Financial Internet Quarterly 2026, vol. 22 / no. 3, p. 78-90
https://dx.doi.org/10.65748/fiqf-2026-0020

Financial Internet Quarterly

RECONCILING GDPR AND BLOCKCHAIN ON DATA PROTECTION ISSUES

Melko Dragojević[1], Željka Krolo Ivanov[2], Tonći Svilokos[3]

Abstract

As blockchain technologies become increasingly prevalent in everyday applications, integrating them with the General Data Protection Regulation (GDPR) raises significant challenges. This paper analyses the relationship between GDPR and blockchain by examining how the literature identifies key points of conflict and possible compliance pathways. The study asks which thematic areas dominate this literature, which data protection issues are most frequently identified, and which technical or governance-oriented solutions are proposed. Using bibliographic coupling and term co-occurrence analysis, the paper analyses 695 unique papers derived from selected review and survey articles indexed in Scopus and Web of Science. The results identify six thematic clusters covering the right to erasure, blockchain mutability, architecture alternatives, IoT and FinTech integration, system changes for GDPR compliance, smart contracts, privacy, identity management, and data protection. The findings highlight privacy-by-design and interdisciplinary cooperation as key conditions for reconciling blockchain innovation with GDPR requirements.

JEL classification: G18, G28, K24, O33
Keywords: Blockchain, GDPR, Regulation Compliance

Received: 24.06.2025 Accepted: 03.08.2026

Cite this:
Dragojević, M., Ivanov, Ž.K. & Svilokos, T. (2026). Reconciling GDPR and blockchain on data protection issues. Financial Internet Quarterly 22(3), pp. 78-90. https://dx.doi.org/10.65748/fiqf-2026-0020.

© 2026 Melko Dragojević et al. published by University of Information Technology and Management in Rzeszów. This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 License.

[1] Faculty of Economics and Business, University of Dubrovnik, Croatia, e-mail: melko.dragojevic@unidu.hr, ORCID: https://orcid.org0009-0005-3401-1642.
[2] PhD student at University of Dubrovnik, Croatia, e-mail: zeljka.krolo@gmail.com, ORCID: https://orcid.org/0000-0003-4159-7918.
[3] Faculty of Economics and Business, University of Dubrovnik, Croatia, e-mail: tonci.svilokos@unidu.hr, ORCID: https://orcid.org/0000-0002-7568-5708.

Introduction

The relationship between blockchain technology and General Data Protection Regulation (GDPR) is the core focus of this study. Although often used as catchphrases, these terms represent significant and evolving fields that intersect in complex ways. While the frequency with which these topics are covered inevitably leads to redundancy, it does not mean the research related to them is futile. In reality, the opposite is true, large amounts of discussions are taking place, and from them niches are formed. As with any other field of research, certain papers gain much more traction than others. These specific fields are perhaps best covered in literature reviews trying to summarize the most influential works from that particular area. We try to leverage these reviews and address the following research questions:

RQ_1: What thematic clusters structure the literature on blockchain technology and GDPR compliance?

RQ_2: Which GDPR-related data protection issues are most frequently associated with blockchain technology?

RQ_3: Which technical and governance-oriented compliance strategies are proposed in the literature, and what limitations remain?

More briefly stated, the objective of the paper is not to provide a normative legal interpretation of GDPR or to test a technical blockchain solution empirically, but to map the intellectual structure of the field and identify the main compliance pathways discussed in the literature.

This is not to say that the research on how GDPR enables or disables disruptive innovations of blockchain is lacking, but more to state that this area is the niche we cater the most to. Although blockchain technology and the GDPR regulatory framework differ fundamentally in nature, they intersect when blockchain-based systems process personal data. The subject of this research paper relates to the OECD discussion on blockchain technologies, recognized as a technology with upcoming challenges and novel questions. What we try to do in this paper is to identify what are key issues, where the interdisciplinary approaches originate from, how the authors' points of view differ from field to field, and the current issues discussions are taking place on. We employ bibliographic coupling analyses of selected existing literature reviews and their references that best summarize the relationship of blockchain and GDPR. We detect 6 (six) particular clusters from the 695 unique papers we analyse, more specifically:

- Right to erasure, blockchain mutability, and information governance,
- Blockchain architecture alternatives, case-studies of compliance solutions in different fields with GDPR,
- Integrating IoT, FinTech, and blockchain technologies,
- Blockchain system changes to achieve compliance with GDPR,
- Cryptocurrencies, smart contracts, applications of blockchain on data,
- Privacy, identity management, and data protection in blockchain-based technology.

This analysis functions as the backbone for the structure we use. Precisely these clusters, along with other literature findings pushed us into the data protection direction, i.e. to examine whether blockchain-based systems can be compliant with GDPR, and under which technical and organisational conditions such compliance may be improved. To more focus our discussion, we single out exact issues and solutions the two have encountered or are yet to do so. More specifically, we examine reference-based tree structures and related architectural variants as technical blockchain design solutions proposed to improve GDPR compliance, especially for issues such as data erasure, data minimization, and accountability. We argue that while no singular solution exists for all data protection unresolved issues, we should advocate for an interdisciplinary approach to new proposals of both regulation and of new technology improvements.

This issue is particularly relevant for financial services because blockchain-based applications are increasingly discussed in banking, digital identity, payments, asset tokenisation, smart contracts, regulatory reporting, and FinTech infrastructures. In these areas, protection of personal data is continuously examined as a core condition for lawful deployment. Therefore, the reconciliation of blockchain and GDPR has direct implications for financial innovation, compliance costs, operational resilience, and trust in digital financial ecosystems.

The paper is structured as follows. Following the Introduction, the Literature review section covers the data aspect of blockchain and how it operates, alongside with how the GDPR demands data be treated. The Data and methods section details which data we opt for, how we obtain it, and what methods we use to analyze it. The Results section provides information on the clusters we detect within the data. The Discussion gives more insight into the privacy by design principle that emerges in the literature, and compliance strategies that can settle the conflicts between blockchain technologies and GDPR. Conclusions are set in the final section.

Literature review

The blockchain data treatment

Blockchain is usually recognized as a cornerstone of all cryptocurrencies, but primarily bitcoin. In reality, it is a database that contains records of transactions be-

tween participants where each transaction is confirmed by the majority of participants themselves – effectively eliminating fraud and any subsequent altering of the database. It does not have a centralized institution (with a few exceptions), but instead relies on sharing the database with the participants, making great use of cryptography and peer-to-peer technology within the process (Efanov & Roschin, 2018). Blockchain, or blockchain technology can get highly technical, and while the focus of this paper is not oriented to the technical explanations, we still discuss those which are truly necessary.

The trust-based model (which blockchain was proposed to replace) relies on trust in a traditional finance sector incumbent as a reliable party, or in the eyes of Nakamoto (2008), on any third party willing and reputable enough to mediate and confirm, i.e. to validate the payment process. A peer-to-peer electronic payment system was speculated for a long time as a replacement to the trust-based model, but the element of trust in such a system was lacking. More importantly, the question was how to ensure a system with no authority to equally protect buyers and sellers from fraud while the integrity of the system remains intact. As of today, the trust-based model is nowhere near replacement, but the blockchain alternative to it - proof -of-work- and the iterations on it that followed gained much steam since their inception.

Proof-of-work is used for the first type of blockchain system where only blocks that contain correct solutions to complex math problems can be added to the database - the blockchain (Efanov & Roschin, 2018). As stated, it has evolved through time so the discussions today often revolve around the differences between proof-of-work, proof-of-stake, proof-of-authority, proof-of-identity, and proof-of-elapsed-time consensus models. A detailed discussion of consensus mechanisms falls beyond the scope of this paper, but Yaga et al. (2019) provide a useful overview of the technical aspects of blockchain architecture and implementation. Blockchain is frequently a polarizing subject in the finance world, perhaps more in line with the innovations of big data or Internet-of-Things. It is often seen as a disruption to the largely undisturbed finance sector, but it is a rather necessary one. To some, blockchain promises a way of addressing inefficiencies and transaction costs in financial intermediation. However, as Philippon (2016) argues, technological innovation in finance has not necessarily reduced the overall cost of financial services, partly because incumbent institutions may use innovation to preserve market power and rent-seeking opportunities.

Because of its decentralized nature, blockchain does not possess a single point of failure which cannot be stated for the models of trust. Blockchain is, however, at the first sight immutable and transparent. To be precise, let us use the blockchain characteristics of Aste et al. (2017).

1. Decentralized and Transparent Consensus - all transactions must be valid under a ruleset/protocol that is chronologically consistent. Validation is done by many nodes that make the blockchain, meaning, all records are visible and traceable to all.
2. Security and Immutability - blockchain records cannot be changed once validated, it is tamper-proof (with certain caveats).
3. Automation - validation does not need human interaction, but is done via algorithms that “self-execute, self-enforce, self-verify, and self-constraint” the contracts.
4. Metadata - blockchain can store small amounts of metadata for each record.

Immutability and transparency are the two characteristics that can largely be argued as pros but do create points of conflict with certain regulations or even simply with user needs and preferences.

Aside from these, Efanov and Roschin (2018) also mention many potential security threats that would have large impacts on blockchain technologies if they were ever to be breached. On top of that, there is the question of personal identity. On the blockchain, it exists only in the form of a private key, which if lost means the wallet, or any other kind of record in ownership of the person is now then unobtainable. Security, in terms of reliability, is often on the line for blockchain as well because of the volatility cryptocurrencies exhibit (Adrian & Mancini-Griffoli, 2021). Bear in mind that this pertains only to cryptocurrencies, and we have already mentioned that these are only a part of technologies that are based on the blockchain.

Every blockchain is a DLT, however, not all DLTs are blockchains, as blockchain is a DLT that is built on community consensus (Aste et al., 2017). Meaning that it is a decentralized, shared, and replicated record of transactions that is (with time) synchronized across all participants (Treleaven et al., 2017). The main unit of records on such a DLT are unsurprisingly - blocks. One block contains both one or more transactions, and the respective metadata, along with the necessary cryptographic link to the immediately preceding block (Yaga et al., 2019). When discussing data processing on a blockchain, it is important to distinguish between transaction data and block data. In most blockchain systems, transactions are digitally signed by the holder of the relevant private key, while blocks are created by miners, validators, or other authorized nodes. In some systems blocks may also be signed by the producing node, but this is not a universal feature of all blockchains. Once transaction or block data is recorded and finalized on-chain, it is generally tamper-evident and

very difficult to alter. Whether a blockchain is permissioned will decide who exactly has, or rather, has not the permission to see every written block.

Immutability and transparency have proven to be blockchain's strong points where there are significant benefits of it in operational efficiency, as Aste et al. (2017) state. A single version of the "truth" gets rid of any potential for dispute. It also allows for easier cooperation with any regulatory bodies, and makes the issue of informational asymmetry quite less impactful. DLT's also enable smart contracts - that essentially function as protocols. They contain (and execute) actions when certain conditions based on the already existing blockchain data are met (examples include automatic reimbursement, loan approval, etc.), thus transforming the traditional principles of contracting.

Smart contracts are a huge leap forward as they allow for automatization of both business and regulatory requirements. However, when dealing with them in the EU, one particular privacy regulation muddled the waters - GDPR. Personal data itself has come under much scrutiny prompted by discussions that usually focus on the topic of data regulation, use, and transparency from either the perspective of a concerned system participant, or from a benefit-seeking side that views the potential in new advancements. The question that emerges is whether automated or even black-box type contracts can be designed in a way that they are compliant with GDPR requirements. The current EU answer to this is to establish service-based rules regardless of the provider, although the regulation may not yet fully reflect this stance. This, in turn, leads us to the following section.

GDPR - the key to all things "data"

General Data Protection Regulation is a direct successor to the EU's Data Protection Directive (hereinafter: GDPR or Regulation). It is well known that the GDPR is a cornerstone of data protection in the European Union, setting stringent requirements for organizations handling personal data and ensuring adequate levels of privacy. It is based on the philosophical, and the Charter of EU Rights idea that privacy is a fundamental human right. This right is guarded by six principles of data protection (Goddard, 2017). This section explores the key principles, scope, and implications of GDPR, particularly in the context of blockchain technology, focusing on the privacy by design mandatory principle. To be compliant with article 5. of Regulation, data controllers shall process data lawfully, respect data processing purpose limitation, collect only necessary personal data, have in place retention policies, be accurate and act in accordance with integrity and confidentiality principle (IAPP, 2020). Article 24. of the GDPR sets forth general obligation of data controller to implement organizational and technical measures to ensure and be able to demonstrate compliance with the GDPR.

The main goal of GDPR is to safeguard individuals' personal data. By its introduction, the GDPR establishes and levels up protection of personal data, primarily within the EU. Van Ooijen and Vrabec (2019) argue that although this is its goal, it still has flaws that occur in different stages of data processing. One of the significant challenges is to achieve full regulatory compliance in already developed technologies. The paper examines blockchain technologies and considers whether the identified GDPR-related compliance issues can be addressed through technical and organisational measures. Researchers and privacy professionals were focused on non-compliance with the principle of data accuracy and storage limitation and right to erasure or right to be forgotten (set forth in article 17 and article 19 of the GDPR as mandatory right). Article 17 of GDPR states that data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the grounds subject to the Article 17 applies. Due to immutability challenges, one group of stakeholders wish to reform GDPR in a way so it does not have unintended consequences. GDPR entered into force to ensure privacy and trust, so it is unlikely that GDPR is going to be entirely reformed (see the discussion by Wloczka (2024)). Moreover, European regulators strive to impose stricter regulation, which is even more true for the financial sector (Altman et al., 2023) and enhance privacy in an AI environment. In that context, data controllers shall inform data subjects, among other, on means and purposes of data processing and make available exercising their rights.

Campbell et al. (2015) conclude the consent-based approach is favourable to the incumbents, to the firms that offer a large scope of services. It stifles small and new businesses by disproportionately increasing the customer-subjective transaction cost. This is backed up by the Gal and Aviv (2020) detected mechanisms that benefit the monopolistic tendency of the KYD trend, and empirically corroborated by Johnson et al. (2023) and Goldberg et al. (2024). The Philippon (2016) advocated changes on financial regulation that would further enable new entrants who have not been introduced well enough in the EU, if at all. There are many ideas to overcome the data processing issues, but none are the silver bullet. Arner et al. (2017) argue that sandboxes are the future, while not failing to mention other approaches that include self-regulation until a certain point, forms of tiered compliance, increased support to SMEs and others. This leads us back to blockchain,

which itself offers some opportunities that can address the GDPR challenges, but has its own downfalls.

In the review of Kavuri and Milne (2018) the topic of identity, security, and data protection is precisely the one that is detected as a gap in the FinTech literature. Still, dichotomous views on data protection and the related regulation do exist, but are not often discussed in overlap. In the following section we conduct a meta-review of sorts on a set of selected notable articles. We focus on examining the recent developments of the Kavuri and Milne (2018) detected gap of data protection, contrasting the EU's GDPR with blockchain technology.

Data and methods

Academic interest in the intersection of blockchain technology and the General Data Protection Regulation (GDPR) has grown substantially since the GDPR came into force in May 2018. Table 1 presents annual Scopus records for the keywords 'GDPR' and 'blockchain', together with year-to-year changes. The data related to the year 2026 refers only to the papers published in the January-May period. The data show a strong increase in both research streams, especially after 2017.

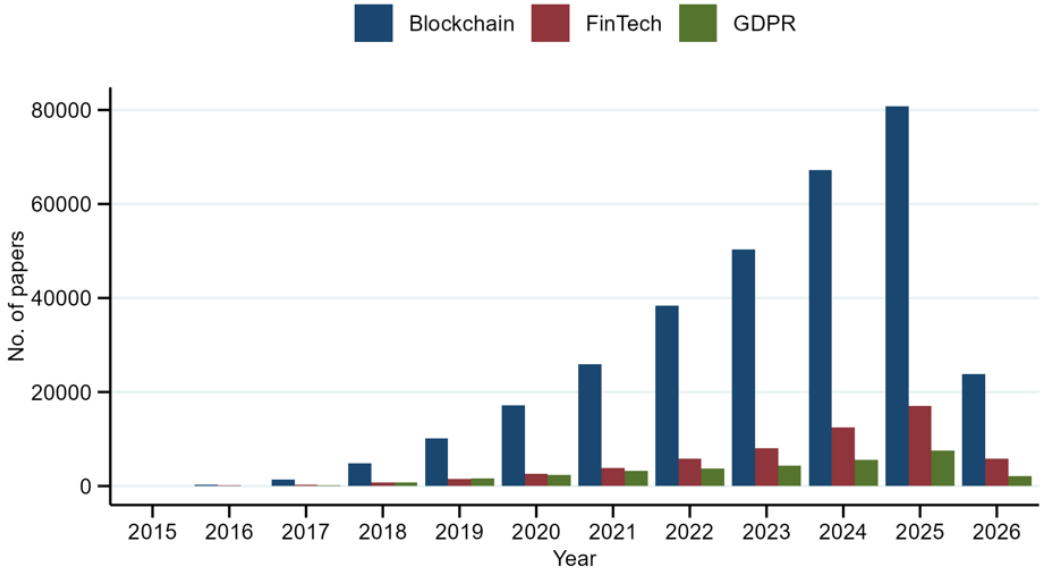
Table 1: Published papers containing selected keywords

	GDPR			Blockchain		
Year	Total Publications	Annual Delta	Growth Rate (%)	Total Publications	Annual Delta	Growth Rate (%)
2015	28	4	16.67%	133	72	118.03%
2016	78	50	178.57%	430	297	223.31%
2017	270	192	246.15%	1,803	1,373	319.30%
2018	1,070	800	296.30%	6,610	4,807	266.61%
2019	2,686	1,616	151.03%	16,804	10,194	154.22%
2020	5,100	2,414	89.87%	33,951	17,147	102.04%
2021	8,327	3,227	63.27%	59,869	25,918	76.34%
2022	12,111	3,784	45.44%	98,204	38,335	64.03%
2023	16,473	4,362	36.02%	148,554	50,350	51.27%
2024	22,031	5,558	33.74%	215,735	67,181	45.22%
2025	29,622	7,591	34.46%	296,502	80,767	37.44%
2026 (Jan-May)	31,729	2,107	7.11%	320,356	23,854	8.05%

Notes: Growth Rate (%) is the year-on-year relative change computed as Annual Delta_t / $\text{Total Publications}_{t-1}$

Source: Author's own work.

Figure 1: Published papers containing selected keywords



Source: Author's own work.

GDPR-related publications increased from 192 records in 2017 to 7,591 in 2025, while blockchain-related publications increased from 1,373 to 80,767 over the same period. The 2026 figures are reported separately because they refer only to records indexed up to the date of data extraction and are therefore not directly comparable with full-year observations. Alongside these figures, Table 1 confirms that both fields have experienced substantial and sustained growth in scholarly output, with no sign of saturation in either area through 2025. Figure 1 presents the annual distribution of Scopus records containing the selected keywords used in the preliminary search.

The starting point for data collection was a systematic search of the Scopus and Web of Science (WoS) databases. Search queries combined the terms blockchain, GDPR, and review, targeting title, abstract, and keyword fields. Initially we tried to focus on the overlap of these, however this resulted in a sample of only 4 works according to the Scopus citation database. Once we exclude FinTech from the keywords we match, it gives us a manageable sample size of 477 works (Used advanced query: (ALL(GDPR) AND ALL (blockchain) AND ALL(review) AND PUBYEAR>2006 AND (LIMIT-TO(DOCTYPE,"ar")) AND (LIMIT-TO (LANGUAGE, "English")))). From the results, we identified the set of existing review and survey papers that most comprehensively cover the published literature on the relationship between blockchain technology and GDPR compliance; these papers are listed in Table 2.

The selection of the eight review and survey papers was purposive rather than exhaustive. The criterion was their relevance for mapping the blockchain–GDPR debate and their ability to represent different strands of the literature. This approach is appropriate for a meta-review and bibliometric mapping exercise, but it also limits the generalisability of our findings. To reduce selection bias, we leveraged the diversity of selection criteria already applied by the identified review papers by consolidating and deduplicating their reference lists across Scopus and WoS. After deduplication, this process yielded a final sample of 695 unique papers, which form the empirical basis of the analysis, while the cluster interpretation is based on the largest connected set of 125 items generated in VOSviewer.

The 695-paper sample was analysed using VOSviewer, a widely used tool for constructing and visualising bibliometric networks. Two complementary analytical methods were applied within it. Bibliographic coupling that identifies structural relationships between papers based on the proportion of references they share. Two papers are considered related when they frequently cite the same underlying literature, which signals thematic overlap even when direct citation links are absent. This method is suited to mapping the intellectual structure of a research field without relying on the assumption that related papers necessarily cite one another. Term co-occurrence analysis (or text-based analysis) extracts key terms from titles and abstracts of the sample papers and constructs a network in which nodes represent terms and edges reflect how often pairs of terms appear together across documents. This technique reveals the conceptual vocabulary of the field and highlights the thematic subdomains around which research has coalesced.

Both analyses were run simultaneously within VOSviewer using Paper as the unit of analysis for bibliographic coupling and Term as the unit of analysis for text-based analysis. The minimum cluster size was set to 10, and the analysis focused on the largest connected set. Visualisation parameters were set as follows: attraction = 2, repulsion = 1, and clustering resolution = 1. The resulting networks were then partitioned into clusters using VOSviewer's built-in clustering algorithm, which optimises modularity to identify groups of closely related items. The clustering algorithm partitioned the resulting network into six thematically coherent clusters, which emerged inductively from the co-occurrence and coupling patterns in the data. The six clusters identified in this way are visualised in Figure 2 and serve as the organising framework for the Results section. Each cluster is labelled according to the dominant thematic content of its constituent papers, as determined by the most frequently co-occurring terms within that cluster.

It should be noted that the analysis is based on bibliometric relationships rather than on full-text natural language processing (NLP). The term co-occurrence method operates on titles and abstracts only, which is the standard approach in large-scale bibliometric research and is consistent with the procedures adopted by the review papers from which the sample was drawn (see Table 2). Given that the objective of the analysis is to map the intellectual structure of the field rather than to derive causal inferences, we believe this scope is appropriate. The reviews we analyse are chosen with our own discretion, and as any other paper, we cannot guarantee an all-encompassing review. This is the greatest limitation of our research, as we cannot analyse entire fields' worth of literature.

Another limitation of our approach is that the bibliometric and term co-occurrence results were generated exclusively in VOSviewer. The analysis was not replicated in alternative tools. Future research could compare outputs across tools to test the robustness of the detected clusters. Nevertheless, we try to offer an as comprehensive and unbiased analysis of the discussions taking place in the world of FinTech, blockchain, and GDPR. We borrow from the creative idea of the Digital Finance Cube of Gomber et al. (2017), as opposed to the more standard summary approach to lit-

erature reviews. The results of the cluster analysis are presented and discussed in the Results section.

Results

As previously stated, the development of blockchain technologies is commonly traced to Nakamoto's (2008) Bitcoin white paper and the subsequent implementation of the Bitcoin blockchain in 2009. From then, blockchain exponentially gains traction both in scientific discussions and in actual related innovations. We have already singled out certain studies that have tried to aggregate and provide an overview of the literature at the time of their writing. They serve as great starting points for a certain perspective. What we try to do in this section is to provide an overview and map these perspectives. We wish to provide a sort of a meta-discussion that helps identify potential connections, issues, solutions, and sources of them in the process of integrating blockchain with GDPR.

We identify eight key papers as perspective-setters in this aspect. We began with a manual search for notable review works in the field. Specifically, we searched the Scopus and Web of Science (WoS) databases using multiple iterations and interactions of terms 'blockchain', 'GDPR', and 'review'. From the results we identified, we select the eight papers listed in Table 2 - we consider these to best cover the existing literature on the topic. This initial selection was based on our own judgement. Each of these papers applies its own selection criteria and data-gathering techniques; we choose to leverage this diversity by consolidating their reference lists from Scopus and WoS. After deduplication, this makes the final data of 695 unique papers that form the basis of our analysis.

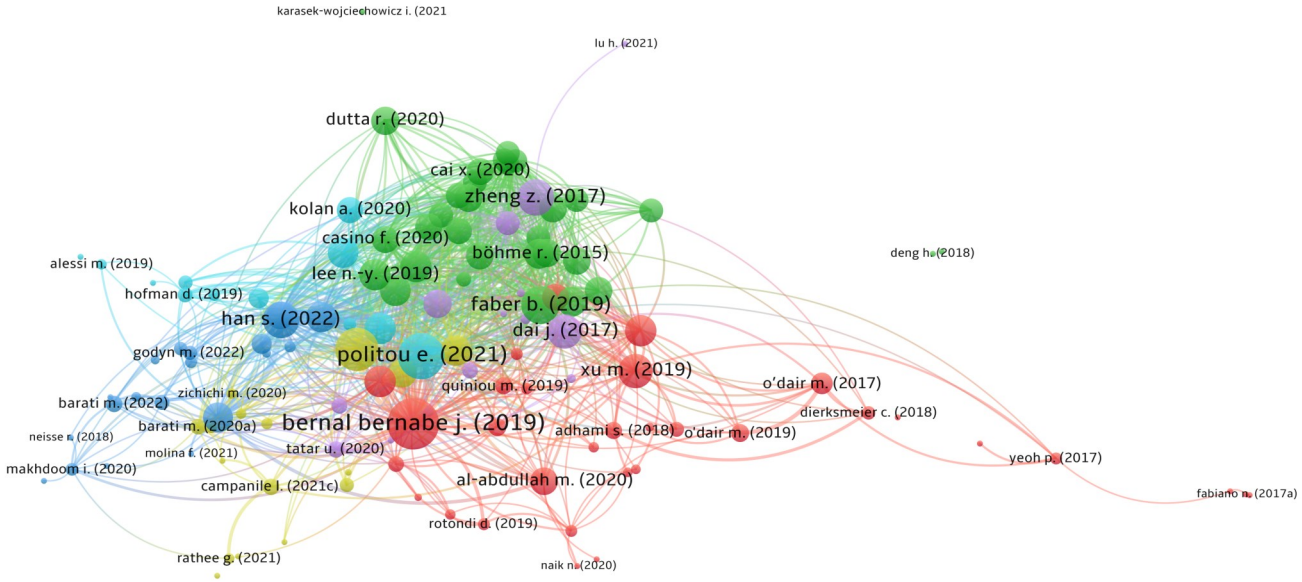
Our discussion so far has benefited greatly from these papers even if they were not directly cited. Of course, we cannot claim that these papers are the only notable ones, and they most certainly are not. We use bibliographic and text-based data to systematize the selected papers in two ways. We note which papers we select in Table 2. These eight papers cite 695 other unique works. Each of these 695 papers offers a perspective on its own, but by using bibliographic coupling and term co-occurrence analysis we are able to pinpoint a more precise location. These methods allow us to understand connections between different studies and to see how ideas within a large scope such as this one are related or grouped together.

Table 2: Systematic overview of selected research

Authors	Main Contributions
Yeoh (2017)	Issues in regulating disruptive blockchain technology implementations.
Bernabé et al. (2019)	Existing & potential privacy solutions for blockchain.
Politou et al. (2019)	Blockchain mutability challenges and resolutions.
Xu et al. (2019)	Cluster analysis of research themes in blockchain technologies.
Haque et al. (2021)	A list of blockchains semi-compliant with GDPR.
Godyn et al. (2022)	Overview of solutions for blockchain compliance with GDPR.
Han and Park (2022)	Gaps that remain in regulating blockchain with GDPR.
Belen-Saglam et al. (2023)	Points of conflict and potential solutions in mediating GDPR & blockchain.

Source: Author's own work.

Figure 2: Bibliographic coupling analysis



Source: Author's own work.

The bibliographic coupling analysis network plot is visible in Figure 2. Using the same data, the articles can be broadly classified into the following clusters.

1. Right to erasure, blockchain mutability, and information governance (cyan). The smallest cluster of 12 papers, primarily centred around Politou et al. (2019) with the largest link strength. They cover the ability to request the deletion of personal data. Solutions such as on-chain/off-chain data storage, cryptographic techniques like hash anonymization, and governance frameworks are this cluster's topics of discussion.
2. Blockchain architecture alternatives, case-studies of compliance solutions in different fields with GDPR (violet). Blockchain architecture alternatives offer various approaches to reconciling compliance with regulations like the GDPR. Case studies illustrate diverse applications: in healthcare, solutions like private blockchains emerge; in finance, hash-based techniques anonymize personal information to comply with erasure rights; and in supply chains, pseudonymization aids GDPR compliance without sacrificing traceability. Permissioned blockchains, for example, provide controlled access, allowing for greater flexibility in implementing data governance. Most notable articles in this cluster of 14 articles are Zheng et al. (2017) and Dai and Vasarhelyi (2017).
3. Integrating IoT, FinTech, and blockchain technologies (yellow). Real-time data collection, financial services, and secure decentralized systems are mainly discussed in this cluster with 16 articles. Stemming from Gomber et al. (2017), Truong et al. (2020) appears as the most linked to article. Articles on the synergy of these technologies mostly cover operational efficiency, how to foster trust in digital transactions, and how to drive new business models across industries.
4. Blockchain system changes to achieve compliance with GDPR (blue). In the 20 papers that construct this cluster, Belen-Saglam et al. (2023) and Haque et al. (2021) are the main sources along with Han and Park (2022) as an important centre point. Among others, these are further discussed in section 5.
5. Cryptocurrencies, smart contracts, applications of blockchain on data (green). This cluster contains 31 articles, out of which Dutta et al. (2020) and Faber et al. (2019) can be mentioned as most notable. Even beyond finance which is at our focus, blockchain's ability to securely store and verify data has potential for implementation in supply chain management, healthcare, and identity verification.
6. Privacy, identity management, data protection in blockchain-based technology (red). This cluster includes 32 remaining articles (It is necessary to state that this totals to 125 articles, which is also visible in figure 2. This set of articles is the largest connected set, and we deem it suitable for analysis as this set contains all of the articles that serve as original sources for the literature analyzed. The full network graph based on all observations before final deduplication is available upon request) out of which Bernabe et al. (2019) prevails as the node with the largest link strength. Alongside it, other remaining sources are all present, and Raikwar et al. (2019) and Treiblmaier (2018) are deemed to be the most linked to articles outside the starting 8 papers. Privacy, identity management, and data protection are central challenges in blockchain-based technologies, hence why this is the largest remaining cluster. By integrating methods these papers discuss, blockchain systems can better support privacy and data protection while preserving decentralization and security, aligning with GDPR as a regulatory framework.

This approach shows how different research streams frame the GDPR–blockchain compliance debate. More precisely, the tension between GDPR requirements and blockchain design features is at the core of our interest. Despite the extensive research on blockchain, there is still a noticeable gap in studies addressing practical solutions for GDPR compliance in blockchain applications. As Guo and Liang (2016) state, blockchain technology could be the long-awaited upgrade in terms of efficiency in the banking industry, but it needs not to be left to its own devices. Let us focus now on why some argue that may and may not be the case.

Discussion

The interaction between law and technology for the protection of privacy has been a subject of research since the 1960s (Bincoletto et al., 2021). In this context, many authors argue that blockchain technology may be technically difficult to reconcile with the right to erasure (Article 17. of the GDPR), right to rectification (Article 16 of the GDPR) and the right to object (Article 21. of the GDPR). The right of erasure, commonly known as a right to be forgotten, ensures individuals that can request deletion of their personal data, which right is a logical consequence of data minimization and data storage limitation GDPR principles.

Finck (2020) states that blockchain technologies challenge core assumptions of the European data protection law, such as data minimization and purpose limitation. To be in line with data minimization and data storage limitation principle, Data controllers must have procedures in place, identifying the legal basis and purposes of the data processing, data retention periods, locations of data processing, etc (see preamble, point 39. of the GDPR.). The right to be forgotten, due to blockchain immutability, is followed by right to rectification and right to object. The right to object (defined in the Article 21 of the GDPR) brought possibility to

data subject to request from the Data controller to stop processing data, unless Data controller is in a position to demonstrate compelling legitimate grounds for processing that override the interests, rights and freedoms of the Data subject (Finck, 2020). All rights seem to be challenging to implement in blockchain technologies, which conclusion was subject to European Data Protection Board Guidelines (2025). Analysed papers also showed that implementation of GDPR principles and Data subjects rights may face difficulties when personal data is stored in blockchain blocks. Even blockchain technology might face possible regulatory issues, it has numerous advantages. On that point, CNIL (French supervisory authority) published guidelines CNIL (2018) on using blockchain technology in the era of the GDPR and explained compatibility with GDPR in detail. Due to the technical nature of blockchain technology, in accordance with the CNIL guidelines, blockchain solutions are fully compliant with the information right of the Data subjects (article 13 and article 14 of the GDPR) and their right of access to the personal data and the right to portability.

Regarding possible issues in regulatory compliance due to the right to be forgotten, similar conclusions are stated in the Finck (2020) and Sangha et al. (2020) reports. The mentioned studies agree on the same point: the irreversibility character of blockchain technology conflicts with the right to erase or the right to modify personal data. But, although blockchain technology faces potential implementation challenges, Godyn et al. (2022) conclude that it is also possible to design blockchain technology in a way that it can fulfil the need for transparency. So, blockchain technology should not be a priori marked as GDPR noncompliant and rejected in general. The advantage of blockchain technology is immutability, but by GDPR entering into force it potentially becomes its disadvantage and leads to the question, by what means can it overcome such a serious conflict?

Blockchain and privacy by design

As an answer to the regulatory demands, legal practice developed the privacy by design approach, defined as stated by the author Bincoletto et al. (2021). It proposes building privacy principles and provisions into the design and architecture of ICTs to improve legal compliance. Privacy by design, in the opinion of Cavoukian et al. (2009) may consist of the following principles.

1. 'Proactive not reactive, Preventative not remedial'. Privacy risk should be identified in the design stage conducting privacy risk assessments.
2. 'Privacy as the Default Setting'. Personal data and business process shall be protected by default.
3. 'Privacy Embedded into design'. Privacy should be a fundamental concept implemented into design, without diminishing component functionality.
4. 'Full functionality – Positive-sum, not zero-sum'. Business interests should coexist with privacy.
5. 'End-to-end security – full lifecycle protection'. Privacy by design should be valid through entire data lifecycle;
6. 'Visibility and transparency – keep it Open'. The Data subject should be informed of the purposes of data processing in a clear and transparent way;
7. 'Respect for User Privacy – keep it User-Centric'. Business interest should not prevail over individual privacy interest.

Privacy by design (and by default) as a non-mandatory concept became mandatory on the day GDPR entered into force. Under GDPR Article 25 controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures which appropriateness is evaluated case by case. GDPR emphasized the need to embed privacy into the design and operation of IT systems, similarly to Cavoukian et al. (2009). It is worth noting that privacy by design is an adaptable concept and often is subject to modifications, regarding what business model or industry sector is it applied to. Agostinelli et al. (2019) state that privacy should be considered as a first-class citizen and should be introduced by design and not as an afterthought . One of the purposes of privacy by design is to mandate products and technologies are (from the start) made compliant with the GDPR. Certain industry sectors are more regulated than others, for example digital finance providers shall be compliant with Digital Operational Resilience Regulation (DORA) - 2022/2554/EU, Markets in Crypto-assets Regulation (MiCA) - 2023/1114/EU, the digital payment are subject to Cross-Border Payments Regulation - 924/2009/EC, E-Money Directive - 2009/110/EC, Payment Services Directive (PSD 2) - 2015/2366/EU, Payment Services Directive (PSD 1) 2007/64/EC, Single Euro Payments Area (SEPA) Regulation - 260/2012/EU. Enforcement of privacy by design demands knowledge and an understanding of the GDPR provisions and guidelines issued by working groups' supervisory authorities.

Compliance strategies for blockchain with GDPR

Several authors have discussed how regulatory vulnerabilities of blockchain technologies might be solved in part by privacy by design. Godyn et al. (2022) state that compliance with GDPR might be achievable, using a few different approaches (chameleon hash, a linkable digital multi-signature, the reconstructable

[1] https://finance.ec.europa.eu/regulation-and-supervision/financial-services-legislation/overview-financial-services-legislation (Accessed: 29.06.2024).

ephemeral key with proof of reduction, tree structure, reference-based tree structure, etc.). Among other options, Godyn et al. (2022) advocate for reference-based tree structure approach and the reference variation approach as tools with minimal weaknesses and maximum potential to achieve GDPR's requirements while reducing risks in implementation. To achieve compliance with the right to be forgotten, the reference variation approach is explained with a hypothetical scenario.

Consider three participants, A, B, and C (where C is not directly involved in this transaction). First, a transaction involving B is recorded in block α, and α is extracted to B's personal subchain, B'. Next, an agreement transaction between A and B is recorded in block β on the shared subchain A–B, with β explicitly referencing the earlier transaction in α. After B leaves the blockchain and the system state is observed to confirm consistency, a finalization block γ is added on A–B. At that point, the data in α on B' can be deleted without creating consistency errors. Following Godyn et al. (2022), the experiment is considered successful only if subchain B' is fully deleted. A known limitation of this approach is the extra time required to mine/finalize the additional blocks.

Motivated by the blockchain flaws, several authors recommend Unlichain as a universal blockchain architecture with unlimited data modification features, using a block indexing technique for an unlimited workload (Tulkinbekov & Kim, 2023). Unlichain's approach enables deletion of data with predefined retention periods. The authors explain that each node must agree to deletion in order to preserve system integrity. Comparing previously mentioned approaches, Unlichain's approach might be more convenient to achieve compatibility with the right to be forgotten and the right to modification. However, to the authors' best knowledge, there are not any empirical studies that prove such a point, although theoretically, Unlichain's approach might be one of solutions to be fully compliant, which brings us to the starting point- privacy (including retention periods) must form part of the business framework and be planned in advance.

Conclusions

In this paper, we examined the relationship between GDPR requirements and blockchain-based technologies, highlighting the inherent conflicts and potential reconciliation methods. Our literature review confirmed critical challenges, such as the immutability of blockchain conflicting with GDPR's right to erasure. As Johnson et al. (2023) state, there are consequences that emerge from intent, and there are ones that occur for other reasons. The intent of the GDPR is to safeguard personal data, so blockchain seems to be the logical answer to the data protection challenges, brought up with the GDPR and other sectoral cybersecurity regulations. Blockchain is a decentralized, shared, and replicated record of transactions that is (with time) synchronized across all participants (Treleaven et al., 2017).

Immutability and transparency, staples of blockchain, have proven to be its strong points as there are significant benefits of it in operational efficiency (Aste et al., 2017). In the work of Godyn et al. (2022) immutability and transparency are confirmed to be one of the main points of conflict with GDPR. Solutions for this, and other issues we list in subsection 5.2., constitute an entire cluster of research as we find in subsection 4.2. We deem this field should be expanded on much further in the future. We single out possible solutions to these issues and briefly discuss the reference-based tree structure and reference variation approaches alongside with the Unlichain's approach.

The application of GDPR requirements to blockchain-based systems remains challenging because appropriate technical and organisational measures must be designed before personal data are processed. However, GDPR entered into force to protect personal data from unauthorized use, so it is not surprising that blockchain-based technologies are according to Sangha et al. (2020) called custodians of trust. In conclusion, despite the limitations that this, and every review study inevitably faces as we have to draw the line somewhere we trust that the future researchers will fill in the gaps we leave behind.

We call for more case-by-case studies focusing on really specific issues and solutions. However, while specific, they should not be bound to a single cluster. Future research should investigate the practical implementation of reference-based tree structures in live blockchain environments and explore alternative solutions that could offer greater flexibility and compliance. Additionally, interdisciplinary studies involving legal experts, technologists, and data protection authorities are essential to develop holistic solutions. This paper contributes to the ongoing discourse on data protection and blockchain by providing a comprehensive review of existing literature and proposing practical solutions for GDPR compliance. Our approach bridges the gap between regulatory requirements and technological capabilities. We argue that only with such discussions progress in reconciling blockchain with GDPR can be made. While challenges remain, the progress achieved thus far provides a solid foundation for future research.

References

Adrian, T. & Mancini-Griffoli, T. (2021). The rise of digital money. Annual Review of Financial Economics, 13, 57–77. https://dx.doi.org/10.1146/annurev-financial-101620-063859.

Agostinelli, S., Maggi, F.M., Marrella, A. & Sapio, F. (2019). Achieving GDPR compliance of BPMN Process Models. Responsible Information Systems: CAiSE Forum. Springer, Berlin.

Altman, E.I., Balzano, M., Giannozzi, A. & Srhoj, S. (2023). The omega score: An improved tool for SME default predictions. Journal of the International Council for Small Business, 4(4), 362–373. https://dx.doi.org/10.1080/26437015.2023.2186284.

Arner, D. W., Barberis, J. & Buckley, R.P. (2017). FinTech and RegTech in a Nutshell, and the Future in a Sandbox. CFA Institute Research Foundation, New York.

Aste, T., Tasca, P. & Di Matteo, T. (2017). Blockchain technologies: The foreseeable impact on society and industry. Computer, 50(9), 18–28.

Belen-Saglam, R., Altuncu, E., Lu, Y. & Li, S. (2023). A systematic literature review of the tension between the GDPR and public blockchain systems. Blockchain: Research and Applications, 4(2), 100-129. https://dx.doi.org/10.1016/j.bcra.2023.100129.

Bernabe, J.B., Canovas, J.L., Hernandez-Ramos, J.L., Moreno, R.T. & Skarmeta, A. (2019). Privacy-preserving solutions for blockchain: Review and challenges. IEEE Access, 7, 164908–164940. https://dx.doi.org/10.1109/ACCESS.2019.2950872.

Bincoletto, G. (2021). Data Protection by Design in the E-health Care Sector: Theoretical and Applied Perspectives (Vol. 22). Nomos Verlagsgesellschaft, Baden.

Campbell, J., Goldfarb, A. & Tucker, C. (2015). Privacy regulation and market structure. Journal of Economics & Management Strategy, 24(1), 47–73. https://dx.doi.org/10.1111/jems.12079.

Cavoukian, A. (2009). Privacy by design: The 7 foundational principles. Information and Privacy Commissioner of Ontario, Canada, 5(2009), 12-37.

Commission Nationale de l'Informatique et des Libertés. (2018). Blockchain and the GDPR: Solutions for a responsible use of the blockchain in the context of personal data. https://www.cnil.fr/en/blockchain-and-gdpr-solutions-responsible-use-blockchain-context-personal-data (Accessed: 29.06.2024).

Dai, J. & Vasarhelyi, M.A. (2017). Toward blockchain-based accounting and assurance. Journal of Information Systems, 31(3), 5–21. https://dx.doi.org/10.2308/isys-51804.

Dutta, R., Das, A., Dey, A. & Bhattacharya, S. (2020). Blockchain vs GDPR in Collaborative Data Governance. Cooperative Design, Visualization, and Engineering: 17th International Conference. Springer, Berlin.

Efanov, D. & Roschin, P. (2018). The All-Pervasiveness of the Blockchain Technology. Procedia Computer Science, 123, 116–121. https://dx.doi.org/10.1016/j.procs.2018.01.019.

European Data Protection Board. (2025). Guidelines 02/2025 on processing of personal data through blockchain technologies [Draft]. https://www.edpb.europa.eu/system/files/2025-04/edpb_guidelines_202502_blockchain_en.pdf (Accessed: 29.06.2024).

Faber, B., Michelet, G., Weidmann, N., Mukkamala, R.R. & Vatrapu, R. (2019). Bpdims: A Blockchain-based Personal Data and Identity Management System. The 52nd Hawaii International Conference on System Sciences. HISS, Hilton Waikoloa Village.

Finck, M. (2020). Blockchain and the General Data Protection Regulation: can distributed ledgers be squared with European data protection law? European Parliament, Brussel.

Gal, M.S. & Aviv, O. (2020). The competitive effects of the GDPR. Journal of Competition Law & Economics, 16(3), 349–391. https://dx.doi.org/10.1093/joclec/nhaa012.

Goddard, M. (2017). The EU General Data Protection Regulation (GDPR): European regulation that has a Global Impact. International Journal of Market Research, 59(6), 703–705. https://dx.doi.org/10.2501/IJMR-2017-050.

Godyn, M., Kedziora, M., Ren, Y., Liu, Y. & Song, H.H. (2022). Analysis of solutions for a blockchain compliance with GDPR. Scientific Reports, 12(1), 15-21. https://dx.doi.org/10.1038/s41598-022-19341-y.

Goldberg, S.G., Johnson, G.A. & Shriver, S.K. (2024). Regulating Privacy Online: An Economic Evaluation of the GDPR. American Economic Journal: Economic Policy, 16(1), 325–358. https://dx.doi.org/10.1257/pol.20210309.

Gomber, P., Koch, J.A. & Siering, M. (2017). Digital finance and fintech: current research and future research directions. Journal of Business Economics, 87, 537–580. https://dx.doi.org/10.1007/s11573-017-0852-x.

Guo, Y. & Liang, C. (2016). Blockchain application and outlook in the banking industry. Financial Innovation, 2, 1–12. https://dx.doi.org/10.1186/s40854-016-0034-9.

Han, S. & Park, S. (2022). A Gap Between Blockchain and General Data Protection Regulation: A Systematic Review. IEEE Access, 10, 103888-103905. https://dx.doi.org/10.1109/ACCESS.2022.3210110.

Haque, A.B., Islam, A.N., Hyrynsalmi, S., Naqvi, B. & Smolander, K. (2021). GDPR Compliant Blockchains-A Systematic Literature Review. IEEE Access, 9, 50593–50606. https://dx.doi.org/10.1109/ACCESS.2021.3069877.

Johnson, G.A., Shriver, S.K. & Goldberg, S.G. (2023). Privacy and market concentration: Intended and unintended consequences of the GDPR. Management Science, 69(10), 5695–5721. https://dx.doi.org/10.1287/mnsc.2023.4709.

Kavuri, A. & Milne, A. (2018). Fintech and the Future of Financial Services: What are the Research Gaps? SSRN Working Paper. https://dx.doi.org/10.2139/ssrn.3215849.

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf (Accessed: 29.06.2024).

Philippon, T. (2016). The FinTech Opportunity (No. w22476). National Bureau of Economic Research, Cambridge. https://dx.doi.org/10.3386/w22476.

Politou, E., Casino, F., Alepis, E. & Patsakis, C. (2019). Blockchain mutability: Challenges and proposed solutions. IEEE Transactions on Emerging Topics in Computing, 9(4), 1972–1986. https://dx.doi.org/10.1109/TETC.2019.2949510.

Raikwar, M., Gligoroski, D. & Kralevska, K. (2019). Sok of Used Cryptography in Blockchain. IEEE Access, 7, 148550–148575. https://dx.doi.org/10.1109/ACCESS.2019.2946983.

Sangha, P., Pureswaran, V. & Soman, S. (2020). Advancing global trade with blockchain: How to unleash value from trusted, interconnected marketplaces. BM Institute for Business Value. https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/blockchain-global-trade (Accessed: 29.06.2024).

Treiblmaier, H. (2018). The Impact of the Blockchain on the Supply Chain: a Theory-Based Research Framework and a Call for Action. Supply Chain Management: An International Journal, 23, 545–559. https://dx.doi.org/10.1108/SCM-01-2018-0029.

Treleaven, P., Brown, R.G. & Yang, D. (2017). Blockchain Technology in Finance. Computer, 50(9), 14–17. https://dx.doi.org/10.1109/MC.2017.3571047.

Truong, N.B., Sun, K., Lee, G.M. & Guo, Y. (2020). GDPR-Compliant Personal Data Management: A Blockchain-based Solution. IEEE Transactions on Information Forensics and Security, 15, 1746–1761. https://dx.doi.org/10.1109/tifs.2019.2948287.

Tulkinbekov, K. & Kim, D.H. (2023). Data Modifications in Blockchain Architecture for Big- Data Processing. Sensors, 23(21), 62-87. https://dx.doi.org/10.3390/s23218762.

Van Ooijen, I. & Vrabec, H.U. (2019). Does the GDPR Enhance Consumers' Control over Personal Data? An Analysis from a Behavioural Perspective. Journal of Consumer Policy, 42, 91–107. https://dx.doi.org/10.1007/s10603-018-9399-7.

Wloczka, R. (2024). Markets in Crypto-assets (MiCA)–New EU law on crypto-assets. Access: https://www.twobirds.com/en/insights/2024/global/markets-in-crypto-assets-new-eu-law-on-crypto-assets (Accessed: 29.06.2024).

Xu, M., Chen, X. & Kou, G. (2019). A systematic review of blockchain. Financial Innovation 5(1), 1–14. https://dx.doi.org/10.1186/s40854-019-0147-z.

Yaga, D., Mell, P., Roby, N. & Scarfone, K. (2019). Blockchain Technology Overview. Retrieved from http://arxiv.org/abs/1906.11078

Yeoh, P. (2017). Regulatory issues in blockchain technology. Journal of Financial Regulation and Compliance, 25(2), 196–208. https://dx.doi.org/10.1108/JFRC-08-2016-0068.

Zheng, Z., Xie, S., Dai, H., Chen, X. & Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends. 2017 IEEE international congress on big data (BigData congress). IEEE, New York.