private Law came into effect on February 1, 2021. These amendments allow for the introduction of ledger-based securities represented on a blockchain.

The remaining provisions of the DLT bill, along with their accompanying blanket ordinance (the 'Ordinance'), came into force on August 1, 2021. These amendments include modifications to the Financial Services Act (FinSA), the National Bank Act (NBA), the Banking Act (BA), the Financial Institutions Act (FinIA), the Anti-Money Laundering Act (AMLA), the Financial Market Infrastructure Act (FMIA), and the Debt Enforcement and Bankruptcy Act (DEBA). They acknowledge the legal validity of transactions conducted using DLT and smart contracts under Swiss law and establish a regulatory framework for the utilisation of these technologies in the financial sector.

In summary, countries like the US, UK, Singapore, and Switzerland have recognised the legal validity of smart contracts and implemented frameworks for their enforceability. This reflects a global trend towards supporting digital technology adoption and ensuring regulatory oversight.

Jurisdiction and conflict of laws

Blockchain technology has the potential to revolutionise the way cross-border transactions are conducted (Tian et al. 2022). However, the decentralised and global

nature of blockchain technology presents unique challenges in determining the legal jurisdiction that applies to such transactions and resolving conflicts of laws.

One challenge is determining which legal jurisdiction has authority over blockchain-based transactions that cross borders. With traditional transactions, the jurisdiction is typically determined by the physical location of the parties involved or the location where the transaction occurred. However, with blockchain-based transactions, the parties involved may be located in different countries, and the transaction may occur entirely online.

The lack of a physical location makes it difficult to determine which legal system applies to the transaction. This can create legal uncertainty, as different legal systems may have different laws and regulations that apply to the transaction. In addition, the lack of a central authority to oversee blockchain transactions makes it difficult to enforce legal decisions across borders.

To address these challenges, several countries have taken steps to establish legal frameworks for blockchain-based transactions that cross borders. For example, the European Union has proposed regulations that would create a legal framework for blockchain technology, including rules on jurisdiction and choice of law (EUR-Lex 2020). The proposed regulations would provide legal certainty for cross-border blockchain transactions by establishing a single set of rules that apply throughout the EU.

In the United States, the Uniform Law Commission has proposed the Uniform Regulation of Virtual-Currency Businesses Act (URVCBA), which would establish a legal framework for virtual currency transactions, including those conducted on blockchain platforms (Uniform Law Commission 2017). The URVCBA would provide legal certainty for virtual currency transactions by establishing a set of rules that apply across different legal jurisdictions in the US.

Another challenge in cross-border blockchain transactions is resolving conflicts of laws. Conflicts of laws can arise when different legal systems have different rules that apply to the same transaction. For example, a blockchain-based transaction may involve parties located in different countries, and the transaction may be subject to different legal systems depending on the location of the parties.

To resolve conflicts of laws, parties to a cross-border blockchain transaction can include choice-of-law clauses in their contracts. A choice-of-law clause specifies which legal system will apply to the transaction in the event of a dispute. However, enforcing choice-of-law clauses in cross-border transactions can be challenging, as different legal systems may have different rules for interpreting and enforcing such clauses.

In addition to choice-of-law clauses, parties to a cross-border blockchain transaction can also use alternative dispute resolution (ADR) mechanisms to resolve conflicts of laws. ADR mechanisms, such as arbitration or mediation, can provide a more flexible and efficient way to resolve disputes compared to traditional litigation.

Identity verification

The potential of blockchain technology to revolutionise the verification of digital identities can have significant implications for the legal system (Swan 2015). Tra-

ditional methods of identity verification, such as relying on a centralised authority to verify identities, are vulnerable to hacking and fraud. Blockchain-based identity verification can offer a more secure and decentralised approach.

One of the main challenges in developing blockchain-based identity verification protocols is ensuring that they comply with the legal requirements of various jurisdictions. In many countries, identity verification is a legal requirement for certain activities, such as opening a bank account, obtaining a loan, or voting in an election. For example, in the United States, the Bank Secrecy Act (BSA) requires financial institutions to verify the identity of their customers (FinCEN 2021). Similarly, in Germany, the Anti-Money Laundering Act (GwG) requires banks and other financial institutions to verify the identity of their customers (BaFin 2020). In Australia, the Financial Transaction Reports Act (FTR Act) requires financial institutions to verify the identity of their customers before conducting certain transactions (AUSTRAC 2022).

Blockchain-based identity verification protocols must comply with these legal requirements in order to be accepted by the legal system. This requires that the protocols provide a high level of assurance that the person presenting the digital identity is indeed who they claim to be. It also requires that the protocols provide a way for the user to revoke their digital identity in case it is compromised or stolen.

To meet these requirements, blockchain-based identity verification protocols must incorporate strong authentication mechanisms, such as multi-factor authentication, biometrics, or digital signatures. They must also provide a way for users to securely store and manage their personal information, while ensuring that the information is not accessible to unauthorised parties.

In addition to these technical requirements, blockchain-based identity verification protocols must also comply with legal requirements related to data protection, privacy, and security. For example, in the European Union, the GDPR requires that personal data be processed in a secure and transparent manner, and that users be informed about how their data is being used (EUR-Lex 2016).

Blockchain-based identity verification protocols can be complex and technical in nature, requiring a certain level of technical knowledge to use them effectively. This can pose a challenge for many users who are not familiar with the intricacies of blockchain technology. In addition, access to specialised software may also be a barrier for some users, particularly those who do not have access to modern technology or are not comfortable using it (U.S. Government Accountability Office 2022).

To address it, developers of blockchain-based identity verification protocols must take a user-centered approach, focusing on developing user-friendly interfaces and simplified processes for identity verification. For example, the uPort platform developed by ConsenSys includes a mobile app that allows users to create and manage their digital identities using a simple, user-friendly interface (uPort n.d.). Similarly, the Sovrin Network developed by the Sovrin Foundation provides a set of user-friendly tools that allow users to create and manage their digital identities using a simple, intuitive interface (Sovrin Foundation 2018).

In addition, many blockchain-based identity verification protocols are being developed with the goal of interoperability, which means that they can be used across different platforms and systems. This can help to increase accessibility and reduce

barriers for users, as they can use their digital identity across a range of applications and services. For example, the Trust over IP Foundation is working on developing standards for digital identities that can be used across different blockchain networks and traditional systems (Trust over IP Foundation 2021).

Several countries have taken steps to establish legal frameworks for blockchain-based identity verification. For example, in Estonia, the government has developed a digital identity system that uses blockchain technology to verify the identities of citisens (Vigna and Casey 2018). The Estonian digital identity system has been used for a wide range of activities, including voting in elections and accessing government services. In the United Arab Emirates, the government has launched the Emirates Blockchain Strategy 2021, which aims to use blockchain technology for identity verification and to improve government services (Government of Dubai 2020). In Canada, the government has established the Pan-Canadian Trust Framework, which includes guidelines for the use of digital identity and authentication services, including those based on blockchain technology (Government of Canada 2021). According to the Swiss electorate vote on March 7, 2021, the Federal Act on Electronic Identification Services (e–ID Act) was proposed in Switzerland. This act aims to enable the use of blockchain technology for identity verification (Swiss Federal Council 2021). In India, the government has launched the Aadhaar program, which uses biometric data and a unique identification number to verify the identity of citizens. The program has been linked to blockchain-based systems to increase security and reduce the risk of fraud (Sachan 2018).

These initiatives demonstrate the growing interest and investment in blockchain-based identity verification systems by governments around the world. As more countries adopt these systems, it is likely that legal frameworks will continue to evolve to accommodate the use of blockchain technology for identity verification in various contexts. However, it is important to ensure that these systems are developed with a user-centered approach and meet legal requirements for identity verification in order to gain widespread acceptance and adoption.

AML/KYC compliance

Anti-Money Laundering (AML) and Know Your Customer (KYC) compliance are crucial for financial institutions to prevent money laundering, terrorist financing, and other illegal activities. With the increasing adoption of blockchain technology, there is a need for developing regulations for AML/KYC compliance in blockchain-based transactions.

The Financial Action Task Force (FATF), a global intergovernmental organisation that sets AML standards, has identified virtual assets, including cryptocurrencies, as a high risk for money laundering and terrorist financing due to their anonymity and lack of regulation (FATF 2021). The FATF has recommended that countries implement regulations for virtual asset service providers (VASPs), including those that operate on blockchain-based platforms, to ensure AML/KYC compliance.

In response to the FATF recommendations, many countries have introduced regulations for AML/KYC compliance in blockchain-based transactions. For example, the European Union's Fifth Anti-Money Laundering Directive (5AMLD) requires

VASPs to implement AML/KYC measures and register with national authorities (EUR-Lex 2018). Similarly, the Financial Crimes Enforcement Network (FinCEN) in the United States has issued guidance on AML/KYC compliance for virtual currency businesses, including those that operate on blockchain-based platforms (FinCEN 2019).

To enhance AML/KYC compliance in virtual asset transactions, blockchain technology has been utilised for various purposes. For instance, blockchain-based identity verification systems can be implemented to ensure the authenticity of customers' identities, while blockchain-based transaction monitoring systems can be leveraged to detect suspicious activity and track the flow of virtual assets (Malhotra et al. 2022).

Apart from meeting regulatory requirements, blockchain technology has the potential to enable more innovative and secure solutions for AML/KYC compliance. Decentralised identity verification is one such solution that utilises the immutability and transparency of blockchain to create a trustworthy identity verification process (Kshetri 2018). By eliminating the need to share personal information, decentralised identity verification systems offer a privacy-preserving alternative to traditional methods.

In decentralised identity verification systems, users are assigned a unique identifier or digital identity, which is stored on the blockchain. This identifier is linked to the user's personal information, such as their name and address, which is stored off-chain. When the user needs to verify their identity, they provide their digital identity to the verifying party, who then uses the blockchain to verify the authenticity of the identifier. Once the identifier is verified, the verifying party can then access the user's personal information stored off-chain.

In order to ensure effective AML/KYC compliance in blockchain-based transactions, it is also important to strike a balance between privacy and transparency. While blockchain technology provides a high degree of transparency, it also poses a risk to user privacy. This is particularly true in the case of public blockchains, where all transactions are visible to anyone on the network. To address this challenge, some blockchain-based solutions have been developed that use techniques such as zero-knowledge proofs to enable private transactions while maintaining transparency (Sedlmeir et al. 2022).

Another challenge in implementing AML/KYC compliance in blockchain-based transactions is the difficulty of identifying the beneficial owners of virtual assets. Because virtual assets can be transferred anonymously and without the need for a central authority, it can be difficult to determine who ultimately owns them. This creates a risk of money laundering and terrorist financing, as it allows criminals to move funds without detection. To address this challenge, some countries have implemented regulations requiring VASPs to identify the beneficial owners of virtual assets and report suspicious transactions to relevant authorities (Schwarz et al. 2021).

For example, in the United States, the Financial Crimes Enforcement Network (FinCEN) requires VASPs to register with the agency as a Money Services Business (MSB) and to implement AML/KYC policies that comply with the Bank Secrecy Act (BSA) and other relevant regulations. FinCEN also requires VASPs to file Suspicious Activity Reports (SARs) for any transactions that they suspect may be involved in money laundering or terrorist financing (Scharfman 2022).

Similarly, the European Union's Fifth Anti-Money Laundering Directive (5AMLD) requires VASPs to register with national financial authorities and implement AML/KYC policies that comply with the directive. The directive also requires VASPs to report suspicious transactions to relevant authorities and to identify and verify the beneficial owners of virtual assets (EUR-Lex 2018).

Other countries have also implemented similar regulations to address the challenges associated with virtual asset transactions. For instance, in Singapore, the Payment Services Act (PSA) regulates virtual asset service providers, and requires them to comply with AML/KYC requirements, report suspicious transactions, and identify beneficial owners of virtual assets (Government of Singapore 2019).

Despite these challenges, the use of blockchain technology for AML/KYC compliance offers several potential benefits. By leveraging the transparency and immutability of blockchain, it is possible to create a secure and reliable identity verification process while maintaining user privacy. Additionally, blockchain-based solutions can potentially reduce costs and increase efficiency by automating compliance processes and reducing the need for intermediaries. As such, there is a growing interest in the use of blockchain technology for AML/KYC compliance in the financial industry (Xu et al. 2017).

Consumer protection

In the context of blockchain technology, consumer protection becomes particularly important due to the decentralised nature of the blockchain. Transactions on the blockchain are conducted without the need for intermediaries, which can create opportunities for fraudulent activities.

One such activity is the Ponzi scheme, where investors are promised high returns but the returns are paid from the capital invested by new investors rather than from actual profits. The decentralied nature of the blockchain can make it difficult for authorities to detect and shut down these schemes.

Hacking attacks and data breaches are also concerns in the blockchain space. In 2019, the cryptocurrency exchange Binance suffered a hack that resulted in the loss of over $40 million worth of Bitcoin. The hack was made possible due to a vulnerability in the exchange's security measures (DuPont 2019).

To address these risks, regulatory bodies are beginning to develop consumer protection regulations for blockchain technology. For example, the European Union's GDPR applies to blockchain technology and provides individuals with the right to have their personal data erased from the blockchain (Eichler et al. 2018). In the United States, the Securities and Exchange Commission (SEC) has taken action against companies that conducted initial coin offerings (ICOs) without registering them as securities, which is required by law (DuPont 2019).

In addition to Ponzi schemes, hacking attacks, and data breaches, there are other types of illegal activities that may occur on the blockchain. One example is the use of blockchain for money laundering and terrorist financing. Because blockchain transactions are anonymous and difficult to trace, criminals may use the technology to move funds without detection (Forgang 2019). In fact, the FATF has identified virtual

assets, including cryptocurrencies, as a high risk for money laundering and terrorist financing due to their anonymity and lack of regulation (FATF 2020).

Another type of illegal activity that may occur on the blockchain is the sale of illegal goods or services. Because blockchain transactions are anonymous, criminals may use the technology to buy and sell illegal goods and services, such as drugs, weapons, and counterfeit goods (DuPont 2019). In fact, there have been several cases of illegal marketplaces operating on the blockchain, such as the Silk Road marketplace, which was shut down by the FBI in 2013 (Christin 2013).

Additionally, blockchain technology may be used for fraudulent activities, such as scams and phishing attacks. Scammers may use the technology to create fake tokens or ICOs to trick investors into investing in fraudulent projects (DuPont 2019). In fact, there have been several high-profile cases of ICO fraud in recent years, such as the case of the PlexCoin ICO, which was shut down by the U.S. Securities and Exchange Commission (SEC) in 2017 (U.S. Securities and Exchange Commission 2017).

Overcoming these types of illegal activities on the blockchain requires a multifaceted approach that involves technological solutions, regulatory frameworks, and industry cooperation. One approach is to implement technological measures, such KYC and AML checks, to increase transparency and reduce anonymity on the blockchain. These measures can help identify and prevent illegal activities, such as money laundering and terrorist financing.

Industry cooperation is also important in addressing illegal activities on the blockchain. Blockchain companies and industry organisations can work together to establish best practices and standards for blockchain transactions that prioritise consumer protection. For example, the Blockchain Alliance is a coalition of blockchain companies, law enforcement agencies, and regulators that aims to promote best practices for blockchain technology and prevent its use in illegal activities (Blockchain Alliance n.d.).

Some companies are developing blockchain-based identity verification systems, which can help to prevent identity theft and fraud (DuPont 2019). Additionally, some blockchain-based projects are developing reputation systems that use blockchain technology to track and verify the reputation of users and organisations, which can help to prevent scams and other fraudulent activities (Battah et al. 2021).

One area of concern related to blockchain technology is the use of smart contracts. To address the challenges surrounding the use of smart contracts on the blockchain, a potential solution is the development of a smart contract code of ethics. The code of ethics would establish guidelines for the use of smart contracts and ensure that they are designed and implemented with a focus on consumer protection. In addition, it would require smart contract developers to disclose any vulnerabilities or potential issues with the contracts, providing consumers with the information needed to make informed decisions about their use.

One proposal for a smart contract code of ethics comes from legal scholar Anupam Ghosh. In his paper “A Smart Contract Code of Ethics”, Ghosh outlines several principles that should be included in such a code. These principles include ensuring that smart contracts are designed in a way that protects the privacy and security of all parties involved, ensuring that contracts are transparent and auditable, and providing mechanisms for dispute resolution.

In addition to the development of a smart contract code of ethics, there is also a need for ongoing education and training for smart contract developers. This would ensure that developers are aware of potential vulnerabilities and are able to design contracts that prioritise security and consumer protection. Furthermore, there is a need for ongoing research and development in the area of smart contract security, to ensure that the technology continues to evolve and improve over time.

In addition to these specific regulations, there is a need for general consumer protection laws that apply to blockchain-based transactions. These laws should protect consumers from fraud, misrepresentation, and other illegal activities. They should also ensure that consumers have access to clear and accurate information about blockchain-based products and services. To this end, some legal experts have proposed the development of a "Blockchain Consumer Protection Act" that would provide a framework for consumer protection in the blockchain industry (DuPont 2019).

The proposed Blockchain Consumer Protection Act would establish a regulatory framework for consumer protection in the blockchain industry. This act would require blockchain-based companies to disclose certain information to consumers, such as the identity of the company's developers and key personnel, the intended use of funds, and any risks associated with the investment. It would also require companies to provide consumers with clear and accurate information about the products and services they offer, including the risks and benefits associated with them.

In addition, the act would establish penalties for companies that engage in fraudulent or deceptive practices, and would provide consumers with avenues for redress in the event of a dispute. This could include the establishment of a dispute resolution mechanism or the creation of a blockchain ombudsman who could assist consumers in resolving disputes.

Moreover, some legal experts suggest that the development of a self-regulatory organisation (SRO) could help to ensure consumer protection in the blockchain industry (Bauknight and Ebbink 2022). An SRO would be an independent, industry-led organisation that would establish and enforce industry standards for blockchain-based transactions. By establishing industry-wide standards for consumer protection, an SRO could help to build consumer trust in the blockchain industry and prevent fraudulent or illegal activities.

Intellectual property rights

Intellectual property rights (IPRs) have become increasingly important in the digital age, particularly with the rise of new technologies such as blockchain (Nappert 2021). The use of blockchain technology in the realm of IPRs has opened up new possibilities for creators and innovators to protect and enforce their intellectual property rights. However, it has also raised several legal challenges that need to be addressed.

The decentralised and immutable nature of the blockchain makes it an attractive platform for storing and sharing intellectual property. Blockchain technology can be used to create unique digital assets that can be tracked and verified, which is particularly useful in protecting copyrighted material, trademarks, and patents. Blockchain can also provide a secure and transparent platform for licensing and monetising intel-

lectual property, allowing creators to control and profit from their creations (Swan 2015).

However, the use of blockchain technology in the realm of IPRs raises several legal challenges. One of the main challenges is the issue of jurisdiction. Blockchain is a decentralised technology that operates across borders, making it difficult to determine which laws apply in case of a dispute (Dimitropoulos 2020). The lack of a clear legal framework for blockchain-based intellectual property also makes it challenging to enforce these rights.

In addition to the issue of jurisdiction, the lack of a clear legal framework for blockchain-based intellectual property poses a significant challenge for the protection and enforcement of IPRs. Traditional legal frameworks for intellectual property, such as copyright and patent law, were designed for a centralised system where ownership and control are clear and easy to identify. However, blockchain's decentralised nature makes it challenging to apply these traditional legal frameworks to blockchain-based intellectual property (Kshetri 2018).

Furthermore, the anonymity and pseudonymity of blockchain transactions create difficulties in identifying infringers and enforcing intellectual property rights. In traditional legal frameworks, infringers can be identified through their personal information and can be held accountable for their actions. However, on a decentralised blockchain network, the identity of the infringer may not be readily apparent, and therefore, enforcing IPRs can be challenging (Singh and Tripathi 2019).

To address these challenges, several initiatives are underway to establish legal frameworks for the protection and enforcement of intellectual property rights on the blockchain. For instance, the World Intellectual Property Organisation (WIPO) has been exploring the use of blockchain technology for the protection and management of intellectual property rights. WIPO has recognised the potential of blockchain technology to create a decentralised and secure platform for intellectual property management, but also acknowledges the need for clear legal frameworks to ensure effective protection and enforcement of these rights (WIPO 2019).

Another example of initiatives aimed at addressing these challenges is the Open Music Initiative (OMI), which is a collaboration between music industry stakeholders and technology companies that seeks to develop an open-source blockchain-based platform for managing music rights and royalties. OMI aims to create a decentralised and transparent platform for the management of music rights and royalties, which would ensure fair compensation for artists and simplify the complex and fragmented music licensing ecosystem (Open Music Initiative 2020).

Additionally, the European Union Intellectual Property Office (EUIPO) has launched a project called "Blockathon" to explore the potential of blockchain technology for the protection of intellectual property rights. The project aims to develop blockchain-based solutions for intellectual property management and enforcement, with a particular focus on copyright and trademark issues. The project also seeks to identify the legal and technical challenges associated with the use of blockchain technology for intellectual property management and enforcement and develop strategies to overcome these challenges (European Union Intellectual Property Office n.d.).

In the traditional model of intellectual property rights, ownership is relatively straightforward, as it is held by a single entity or individual. However, the use of

blockchain technology in the realm of IPRs has introduced new ownership structures that are more complex and difficult to navigate. Blockchain technology allows for the creation of decentralised autonomous organisations (DAOs), which can hold intellectual property rights. These organisations are managed by smart contracts, which are self-executing and do not require human intervention.

While the use of DAOs can have benefits, such as increased transparency and decentralisation, it also raises challenges in terms of ownership. With multiple stakeholders involved in the ownership and management of a DAO, it can be difficult to determine who has the ultimate say over the use and distribution of intellectual property rights. Additionally, DAOs can be vulnerable to hacking or other security breaches, which can compromise the ownership and control of intellectual property rights.

As noted by Werbach (2018a), "DAOs present unique challenges to intellectual property law because they do not fit within the traditional legal categories of corporations, partnerships, or other entities. They are designed to be self-executing and do not require human intervention, making it difficult to determine who owns and controls the intellectual property held by a DAO".

There are a few successful examples of legal frameworks being established to address ownership challenges related to blockchain-based intellectual property held by DAOs. One notable example is the Ethereum Name Service (ENS), which is a decentralised domain name system built on the Ethereum blockchain. ENS allows users to register domain names as non-fungible tokens (NFTs) and manage them through DAOs. To address ownership challenges related to these NFTs, ENS has established a legal framework that defines the rights and responsibilities of the NFT holders, including the DAOs that hold them. The framework also provides mechanisms for resolving disputes related to ownership and control of NFTs held by DAOs (Trujillo 2022).

Another example is the Ocean Protocol, which is a decentralised data exchange platform that uses blockchain technology. Ocean Protocol allows individuals and organisations to monetise and share their data through DAOs. To address ownership challenges related to data held by DAOs, Ocean Protocol has established a legal framework that defines the rights and responsibilities of the data holders, including the DAOs that hold them. The framework also provides mechanisms for resolving disputes related to ownership and control of data held by DAOs.

These examples demonstrate the importance of establishing legal frameworks to address ownership challenges related to blockchain-based intellectual property held by DAOs. By providing clarity on issues such as ownership, management, and control, these frameworks can help promote innovation and creativity while also addressing potential risks and disputes.

Governance

The governance of blockchain systems is crucial for their efficient and effective operation. Blockchain governance mechanisms are critical because they enable stakeholders to coordinate, communicate, and make decisions related to the operation of blockchain-based systems and networks (Böhme et al. 2015).

Governance mechanisms for blockchain-based systems and networks involve a variety of factors, including technical specifications, community consensus, and legal compliance. Technical specifications define the rules and parameters that govern the operation of the blockchain network, such as the consensus algorithm used to validate transactions, the block size limit, and the reward mechanism for network participants. Community consensus refers to the agreement among stakeholders on the rules and decisions that govern the blockchain network, such as changes to the technical specifications, adding or removing network participants, and resolving disputes. Legal compliance involves ensuring that the blockchain network operates within the legal framework of the jurisdiction in which it operates, such as complying with data protection laws and anti-money laundering regulations (Böhme et al. 2015).

The development of appropriate governance mechanisms for blockchain-based systems and networks is challenging due to the complexity of the technology and the need for collaboration between legal and technical experts. Blockchain technology is still relatively new, and its underlying technical specifications are constantly evolving, making it challenging to establish stable and effective governance mechanisms. Moreover, blockchain governance mechanisms often involve complex legal and regulatory issues, which require expertise in legal and regulatory frameworks (Swan 2015).

To elaborate further, the tension between decentralisation and centralisation is a central concern for blockchain governance (Iansiti and Lakhani 2017). On the one hand, decentralisation is a key feature of blockchain technology, as it enables a distributed network of nodes to verify transactions and maintain the integrity of the ledger. This decentralisation also provides a level of transparency, as all network participants can access the same information and are able to track the movement of assets on the network.

On the other hand, some degree of centralisation may be necessary to ensure that the network operates effectively (Böhme et al. 2015). For example, in a proof-of-work blockchain, where miners compete to solve complex algorithms to validate transactions and earn rewards, there is a risk that a few large entities could control a majority of the mining power (Narayanan et al. 2016). This concentration of power could lead to a situation where the network becomes vulnerable to attacks, and the integrity of the ledger could be compromised.

To tackle these challenges, governance mechanisms need to strike a balance between decentralisation and centralisation (Yli-Huumo et al. 2016). For example, some blockchain networks have developed mechanisms to prevent the concentration of mining power, such as limiting the number of blocks that a single miner can validate. Other networks have developed more complex mechanisms, such as delegated proof-of-stake, which involves electing a smaller group of nodes to validate transactions on behalf of the network.

One example is Bitcoin, the world's first and most well-known blockchain network. Bitcoin uses a proof-of-work consensus mechanism, where miners compete to solve a complex algorithm to validate transactions and earn rewards. However, the concentration of mining power among a few large entities has been a concern for Bitcoin's governance (Nakamoto 2008). To address this, Bitcoin has implemented a mechanism called the "difficulty adjustment", which regulates the difficulty of the

algorithm based on the total mining power on the network. This helps prevent any one entity from controlling the majority of the mining power, and thus maintaining the decentralisation of the network (Zhang et al. 2018b).

Another example is Ethereum, the second-largest blockchain network in terms of market capitalisation. Ethereum originally used a proof-of-work consensus mechanism like Bitcoin but has recently begun transitioning to a proof-of-stake mechanism. Proof-of-stake involves validators, who hold a certain amount of the network's native token, to validate transactions and earn rewards. However, to prevent the concentration of stake among a few validators, Ethereum uses a mechanism called "slashing", which penalises validators who act maliciously or do not follow the network's rules (Ethereum.org n.d.). This incentivises validators to act in the best interest of the network, ensuring its integrity and decentralisation.

Finally, there is EOS, a blockchain network that uses delegated proof-of-stake. In this mechanism, token holders elect a group of nodes to act as validators, known as "block producers", who are responsible for validating transactions on the network. This reduces the number of nodes required to validate transactions, which improves the network's scalability and efficiency. However, to prevent centralisation, EOS limits the number of votes a token holder can cast and requires block producers to rotate periodically, ensuring that no one entity has too much control over the network (EOSIO n.d.).

Interoperability

Interoperability is a critical challenge facing the blockchain industry. With the proliferation of different blockchain networks and systems, there is a growing need to ensure that these networks can communicate with each other seamlessly. Interoperability refers to the ability of different blockchain networks and systems to work together, enabling the transfer of value and data across these networks (ElBahrawy et al. 2017).

Ensuring interoperability between different blockchain networks and systems is essential for the development of a robust and interconnected blockchain ecosystem (Swan 2015). Interoperability can enable new use cases, such as cross-chain token transfers, and can also help to reduce fragmentation and improve network efficiency (Swan 2015).

However, achieving interoperability between different blockchain networks and systems is not a simple task. One of the main challenges is the lack of a common standard for interoperability (Zhang et al. 2018a). Different blockchain networks and systems use different consensus mechanisms, data formats, and smart contract languages, making it difficult to achieve interoperability. Additionally, regulatory frameworks for blockchain networks can vary widely between jurisdictions, which can further complicate efforts to achieve interoperability (Marusevich 2021).

In response to the challenge of achieving interoperability, several proposed solutions have emerged. One approach is to use interoperability protocols that enable communication between different blockchain networks and systems. Examples of interoperability protocols include Polkadot, Cosmos, and Chainlink (ElBahrawy et al. 2017). These protocols use different approaches to achieve interoperability,

such as cross-chain messaging, inter-blockchain communication, and oracle-based solutions.

Another approach is to use interoperability bridges that enable the transfer of value and data between different blockchain networks and systems. Examples of interoperability bridges include Arkane Network, Wanchain, and Ren (Ray 2023). Interoperability bridges typically use a two-way pegging mechanism to lock up assets on one blockchain network and release them on another network.

Regulatory harmonisation can also play a role in achieving interoperability between different blockchain networks and systems. Inconsistent regulatory frameworks can create barriers to interoperability by making it difficult for blockchain networks to comply with different regulations in different jurisdictions. Regulatory harmonisation can help to create a more consistent regulatory environment, enabling blockchain networks to operate across different jurisdictions more easily.

Identification of future challenges and issues

After succinctly summarising the legal and regulatory challenges associated with the integration of blockchain into the contemporary legal system, certain blind spots emerge as blockchain continues to advance within the legal domain. These are primarily linked to the rapid development of technology and the bureaucratic nature of the legal system, necessitating careful consideration of necessary changes. For instance, while the feasibility of blockchain integration is still being discussed, a new actor, AI, has emerged on the scene in recent years (2022–2023). This section aims to identify perspectives for further research rather than critique existing paradigms.

In the relevant literature, various sources provide descriptive insights into the complexities associated with predicting the development of the integration of blockchain, AI, IoT, and big data. Rabah (2018) emphasises integration complexities and interoperability challenges arising from the combination of these technologies. Salah et al. (2019) identify issues in ensuring the transparency, security, and scalability of blockchain-based AI systems, suggesting avenues for research to address these concerns. Gulati et al. (2020) highlight the need for standardised protocols, ethical considerations, and regulatory frameworks when integrating blockchain with AI. Reyna et al. (2018) discuss challenges such as data privacy, scalability, and consensus mechanisms in the integration of blockchain with IoT, proposing decentralised solutions. Kumar and Mallick (2018) address security challenges within the IoT ecosystem by advocating for blockchain's role in enhancing data integrity and trust. Dorri et al. (2016) delve into scalability, latency, and resource consumption issues in applying blockchain to IoT and present solutions like lightweight consensus algorithms. Karafiloski and Mishev (2017) offer insights into leveraging blockchain for data provenance and integrity in big data applications, acknowledging challenges related to storage and processing efficiency.

In exploring the potential challenges, one notable aspect is the integration of blockchain with other emerging technologies, such as the IoT, AI, and big data. For example, the integration of blockchain and IoT devices could enable secure and decentralised data sharing, but it also raises concerns about the scalability, security,

and privacy implications of such a system (Dorri et al. 2017). Firstly, IoT devices generate vast amounts of data, and if all of this data were to be stored on the blockchain, it could quickly become unwieldy and difficult to manage. Additionally, the processing power and storage capacity required to support a blockchain-based IoT system could be significant, potentially limiting the scalability of such a system. Secondly, IoT devices are often vulnerable to cyber attacks, and the addition of blockchain technology could potentially create new attack vectors or vulnerabilities. For example, a malicious actor could attempt to compromise a large number of IoT devices and then use them to manipulate the blockchain network. Finally, while blockchain technology can enable secure and decentralised data sharing, it can also make it difficult to remove or modify data once it has been added to the blockchain. This means that individuals may have little control over the data that is collected and shared by IoT devices.

Similarly, the integration of blockchain and AI could facilitate the creation of new decentralised applications and autonomous agents, but it also raises concerns about the transparency and accountability of such systems (Crosby et al. 2016). Since blockchain-based systems operate in a decentralised and trustless environment, it may be difficult to determine who is responsible for the actions of an AI agent running on a blockchain network (Crosby et al. 2016).

Moreover, blockchain-based systems are designed to be immutable, meaning that once a transaction is added to the blockchain, it cannot be changed. This feature is important for maintaining the integrity and security of the system, but it can also make it difficult to correct errors or mistakes made by an AI agent. This lack of flexibility and adaptability in blockchain-based systems could limit their effectiveness in certain use cases involving AI.

Finally, the integration of blockchain and AI raises concerns about data privacy and security. AI agents rely on large amounts of data to train and make decisions, and blockchain-based systems are designed to be transparent and secure. However, if sensitive or confidential data is included in a blockchain transaction, it could be accessible to anyone with access to the network. This could pose a significant threat to data privacy and security.

Therefore, it is important to carefully consider the implications of integrating blockchain and AI, and to develop solutions that address the challenges and risks associated with these technologies. This could involve developing new governance models, technical standards, and best practices for the use of blockchain-based systems in combination with AI (Crosby et al. 2016).

The increasing energy consumption and carbon footprint of some blockchain networks are becoming a major concern for environmentalists and sustainability advocates. The decentralised and distributed nature of blockchain technology requires a massive amount of computational power, which in turn requires significant energy consumption. For instance, the Bitcoin network alone consumes as much electricity as the entire country of Argentina, according to a study by the University of Cambridge (Sargisyan 2023). This energy consumption not only leads to high costs but also contributes to greenhouse gas emissions.

As blockchain technology continues to grow and expand, the need for sustainable approaches to its implementation and operation becomes even more pressing.

One solution to this issue may be the development of new consensus algorithms and mining techniques that are more energy-efficient. For example, Proof of Stake consensus algorithms can reduce energy consumption by eliminating the need for energy-intensive mining processes. This approach is being adopted by many newer blockchain networks, including Ethereum 2.0. Similarly, new mining techniques, such as the use of renewable energy sources, can help reduce the carbon footprint of blockchain networks.

Another way to address the environmental sustainability issue is through the use of renewable energy sources to power blockchain operations. Many blockchain companies are already exploring this option by using renewable energy sources, such as solar or wind power, to run their mining operations. For instance, a solar-powered Bitcoin mining operation was launched in the United States in 2021, which is expected to reduce the carbon footprint of Bitcoin mining significantly.

Upon comprehensive scrutiny of the legal and regulatory challenges stemming from the integration of blockchain into the contemporary legal system, this concluding section embarked on a quest to delineate crucial avenues for future research. It sought to shed light on how blockchain would engage with emerging technologies like AI, big data, and IoT, offering a brief glimpse into potential adverse effects on the environment. As conclusions were drawn, a multitude of facets emerged, demanding meticulous consideration. This paper aspired to encapsulate and synthesise these facets in the context of blockchain's application within the legal sphere, contributing to a nuanced understanding of the intricate dynamics at play.

Conclusion

This research paper delves into the myriad challenges arising from the integration of blockchain into the legal domain. Acknowledging the inherent difficulty in providing an exhaustive list due to uncertainties in future developments, the study uniquely compiles a comprehensive overview of challenges, distinguishing itself from studies that exclusively focus on specific areas. This underscores the broad and speculative nature of the topic, revealing discernible demand across various sectors as blockchain technology becomes increasingly integrated not only into the legal landscape.

To fortify privacy, data protection, and security within the legal sphere, a comprehensive strategy involves implementing advanced technical measures such as encryption techniques, zero-knowledge proofs, and secure smart contracts. Regulatory compliance plays a crucial role, necessitating adherence to data protection regulations like GDPR and robust AML and KYC procedures. Regular security audits, adaptive policies, and staying informed about technological advancements and regulatory changes ensure a proactive and resilient stance against evolving threats.

The discussions span a wide range, from foundational aspects like consensus mechanisms to nuanced considerations such as privacy, compliance, consumer protection, and governance. The study elucidates the complexity and diversity of challenges surrounding blockchain technology, emphasizing the need for a delicate balance between innovation and responsible governance as the technology evolves. Collaborative efforts among industry stakeholders, regulatory bodies, and the broader

community are deemed pivotal for shaping the future trajectory of blockchain's integration into the legal sphere.

To fortify regulatory measures in the integration of blockchain into the legal sphere, a multifaceted approach is imperative. Clear and standardised frameworks addressing the potential conflict of laws should be developed, promoting international collaboration to harmonize regulatory practices. Smart contract enforceability can be bolstered through the establishment of comprehensive legal frameworks that acknowledge their validity and provide guidelines for dispute resolution in case of breaches. Assurance of legal admissibility involves crafting specific regulations recognizing blockchain data as evidence, ensuring its acceptance in legal proceedings.

Identity verification can be enhanced by establishing robust and privacy-preserving blockchain-based systems, aligning with evolving data protection regulations. Ensuring consumer and intellectual property rights protection requires proactive legislation and enforcement, aligning with established norms and extending legal safeguards to blockchain transactions. Governance complexities can be navigated through the development of adaptive regulatory mechanisms, learning from existing case studies, and incorporating community-driven approaches into regulatory frameworks.

To address AML and KYC compliance, regulatory bodies should collaborate to establish unified standards, ensuring consistent adherence across jurisdictions. Finally, interoperability challenges can be mitigated by fostering industry collaboration and encouraging the development of interoperable protocols. Regulatory bodies should proactively engage with the blockchain community to establish standards that facilitate seamless communication between different blockchain networks, fostering a connected and efficient legal landscape.

Despite providing a comprehensive overview, this study acknowledges its limitations. The rapidly evolving nature of blockchain technology may introduce new challenges, and regulatory frameworks may need to adapt accordingly. The focus on legal aspects might not capture all technical intricacies, necessitating future interdisciplinary research. The environmental impact of blockchain technology, briefly touched upon in the literature review, warrants more in-depth investigation.

In fostering future interactions, future research should focus on the connection between blockchain, AI, big data, and IoT within the legal sphere. Regulatory bodies should proactively engage with emerging technologies to formulate guidelines that facilitate their seamless integration. The development of clear ethical guidelines and privacy-preserving measures is imperative, safeguarding sensitive data in the crossroads of these advanced technologies.

Acknowledgement Not applicable.

Author contributions The author conducted research on the legal and regulatory challenges related to blockchain technology, including privacy, data protection, data security, and regulatory issues. The author analysed current legal frameworks and evaluated their effectiveness and potential challenges. They also identified future challenges and issues that may arise in the field of blockchain technology. The author was responsible for writing and revising the manuscript.

Funding Open Access funding provided thanks to the CRUE-CSIC agreement with Springer Nature. The author declares that no funding was received for this paper.

Data availability All data used in this article is based on publicly available information and can be accessed through the references cited. No new primary data was generated for this paper.

Declarations

Ethical approval This article does not contain any studies with human participants performed by any of the authors.

Informed consent This article does not contain any studies with human participants performed by any of the authors.

Conflict of interest The author declares no competing financial or non-financial interests that are directly or indirectly related to the work submitted for publication.

References

Abu Dhabi Global Market (ADGM) (2021) Electronic Transactions Regulations 2021. https://adgmen.thomsonreuters.com/rulebook/electronic-transactions-regulations-2021. Accessed 12 May 2023

AUSTRAC (2022) Know your customer (KYC) requirements. https://www.austrac.gov.au/business/how-comply-and-report-guidance-and-resources/customer-identification-and-verification/customer-identification-know-your-customer-kyc. Accessed 12 May 2023

Aydar M, Ayvaz S, Cetin SC (2019) Towards a blockchain based digital identity verification, record attestation and record sharing system. arXiv preprint arXiv:1906.09791

BaFin (2020) Anti-Money Laundering Act. https://www.bafin.de/SharedDocs/Downloads/EN/Aufsichtsrecht/dl_gwg_en.html. Accessed 12 May 2023

Bal A (2018) Taxation, virtual currency and blockchain. Kluwer Law International BV

Battah A, Iraqi Y, Damiani E (2021) Blockchain-based reputation systems: implementation challenges and mitigation. Electronics 10(3):289

Bauknight PC, Ebbink BM (2022) Cryptocurrency as commodities? Bipartisan Senate Bill proposes comprehensive legislation to regulate digital assets

Berto R (2019) Blockchain records: is the evidence admissible? A challenge for European Member States. Civil Proc Rev 10(3):49–66

Blockchain Alliance (n.d.) Home. https://blockchainalliance.org. Accessed 8 June 2023

Blockchain Legal and Regulatory Group (2023) Blockchain: legal and regulatory guidance (third edition). https://www.lawsociety.org.uk/topics/research/blockchain-legal-and-regulatory-guidance-report. Accessed 8 June 2023

Böhme R, Christin N, Edelman B, Moore T (2015) Bitcoin: economics, technology, and governance. J Econ Perspect 29(2):213–238

Christin N (2013) Traveling the Silk Road: a measurement analysis of a large anonymous online marketplace. In: Proceedings of the 22nd international conference on World Wide Web, pp 213–224

Crosby M, Pattanayak P, Verma S, Kalyanaraman V (2016) Blockchain technology: beyond bitcoin. Appl Innov 2(6–10):71

Cumming DJ, Johan S, Pant A (2019) Regulation of the crypto-economy: managing risks, challenges, and regulatory uncertainty. J Risk Financial Manage 12(3):126
Daneshgar F, Ameri Sianaki O, Guruwacharya P (2019) Blockchain: a research framework for data security and privacy. In: Web, Artificial Intelligence and Network Applications: proceedings of the Workshops of the 33rd International Conference on Advanced Information Networking and Applications (WAINA-2019), vol 33. Springer International Publishing, pp 966–974
De Filippi P, Wright A (2018) Blockchain and the law: the rule of code
De Hert P, Kumar A (2021) Blockchain, privacy, and data protection. In: Blockchain and Public Law. Edward Elgar Publishing, pp 141–156
Deloitte (2018) Deloitte's 2018 global blockchain survey: blockchain reaching beyond the hype [PDF]. https://www2.deloitte.com/content/dam/Deloitte/cz/Documents/financial-services/cz-2018-deloitte-global-blockchain-survey.pdf. Accessed 8 June 2023
Dimitropoulos G (2020) The law of blockchain. Wash L Rev 95:1117
Dorri A, Kanhere SS, Jurdak R (2016) Blockchain in internet of things: challenges and solutions. arXiv preprint arXiv:1608.05187
Dorri A, Kanhere SS, Jurdak R, Gauravaram P (2017) Blockchain for IoT security and privacy: the case study of a smart home. In: 2017 IEEE international conference on pervasive computing and communications workshops (PerCom workshops), pp 618–623
Drummer D, Neumann D (2020) Is code law? Current legal and technical adoption issues and remedies for blockchain-enabled smart contracts. J Inf Technol 35(4):337–360
DuPont Q (2019) Cryptocurrencies and blockchains. John Wiley & Sons
Durovic M, Lech F (2019) The enforceability of smart contracts. Italian LJ 5:493
Dwivedi V, Pattanaik V, Deval V, Dixit A, Norta A, Draheim D (2021) Legally enforceable smart-contract languages: a systematic literature review. ACM Comput Surv (CSUR) 54(5):1–34
Eichler N, Jongerius S, McMullen G, Naegele O, Steininger L, Wagner K (2018) Blockchain, data protection, and the GDPR. Blockchain Bundesverband eV, Tech. Rep
ElBahrawy A, Alessandretti L, Kandler A, Pastor-Satorras R, Baronchelli A (2017) Evolutionary dynamics of the cryptocurrency market. Royal Soc Open Sci 4(11):170623
Electronic Transactions (Amendment) Act 2019, s 2
EOSIO (n.d.) About us. https://eos.io/about/. Accessed 8 June 2023
Ethereum.org (n.d.) Ethereum Proof of Stake FAQ. https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/. Accessed 8 June 2023
EUR-Lex (2016) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). https://eur-lex.europa.eu/eli/reg/2016/679/oj. Accessed 8 June 2023
EUR-Lex (2018) Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32018L0843. Accessed 8 June 2023
EUR-Lex (2020) Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0593. Accessed 8 June 2023
European Central Bank (2020a) Report on a digital euro. https://www.ecb.europa.eu/pub/pdf/other/Report_on_a_digital_euro%7E4d7268b458.en.pdf#page=17. Accessed 17 Aug 2023
European Central Bank (2020b) Stablecoins: implications for monetary policy, financial stability, market infrastructure and payments, and banking supervision in the euro area. https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op247%7Efe3df92991.en.pdf?b85631de8b2fdfa5395c2a4c87de05e1. Accessed 19 Jul 2023
European Central Bank (2022) Investigation phase report on the Digital Euro Project (Report No. 1/2022). https://www.ecb.europa.eu/paym/digital_euro/investigation/profuse/shared/files/dedocs/ecb.dedocs220420.en.pdf. Accessed 17 Aug 2023
European Investment Bank (2021) Artificial intelligence, blockchain and the future of Europe. https://www.eib.org/attachments/thematic/artificial_intelligence_blockchain_and_the_future_of_europe_report_en.pdf. Accessed 17 Aug 2023

European Union Agency for Cybersecurity (ENISA) (n.d.) Blockchain glossary. https://www.enisa.europa.eu/topics/incident-response/glossary/blockchain. Accessed 17 Aug 2023
European Union Intellectual Property Office (n.d.) Blockathon: anti-counterfeiting blockathon infrastructure. https://euipo.europa.eu/ohimportal/es/web/observatory/blockathon. Accessed 8 June 2023
Fabiano N (2017) Internet of things and blockchain: legal issues and privacy. The challenge for a privacy standard. In: 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), pp 727–734
Feng Q, He D, Zeadally S, Khan MK, Kumar N (2019) A survey on privacy protection in blockchain system. J Network Comput Appl 126:45–58
Financial Action Task Force (2020) FATF Report: virtual assets red flag indicators of money laundering and terrorist financing. https://www.fatf-gafi.org/en/publications/Methodsandtrends/Virtual-assets-red-flag-indicators.html. Accessed 8 June 2023
Financial Action Task Force (FATF) (2021) Guidance for a risk-based approach to virtual assets and virtual asset service providers. https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html. Accessed 8 June 2023
Financial Crimes Enforcement Network (FinCEN) (2019) Guidance on the application of FinCEN's regulations to certain business models involving convertible virtual currencies. https://www.fincen.gov/resources/statutes-regulations/guidance/application-fincens-regulations-certain-business-models. Accessed 8 June 2023
FinCEN (2021) Bank Secrecy Act. https://www.fincen.gov/resources/statutes-and-regulations/bank-secrecy-act. Accessed 8 June 2023
Forgang G (2019) Money laundering through cryptocurrencies. Econ Crime Foren Capstones 4:1–25
Fulmer N (2018) Exploring the legal issues of blockchain applications. Akron L Rev 52:161
Garcia-Teruel RM (2020) Legal challenges and opportunities of blockchain technology in the real estate sector. J Prop Plan Environ Law 12(2):129–145
Giordano MT (2020) Blockchain and the GDPR: new challenges for privacy and security. In: Blockchain, law and governance. Springer International Publishing, Cham, pp 275–286
Government of Canada (2021) Pan-Canadian Trust Framework. https://canada-ca.github.io/PCTF-CCP/. Accessed 8 June 2023
Government of Dubai (2020) Emirates blockchain strategy 2021. https://www.digitaldubai.ae/initiatives/blockchain. Accessed 8 June 2023
Government of Singapore (2019) Payment Services Act 2019 (Act No. 2 of 2019). Government Gazette, Acts Supplement, (No. 7). https://sso.agc.gov.sg/Acts-Supp/2-2019/Published/20190220?DocDate=20190220. Accessed 8 June 2023
Gulati P, Sharma A, Bhasin K, Azad C (2020) Approaches of blockchain with AI: challenges & future direction. In: Proceedings of the international conference on innovative computing & communications (ICICC)
Guo A (2016) Blockchain receipts: patentability and admissibility in court. Chi -Kent J Intell Prop 16:440
Iansiti M, Lakhani KR (2017) The truth about blockchain. Harv Bu Rev 95(1):118–127
Jamal A, Helmi RAA, Syahirah ASN, Fatima MA (2019) Blockchain-based identity verification system. In: 2019 IEEE 9th international conference on system engineering and technology (ICSET). IEEE, pp 253–257
Jiménez-Gómez BS (2019) Risks of blockchain for data protection: a European approach. Santa Clara High Tech LJ 36:281
Jin H, Luo Y, Li P, Mathew J (2019) A review of secure and privacy-preserving medical data sharing. IEEE Access 7:61656–61669
Joshi AP, Han M, Wang Y (2018) A survey on security and privacy issues of blockchain technology. Math Found Comput 1(2)
Karafiloski E, Mishev A (2017) Blockchain solutions for big data challenges: a literature review. In: IEEE EUROCON 2017-17th International Conference on Smart Technologies. IEEE, pp 763–768
Kethineni S (2019) Criminal activity and cryptocurrency. In: Global Crime: an Encyclopedia of Cyber Theft, Weapons Sales, and Other Illegal Activities [2 volumes], pp 136
Kosba A, Miller A, Shi E, Wen Z, Papamanthou C (2016) Hawk: the blockchain model of cryptography and privacy-preserving smart contracts. In: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS '16), pp 839–851
Kshetri N (2018) Blockchain's roles in meeting key supply chain management objectives. Int J Inf Manag 39:80–89. https://doi.org/10.1016/j.ijinfomgt.2017.12.003

Kumar NM, Mallick PK (2018) Blockchain technology for security issues and challenges in IoT. Procedia Comput Sci 132:1815–1823
LawTech Delivery Panel (2019) Legal statement on the status of cryptoassets and smart contracts. https://www.blockchain4europe.eu/wp-content/uploads/2021/05/6.6056_JO_Cryptocurrencies_Statement_FINAL_WEB_111119-1.pdf. Accessed 8 June 2023
Lianos I, Hacker P, Eich S, Dimitropoulos G (Eds.) (2019) Regulating blockchain: techno-social and legal challenges. Oxford University Press
Mahmood Z, Vacius J (2020) Privacy-preserving block-chain framework based on Ring Signatures (RSs) and Zero-Knowledge Proofs (ZKPs). In: 2020 International Conference on Innovation and Intelligence for Informatics, Computing and Technologies (3ICT). IEEE, pp 1–6
Malhotra D, Saini P, Singh AK (2022) How blockchain can automate KYC: systematic review. Wireless Pers Commun 122(2):1987–2021
Marusevich A (2021) The uncertainty of cryptocurrency regulation: achieving effective regulation without stifling law enforcement and innovation. Ethos 260:26–30
Moerel L (2018) Blockchain & data protection… and why they are not on a collision course. Eur Rev Private Law 26(6)
Möslein F (2018) Conflicts of laws and codes: defining the boundaries of digital jurisdictions. Available at SSRN 3174823
Nakamoto S (2008). Bitcoin: a peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf. Accessed 8 June 2023
Nappert S (2021) Twenty first century arbitration: the question of trust. https://ssrn.com/abstract=3956155 or https://doi.org/10.2139/ssrn.3956155. Accessed 8 June 2023
Narayanan A, Bonneau J, Felten E, Miller A, Goldfeder S (2016) Bitcoin and cryptocurrency technologies: a comprehensive introduction. Princeton University Press
National Institute of Standards and Technology (NIST) (2018) NISTIR 8202: blockchain technology overview [PDF]. https://csrc.nist.gov/publications/detail/nistir/8202/final. Accessed 8 June 2023
Naves J, Audia B, Busstra M, Hartog KL, Yamamoto Y, Rikken O, van Heukelom-verhage S (2019) Legal aspects of blockchain. Innov Technol Gov Glob 12(3–4):88–93
Open Music Initiative (2020) Open music initiative. https://open-music.org/. Accessed 8 June 2023
Quintais JP, Bodó B, Giannopoulou A, Ferrari V (2019) Blockchain and the law: a critical evaluation. Stan J Blockchain Law Policy 2(1):86–112
Rabah K (2018) Convergence of AI, IoT, big data and blockchain: a review. Lake Inst J 1(1):1–18
Raskin M (2016) The law and legality of smart contracts. Geo L Tech Rev 1:305
Ray PP (2023) Web3: a comprehensive review on background, technologies, applications, zero-trust architectures, challenges and future directions. Internet of Things Cyber-Phys Syst
Reyna A, Martín C, Chen J, Soler E, Díaz M (2018) On blockchain and its integration with IoT. Challenges and opportunities. Future Gener Comput Syst 88:173–190
Sachan K (2018) Aadhaar & blockchain: opportunities and challenges for India. Doctoral dissertation, Massachusetts Institute of Technology.
Şahan S, Ekici AF, Bahtiyar Ş (2019) A multi-factor authentication framework for secure access to blockchain. In: Proceedings of the 2019 5th international conference on computer and technology applications, pp 160–164
Salah K, Rehman MHU, Nizamuddin N, Al-Fuqaha A (2019) Blockchain for AI: review and open research challenges. IEEE Access 7:10127–10149
Sargisyan AG (2023) The Harm of cryptocurrency mining to the environment: how serious is it. In: Current problems of the global environmental economy under the conditions of climate change and the perspectives of sustainable development. Springer International Publishing, Cham, pp 13–21
Savelyev A (2018) Copyright in the blockchain era: promises and challenges. Comput Law Secur Rev 34(3):550–561
Scharfman J (2022) Anti-money laundering compliance for cryptocurrencies. In: Cryptocurrency compliance and operations: digital assets, blockchain and DeFi, pp 91–114
Schellinger B, Völter F, Urbach N, Sedlmeir J (2022) Yes, I do: marrying blockchain applications with GDPR. e-government 19:22
Schwarz N, Chen MK, Poh MK, Jackson MG, Kao K, Fernando MF, Markevych M (2021) Virtual assets and anti-money laundering and combating the financing of terrorism (1): some legal and practical considerations. International Monetary Fund
Sedlmeir J, Lautenschlager J, Fridgen G, Urbach N (2022) The transparency challenge of blockchain in organizations. Electron Mark 1–16

Singh BP, Tripathi AK (2019) Blockchain technology and intellectual property rights. J Intellect Prop Rights 24:41–44
Sovrin Foundation (2018) Sovrin Network. https://sovrin.org/overview/. Accessed 8 June 2023
Spring JC (2019) The blockchain paradox: almost always reliable, almost never admissible. SMU L Rev 72:925
Staples M, Chen S, Falamaki S, Ponomarev A, Rimba P, Tran AB, Weber I, Xu X, Zhu J (2017) Risks and opportunities for systems using blockchain and smart contracts. Data61 (CSIRO), Sydney
Suff M (1997) Essential contract law. Cavendish Publishing
Sung HC (2019) Prospects and challenges posed by blockchain technology on the copyright legal system. Queen Mary J Intellect Prop 9(4):430–451
Swan M (2015) Blockchain: blueprint for a new economy. O'Reilly Media
Swiss Federal Council (2019) Federal Act on the adaptation of Federal Law to developments in distributed ledger technology (DLT Act). https://www.newsd.admin.ch/newsd/message/attachments/60601.pdf. Accessed 8 June 2023
Swiss Federal Council (2021) Federal Act on electronic identification services (e-ID Act). https://www.admin.ch/gov/en/start/documentation/votes/20210307/federal-act-on-electronic-identification-services.html. Accessed 8 June 2023
Szostek D (2019) Blockchain and the Law
The Act on the Promotion of Utilizing Information Communication Technology in Legal Affairs (Act No. 49 of 2001, as amended by Act No. 77 of 2020)
Tian X, Zhu J, Zhao X, Wu J (2022) Improving operational efficiency through blockchain: evidence from a field experiment in cross-border trade. Prod Plann Control 1–16
Trujillo A (2022) The surge of non-fungible tokens and its implications for digital ownership from an Internet governance perspective. Rivista Italiana Di Informatica E Diritto 4(1):125–132
Trust over IP Foundation (2021) About Us. https://trustoverip.org/about/about/. Accessed 8 June 2023
U.S. Government Accountability Office (GAO) (2022) Blockchain: financial and non-financial uses and challenges. https://www.gao.gov/blog/blockchain-financial-and-non-financial-uses-and-challenges. Accessed 12 May 2023
U.S. Securities and Exchange Commission (SEC) (2017) SEC halts initial coin offering scam. https://www.sec.gov/news/press-release/2017-219. Accessed 8 June 2023
Uniform Law Commission (2017) Uniform Regulation of Virtual-Currency Businesses Act. https://shorturl.at/kswCM. Accessed 8 June 2023
Uniform Law Commission (n.d.a) Uniform Commercial Code. https://shorturl.at/AGKT7. Accessed 8 June 2023
Uniform Law Commission (n.d.b) Uniform Electronic Transactions Act. https://shorturl.at/ixyVY. Accessed 8 June 2023
uPort (n.d.) Introducing the next generation of decentralized identity. https://www.uport.me. Accessed 8 June 2023
Vigna P, Casey MJ (2018) The truth machine: the blockchain and the future of everything. St. Martin's Press
Werbach K (2018a) The blockchain and the new architecture of trust. MIT Press
Werbach K (2018b) Trust, but verify: why the blockchain needs the law. Berkeley Technol Law J 33(2):487–550
WIPO (2019) WIPO technology trends 2019: artificial intelligence. WIPO
Wirth C, Kolain M (2018) Privacy by blockchain design: a blockchain-enabled GDPR-compliant approach for handling personal data
Wylde V, Rawindaran N, Lawrence J, Balasubramanian R, Prakash E, Jayal A, Khan I, Hewage C, Platts J (2022) Cybersecurity, data privacy and blockchain: a review. SN CompuT Sci 3(2):127
Xu X, Weber I, Staples M, Zhu L, Bosch J, Bass L, Pautasso C, Rimba P (2017) A taxonomy of blockchain-based systems for architecture design. In: 2017 IEEE international conference on software architecture (ICSA), pp 243–252
Yassein MB, Shatnawi F, Rawashdeh S, Mardin W (2019) Blockchain technology: characteristics, security and privacy; issues and solutions. In: 2019 IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA). IEEE, pp 1–8
Yeoh P (2017) Regulatory issues in blockchain technology. J Financ Regul Compliance 25(2):196–208
Yli-Huumo J, Ko D, Choi S, Park S, Smolander K (2016) Where is current research on blockchain technology?—a systematic review. PloS One 11(10):e0163477

Zhang P, Schmidt DC, White J, Lenz G (2018a) Blockchain technology use cases in healthcare. In: Advances in computers, vol 111. Elsevier, pp 1–41

Zhang X, Qin R, Qin R, Yuan Y, Wang F-Y (2018b) An analysis of blockchain-based bitcoin mining difficulty: techniques and principles. In: 2018 Chinese Automation Congress (CAC). Xi'an, China. https://doi.org/10.1109/CAC.2018.8623140

Zohar A (2015) Bitcoin: under the hood. Commun ACM 58(9):104–113