HAKEMLİ Denetişim
Ortak Aklın Harmanı
Kamu İç Denetçileri Derneği Meşrutiyet Caddesi Konur Sokak No: 36/6 Kızılay - ANKARA
www.kidder.org.tr/denetisim/ • denetisim@kidder.org.tr
ISSN 1308-8335
Yıl: 17, Sayı: 35, 278-295, 2026
Gönderilme Tarihi: 19 Nisan 2026 Kabul Tarihi: 4 Temmuz 2026

**Review Article**

# ETHICAL CHALLENGES OF THE RIGHT TO BE FORGOTTEN IN BLOCKCHAIN SYSTEMS: A SYSTEMATIC REVIEW

*(BLOKZİNCİR SİSTEMLERİNDE UNUTULMA HAKKININ ETİK ZORLUKLARI: SİST*

**Abdulkadir TAŞDELEN**[1]

## ABSTRACT

**The General Data Protection Regulation (GDPR) defines the Right to Be Forgotten (RTBF) as the right of individuals to request the deletion of their personal data under certain conditions. While this right reflects key ethical principles such as autonomy and control over personal information, its implementation poses significant challenges in blockchain systems, where immutability is a core design feature. This tension creates ethical, technical, and governance-related concerns. This study systematically reviews the academic literature on the relationship between RTBF and blockchain technologies, with a particular focus on ethical issues. Following the PRISMA 2020 guidelines for Systematic Reviews and Meta-Analyses, a comprehensive literature search conducted on January 3, 2026 resulted in the inclusion of 46 peer-reviewed studies. The selected studies were analyzed based on four research questions addressing: (1) the conceptualization of RTBF, (2) ethical conflicts arising from blockchain immutability, (3) proposed technical and governance-oriented solutions, and (4) existing limitations and research gaps. The findings indicate that RTBF is predominantly interpreted as a legal obligation rather than an ethical principle. The most frequently identified ethical challenge concerns the conflict between immutable ledgers and data deletion requirements. Proposed mitigation strategies include privacy-by-design approaches, off-chain data storage, hash-based referencing, and redactable blockchain mechanisms. However, significant challenges remain, including legal uncertainty, scalability and interoperability limitations, and unclear governance responsibilities. Overall, this review provides a structured synthesis of existing research, contributing to a deeper ethical understanding of RTBF in blockchain systems and offering insights for future research, system design, and regulatory policymaking.**

**Keywords:** Blockchain Technologies; Right to Be Forgotten (RTBF); General Data Protection Regulation (GDPR); Ethical Challenges; Data Erasure
**JEL Codes:** K24, K38, O33

## *ÖZ*

***Genel Veri Koruma Tüzüğü (GVKT), Unutulma Hakkı'nı (UH), bireylerin belirli koşullar altında kişisel verilerinin silinmesini talep etme hakkı olarak tanımlar. Bu hak, bireysel özerklik ve kişisel bilgi üzerinde kontrol gibi temel etik ilkeleri yansıtsa da uygulanması blokzincir sistemlerinde önemli zorluklar doğurmaktadır; çünkü değiştirilemezlik bu sistemlerin temel bir tasarım özelliğidir. Bu durum, etik, teknik ve yönetişimle ilgili gerilimler yaratmaktadır. Bu çalışma, UH ile blokzincir teknolojileri arasındaki ilişkiyi inceleyen akademik literatürü, özellikle etik meseleler bağlamında sistematik olarak gözden geçirmektedir. PRISMA 2020 Sistematik İnceleme ve Meta-Analiz yönergeleri izlenerek, 3 Ocak 2026 tarihinde gerçekleştirilen kapsamlı literatür taraması sonucunda 46 hakemli çalışma analize dahil edilmiştir. Seçilen çalışmalar dört araştırma sorusu çerçevesinde incelenmiştir: (1) UH'nin kavramsallaştırılması, (2) blokzincir değiştirilemezliğinden kaynaklanan etik çatışmalar, (3) önerilen çözümler ve (4) mevcut sınırlılıklar ve araştırma boşlukları. Bulgular, UH'nin çoğunlukla etik bir ilke olmaktan ziyade hukuki bir yükümlülük olarak yorumlandığını göstermektedir. En sık vurgulanan etik sorun, değiştirilemez kayıt yapıları ile veri silme gereklilikleri arasındaki çatışmadır. Önerilen çözüm yaklaşımları arasında gizlilik-odaklı tasarım, zincir dışı veri depolama, hash tabanlı referanslama ve düzenlenebilir blokzincir mekanizmaları yer almaktadır. Ancak hukuki belirsizlikler, ölçeklenebilirlik ve birlikte çalışabilirlik sorunları ile yönetişim sorumluluklarının net olmaması gibi önemli zorluklar devam etmektedir. Genel olarak bu inceleme, blokzincir sistemlerinde UH'nin etik boyutuna dair mevcut araştırmaları yapılandırılmış bir şekilde sentezleyerek, gelecekteki araştırmalar, sistem tasarımı ve düzenleyici politika geliştirme süreçleri için önemli çıkarımlar sunmaktadır.***

***Anahtar kelimeler:*** *Blokzincir Teknolojileri; Unutulma Hakkı (UH); Genel Veri Koruma Tüzüğü (GVKT); Etik Zorluklar; Veri Silme*
***JEL Kodları:*** *K24, K38, O33*

[1] Asst. Prof. Dr., Department of Software Engineering, Faculty of Engineering and Natural Sciences, Ankara Yıldırım Beyazıt University, Ankara, Türkiye, ORCID: 0000-0003-4402-1463, abdulkadirtasdelen@aybu.edu.tr

## 1. INTR

Blockchain technologies have been increasingly promoted as a revolutionary framework for decentralized data management and trustless digital interactions. Blockchain systems aim to reduce reliance on centralized intermediaries and enhance data integrity across a wide range of application domains, including finance, healthcare, supply chain management, and public administration (Taşdelen, 2024). They do this by using features like distributed consensus, transparency, and immutability. These traits have made blockchain a key technology that will help new digital ecosystems grow.

The same features that make blockchain appealing from a technical standpoint also create serious ethical and regulatory problems, especially when it comes to how personal data is handled. Blockchain architectures are specifically designed to be hard to change or delete, unlike regular information systems. While immutability strengthens trust and auditability, it also complicates compliance with data protection principles that assume data can be altered or erased when necessary. This tension becomes especially pronounced in the context of personal data processing (Giordano, 2021; Zhuk, 2025).

One of the most debated issues that comes up because of this tension is the RTBF, which is written down in Article 17 of the GDPR. The RTBF gives people the right to ask for their personal data to be deleted in certain situations. This is in line with important moral principles like autonomy, dignity, and the right to control their own information. On the other hand, blockchain systems are built in such a way that data cannot be deleted, which creates a direct conflict between the ethics of data protection and the choices made in technology design (GDPR.Eu, n.d.). Consequently, the implementation of RTBF in blockchain-based systems remains conceptually and practically unresolved.

The moral consequences of this conflict go beyond just whether or not it can be done. The ongoing existence of on-chain data undermines conventional principles concerning data minimization, consent retraction, and accountability. When personal data is stored on an unchangeable ledger, people may lose important control over their information, even if there are legal reasons to delete it. Researchers have suggested a number of technical solutions to this problem, such as off-chain data storage, deleting cryptographic keys, chameleon hash functions, self-destruction mechanisms, and meta-transaction-based approaches (Politou et al., 2021). However, there is still debate about whether these solutions fully meet the ethical goals of the RTBF.

In addition to technical issues, implementing RTBF on blockchain raises complex questions about governance. In decentralized or semi-decentralized environments, traditional roles like data controller and data processor often become unclear or missing. This uncertainty makes it difficult to determine who is responsible for handling erasure requests (Angón, 2024). This lack of clarity leads to ethical challenges regarding accountability, oversight, and the ability to enforce data subject rights. Therefore, RTBF in blockchain systems should not be viewed only as a technical problem but also as a governance and ethical concern.

Recent academic literature has investigated the relationship between blockchain technologies and the RTBF from legal, technical, and ethical perspectives. Existing studies analyze conceptual tensions between immutability and fundamental rights, evaluate strategies for GDPR compliance, and propose design principles for privacy-aware or ethically aligned blockchain architectures (Politou et al., 2021; Xiao et al., 2023). However, the literature remains fragmented across disciplines and application contexts. A comprehensive analysis that systematically examines the conceptualization of the RTBF, the ethical conflicts identified, and the effectiveness of proposed solutions is currently lacking.

To address this gap, the present study conducts a systematic literature review (SLR) in accordance with following the Preferred Reporting Items for the PRISMA 2020 guidelines (Page et al., 2021), focusing explicitly on the ethical challenges of implementing the RTBF in blockchain systems. By synthesizing peer-reviewed research from Web of Science (WoS), IEEE Xplore, and Scopus, this review aims to examine: (i) how the RTBF is conceptualized in blockchain-related research, (ii) the ethical conflicts arising from blockchain immutability, (iii) the technical and governance-oriented solutions proposed in the literature, and (iv) the limitations and unresolved ethical challenges that persist. Through this structured analysis, the study seeks to contribute to a more ethically grounded understanding of RTBF in blockchain systems and to inform future research, system design, and regulatory debate.

## 2. METHODOLOGY

This study adopts a SLR methodology in accordance with the PRISMA 2020 guidelines (Page et al., 2021). The PRISMA framework was selected to ensure methodological rigor, transparency, and reproducibility, which are particularly important given the interdisciplinary and conceptually fragmented nature of research on the RTBF in blockchain systems.

### 2.1 Review

The review process followed the four standard PRISMA phases: identification, screening, eligibility, and inclusion. During the identification phase, potentially relevant studies were retrieved from selected academic databases. In the screening phase, duplicate records were removed and titles and abstracts were reviewed for relevance. The eligibility phase involved full-text assessment based on predefined inclusion and exclusion criteria. Finally, studies meeting all criteria were included in the qualitative synthesis.

A PRISMA flow diagram is used to transparently document each stage of the selection process and to illustrate how the final corpus of studies was derived.

### 2.2 Data Sources

To capture high-quality and peer-reviewed research across technical, legal, and ethical domains, the literature search was conducted using three major academic databases: WoS, IEEE Xplore, and Scopus. These databases were selected due to their extensive coverage of computer science, information systems, engineering, and interdisciplinary technology-related research, where blockchain and data protection issues are most frequently discussed.

### 2.3 Search Strategy

The search strategy was deliberately designed to ensure thematic precision (Table 1). In order to focus on studies where the RTBF constitutes a central research concern, RTBF-related terms were required to appear in the article title. Blockchain-related terms, by contrast, were searched across broader fields such as titles, abstracts, and keywords.

Core search terms included variations of “right to be forgotten,” “right of erasure,” “data erasure,” and “GDPR compliance,” combined with blockchain-related terminology such as “blockchain” and “distributed ledger.” Search strings were adapted to the specific syntax and field structures of each database to ensure consistency and comparability across search results.

Rather than imposing an arbitrary starting date, the search strategy encompassed the entire timeline of blockchain and privacy technology's two-decade evolution. Consequently, the final search across all databases was anchored to January 3, 2026, as the strict end date to avoid potential bias from retrospective database updates.

Table 1. Database Search Strategy and Number of Retrieved Studies

| **Database** | **Searching Pattern** | **# of Paper** |
|---|---|---|
| WoS | TI = ("right to be forgotten" OR "data erasure" OR "right of erasure" OR "GDPR compliance") AND TS = ("blockcha" OR "distributed ledger") | 17 |
| IEEE Xplore | ((("Document Title":"right to be forgotten" OR "Abstract":"right to be forgotten" OR "Author Keywords":"right to be forgotten" OR "Document Title":"data erasure" OR "Abstract":"data erasure" OR "Author Keywords":"data erasure") AND ("Abstract":blockchain OR "Document Title":blockchain OR "Author Keywords":blockchain OR "Abstract":"distributed ledger" OR "Document Title":"distributed ledger" OR "Author Keywords":"distributed ledger"))) | 30 |
| Scopus | TITLE ("right to be forgotten" OR "right of erasure" OR "data erasure" OR "GDPR compliance") AND TITLE-ABS-KEY ("blockchain" OR "distributed ledger") | 25 |

### 2.4 Inclusion and Exclusion Criteria

Clear inclusion and exclusion criteria were defined prior to the screening process to ensure consistency, relevance, and analytical focus.

Studies were included if they: (i) were peer-reviewed journal articles or conference papers, (ii) explicitly addressed the RTBF or data erasure in blockchain systems, (iii) engaged with ethical, legal, technical, or governance-related aspects of RTBF, (iv) were written in English, and (v) were available in full text.

Studies wer re, (ii) were purely technical in nature without ethical, legal, or governance discussion, (iii) consisted of editorials, opinion pieces, tutorials, posters, or book reviews, or (iv) were duplicate records retrieved from multiple databases.

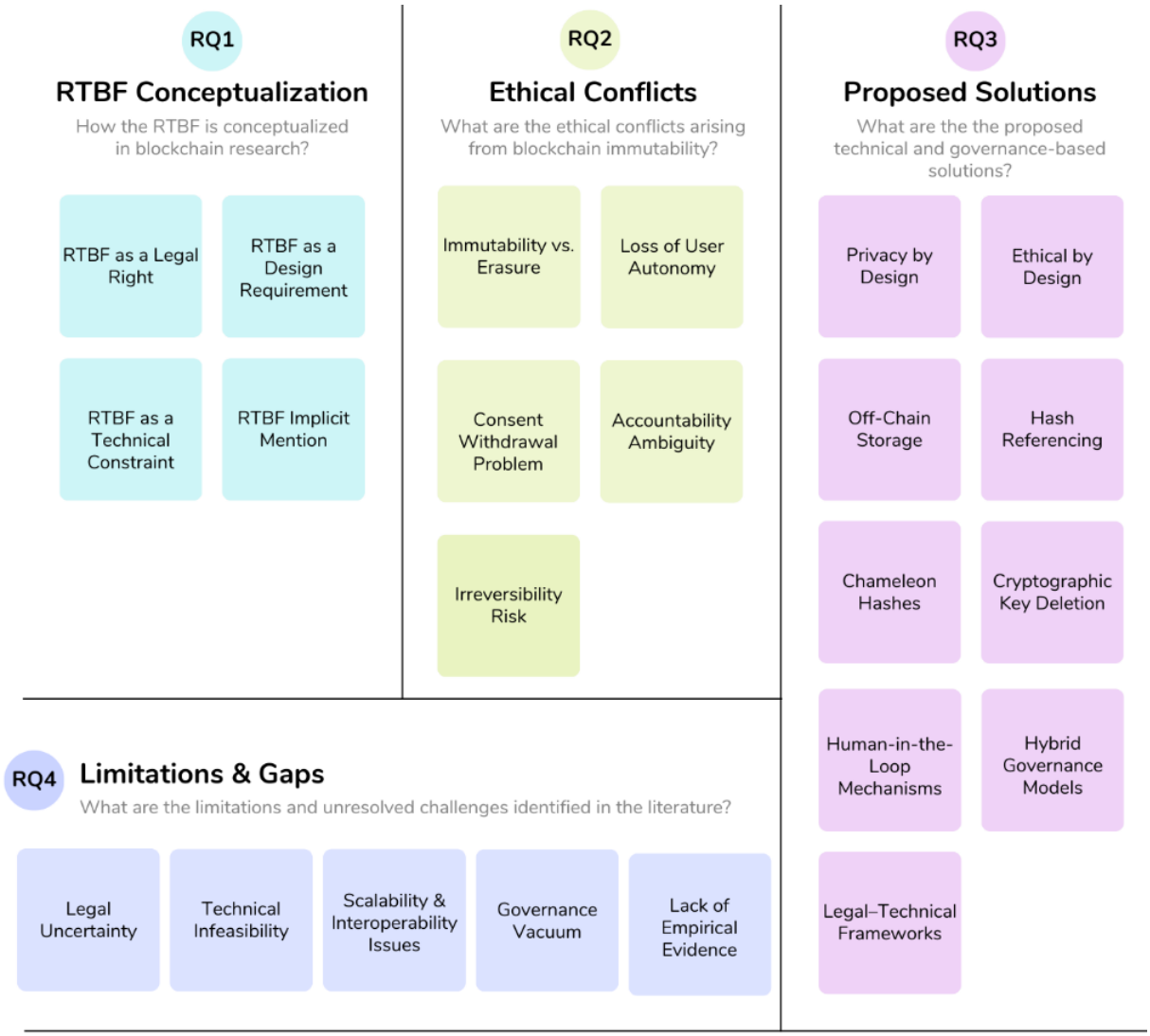
### 2.5 Study Selection Process

All retrieved records were exported to a reference management tool, where duplicate entries were identified and removed. The remaining studies underwent a two-stage selection process. First, titles and abstracts were screened to exclude studies that did not clearly address RTBF within a blockchain context. Second, full-text versions of potentially relevant studies were assessed in detail against the predefined inclusion and exclusion criteria. Only studies that satisfied all inclusion criteria were retained for the final analysis.

### 2.6 Data Extraction

A standardized data extraction form was developed to ensure systematic and consistent data collection across all included studies. For each study, the following information was extracted: authorship, conceptualization of the RTBF, identified ethical and regulatory challenges, proposed technical or governance-based solutions, and reported limitations or research gaps.

**Figure 1.** Analytical Coding and RQ Mapping (Coded by the Author.)



### 2.7 Analyti

Each included study was systematically coded in relation to the four research questions (RQ1–RQ4). A deductive coding scheme was developed prior to analysis, informed by recurring conceptual patterns in the RTBF–blockchain literature (Politou et al., 2021; Xiao et al., 2023).

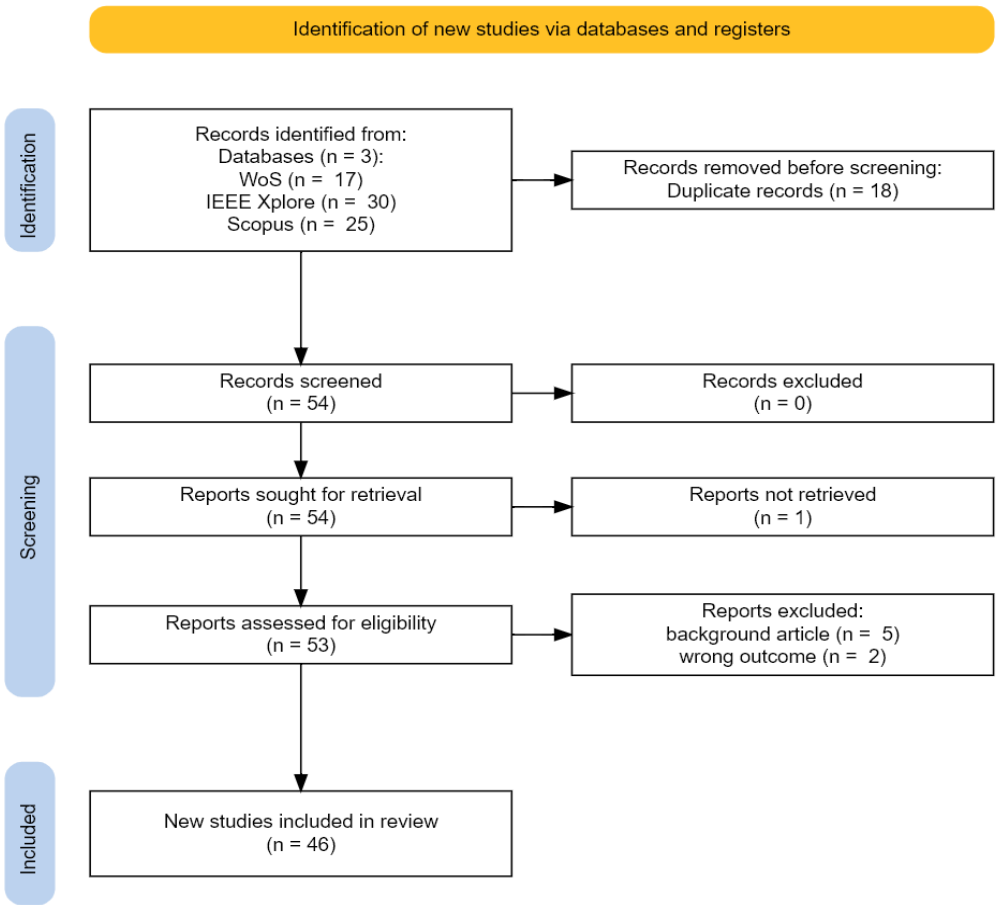
For RQ1, studies were classified according to how the RTBF was conceptualized, such as a legal right, a system design requirement, a technical constraint, or an implicit reference. For RQ2, ethical conflicts were identified and coded, including tensions between immutability and erasure, loss of user autonomy, consent withdrawal challenges, accountability ambiguity, and irreversibility risks. For RQ3, proposed solutions were categorized into technical, organizational, and governance-based approaches, including off-chain storage, cryptographic mechanisms, privacy-by-design principles, and hybrid governance models. For RQ4, limitations and research gaps were extracted, such as legal uncertainty, technical infeasibility, scalability and interoperability challenges, governance vacuums, and the lack of empirical validation. The resulting mapping between studies and research questions is summarized in Figure 1.

### 2.8 Data Synthesis and Analysis

Given the predominantly qualitative and conceptual nature of the reviewed literature, a thematic synthesis approach was employed. Extracted data were coded and grouped into recurring themes, including immutability versus data erasure, GDPR compliance and accountability, on-chain versus off-chain data ethics, cryptographic deletion, and governance responsibility in decentralized systems.

Where appropriate, descriptive statistics were used to summarize publication trends by year, application domain, and publication type. The analysis prioritizes the identification of ethical tensions, conceptual patterns, and unresolved challenges rather than quantitative aggregation.

**Figure 2.** PRISMA 2020 Flow Diagram of the Study Selection Process (Created by the Author.)



### 2.9 Reporti

This review adheres to the PRISMA 2020 reporting checklist. All relevant checklist items are addressed within the manuscript or supplementary materials, and a PRISMA flow diagram is included to visually represent the study selection process (Figure 2).

## 3. RESULTS

This section presents the findings of the SLR-based on the analysis of 46 peer-reviewed studies. The results are structured in accordance with the four research questions, focusing on (i) how the RTBF is conceptualized in blockchain research, (ii) the ethical conflicts arising from blockchain immutability, (iii) the proposed technical and governance-based solutions, and (iv) the limitations and unresolved challenges identified in the literature.

The distribution of included studies by year of publication is presented in Figure 3. The number of publications shows an overall increasing trend over time, with the lowest count in 2017 (n = 1) and a peak in 2025 (n = 9).

**Figure 3.** Distribution of Included Studies by Year of Publication

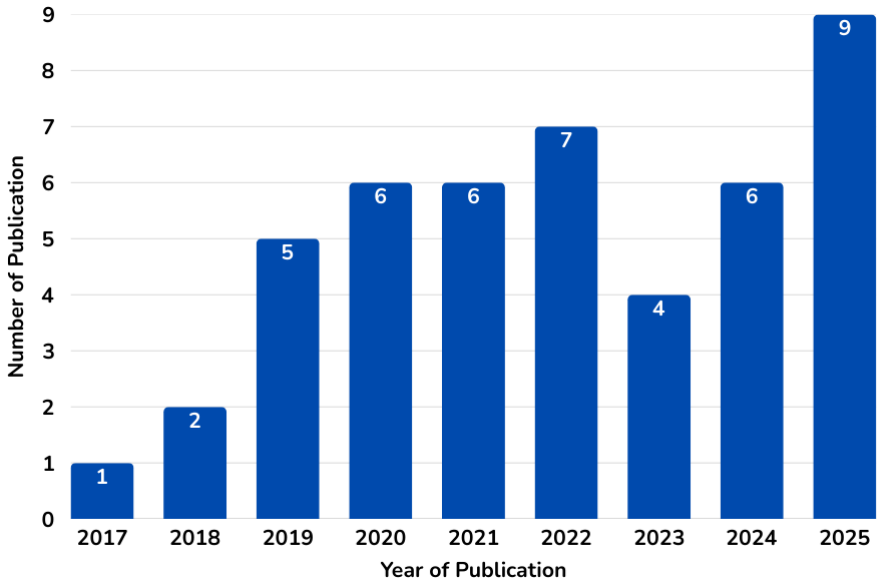



Table 2 summarizes the distribution of RTBF conceptualizations, ethical conflicts, proposed solutions, and identified research gaps across the included studies, highlighting the dominance of legal framings and privacy-by-design approaches.

Table 2. Distribution of RTBF Conceptualizations and Ethical Themes Across Included Studies

| Analytical Dimension | Category | Number of Studies | Description |
|---|---|---|---|
| RQ1: RTBF Conceptualization | RTBF as a Legal Right | 23 | RTBF framed explicitly as a GDPR Article 17 obligation and fundamental right |
| | RTBF as a Design Requirement | 8 | RTBF treated as an architectural or system-level requirement |
| | RTBF as a Technical Constraint | 4 | RTBF framed as a cryptographic or protocol-level limitation |
| | RTBF Implicit Mention | 11 | RTBF referenced indirectly within broader GDPR discussions |
| RQ 2: Et hi | Immutability vs. Erasure | 32 | Fundamental tension between append-only ledgers and deletion rights |

| | | | |
|---|---|---|---|
| | | | after on-chain registration |
| | Consent Withdrawal Problem | 6 | Inability to effectively revoke consent |
| | Accountability Ambiguity | 9 | Unclear responsibility for erasure enforcement |
| | Irreversibility Risk | 8 | Persistent data traces despite redaction mechanisms |
| **RQ3: Proposed Solutions** | Privacy by Design | 40 | GDPR principles embedded at architectural level |
| | Ethical by Design | 6 | Embedding ethical principles into systems from the design stage. |
| | Off-Chain Storage | 13 | Separation of personal data from immutable ledger |
| | Hash Referencing | 10 | Integrity verification without storing raw data |
| | Chameleon Hashes | 11 | Controlled modification of blockchain records |
| | Cryptographic Key Deletion | 5 | Effective erasure through key destruction |
| | Human-in-the-Loop Mechanisms | 8 | Human oversight in erasure and consent decisions |
| | Hybrid Governance Models | 11 | Combination of technical enforcement and institutional control |
| | Legal–Technical Frameworks | 9 | Joint legal and technical compliance models |
| **RQ4: Limitations & Gaps** | Legal Uncertainty | 5 | Ambiguity regarding GDPR compliance of technical solutions |
| | Technical Infeasibility | 2 | Challenges in permissionless or large-scale systems |
| | Scalability & Interoperability Issues | 5 | Performance and cross-system integration limitations |
| | Governance Vacuum | 2 | Absence of clear enforcement authorities |
| | Lack of Empirical Evidence | 2 | Predominance of conceptual or proof-of-concept studies |

(The complete study-level coding and mapping to RQ1–RQ4 are provided in Appendix-Table A.)

*RQ1: Conceptualization of the RTBF in Blockchain Research*

The reviewed studies demonstrate that the RTBF is most commonly conceptualized as a legal right derived directly from Article 17 of the GDPR. In these works, RTBF is discussed primarily in terms of regulatory compliance and legal obligations imposed on system designers, service providers, or data controllers. This legal framing dominates the literature and shapes how both problems and solutions are articulated.

A smaller but significant group of studies approaches the RTBF as a system design requirement. These studies don't just see erasure as a legal requirement; they also see RTBF as a functional property that should be taken into account when making architectural decisions, like separating personal data from immutable ledgers or adding controlled redaction mechanisms.

Only a limited number of studies conceptualize RTBF as a technical constraint. In these cases, the right to erasure is framed as a cryptographic or protocol-level challenge that directly confronts blockchain immutability. This perspective is most common in research on redactable or modifiable blockchains.

Finally, several studies refer to the RTBF only implicitly, typically within broader discussions of GDPR compliance, privacy preservation, or data governance. In these cases, RTBF is acknowledged but not explicitly theorized or problematized.

*RQ2: Ethical Conflicts Arising from Blockchain Immutability*

Across the blockchain immutability and data erasure requirements. A significant majority of studies underscore that append-only ledger structures fundamentally contradict ethical principles pertaining to data protection, especially data minimization and individual autonomy over personal information.

Loss of user autonomy emerges as another recurring ethical concern. Many studies argue that once personal data are anchored on-chain, data subjects lose effective control over how their information is used, modified, or withdrawn, even when legal grounds for erasure exist.

Closely related to this issue is the consent withdrawal problem. Several studies highlight that while GDPR formally grants individuals the right to revoke consent, blockchain systems often lack practical mechanisms to enforce such revocation in a meaningful way.

Accountability ambiguity is also prominently discussed, particularly in decentralized or permissionless blockchain environments. The absence of clearly defined data controllers or enforcement authorities raises ethical concerns regarding responsibility for responding to erasure requests.

Finally, a subset of studies identifies irreversibility risk as an ethical challenge, noting that even when redaction or deletion mechanisms are implemented, residual data traces or metadata may persist. This concern is especially pronounced in research on redactable and modifiable blockchains.

*RQ3: Proposed Technical and Governance-Based Solutions*

The literature proposes a wide range of solutions aimed at reconciling blockchain immutability with RTBF requirements. The most commonly suggested approach involves off-chain storage, whereby personal data are stored outside the blockchain and only references or hashes are recorded on-chain. This strategy seeks to preserve ledger integrity while enabling data erasure at the storage layer.

Hash referencing mechanisms are frequently used in conjunction with off-chain storage to support data integrity verification without exposing raw personal data. Several studies also propose chameleon hash functions, which enable controlled modification of blockchain records under predefined conditions.

Another recurring solution is cryptographic key deletion, where erasure is achieved by destroying encryption keys rather than deleting the underlying data. While often described as “effective erasure,” the ethical adequacy of this approach remains contested within the literature.

Several studies stress privacy-by-design principles and suggest governance-oriented solutions, like human-in-the-loop mechanisms and hybrid governance models, in addition to purely technical measures. These strategies seek to harmonize automated enforcement with institutional supervision and moral responsibility.

*RQ4: Limitations and Unresolved Gaps*

Despite the breadth of proposed solutions, the reviewed literature consistently reports several unresolved challenges. Legal uncertainty remains a prominent concern, particularly regarding whether technical erasure mechanisms fully satisfy GDPR requirements.

Technical infeasibility is frequently highlighted in large-scale or permissionless blockchain systems, where redaction mechanisms may undermine security, consensus stability, or performance. Scalability and interoperability issues further complicate the deployment of RTBF-compliant solutions across heterogeneous systems.

Several studies indicate a governance vacuum, highlighting the lack of clearly defined institutional actors tasked with enforcing erasure decisions. Finally, the literature shows that there isn't enough empirical evidence because many proposals are still just ideas or have only been tested in limited proof-of-concept implementations.

A further, and arguably more fundamental, gap concerns the Data Protection Impact Assessment (DPIA) mandated by Article 35 of the GDPR: none of the 46 included studies engages with DPIA as a central theme, despite its centrality as the design-stage mechanism for assessing the GDPR-compliance of high-risk processing operations such as those characteristics of blockchain systems. This absence is itself a substantive finding of this review, pointing to an unresolved governance gap in the RTBF–blockchain literature (see also Section 4.4).

## 4. DISCUSSIONS

This discussion interprets the findings of the systematic review through an ethical lens, focusing on how blockchain research conceptualizes the RTBF and how proposed solutions respond to the normative tension between technological

immutabilit this section synthesizes broader patterns, assumptions, and omissions that shape the current discourse.

### 4.1 Dominant Conceptual Framings of the RTBF

The review reveals a strong tendency to frame the RTBF primarily as a legal obligation derived from the GDPR. While this legal framing provides a clear reference point for compliance-oriented research, it also narrows the ethical scope of the discussion. By treating RTBF mainly as a regulatory constraint, many studies implicitly assume that ethical concerns are addressed once formal compliance is achieved.

Only a small number of works address RTBF as an ethical principle based on autonomy, dignity, and the right to control one's own information. Consequently, profound normative inquiries, such as whether suggested erasure mechanisms authentically reestablish user agency or merely replicate compliance, remain insufficiently examined. This imbalance indicates that blockchain research frequently emphasizes regulatory compliance over ethical consideration.

### 4.2 Ethical Tensions Between Law and Technology

The findings confirm that blockchain immutability constitutes the central ethical tension in RTBF-related research. Immutability is frequently portrayed as a foundational security feature and a source of trust. However, from an ethical perspective, this design choice systematically constrains individuals' ability to exercise control over their personal data.

This tension highlights that blockchain technologies are not value-neutral. Architectural commitments to immutability embed normative assumptions that privilege system integrity and auditability over individual autonomy. Consequently, ethical conflicts surrounding RTBF are not incidental side effects but structural outcomes of technological design decisions. The persistence of these conflicts across diverse application domains suggests that they cannot be fully resolved through incremental technical adjustments alone.

### 4.3 Technological Solutionism and Its Ethical Limits

A recurring pattern in the reviewed literature is a strong reliance on technical mechanisms to address RTBF-related challenges. Solutions such as off-chain storage, cryptographic key deletion, and redactable ledgers are frequently presented as sufficient responses to both legal and ethical requirements.

This focus on finding solutions, on the other hand, raises important ethical concerns. Destroying or redacting keys to make data unavailable doesn't always mean that the data subject has really erased it. In numerous instances, the authority over erasure processes is delegated from individuals to system designers, consortium members, or governance authorities. Consequently, technical compliance might be attained without fundamentally reinstating user autonomy or solving inherent power imbalances.

### 4.4 Governance, Responsibility and Accountability

The review also exposes persistent governance gaps in RTBF-compliant blockchain architectures. While decentralization is often promoted as a core advantage of blockchain systems, it frequently obscures responsibility for enforcing data subject rights. In the absence of clearly defined roles and decision-making structures, accountability becomes diffuse.

This governance vacuum has direct ethical implications. Without identifiable actors responsible for evaluating and executing erasure requests, data subjects may face significant barriers in exercising their rights. Legal uncertainty further exacerbates this problem, as system participants may be unwilling or unable to assume responsibility in ambiguous regulatory environments. These findings indicate that effective RTBF implementation requires not only technical mechanisms but also institutional and organizational frameworks capable of ethical oversight.

One concrete instrument for such institutional oversight is the DPIA mandated by Article 35 of the GDPR. DPIA constitutes the principal design-stage procedural mechanism through which a data controller must assess, prior to deployment, whether a processing operation that is likely to result in high risk to individuals' rights such as one involving novel technologies, large-scale processing, or systematic restrictions on data subject rights, all of which are characteristic of blockchain-based systems can be carried out in a manner compatible with GDPR obligations, including the right to erasure (Metin et al., 2019). DPIA is therefore not merely a compliance checkpoint but the procedural locus at which the ethical principles invoked throughout this review autonomy, accountability, and transparency are intended to be operationalized at the design stage, before architectural commitments to immutability become difficult to reverse.

As reported This is not merely a gap in the underlying literature but a substantive indication that compliance-oriented blockchain research has so far bypassed the very mechanism through which the tension between immutability and erasure obligations could be anticipated and addressed before deployment, underscoring the need to integrate DPIA explicitly into future blockchain RTBF research as both an analytical lens and a design requirement (Metin et al., 2019).

### 4.5 Toward Ethically Grounded RTBF Implementation

Taken together, the findings suggest that current approaches to RTBF in blockchain systems remain fragmented and incomplete. Technical solutions, while necessary, are insufficient on their own to resolve fundamentally normative conflicts between immutability and data protection principles.

An ethically grounded approach to RTBF implementation should integrate technical design, governance structures, and normative commitments. Ethical-by-design and human-centered governance models offer promising directions by explicitly embedding values such as autonomy, accountability, and transparency into system architectures and decision-making processes. Such approaches move beyond compliance-driven design toward a more substantive realization of data subject rights.

## 5. CONCLUSION

This study presented a PRISMA-based SLR examining the ethical challenges associated with implementing the RTBF in blockchain systems. By synthesizing findings from 46 peer-reviewed studies spanning technical, legal, and governance-oriented perspectives, the review aimed to clarify how RTBF is conceptualized, the ethical conflicts it generates, and the extent to which proposed solutions address these challenges.

The findings indicate that existing blockchain research predominantly frames the RTBF as a legal compliance requirement rather than as an ethical principle rooted in autonomy, dignity, and control over personal information. Ethical conflicts are largely centered on the structural incompatibility between blockchain immutability and data erasure obligations, with recurring concerns related to loss of user autonomy, consent withdrawal, accountability ambiguity, and irreversibility risks.

While the literature proposes a broad range of technical solutions, such as off-chain storage, cryptographic key deletion, and redactable ledger mechanisms, these approaches often prioritize formal compliance over substantive ethical fulfillment. As a result, many solutions mitigate regulatory risk without fully restoring meaningful user agency or resolving governance responsibility. Persistent limitations, including legal uncertainty, scalability and interoperability challenges, and governance vacuums, suggest that current approaches remain partial and context-dependent.

This review offers three primary contributions. First, it presents a structured ethical synthesis of RTBF-related blockchain research, revealing a systematic reliance on legal frameworks that often marginalize deeper normative considerations. By distinguishing between legal compliance and ethical realization, the analysis identifies a significant conceptual gap within the literature. Second, it critically evaluates the dominant solutionist orientation in blockchain research, demonstrating that technical solutions alone are insufficient to address fundamentally normative conflicts. Third, it proposes an integrative perspective that links technical design, governance structures, and ethical accountability, underscoring the necessity for ethical-by-design approaches that extend beyond cryptographic enforcement.

For system designers, these findings underscore the importance of embedding ethical considerations into blockchain architectures from the outset, rather than treating the RTBF as an external regulatory constraint. Designers should critically evaluate how erasure mechanisms affect user autonomy, transparency, and accountability. For policymakers and regulators, the review highlights the limitations of purely technical interpretations of data erasure and points to the need for clearer governance models that assign responsibility in decentralized environments.

Future research should address the broader systemic maturity gap identified across the reviewed corpus. Given that the structural mapping in RQ3 shows nearly 87% of the proposed mitigations (40/46) are confined to conceptual Privacy by Design frameworks, the low frequency of an explicit 'Lack of Empirical Evidence' code in RQ4 reflects a literature that is still too nascent to heavily critique its own implementation failures. Recognizing that the field remains predominantly theoretical, future studies should move beyond conceptual proposals and prioritize rigorous empirical investigations of RTBF implementation in operational blockchain systems.

## APPEND

Table A. Mapping of included studies to research questions (RQ1–RQ4)

| # | Title | RQ1 – RTBF Conceptualization | RQ2 – Ethical Conflicts | RQ3 – Proposed Solutions | RQ4 – Limitations & Gaps |
|---|---|---|---|---|---|
| 1 | A Blockchain-empowered Federated Learning Framework Supporting GDPR-compliance (Xiao et al., 2023) | Implicit Mention | – | Privacy by Design | Legal Uncertainty |
| 2 | A data sharing scheme for GDPR-compliance based on consortium blockchain (Piao et al., 2021) | Implicit Mention | – | Privacy by Design | – |
| 3 | A decentralized personal data store based on Ethereum: Towards GDPR compliance (Alessi et al., 2019) | Implicit Mention | – | Human in the Loop<br>Privacy by Design<br>Off Chain Storage | – |
| 4 | A Privacy-Preserving and Redactable Healthcare Blockchain System (Xu et al., 2024) | Legal Right | Immutability vs Erasure | Chameleon Hashes<br>Privacy by Design | Technical Infeasibility |
| 5 | An Analysis of the GDPR Compliance Issues Posed by New Emerging Technologies (Mone & Sivakumar, 2022) | Implicit Mention | – | Privacy by Design | – |
| 6 | An Intent-Based Networking Framework for Secure and Privacy-Compliant Machine Unlearning Using Meta-Learning and Redactable Blockchain (Shirmohammadi et al., 2025) | Legal Right | Consent Withdrawal Problem<br>Immutability vs Erasure | Ethical by Design<br>Privacy by Design | – |
| 7 | Automating GDPR Compliance using Policy Integrated Blockchain (Mahindrakar & Joshi, 2020) | Implicit Mention | – | Off Chain Storage<br>Privacy by Design | – |
| 8 | Balancing Data Protection and Decentralization: Harnessing Blockchain's Potential While Ensuring GDPR Compliance (Anido-Rifón et al., 2025) | Legal Right | Immutability vs Erasure | Legal Technical Framework<br>Off Chain Storage<br>Privacy by Design | – |
| 9 | Blockchain Graphs (BCGs) to Support Right-To-Be-Forgotten (RTBF) in Blockchains (Semwal & Alfaidi, 2022) | Legal Right | Accountability Ambiguity<br>Immutability vs Erasure | Chameleon Hashes<br>Ethical by Design | – |
| 10 | Blockchain-based consent manager for GDPR compliance (Vargas, 2019) | Design Requirement | Consent Withdrawal Problem<br>Loss of User Autonomy | Human in the Loop<br>Hybrid Governance Model<br>Privacy by Design | Governance Vacuum<br>Lack of Empirical Evidence |

| | | | | | |
|---|---|---|---|---|---|
| 11 | Bloc<br>Immutability and Traceability in the Era of GDPR<br>(Saif & Migliorini, 2025) | | Erasure<br>Loss of User Autonomy | Legal Technical Framework<br>Privacy by Design | |
| 12 | Blockchain-Enabled GDPR Compliance Enforcement for IIoT Data Access<br>(Liagkou et al., 2025) | Implicit Mention | – | Hash Referencing<br>Off Chain Storage<br>Privacy by Design | – |
| 13 | BlockHealth: Blockchain-based secure and peer-to-peer health information sharing<br>(Balistri et al., 2021) | Legal Right | Immutability vs Erasure | Hash Referencing<br>Off Chain Storage<br>Privacy by Design | – |
| 14 | Burnable Pseudo-Identity: A Non-Binding Anonymous Identity Method for Ethereum<br>(Gutierrez-Aguero et al., 2021) | Legal Right | Immutability vs Erasure<br>Loss of User Autonomy | Cryptographic Key Deletion<br>Privacy by Design | – |
| 15 | Checking GDPR Compliance for Cloud-based Services<br>(Barati & Rana, 2021) | Legal Right | Accountability Ambiguity<br>Consent Withdrawal Problem | Human in the Loop<br>Hybrid Governance Model<br>Privacy by Design | – |
| 16 | Decentralized GDPR Compliance: A Blockchain Framework for Personal Data Management<br>(Islam et al., 2024) | Legal Right | Immutability vs Erasure<br>Loss of User Autonomy | Human in the Loop<br>Hash Referencing<br>Off Chain Storage<br>Privacy by Design | Scalability<br>Interoperability Issues |
| 17 | Enabling Right to be Forgotten in a Collaborative Environment Using Permissioned Blockchains<br>(Parikh et al., 2025) | Legal Right | Accountability Ambiguity<br>Immutability vs Erasure | Hash Referencing<br>Hybrid Governance Model<br>Off Chain Storage<br>Privacy by Design | – |
| 18 | Enabling Secure and Scalable GDPR-Compliant Blockchain-Based e-KYC With Efficient Redaction<br>(Fugkeaw et al., 2025) | Legal Right | Immutability vs Erasure<br>Loss of User Autonomy | Chameleon Hashes<br>Cryptographic Key Deletion<br>Off Chain Storage<br>Privacy by Design | – |
| 19 | Escaping From Consensus: Instantly Redactable Blockchain Protocols in Permissionless Setting<br>(Li et al., 2023) | Legal Right | Immutability vs Erasure<br>Irreversibility Risk | Privacy by Design | – |
| 20 | Exploiting the blockchain to guarantee GDPR compliance while consents evolve under data owners' control<br>(Calani et al., 2024) | Legal Right | Consent Withdrawal Problem<br>Loss of User Autonomy | Human in the Loop<br>Off Chain Storage<br>Privacy by Design | – |
| 21 | Fine-Grained Data Rights Governance in Blockchain-Based Cloud-Edge Communications<br>(Gan et al., 2023) | Legal Right | Immutability vs Erasure | Chameleon Hashes;<br>Privacy by Design | – |
| 22 | GDPR Compliance Verification in Internet of Things<br>(Barati et al., 2020) | Legal Right | Immutability vs Erasure | Privacy by Design | Scalability<br>Interoperability Issues |
| 23 | GDPR compliance verification through a user- | Implicit Mention | – | Human in the Loop<br>Privacy by Design | – |

| | | | | | |
|---|---|---|---|---|---|
| | centr<br>in multi-cloud environment<br>(Ahmad & Aujla, 2023) | | | | |
| 24 | Health Record Chain (HRC): Implementation of Mobile Healthcare system using Blockchain<br>(Alfaidi & Chow, 2020) | Legal Right | Immutability vs Erasure | Hash Referencing<br>Off Chain Storage<br>Privacy by Design | – |
| 25 | How to Redact the Bitcoin Backbone Protocol<br>(Larraia et al., 2024) | Legal Right | Immutability vs Erasure<br>Irreversibility Risk | Ethical by Design<br>Privacy by Design | – |
| 26 | K-Time Modifiable and Epoch-Based Redactable Blockchain (Xu et al., 2021) | Legal Right | Accountability Ambiguity<br>Immutability vs Erasure | Chameleon Hashes<br>Ethical by Design<br>Hybrid Governance Model | – |
| 27 | MerkleChain: A Privacy-enhanced and Flexible Merkle-tree-based Blockchain Architecture<br>(Mukkamala et al., 2025) | Legal Right | Immutability vs Erasure<br>Loss of User Autonomy | Chameleon Hashes<br>Privacy by Design | – |
| 28 | Modifiable Public Blockchains Using Truncated Hashing and Sidechains<br>(N. Y. Lee et al., 2019) | Legal Right | Immutability vs Erasure<br>Irreversibility Risk | Hash Referencing<br>Privacy by Design | – |
| 29 | PRBCP: Publicly Redactable Blockchain With Off-Chain Reputation-Based Consensus Protocol<br>(Hou et al., 2025) | Legal Right | Accountability Ambiguity<br>Immutability vs Erasure | Privacy by Design<br>Ethical by Design<br>Hybrid Governance Model<br>Chameleon Hashes | Governance Vacuum |
| 30 | Privacy-Aware Cloud Auditing for GDPR Compliance Verification in Online Healthcare<br>(Barati et al., 2022) | Implicit Mention | – | Privacy by Design | – |
| 31 | Privacy-aware cloud ecosystems and GDPR compliance<br>(Barati et al., 2019) | Implicit Mention | – | Privacy by Design<br>Hybrid Governance Model | – |
| 32 | Privacy-Preserving “Right to Be Forgotten” in Configurable Blockchain Tokenization: A Cryptographic Audit Framework<br>(Ghaly et al., 2025) | Technical Constraint | Immutability vs Erasure<br>Irreversibility Risk | Cryptographic Key Deletion<br>Ethical by Design<br>Hash Referencing<br>Off Chain Storage<br>Privacy by Design | Lack of Empirical Evidence<br>Legal Uncertainty |
| 33 | Privacy-Preserving and Revocable Redactable Blockchains with Expressive Policies in IoT<br>(Guo et al., 2024) | Legal Right | Immutability vs Erasure | Chameleon Hashes<br>Privacy by Design | – |
| 34 | Privacy-Preserving Blockchain Framework Based<br>on Ring Signatures (RSs) and Zero-Knowledge Proofs(ZKPs)<br>(Mahmood & Vacius, 2020) | Legal Right | Immutability vs Erasure | Privacy by Design | – |

| | | | | | |
|---|---|---|---|---|---|
| 35 | Reda<br>– Rewriting History in Bitcoin and Friends<br>(Ateniese et al., 2017) | | Erasure<br>Irreversibility Risk | Hybrid Governance Model | |
| 36 | Redacting Without Regret: A Dual-Layer Framework for Policy-Compliant Blockchains<br>(Biswas et al., 2025) | Design Requirement | Accountability Ambiguity<br>Immutability vs Erasure<br>Irreversibility Risk | Hybrid Governance Model<br>Legal Technical Framework<br>Privacy by Design | Scalability Interoperability Issues |
| 37 | Secure Redactable Blockchain with Dynamic Support<br>(Zhang et al., 2024) | Technical Constraint | Immutability vs Erasure<br>Irreversibility Risk | Chameleon Hashes<br>Hybrid Governance Model | – |
| 38 | Secure semi-automated GDPR compliance service with restrictive fine-grained access control<br>(Eiza et al., 2024) | Implicit Mention | Accountability Ambiguity<br>Loss of User Autonomy | Human in the Loop<br>Legal Technical Framework<br>Privacy by Design | – |
| 39 | SPChain: A Smart and Private Blockchain-Enabled Framework for Combining GDPR-Compliant Digital Assets Management With AI Models<br>(W. S. Lee et al., 2022) | Design Requirement | Immutability vs Erasure<br>Loss of User Autonomy<br>Consent Withdrawal Problem | Off Chain Storage<br>Hash Referencing<br>Privacy by Design<br>Legal Technical Framework | Scalability Interoperability Issues |
| 40 | The right to be forgotten in post-Google Spain case law: an Example of Legal Interpretivism in Action?<br>(Krupa-Lipińska & Wulff, 2021) | Legal Right | Immutability vs Erasure<br>Accountability Ambiguity | Legal Technical Framework | Legal Uncertainty |
| 41 | The Right to Be Forgotten: Privacy and Security in Blockchain with Multi-authority Based Chameleon Hash Function MAP-ABCH Solution<br>(Alfaidi & Semwal, 2022) | Technical Constraint | Immutability vs Erasure<br>Consent Withdrawal Problem | Chameleon Hashes<br>Cryptographic Key Deletion<br>Hybrid Governance Model | – |
| 42 | Towards Data Redaction in Bitcoin<br>(Botta et al., 2022) | Technical Constraint | Immutability vs Erasure<br>Irreversibility Risk | Cryptographic Key Deletion<br>Privacy by Design | – |
| 43 | Towards Enabling Deletion in Append-Only Blockchains to Support Data Growth Management and GDPR Compliance<br>(Kuperberg, 2020) | Design Requirement | Immutability vs Erasure<br>Loss of User Autonomy | Hybrid Governance Model<br>Privacy by Design | – |
| 44 | Towards Enforcement of the EU GDPR: Enabling Data Erasure<br>(Sarkar et al., 2018) | Design Requirement | Immutability vs Erasure<br>Loss of User Autonomy | Legal Technical Framework<br>Privacy by Design | Legal Uncertainty<br>Technical Infeasibility |
| 45 | Tracking GDPR Compliance in Cloud-Based Service Delivery<br>(Barati & Rana, 2022) | Implicit Mention | Accountability Ambiguity | Human in the Loop<br>Legal Technical Framework<br>Privacy by Design | Legal Uncertainty<br>Scalability<br>Interoperability Issues |
| 46 | When Blockchain Meets the Right to Be Forgotten: | Design Requirement | Immutability vs Erasure | Off Chain Storage<br>Hash Referencing<br>Privacy by Design | – |

| | | | | | |
|---|---|---|---|---|---|
| | Tech<br>the Healthcare Industry<br>(Bayle et al., 2018) | | Autonomy | Framework | |

## References

Ahmad, H., & Aujla, G. S. (2023). GDPR compliance verification through a user-centric blockchain approach in multi-cloud environment. *Computers and Electrical Engineering*, *109*, 108747. https://doi.org/10.1016/J.COMPELECENG.2023.108747

Alessi, M., Camillò, A., Giangreco, E., Matera, M., Pino, S., & Storelli, D. (2019). A decentralized personal data store based on Ethereum: towards GDPR compliance. *Journal of Communications Software and Systems*, *15*(2), 79–88. https://doi.org/10.24138/JCOMSS.V15I2.696

Alfaidi, A., & Chow, E. (2020). Health Record Chain (HRC): Implementation of mobile healthcare system using blockchain to enhance privacy of electronic health record EHR. *Proceedings - 2020 International Conference on Computational Science and Computational Intelligence, CSCI 2020*, 863–866. https://doi.org/10.1109/CSCI51800.2020.00161

Alfaidi, A., & Semwal, S. (2022). The right to be forgotten: privacy and security in blockchain with multi-authority based chameleon hash function MAP-ABCH solution. *Lecture Notes in Networks and Systems*, *438 LNNS*, 861–876. https://doi.org/10.1007/978-3-030-98012-2_60/FIGURES/6

Angón, O. C. (2024). General data protection regulation, right to be forgotten, blockchain technology and human rights. *The Age of Human Rights Journal*, *23*(23), e8702–e8702. https://doi.org/10.17561/TAHRJ.V23.8702

Anido-Rifón, L., von-Eitzen-Delgado, C., Ruiz Molina, M., Molina Martínez, P., Álvarez González, S., Rodríguez Vázquez, V., Fernández-Iglesias, M. J., Mikic Fonte, F., & Llamas Nistal, M. (2025). balancing data protection and decentralization: harnessing blockchain's potential while ensuring GDPR compliance. *Lecture Notes in Networks and Systems, 1256 LNNS*, 393–402. https://doi.org/10.1007/978-3-031-81928-5_38

Ateniese, G., Magri, B., Venturi, D., & Andrade, E. R. (2017). Redactable Blockchain - Or - rewriting history in bitcoin and friends. *Proceedings - 2nd IEEE European Symposium on Security and Privacy, EuroS and P 2017*, 111–126. https://doi.org/10.1109/EUROSP.2017.37

Balistri, E., Casellato, F., Giannelli, C., & Stefanelli, C. (2021). BlockHealth: Blockchain-based secure and peer-to-peer health information sharing with data protection and right to be forgotten. *ICT Express*, *7*(3), 308–315. https://doi.org/10.1016/J.ICTE.2021.08.006

Barati, M., Aujla, G. S., Llanos, J. T., Duodu, K. A., Rana, O. F., Carr, M., & Ranjan, R. (2022). Privacy-aware cloud auditing for GDPR compliance verification in online healthcare. *IEEE Transactions on Industrial Informatics*, *18*(7), 4808–4819. https://doi.org/10.1109/TII.2021.3100152

Barati, M., & Rana, O. (2021). Checking GDPR compliance for cloud-based services. *Proceedings - 2021 IEEE World Congress on Services, SERVICES 2021*, 2. https://doi.org/10.1109/SERVICES51467.2021.00013

Barati, M., & Rana, O. (2022). Tracking GDPR compliance in cloud-based service delivery. *IEEE Transactions on Services Computing*, *15*(3), 1498–1511. https://doi.org/10.1109/TSC.2020.2999559

Barati, M., Rana, O., Petri, I., & Theodorakopoulos, G. (2020). GDPR compliance verification in internet of things. *IEEE Access*, *8*, 119697–119709. https://doi.org/10.1109/ACCESS.2020.3005509

Barati, M., Rana, ompliance. *Proceedings - 2019 International Conference on Future Internet of Things and Cloud, FiCloud 2019*, 117–124. https://doi.org/10.1109/FICLOUD.2019.00024

Bayle, A., Koscina, M., Manset, D., & Perez-Kempner, O. (2018). When blockchain meets the right to be forgotten: technology versus law in the healthcare industry. *2018 IEEE/WIC/ACM International Conference on Web Intelligence (WI)*, 788–792. https://doi.org/10.1109/WI.2018.00133

Biswas, S., Chakraborty, S., & Chakraborty, R. S. (2025). Redacting without regret: a dual-layer framework for policy-compliant blockchains. *2025 7th Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)*, 1–9. https://doi.org/10.1109/BRAINS67003.2025.11302930

Botta, V., Iovino, V., & Visconti, I. (2022). Towards data redaction in bitcoin. *IEEE Transactions on Network and Service Management*, *19*(4), 3872–3883. https://doi.org/10.1109/TNSM.2022.3214279

Calani, M., Denaro, G., & Leporati, A. (2024). Exploiting the blockchain to guarantee GDPR compliance while consents evolve under data owners' control. *CEUR WORKSHOP PROCEEDINGS*, *2940*, 331–343. https://boa.unimib.it/handle/10281/328337

Eiza, M. H., Ta, V. T., Shi, Q., & Cao, Y. (2024). Secure semi-automated GDPR compliance service with restrictive fine-grained access control. *Security and Privacy*, *7*(6), e451. https://doi.org/10.1002/SPY2.451

*Everything you need to know about the "Right to be forgotten" - GDPR.eu*. (2026, January 4). https://gdpr.eu/right-to-be-forgotten/

Fugkeaw, S., Sungchai, S., Nakprame, S., & Sreekongpan, P. (2025). Enabling secure and scalable GDPR-compliant blockchain-based e-KYC with efficient redaction. *IEEE Access*, *13*, 136834–136853. https://doi.org/10.1109/ACCESS.2025.3594656

Gan, W., Zhao, M., Guo, H., Zhang, C., Hong, J., & Zhu, L. (2023). Fine-grained data rights governance in blockchain-based cloud-edge communications. *Proceedings - IEEE Global Communications Conference, GLOBECOM*, 904–909. https://doi.org/10.1109/GLOBECOM54140.2023.10436817

Ghaly, P., Gjermundrød, H., & Dionysiou, I. (2025). Privacy-preserving "Right to Be Forgotten" in configurable blockchain tokenization: a cryptographic audit framework. *2025 7th Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)*, 1–8. https://doi.org/10.1109/BRAINS67003.2025.11302955

Giordano, M. T. (2021). Blockchain and the GDPR: New challenges for privacy and security. In *Blockchain, Law and Governance* (pp. 275–286). Springer, Cham. https://doi.org/10.1007/978-3-030-52722-8_20

Guo, H., Chen, L., Ren, X., Zhao, M., Li, C., Xue, J., Zhu, L., & Zhang, C. (2024). Privacy-preserving and revocable redactable blockchains with expressive policies in IoT. *IEEE Internet of Things Journal*, *11*(21), 35390–35404. https://doi.org/10.1109/JIOT.2024.3435729

Gutierrez-Aguero, I., Anguita, S., Larrucea, X., Gomez-Goiri, A., & Urquizu, B. (2021). Burnable pseudo-identity: a non-binding anonymous identity method for Ethereum. *IEEE Access*, *9*, 108912–108923. https://doi.org/10.1109/ACCESS.2021.3101302

Hou, Y., Zou, J., Wang, L., Lu, X., Lu, X., & Wang, M. (2025). PRBCP: Publicly redactable blockchain with off-chain reputation-based consensus protocol. *IEEE Transactions on Network and Service Management*, *22*(5), 4603–4618. https://doi.org/10.1109/TNSM.2025.3578659

Islam, M. R., Ala work for personal data management. *2024 27th International Conference on Computer and Information Technology, ICCIT 2024 - Proceedings*, 3063–3068. https://doi.org/10.1109/ICCIT64611.2024.11022541

Krupa-Lipińska, K., & Wulff, C. M. (2021). The Right to be Forgotten in Post-Google Spain case law: an example of legal interpretivism in action? *Comparative Law Review*, *26*(0), 255–279. https://doi.org/10.12775/CLR.2020.010

Kuperberg, M. (2020). Towards enabling deletion in append-only blockchains to support data growth management and GDPR compliance. *Proceedings - 2020 IEEE International Conference on Blockchain, Blockchain 2020*, 393–400. https://doi.org/10.1109/BLOCKCHAIN50366.2020.00057

Larraia, E., Kiraz, M. S., & Vaughan, O. (2024). How to redact the bitcoin backbone protocol. *2024 IEEE International Conference on Blockchain and Cryptocurrency, ICBC 2024*, 485–493. https://doi.org/10.1109/ICBC59979.2024.10634365

Lee, N. Y., Yang, J., Onik, M. M. H., & Kim, C. S. (2019). Modifiable public blockchains using truncated hashing and sidechains. *IEEE Access*, *7*, 173571–173582. https://doi.org/10.1109/ACCESS.2019.2956628

Lee, W. S., John, A., Hsu, H. C., & Hsiung, P. A. (2022). SPChain: a smart and private blockchain-enabled framework for combining GDPR-compliant digital assets management with AI models. *IEEE Access*, *10*, 130424–130443. https://doi.org/10.1109/ACCESS.2022.3227969

Li, X., Xu, J., Yin, L., Lu, Y., Tang, Q., & Zhang, Z. (2023). Escaping from consensus: instantly redactable blockchain protocols in permissionless setting. *IEEE Transactions on Dependable and Secure Computing*, *20*(5), 3699–3715. https://doi.org/10.1109/TDSC.2022.3212601

Liagkou, V., Stefanidis, K., Isazade, A., Malik, A., & Alshawki, M. B. (2025). Blockchain-enabled GDPR compliance enforcement for IIoT data access. *Journal of Cybersecurity and Privacy 2025, Vol. 5, Page 84*, *5*(4), 84. https://doi.org/10.3390/JCP5040084

Mahindrakar, A., & Joshi, K. P. (2020). Automating GDPR compliance using policy integrated blockchain. *Proceedings - 2020 IEEE 6th Intl Conference on Big Data Security on Cloud, BigDataSecurity 2020, 2020 IEEE Intl Conference on High Performance and Smart Computing, HPSC 2020 and 2020 IEEE Intl Conference on Intelligent Data and Security, IDS 2020*, 86–93. https://doi.org/10.1109/BIGDATASECURITY-HPSC-IDS49724.2020.00026

Mahmood, Z., & Vacius, J. (2020). Privacy-preserving block-chain framework based on ring signatures (RSs) and Zero-Knowledge Proofs(ZKPs). *2020 International Conference on Innovation and Intelligence for Informatics, Computing and Technologies, 3ICT 2020*. https://doi.org/10.1109/3ICT51146.2020.9312014

Metin, B., Erkan, S., Atasu, İ., & Yılmaz, E. (2019). Privacy impact assessment as a tool for GDPR compliance preparation. *Kişisel Verileri Koruma Dergisi*, *1*(2), 75–86. https://dergipark.org.tr/en/pub/kvkd/article/646782

Mone, V., & Sivakumar, C. (2022). An analysis of the GDPR compliance issues posed by new emerging technologies. *Legal Information Management*, *22*(3), 166–174. https://doi.org/10.1017/S1472669622000317

Mukkamala, R., Olariu, S., & Kalari, S. (2025). *MerkleChain: a privacy-enhanced and flexible merkle-tree-based blockchain architecture*. 90–97. https://doi.org/10.1109/BCCA66705.2025.11227179

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., … Moher, D. (2021). The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. *BMJ*, *372*. https://doi.org/10.1136/BMJ.N71

Parikh, A. M., Su ment using permissioned blockchains. *Lecture Notes in Computer Science*, *15722 LNCS*, 156–175. https://doi.org/10.1007/978-3-031-96590-6_9/TABLES/3

Piao, Y., Ye, K., & Cui, X. (2021). A data sharing scheme for GDPR-compliance based on consortium blockchain. *Future Internet 2021, Vol. 13, Page 217*, *13*(8), 217. https://doi.org/10.3390/FI13080217

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. https://doi.org/10.1109/TETC.2019.2949510

Saif, M. Bin, & Migliorini, S. (2025). Blockchain-based data immutability and traceability in the era of GDPR. 546–553. https://doi.org/10.1109/BCCA66705.2025.11229677

Sarkar, S., Banatre, J. P., Rilling, L., & Morin, C. (2018). Towards enforcement of the EU GDPR: enabling data erasure. *Proceedings - IEEE 2018 International Congress on Cybermatics: 2018 IEEE Conferences on Internet of Things, Green Computing and Communications, Cyber, Physical and Social Computing, Smart Data, Blockchain, Computer and Information Technology, IThings/Gre…*, 222–229. https://doi.org/10.1109/CYBERMATICS_2018.2018.00067

Semwal, S., & Alfaidi, A. (2022). Blockchain graphs (BCGs) to support right-to-be-forgotten "RTBF" in blockchains. *Lecture Notes in Networks and Systems*, *438 LNNS*, 892–905. https://doi.org/10.1007/978-3-030-98012-2_62/FIGURES/6

Shirmohammadi, M., Islam, A., & Karimipour, H. (2025). An intent-based networking framework for secure and privacy-compliant machine unlearning using meta-learning and redactable blockchain. *IEEE Internet of Things Journal*. https://doi.org/10.1109/JIOT.2025.3638966

Taşdelen, A. (2024). Fundamentals of blockchain. In *Exploring Blockchain Applications: Management Perspectives* (pp. 6–25). CRC Press. https://doi.org/10.1201/9781003389552-2

Vargas, J. C. (2019). Blockchain-based consent manager for GDPR compliance. 165–170. https://dl.gi.de/handle/20.500.12116/20985

Xiao, L., Han, D., Zhou, S., Xu, N., Chen, L., & Xie, S. (2023). A Blockchain-empowered federated learning framework supprting GDPR-compliance. *Proceedings - 2023 IEEE 10th International Conference on Cyber Security and Cloud Computing and 2023 IEEE 9th International Conference on Edge Computing and Scalable Cloud, CSCloud-EdgeCom 2023*, 399–404. https://doi.org/10.1109/CSCLOUD-EDGECOM58631.2023.00074

Xu, S., Ning, J., Li, X., Yuan, J., Huang, X., & Deng, R. H. (2024). A privacy-preserving and redactable healthcare blockchain system. *IEEE Transactions on Services Computing*, *17*(2), 364–377. https://doi.org/10.1109/TSC.2024.3356595

Xu, S., Ning, J., Ma, J., Huang, X., & Deng, R. H. (2021). K-Time modifiable and epoch-based redactable blockchain. *IEEE Transactions on Information Forensics and Security*, *16*, 4507–4520. https://doi.org/10.1109/TIFS.2021.3107146

Zhang, D., Le, J., Lei, X., Xiang, T., & Liao, X. (2024). Secure redactable blockchain with dynamic support. *IEEE Transactions on Dependable and Secure Computing*, *21*(2), 717–731. https://doi.org/10.1109/TDSC.2023.3261343

Zhuk, A. (2025). Beyond the blockchain hype: addressing legal and regulatory challenges. *SN Social Sciences 2025 5:2*, *5*(2), 11-. https://doi.org/10.1007/S43545-024-01044-Y