Westcliff International Journal of Applied Research
WIJAR

Westcliff International Journal of Applied Research
Vol. 8, No. 1. Spring 2024
https://doi.org/10.47670/wuwijar202481wbcaam

Balancing User Privacy and Legal Demands while Conducting Businesses on the Blockchain

Dr. Wezi Bonono Chipeta
Westcliff University

Dr. Abdullahi Adaviriku Malik
Westcliff University

Abstract

Blockchain technology offers a promising way to improve business processes by providing a secure and transparent transaction platform. However, using this technology brings its own set of challenges, especially when trying to balance user privacy with legal and regulatory needs. This article explores the challenges of keeping user information private, adhering to regulatory frameworks, and fulfilling legal requirements on the blockchain. A key point in this research is the challenge of keeping or maintaining confidentiality while being transparent. The article also discusses the issues of applying legal rules to a system not controlled by one central authority, the risks of privacy and security breaches, and the need to follow data protection laws. The article highlights how some blockchain-based companies have tackled these challenges, mainly through smart blockchain management and innovative technology, by looking at real-world examples from major companies like IBM, Bitpay, Ripple, and Coinbase. The systematic literature review (SLR) methodology involved reviewing literature from the past 15 years (2008-2023) from trusted sources like Google Scholar, ACM Digital Library, IEEE, Springer, and Science Direct. The findings indicate that cutting-edge technologies prioritizing privacy, such as zero-knowledge proofs, ring signatures, and encryption methods, would enable Bitcoin (BTC) platform operations to maintain or balance privacy and transparency. Furthermore, the study indicates the importance of clear privacy guidelines, adhering to relevant regulations, working closely with regulators and law enforcement, and educating users. In summary, it is crucial to approach blockchain carefully, prioritizing user privacy while meeting all legal and regulatory requirements.

Keywords: Blockchain technology, user privacy, legal requirements, data protection, regulations, privacy-focused technologies

Introduction

Blockchain technology (BCT) has been a significant innovation in recent years, notably giving rise to the well-known cryptocurrency, Bitcoin. However, beyond just cryptocurrency, BCT has found its way into various industries, helping many businesses differently. Simply put, BCT is a technology that records transactions securely, clearly, and permanently without a central authority overseeing it (Swan, 2015). Each part of this chain has a unique code linking back to the previous one, creating a secure record of all transactions (Nakamoto, 2008). This system comprises blocks containing transaction records, and a network of computers protects it. Once a block is added to the chain, it cannot be

changed, ensuring the data are safe and accurate.

BCT has changed businesses' operations by combining safety with transaction transparency on a platform system (Swan, 2015). BCT has been used in various areas like managing supply chain (Cole et al., 2019; Gurtu & Johny, 2019), verifying digital identities(Aydar et al., 2019; Tapscott & Tapscott, 2016; Wolfond, 2017), in finance (Chang et al., 2020; Nakamoto, 2008; Tapscott & Tapscott, 2017; Treleaven et al., 2017), protecting intellectual property (Crosby et al., 2016; Tsai et al., 2017; Wang et al., 2019), and handling smart contracts (Khan et al., 2021).

However, using BCT has challenges (Henry et al., 2018). One of the main issues is balancing user privacy with the need to follow laws and regulations (Damgård et al., 2021; Li et al., 2019). This issue includes the challenge of keeping things private while still being transparent (Damgård et al., 2021; Li et al., 2019), the difficulty of applying legal rules to a system not controlled by one central group (Damgård et al., 2021; Li et al., 2019), risks of privacy and security breaches (Böhme et al., 2015; Zyskind et al., 2015), and the need to follow data protection laws (Finck, 2018; Ibáñez et al., 2018; Kuner et al., 2018). To make the most of BCT in business, it is essential to carefully address these challenges and promote the responsible use of blockchain.

In this research article, our primary objectives are to explore the challenges of maintaining privacy in blockchain systems and to propose recommendations for balancing privacy with legal and regulatory aspects. The study investigates how blockchain technology impacts user privacy, assessing the inherent tensions between the transparent nature of blockchain and the need for privacy. Simultaneously, it aims to offer well-informed recommendations for blockchain management, prioritizing user privacy while complying with legal and regulatory requirements. This investigation involves ascertaining how blockchain systems comply with legal standards, describing the regulatory concerns related to BCT, and exploring the feasibility of integrating privacy technologies in blockchains. Furthermore, using real-world applications, it analyzes best practices and lessons learned from major companies like IBM, Bitpay, Ripple, and Coinbase. The recommendations suggest frameworks or guidelines that could aid stakeholders in navigating the complexities of blockchain technology. The ultimate goal is to contribute to a more comprehensive understanding of the delicate balance between privacy, legal compliance, and regulatory challenges in the blockchain landscape.

Literature Review

This section reviews existing literature from articles obtained from search engines such as Google Scholar ACM Digital Library and journals such as IEEE, Springer, Science Direct, and others to understand better BCT, its impact on user privacy, and the challenges of meeting legal and regulatory requirements.

The literature review starts with an overview of BCT, describing it as a decentralized digital system that securely records transactions without central oversight. The review highlights BCT's use across various sectors and its features like decentralization, transparency, permanent data storage, and strong security, primarily through cryptography.

The review then delves into user privacy concerns, acknowledging the risks such as identity theft and fraud due to BCT's transparency. The review discusses advanced cryptographic solutions like zero-knowledge proofs, ring signatures, homomorphic encryption, and privacy-preserving smart contracts to mitigate these risks. These methods are vital in ensuring data privacy while maintaining the integrity and transparency of blockchain transactions.

Following this, the review addresses legal compliance and regulatory requirements for BCT businesses. It notes the difficulties in applying legal rules to a decentralized system, the tension between BCT privacy features, and the need for regulatory oversight in areas like finance.

The review culminates in discussing the challenges of balancing user privacy with legal demands. It emphasizes the complexity of reconciling the need for businesses to comply with legal data-sharing requirements and the protection of user privacy. The review also points out the repercussions for businesses and users failing to meet these demands, highlighting the need for proactive strategies to navigate these challenges effectively.

Overview of Blockchain Technology

In simple terms, BCT is a digital system that records transactions securely and clearly without a central authority overseeing it (Smith, 2020). It has been used in many areas, from tracking products in a supply chain to managing contracts, because of its ability to improve transparency and efficiency (Gurtu & Johny, 2019; Moosavi et al., 2021; Swan, 2015). The system comprises blocks containing transaction records and is protected by a network of computers (Nakamoto, 2008). This composition ensures data are safe and cannot be changed (Hofmann et al., 2017; Nakamoto, 2008; Politou et al., 2021). BCT's main features include its decentralized nature, clear transaction records, permanent data storage, and strong security measures (Nakamoto, 2008). The strength of BCT comes from its use of cryptography, which protects information (Kosba et al., 2016b).

User Privacy Concerns

While BCT gives users more control over their data, it also has risks like identity theft and fraud (Khan et al., 2020). BCT's transparency records can sometimes reveal too much information about users (Sudhakaran et al., 2020). To address this, various methods have been developed to protect user privacy. Cryptographic solutions, such as zero-knowledge proof (ZKP) (W. Li et al., 2020; Sun et al., 2021), ring signatures (X. Li et al., 2020; Mercer, 2016), homomorphic encryption (Breuer & Bowen, 2013; Feng et al., 2019) and privacy-preserving smart contracts (Kosba et al., 2016a), have been developed to address these challenges. These solutions are described in the following sub-section.

Advanced Cryptographic Techniques

BCT's security comes from advanced methods of protecting data. These methods are crucial for keeping data safe and ensuring transparent and trustworthy transactions. Some of the main methods include:

Ring Signature Technology: Introduced by Rivest, Shamir, and Tauman in 2001, ring signatures offer enhanced anonymity in digital transactions. Unlike traditional digital signatures, identifying the signer, ring signatures allow a group member to sign on behalf of the entire group (X. Li et al., 2020). This technology ensures the signature's validity without revealing the individual signer's identity.

Homomorphic Encryption: This technique allows for computations on encrypted data without prior decryption (Breuer & Bowen, 2013). The encryption ensures that data remains confidential even during processing, making it ideal for operations on untrusted servers or third-party platforms.

Zero-Knowledge Proofs (ZKPs): ZKPs enable one party to provide proof of a statement's validity to another without fully revealing the specifics of that statement (Sun et al., 2021). This arrangement ensures data privacy while confirming its authenticity.

Privacy-Preserving Smart Contracts: These blockchain-based contracts protect sensitive data during execution. They employ cryptographic techniques to ensure data confidentiality while maintaining the integrity of the contract's operations (Kosba et al., 2016a).

After discussing user privacy and the methods to protect it, the following section looks at the legal and regulatory challenges of using BCT.

Legal Compliance and Regulatory Requirements

For businesses using BCT, understanding and following the law is crucial. There are strict rules about protecting user data and other legal requirements (Ibáñez et al., 2018). The decentralized nature of BCT may make it challenging to apply these rules significantly since data on the blockchain cannot be changed (Hofmann et al., 2017; Nakamoto, 2008; Politou et al., 2021). As BCT is used more in areas like finance, it is also essential to follow financial regulations. However, the privacy features of BCT complicate the monitoring and enforcing these rules, leading to the challenges of balancing user privacy while meeting legal compliance and regulatory requirements. These are examined in the next section.

Challenges of Balancing User Privacy and Legal Demands

Finding a balance between keeping user data private and meeting legal requirements is complex (Damgård et al., 2021). On the one hand, legal rules might require businesses to share user data, putting user privacy at risk (Damgård et al., 2021; Xue et al., 2019). On the

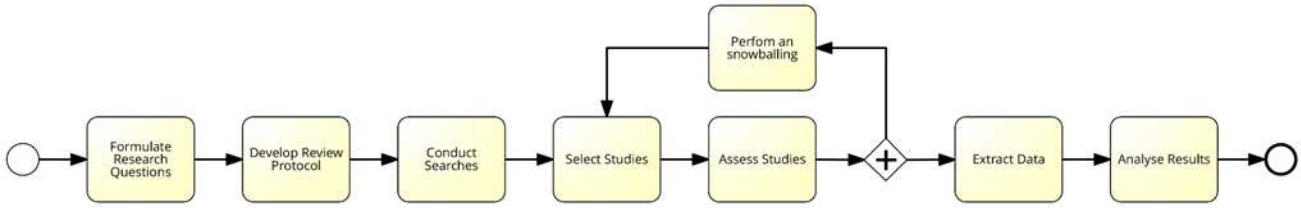
other hand, methods protecting user privacy complicate monitoring and regulations of BCT (Damgård et al., 2021). These challenges can have serious consequences. For businesses, not following the rules can lead to fines, legal problems, and damage to their reputation (Damgård et al., 2021; Martens et al., 2017). For users, it can mean risks to their privacy and personal data (Zyskind et al., 2015). Understanding these challenges is just the beginning. To address them, businesses must be proactive, use strategies protecting user privacy, and meet legal requirements. The following sections will explore these strategies and give examples of their use.

Research Methodology

The research methodology employed was the systematic literature review (SLR) approach as proposed in Kitchenham (2004) and Kitchenham and Charters (2007), the phases of which are shown in Figure 1.

Figure 1

Phases of the Systematic Literature Review



Note: Source (Kitchenham, 2004)

The SLR was meticulously designed to investigate the complexities of BCT, its influence on user privacy, and the associated legal and regulatory challenges. Literature selection, guided by criteria such as publication date (2008-2023), source credibility from search engines and databases like Google Scholar, ACM Digital Library, IEEE, springer, and Science Direct, relevance to the critical themes of BCT, and methodological robustness, was achieved through a combination of keyword searches and manual screening. The analysis phase encompassed thematic analysis to identify critical patterns within the data, comparative analysis to contrast different perspectives and findings, and a synthesis of these findings to understand privacy challenges and legal compliance in BCT comprehensively. This analysis was complemented by a critical evaluation to identify strengths, weaknesses, and gaps in the current research landscape, ensuring a thorough and balanced examination of the topic.

Identification of the Investigation

The article explores the challenges of balancing user privacy with the need to follow laws and regulations. The following are the research questions:

Q1: What are the challenges of maintaining privacy on blockchain systems?

Q2: How can blockchain systems comply with legal standards?

Q3: What are the regulatory concerns related to BCT?

Q4: What is the feasibility of integrating privacy-preserving technologies in blockchains?

Q5: What are the real-world applications and case studies of BCT?

Q6. What are the recommendations for balancing privacy legal and regulatory aspects of blockchain?

Firstly, it involves investigating how blockchain technology impacts user privacy and assessing the inherent tensions between the transparent nature of blockchain and the need for privacy. Secondly, it analyzes the compliance with legal standards in blockchain applications by examining legal frameworks and standards for BCT and how blockchain systems can comply with these legal standards, particularly in different jurisdictions. Thirdly, it identifies key regulatory concerns related to BCT. Fourthly, it investigates the integration of privacy-preserving technologies in blockchains. Fifthly, it assesses real-world applications and case studies, and lastly, it proposes recommendations for balancing privacy and legal and regulatory aspects.

Development of the Review Protocol

The remainder of the procedure, including the subsequent steps, involved defining the databases for searches and setting the criteria for including or excluding articles that would be part of the study. The criteria for inclusion in this study mandated that the reviewed articles include specific keywords such as blockchain technology, user privacy, legal requirements, data protection, regulations, and privacy-focused technologies. Additionally, the reviewed articles needed titles and abstracts relevant to the study's scope and written in English. The articles were excluded if they were duplicates, were not available for download, were written in a language other than English, or if their title and abstract did not align with the study's focus.

Conduct Searches

The study utilized multiple search engines to gather bibliographic references and academic articles. Search terms included "blockchain," "blockchain technology," "user privacy," "legal requirements," "data protection," "regulations," and "privacy-focused technologies." It specifically excluded terms like “Bitcoin” and “Cryptocurrency.” The research focused on publications from 2008 onwards, a timeframe chosen due to its relevance to the release of Nakamoto's Bitcoin paper in 2008 (Nakamoto, 2008). This period also covers the adoption of the EU General Data Protection Regulation (GDPR) on April 14, 2016, with its enforcement deadline set for May 25, 2018. The study investigated the difficulties in maintaining user privacy while adhering to legal and regulatory requirements in blockchain operations.

Early searches revealed a surge in blockchain technology-related publications starting in 2008. The research used various search engines and databases, including Google Scholar (http://scholar.google.com), ACM Digital Library (http://dl.acm.org), Springer (http://link.springer.com), IEEE Xplore Digital Library (http://ieeexplore.ieee.org), and Science Direct (http://www.sciencedirect.com). The search criteria were built around keywords such as "blockchain," "blockchain technology," "user privacy," "legal requirements," "data protection," "regulations," and "privacy-focused technologies." The Boolean operator AND was utilized to ensure the inclusion of all these terms. Additionally, terms like bitcoin and cryptocurrencies were excluded to narrow the focus away from the vast array of publications on these topics. The search was limited to English-language publications from 2008 to 2023. The search strings varied depending on the database, creating a specific set of strings for each, as detailed in Table 1.

Table 1

Search Strings in Scientific Databases

Database	Search String
Google Scholar	Blockchain technology user privacy legal requirements data protection regulations privacy-focused technologies -bitcoin cryptocurrency [interval 2008–2020]
ACM Digital Library	[All: blockchain technology] AND [All: user privacy] AND [All: legal requirements] AND [All: regulations] AND [All: privacy-focused technologies] AND [All: not bitcoin] AND [All: not cryptocurrency] AND [Publication Date: (01/01/2008 TO *)]
Springer	Blockchain technology AND user privacy AND legal requirements AND data protection AND regulations AND privacy-focused technologies AND NOT (bitcoin) AND NOT (cryptocurrency) within 2008–2023
IEEE Xplore Digital Library	(((((((Blockchain technology) AND user privacy) AND legal requirements) AND data protection) AND regulations) AND privacy-focused technologies) NOT bitcoin) NOT cryptocurrency) Filters Applied: 2016–2020
Science Direct	Blockchain technology user privacy legal requirements data protection regulations privacy-focused technologies -bitcoin -cryptocurrency Years: 2008–2023

Selection of Publications

Publications closely related to the search keywords were identified as potentially relevant. One hundred twenty publications were initially chosen for inclusion in the systematic review. The initial step involved summarizing the publishers of the journals and conference papers from which these publications were derived, as presented in Table 2. This demographic information helped determine the forums where researchers publish their scientific literature, guiding future publications.

Table 2

Relevant Journals and Publishers

Relevant Journals	Publishers
IEEE Access	IEEE
arXiv preprint	arXiv
Interactive Technology and Smart Education	Emerald Publishing
Pervasive and Mobile Computing	Elsevier
Journal of Economic Perspectives	American Economic Association
Engineering Secure Software and Systems	Springer
Proceedings of the International Conference.	ACM Digital Library
Technological Forecasting and Social Change	Elsevier
Supply Chain Management: An International Journal	Emerald Publishing
Topics in Cryptology – CT-RSA	Springer
International Journal of Advance Research, Ideas...	IJARI
Proceedings of the ACM SIGSAC Conference ...	ACM Digital Library
Journal of Network and Computer Applications	Elsevier
International Journal of Physical Distribution...	Emerald Publishing
IEEE Transactions on Emerging Topics in Computing	IEEE
Marine Policy	Elsevier
IEEE Access	IEEE
Procedia Computer Science	Elsevier
Peer-to-Peer Networking and Applications	Springer
IEEE Network	IEEE
Data	MDPI
Environmental Science and Pollution Research	Springer
Accounting, Auditing & Accountability Journal	Emerald Publishing
IEEE Network	IEEE
Harvard Business Review	Harvard Business Publishing
Penguin	Penguin Books
Computer	IEEE Computer Society
Procedia Computer Science	Elsevier
Technology Innovation Management Review	Carleton University
IEEE Transactions on Industrial Informatics	IEEE
Computers & Security	Elsevier
Portland International Conference on Management...	IEEE
IEEE Security and Privacy Workshops	IEEE

Following the completion of the searches, 120 publications were found to align with the established search criteria. Only those available for complete access and analysis were retained, while inaccessible ones were excluded. The subsequent phase involved a detailed review of each publication, focusing on the title, keywords, and abstract to assess their relevance to the study's core areas, including blockchain technology, user privacy, legal requirements, data protection, and privacy-focused technologies. The selection process was then narrowed down to include publications that addressed the six questions posed by this study, offering insights into the challenges of balancing user privacy with legal requirements. Ultimately, 62 published publications since 2008 were chosen for detailed information extraction.

Assess Studies

Simultaneously with the data extraction, the quality of the primary studies was assessed. This evaluation was based on their contextual relevance, the significance of the information provided, and its pertinence to our study's focus, as outlined by Kitchenham and Charters (2007). Through this process, one could qualify and validate each study based on the extracted data, which was used as a benchmark for determining whether to accept or reject a publication.

Performing Snowballing

The snowballing phase represents a method in systematic literature research described by Kitchenham (2004), which involves leveraging the references and citations of a document to uncover further relevant documents. This approach made it feasible to identify and incorporate additional articles pertinent to the study. This phase enhanced the understanding and explanation of the study's subject matter.

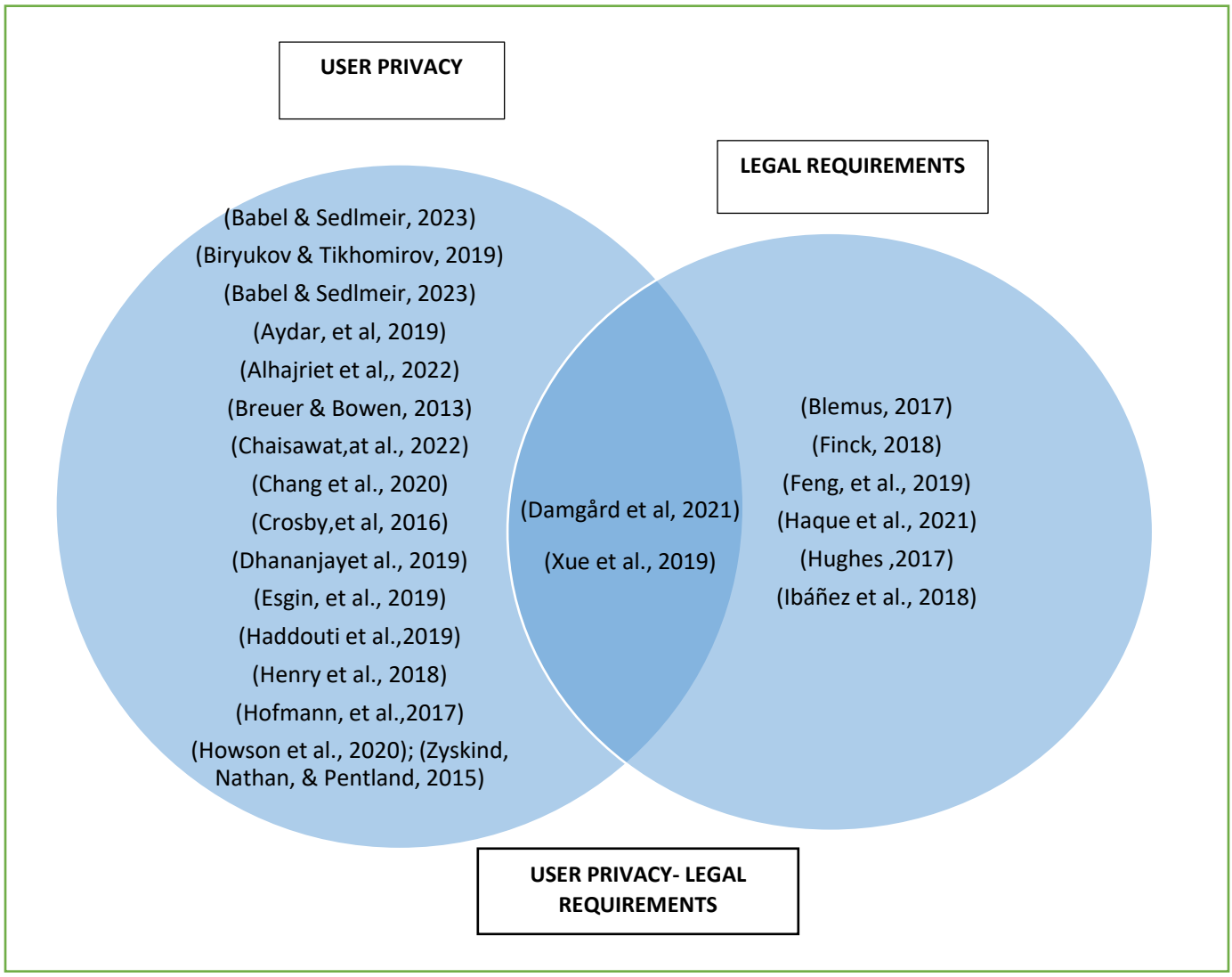
Data Extraction and Synthesis

Each article was reviewed, both the abstract and the complete text, extracting the information related to the possibilities it offers for challenges of maintaining privacy on blockchain, how blockchain systems comply with legal standards, the regulatory concerns related to BCT, the feasibility of integrating privacy-preserving technologies in blockchains, the real-world applications and case studies of BCT, and recommendations for balancing user privacy and legal requirements on blockchains.

While analyzing the extracted information, the focus was on user privacy and legal requirement issues. On the one hand, it was necessary to examine issues such as compliance of blockchain systems with legal standards and the examination of the regulator concerns related to BCT. Furthermore, the feasibility of integrating privacy-preserving technologies in blockchain and real-world applications and case studies of BCT had to be examined.

The whole process of data extraction was designed to answer the initial questions that were proposed (Q1–Q6) at the beginning of the investigation. As shown in Figure 2's Venn diagram, few studies were identified as highlighting a relationship between user privacy and legal requirements or accountability (Damgård et al., 2021; Xue et al., 2019). However, many studies focused solely on user privacy, not legal requirements, while some addressed sorely legal requirements. Not many studies selected for data extraction addressed user privacy and legal requirements and found an intrinsic relationship between the two terms.

Figure 2
Relationship between the Terms Analyzed in Different Studies



Results and Findings

Once the literature selected for the extraction of information had been reviewed, the six questions were answered at the beginning of this article.

Analysis of Results on Issues Raised

Q1: What are the Challenges of Maintaining Privacy on Blockchain Systems?

Many challenges to maintaining privacy on blockchain systems were identified in the literature. A significant concern identified is the tension between the inherent transparency of BCT and the need for user privacy. Studies highlighted the risks of identity theft and data exposure due to the public nature of blockchain ledgers. Finding a balance between keeping user data private and meeting legal requirements is complex (Damgård et al., 2021). Legal rules might require businesses to share user data, which can put user privacy at risk (Damgård et al., 2021; Xue et al., 2019).

However, methods that protect user privacy can make it hard for authorities to monitor and regulate BCT (Damgård et al., 2021). These challenges can have serious consequences. For businesses, not following the rules can lead to fines, legal problems, and damage to their reputation (Damgård et al., 2021; Martens et al., 2017). For users, it can mean risks to their privacy and personal data (Zyskind et al., 2015). Understanding these challenges is just the beginning. To address them, businesses must be proactive and use strategies that protect user privacy and meet legal requirements.

Q2: How can Blockchain Systems Comply with Legal Standards?

For businesses using BCT, understanding and following the law is crucial. There are strict rules about protecting user data and other legal requirements (Ibáñez et al., 2018). The decentralized nature of BCT can make it hard to apply these rules, significantly since data on the blockchain cannot be changed (Hofmann et al., 2017; Nakamoto, 2008; Politou et al., 2021). As BCT is used more in areas like finance, it is also essential to follow financial regulations. However, the privacy features of BCT can make it difficult to monitor and enforce these rules, leading to the challenges of balancing user privacy while meeting legal compliance and regulatory requirements.

Q3: What are the Regulatory Concerns Related to BCT?

The decentralized nature of BCT poses unique regulatory challenges. The literature pointed to the difficulty in applying traditional legal frameworks to decentralized systems, emphasizing the need for new regulatory approaches. The consensus was that regulatory bodies must evolve to accommodate BCT's distinct characteristics, balancing innovation with user protection.

For businesses using BCT, understanding and following the law is crucial. There are strict rules about protecting user data and other legal requirements (Ibáñez et al., 2018). The decentralized nature of BCT may make it challenging to apply these rules, significantly since data on the blockchain cannot be changed (Hofmann et al., 2017; Nakamoto, 2008; Politou et al., 2021). As BCT is used more in areas like finance, it is also essential to follow financial regulations. However, the privacy features of BCT may make it challenging to monitor and enforce these rules, leading to the challenges of balancing the use of privacy while meeting legal compliance and regulatory requirements.

Q4: What is the Feasibility of Integrating Privacy-Preserving Technologies in Blockchains?

Advanced cryptographic techniques emerged as a prominent theme, focusing on their role in addressing privacy and security concerns. Innovations in homomorphic encryption and privacy-preserving smart contracts were identified as key developments, offering new ways to protect data within the blockchain environment.

Advanced Cryptographic Techniques

BCT's security comes from advanced methods that protect data. These methods are crucial for keeping data safe and ensuring transparent and trustworthy transactions. Some of the main methods include:

- **Ring Signature Technology:** Introduced by Rivest, Shamir, and Tauman in 2001, ring signatures offer enhanced anonymity in digital transactions. Unlike traditional digital signatures, which identify the signer, ring signatures allow a group member to sign on behalf of the entire group (X. Li et al., 2020). This technology ensures the signature's validity without revealing the individual signer's identity.
- **Homomorphic Encryption:** This technique allows for computations on encrypted data without prior decryption (Breuer & Bowen, 2013). It ensures data remains confidential even during processing, making it ideal for operations on untrusted servers or third-party platforms.
- **Zero-Knowledge Proofs (ZKPs):** ZKPs enable one party to provide proof of a statement's validity to another without fully revealing the specifics of that statement (Sun et al., 2021). This arrangement ensures data privacy while confirming its authenticity.

- **Privacy-Preserving Smart Contracts:** These blockchain-based contracts protect sensitive data during execution. They employ cryptographic techniques to ensure data confidentiality while maintaining the integrity of the contract's operations (Kosba et al., 2016a).

Q5: What are the Real-World Applications and Case Studies of BCT?

Real-world examples of how companies continue to use the strategies described earlier in the previous section can be given by considering case studies involving four companies. These comprise IBM (n.d), Ripple (n.d), Bitpay (n.d), and Coinbase (n.d).

IBM

IBM (n.d) has developed a blockchain-based solution for supply chain management called IBM Food Trust (Nguyen & Do, 2018), designed to increase transparency and traceability in the food supply chain (Howson, 2020; Kawaguchi, 2019). To balance user privacy and legal demands, IBM (n.d), working with Walmart (Sristy, 2021), has implemented privacy-preserving technologies such as ZKPs and smart contracts to ensure that user data are protected while allowing for legal compliance (W. Li et al., 2020).

Ripple

Ripple (n.d) is a blockchain-based cross-border payment and remittance platform (Jani, 2018). To balance user privacy and legal demands, Ripple has complied with and implemented a comprehensive program that includes anti-money laundering (AML) and know-your-customer (KYC) measures and partnerships with regulators and law enforcement agencies to ensure that legal demands are appropriately addressed (Rosner & Kang, 2015; Sater, 2020).

BitPay

Bitpay (n.d) is a blockchain-based platform that allows merchants to accept cryptocurrency payments (Biryukov & Tikhomirov, 2019). It allows one to buy, store, swap, and spend cryptocurrency all in one app (Bitpay, n.d). To balance user privacy and legal demands, BitPay has implemented a comprehensive privacy policy (Biryukov & Tikhomirov, 2019) that outlines how user data is collected, used, and protected, as well as partnerships with regulators and law enforcement agencies to ensure legal compliance.

Coinbase

Coinbase (n.d) is a centralized cryptocurrency exchange platform allowing users to buy, sell, and trade cryptocurrencies. To balance user privacy and legal demands, Coinbase has complied and implemented a comprehensive compliance program that includes AML and KYC measures and partnerships with regulators and law enforcement agencies to ensure compliance (Hughes, 2017).

Q6: What are the Recommendations for Balancing User Privacy and Legal Requirements on Blockchain?

While the blockchain's inherent complexities present many challenges, its transformative potential cannot be overlooked. As analyzed in these articles, the equilibrium between user privacy and legal compliance is delicate and paramount. Nevertheless, recognizing these challenges is only the beginning. Actionable steps must be taken to harness BCT's transformative power while safeguarding user interests and meeting legal mandates. Thus, based on the authors' comprehensive analysis, the following are the recommendations to guide businesses and policymakers in this evolving landscape.

Develop Clear Privacy Policies

Businesses should develop clear and comprehensive privacy policies that outline how they collect, use, and protect user data on the blockchain. These policies should be transparent and easy to comprehend and should clearly explain how the organization balances the need for user privacy with legal compliance.

Implement Privacy-Preserving Technologies

Businesses can implement privacy-preserving technologies such as ZKPs and homomorphic encryption for user protection while allowing for legal compliance. These technologies can help to ensure the protection of sensitive user data while still allowing organizations to comply with legal demands.

Follow Relevant Regulatory Frameworks

To comply with relevant legal requirements, businesses should follow regulatory frameworks such as the European Union's GDPR or the United States Bank Secrecy Act (BSA). This recommendation can help to ensure that user data is protected and that legal demands are appropriately addressed.

Work with Regulators and Law Enforcement

Businesses and policymakers should work closely with regulators and law enforcement agencies to develop strategies and approaches that balance user privacy and legal compliance on the blockchain. This recommendation can help ensure that legal demands are appropriately addressed while protecting user privacy.

Educate Users

Businesses should educate users about the importance of user privacy on the blockchain and how to protect their data. This recommendation can include providing users with clear information about their privacy rights, how to exercise them, and providing guidance on protecting their data using privacy-preserving technologies.

Emerging Trends

The review identified several emerging trends. One notable trend is the increasing use of BCT for identity management, addressing privacy and regulatory compliance. Another is the development of blockchain governance models that aim to bridge the gap between decentralization and regulatory needs.

Discussion

Interpretation of Findings

The results underscore the intrinsic conflict between the transparency of blockchain technology (BCT) and the necessity of user privacy. As revealed by the findings, this tension raises significant concerns such as identity theft and data exposure, particularly given the public nature of blockchain ledgers. The challenge lies in harmonizing the dual objectives of preserving user privacy and fulfilling legal obligations. Businesses risk legal repercussions and reputational damage for non-compliance, while users confront potential privacy infringements.

The research points to the complexity of this balance, highlighting the need for proactive strategies that adequately address both privacy concerns and legal requirements. The gaps identified in the literature, particularly in regulatory adaptation and the implementation of privacy-enhancing technologies, highlight areas for future research and development. These insights are crucial for practitioners and policymakers as they navigate the rapidly evolving landscape of BCT.

Implications

For businesses, these findings suggest a pressing need to develop blockchain systems that are not only technologically advanced but also legally compliant and user-centric in terms of privacy. The practical implications are vast, from adopting advanced cryptographic techniques like homomorphic encryption and zero-knowledge proofs to implementing privacy-preserving smart contracts. These technologies could be pivotal in safeguarding user data while adhering to legal mandates.

Theoretically, these findings contribute to the ongoing discourse on privacy and legal compliance in the blockchain. They suggest reevaluating traditional legal frameworks to accommodate BCT's decentralized and immutable nature better. This balance could lead to the development of new regulatory approaches that balance innovation with user protection.

Limitations of Study

This research is not without limitations. The evolving nature of blockchain technology and its regulatory environment means that the findings may have a limited shelf-life, necessitating continuous reevaluation. Additionally, the study primarily focused on the technical aspects of privacy and compliance, potentially overlooking broader socio-economic factors that also play a critical role in adopting and regulating BCT. Finally, the findings are derived from existing literature, which may not fully capture the rapidly evolving nature of blockchain applications in diverse contexts.

While the study sheds light on the crucial balance between user privacy and legal requirements in the blockchain space, it also underscores the need for ongoing research and adaptation to evolving technological and regulatory landscapes. Businesses and regulators must work in tandem to foster an

environment where innovation thrives without compromising user privacy or legal compliance.

Conclusion

The exploration into balancing user privacy with legal demands in BCT surfaces a complex and multifaceted landscape. The key findings illuminate the inherent tension between the need for transparency in blockchain systems and the imperative of user privacy. Significant risks like identity theft and data exposure arise from the public nature of blockchain ledgers. Simultaneously, legal compliance poses challenges, often at odds with privacy concerns. Businesses are caught in a delicate balancing act, where non-compliance can result in legal ramifications and reputational damage, while overly stringent privacy measures could hinder legal oversight and regulation. Incorporating advanced cryptographic techniques and privacy-preserving smart contracts has emerged as a pivotal theme, offering potential solutions to these challenges.

Future Research

Looking ahead, one of the avenues for future research to emerge is to investigate how legal frameworks can evolve to better accommodate the unique characteristics of blockchain technology, especially in areas like data immutability and decentralized governance.

References

Aydar, M., Ayvaz, S., & Cetin, S. C. (2019). Towards a blockchain-based digital identity verification, record attestation, and record sharing system. *Computer Science.* https://arxiv.org/abs/1906.09791

Biryukov, A., & Tikhomirov, S. (2019). Security and privacy of mobile wallet users in Bitcoin, Dash, Monero, and Zcash. *Pervasive and Mobile Computing*, *59*, 101030. https://doi.org/https://doi.org/10.1016/j.pmcj.2019.101030

Bitpay (n.d). *The simplest, easiest, best, smartest, safest, most secure, most trusted crypto app*. Bitpay. Retrieved August 26, 2023 from https://bitpay.com/

Böhme, R., Christin, N., Edelman, B., & Moore, T. (2015). Bitcoin: Economics, technology, and governance. *Journal of Economic Perspectives*, *29*(2), 213-238. http://dx.doi.org/10.1257/jep.29.2.213

Breuer, P.T., Bowen, J.P. (2013). A Fully Homomorphic Crypto-Processor Design. In: Jürjens, J., Livshits, B., Scandariato, R. (eds) Engineering Secure Software and Systems. ESSoS 2013. Lecture Notes in Computer Science, vol 7781. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-36563-8_9

Chang, V., Baudier, P., Zhang, H., Xu, Q., Zhang, J., & Arami, M. (2020). How Blockchain can impact financial services – The overview, challenges and recommendations from expert interviewees. *Technological Forecasting and Social Change*, *158*, 120166. https://doi.org/https://doi.org/10.1016/j.techfore.2020.120166

Coinbase. (n.d). *Buy, sell, and store hundreds of cryptocurrencies*. Coinbase. Retrieved August 26, 2023 from https://www.coinbase.com/

Cole, R., Stevenson, M., & Aitken, J. (2019). Blockchain technology: Implications for operations and supply chain management. *Supply Chain Management: An International Journal*, *24*(4), 469-483. https://doi.org/10.1108/SCM-09-2018-0309

Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain technology: Beyond bitcoin. *Applied Innovation*, *2*(71), 6-19. https://scet.berkeley.edu/wp-content/uploads/AIR-2016-Blockchain.pdf

Damgård, I., Ganesh, C., Khoshakhlagh, H., Orlandi, C., & Siniscalchi, L. (2021). Balancing Privacy and Accountability in Blockchain Identity Management. I K. G. Paterson (red.), Topics in Cryptology-CT-RSA 2021 - Cryptographers' Track at the RSA Conference, Proceedings (s. 552-576). Springer. https://doi.org/10.1007/978-3-030-75539-3_23

Feng, Q., He, D., Zeadally, S., Khan, M. K., & Kumar, N. (2019). A survey on privacy protection in blockchain system. *Journal of Network and Computer Applications*, *126*, 45-58. https://doi.org/https://doi.org/10.1016/j.jnca.2018.10.020

Finck, M. (2018). Blockchains and data protection in the European Union. *European Data*

Protection Law Review, *4*, 17-35. https://doi.org/10.21552/edpl/2018/1/6

Gurtu, A., & Johny, J. (2019). Potential of blockchain technology in supply chain management: a literature review. *International Journal of Physical Distribution & Logistics Management*, *49*(9), 881-900. https://doi.org/10.1108/IJPDLM-11-2018-0371

Henry, R., Herzberg, A., & Kate, A. (2018). Blockchain access privacy: Challenges and directions. *IEEE Security & Privacy*, *16*(4), 38-45. https://doi.org/10.1109/MSP.2018.3111245

Hofmann, F., Wurster, S., Ron, E., & Bohmecke-Schwafert, M. (2017). The immutability concept of blockchains and benefits of early standardization. 2017 ITU Kaleidoscope: Challenges for a Data-Driven Society (ITU K), 1-8. https://doi.org/10.23919/ITU-WT.2017.8247004

Howson, P. (2020). Building trust and equity in marine conservation and fisheries supply chain management with blockchain. *Marine Policy*, *115*, 103873. https://shorturl.at/jzC18

Hughes, S. D. (2017). Cryptocurrency regulations and enforcement in the US. *W. St. UL Rev.*, *45*, 1. https://shorturl.at/lyFLO

Ibanez, L-D., O'Hara, K., & Simperl, E. (2018). *On Blockchains and the General Data Protection Regulation*. EU Blockchain Forum and Observatory. https://shorturl.at/myGN6

IBM. (n.d). *IBM supply chain intelligence suite: Food Trust*. IBM. Retrieved August 23. 2023 from https://www.ibm.com/products/supply-chain-intelligence-suite/food-trust

Jani, S. An Overview of Ripple Technology its Comparison with Bitcoin Technology. Master's Thesis, Parul University, Gujarat,India https://shorturl.at/agtZ3

Kawaguchi, N. (2019). Application of Blockchain to Supply Chain: Flexible Blockchain Technology. *Procedia Computer Science*, *164*, 143-148. https://doi.org/ghq47t

Khan, S., Jadhav, A., Bharadwaj, I., Rooj, M., & Shiravale, S. (2020, 11-13 March 2020). Blockchain and the identity-based encryption scheme for high data security. 2020 Fourth International Conference on Computing Methodologies and Communication (ICCMC), Erode, India, 2020, pp. 1005-1008, https://ieeexplore.ieee.org/document/9076552

Khan, S. N., Loukil, F., Ghedira-Guegan, C., Benkhelifa, E., & Bani-Hani, A. (2021). Blockchain smart contracts: Applications, challenges, and future trends. *Peer-to-Peer Networking and Applications*, *14*(5), 2901-2925. https://doi.org/10.1007/s12083-021-01127-0

Kitchenham, B. (2004). Procedures for performing systematic reviews. *Keele, UK, Keele University*, *33*(2004), 1-26. https://legacyfileshare.elsevier.com/promis_misc/525444systematicreviewsguide.pdf

Kitchenham, B., & Charters, S. (2007). Guidelines for performing systematic literature reviews in software engineering. EBSE Technical Report EBSE-2007-01. https://www.researchgate.net/publication/258968007_Kitchenham_B_Guidelines_for_performing_Systematic_Literature_Reviews_in_software_engineering_EBSE_Technical_Report_EBSE-2007-01

Kosba, A., Miller, A., Shi, E., Wen, Z., & Papamanthou, C. (2016a). Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. 839-858. Paper presented at 2016 IEEE Symposium on Security and Privacy (SP). https://doi.org/10.1109/SP.2016.55

Kosba, A., Miller, A., Shi, E., Wen, Z., & Papamanthou, C. (2016b). Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security.

Kuner, C., Cate, F. H., Lynskey, O., Millard, C., Loideain, N. N., & Svantesson, D. J. B. (2018). Blockchain versus data protection. International Data Privacy Law, 8(2), 103-104. https://doi.org/10.1093/idpl/ipy009

Li, W., Guo, H., Nejad, M., & Shen, C. C. (2020). Privacy-Preserving Traffic Management: A Blockchain and Zero-Knowledge Proof Inspired Approach. *IEEE Access*, *8*, 181733-181743. https://doi.org/ghf6md

Li, X., Mei, Y., Gong, J., Xiang, F., & Sun, Z. (2020). A blockchain privacy protection scheme based on ring signature. *IEEE Access*, *8*, 76765-76772. https://doi.org/gjbnr8

Li, Y., Susilo, W., Yang, G., Yu, Y., Du, X., Liu, D., & Guizani, N. (2019). Toward privacy and regulation in blockchain-based cryptocurrencies. *IEEE Network*, *33*(5), 111-117. https://doi.org/10.1109/MNET.2019.1800271

Martens, D., Tuyll Van Serooskerken, A. V., & Steenhagen, M. (2017). Exploring the potential of blockchain for KYC. *Journal of Digital Banking*, *2*(2), 123-131.

Mercer, R. (2016). Privacy on the blockchain: Unique ring signatures. *arXiv preprint arXiv:1612.01188*.

Moosavi, J., Naeni, L. M., Fathollahi-Fard, A. M., & Fiore, U. (2021). Blockchain in supply chain management: a review, bibliometric, and network analysis. *Environmental Science and Pollution Research*. https://doi.org/gnw6ff

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *Decentralized business review*, 21260.

Nguyen, H., & Do, L. (2018). The Adoption of blockchain in food retail supply chain: case: IBM Food Trust blockchain and the food retail supply chain in Malta.

Politou, E., Casino, F., Alepis, E., & Patsakis, C. (2021). Blockchain mutability: challenges and proposed solutions. *IEEE Transactions on Emerging Topics in Computing*, *9*(4), 1972-1986.

Ripple (2023, August 26). *Business impact, powered by crypto*. Ripple. https://ripple.com/

Rosner, M. T., & Kang, A. (2015). Understanding and regulating twenty-first-century payment systems: The ripple case study. *Mich. L. Rev.*, *114*, 649. https://repository.law.umich.edu/cgi/viewcontent.cgi?params=/context/mlr/article/1239/&path_info=

Sater, S. (2020). Do we need KYC/AML: The bank secrecy act and virtual currency exchanges. *Ark. L. Rev.*, *73*, 397. https://scholarworks.uark.edu/cgi/viewcontent.cgi?article=1095&context=alr

Smith, J. (2020). Blockchain technology and its potential impact on business. *Journal of Business and Technology*, *3*(1), 56-71.

Sristy, A. (2021). *Blockchain in the food supply chain - What does the future look like?* Walmart. Retrieved August 26, 2023 from https://tech.walmart.com/content/walmart-global-tech/en_us/news/articles/blockchain-in-the-food-supply-chain.html

Sudhakaran, S., Kumar, S., Ranjan, P., & Tripathy, M. R. (2020, 2020//). Blockchain-based transparent and secure decentralized algorithm. International Conference on Intelligent Computing and Smart Communication 2019, Singapore. https://doi.org/10.1007/978-981-15-0633-8_32

Sun, X., Yu, F. R., Zhang, P., Sun, Z., Xie, W., & Peng, X. (2021). A Survey on Zero-Knowledge Proof in Blockchain. *IEEE Network*, *35*(4), 198-205. https://doi.org/10.1109/MNET.011.2000473

Swan, M. (2015). *Blockchain: Blueprint for a new economy*. O'Reilly Media, Inc.

Tapscott, A., & Tapscott, D. (2017). How blockchain is changing finance. *Harvard Business Review*, *1*(9), 2-5. https://hbr.org/2017/03/how-blockchain-is-changing-finance

Tapscott, D., & Tapscott, A. (2016). *Blockchain revolution: how the technology behind Bitcoin is changing money, business, and the world*. Penguin.

Treleaven, P., Brown, R. G., & Yang, D. (2017). Blockchain technology in finance. *Computer*, *50*(9), 14-17. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8048631

W. -T. Tsai, L. Feng, H. Zhang, Y. You, L. Wang and Y. Zhong, "Intellectual-Property Blockchain-Based Protection Model for Microfilms," *2017 IEEE Symposium on Service-Oriented System Engineering (SOSE)*, San Francisco, CA, USA, 2017, pp. 174-178. https://doi.org/10.1109/SOSE.2017.35

Wang, J., Wang, S., Guo, J., Du, Y., Cheng, S., & Li, X. (2019). A summary of research on blockchain in the field of intellectual property. *Procedia Computer Science*, *147*, 191-197. https://doi.org/10.1016/j.procs.2019.01.220

Wolfond, G. (2017). A blockchain ecosystem for digital identity: improving service delivery in Canada's public and private sectors. *Technology Innovation Management Review*, *7*(10). https://timreview.ca/sites/default/files/article_PDF/Wolfond_TIMReview_October2017.pdf

Xue, L., Liu, D., Ni, J., Lin, X., & Shen, X. S. (2019). Balancing privacy and accountability

for industrial mortgage management. *IEEE Transactions on Industrial Informatics*, *16*(6), 4260-4269. https://ieeexplore.ieee.org/document/8894387

Zyskind, G., Nathan, O., & Pentland, A. (2015, 21-22 May 2015). Decentralizing privacy: Using blockchain to protect personal data. *2015 IEEE Security and Privacy Workshops*, 180-184. https://doi.org/10.1109/SPW.2015.27