European Union Data Act and Blockchain Technology: Challenges and New Directions

Luca Olivieri[1], Luca Pasetto[2], Luca Negrini[1] and Pietro Ferrara[1]

[1]Department of Environmental Sciences, Informatics and Statistics, Ca' Foscari University of Venice, Venice, Italy
[2]Department of Computer Science, University of Luxembourg, Esch-sur-Alzette, Luxembourg

Abstract

The European Union Data Act has been in force since 11 January 2024 to regulate the access and use of data and promote a more fair data sharing within the European Economic Area. This regulation could significantly impact blockchain technology, which can facilitate the secure exchange of data, leading to greater transparency, accountability, and auditability. However, compliance with the European Union Data Act may necessitate that blockchain solutions be adjusted accordingly. This paper aims at investigating the applicability and compatibility of blockchain technology with the European Union Data Act context, also considering aspects relevant for other related European regulations, directives, and strategies.

Keywords

EU Data Act, Blockchain Strategy, distributed ledger technology, blockchain, smart contracts, interoperability, data sharing, GDPR, compliance, data privacy

1. Introduction

Nowadays, the data landscape continues to gain complexity. It led the European Commission to question the ethical, legislative, and commercial implications of this sudden growth. Therefore, the *European Union Data Act* [1] (EU Data Act) has been in force to add new rules and encourage the use of data and ensure it is shared, stored, and processed in full respect of European rules [2]. In particular, among the several topics covered, the document promotes the interoperability of tools for the automated execution of data-sharing agreements, and it suggests the adoption of smart contracts that may be connected to an electronic ledger [1, Whereas point (104)]. Regarding the latter, *Distributed Ledger Technology* (DLT) could be suitable for this purpose, given the incredible popularity of blockchain implementations. Moreover, the European Commission considered blockchain a strategic technology that could revolutionize how we share information and carry out online transactions [3]. This paper aims to investigate blockchain technology's applicability and compatibility with the EU Data Act, considering data protection aspects relevant for the *Blockchain Strategy* [3] of the European Commission.

Contributions In this paper, we make the following contributions:

- a comprehensive summarization of the EU Data Act and the related European regulations, directives, and strategies;
- an investigation on the implications of the EU Data Act on data usage and data sharing within the blockchain ecosystem;
- an examination of essential requirements regarding smart contracts for EU Data Act compliance;
- an analysis related to the concept of interoperability for the EU Data Act and blockchain technology.

6th Distributed Ledger Technologies Workshop (DLT 2024), May, 14-15 2024 – Turin, Italy
luca.olivieri@unive.it (L. Olivieri); luca.pasetto@uni.lu (L. Pasetto); luca.negrini@unive.it (L. Negrini); pietro.ferrara@unive.it (P. Ferrara)
0000-0001-8074-8980 (L. Olivieri); 0000-0003-1036-1718 (L. Pasetto); 0000-0001-9930-8854 (L. Negrini); 0000-0002-4678-933X (P. Ferrara)

Paper structure Section 2 provides an overview of the European Union Data Act. Section 3 introduces preliminary and background notions related to Distributed Ledger Technology and blockchain. Section 4 summarizes the blockchain strategy designed by the European Commission. Section 5 investigates the blockchain benefits and pitfalls for the EU Data Act compliance and European blockchain strategy suitability. Section 6 deals with blockchain smart contract compliance with the EU Data Act. Section 6 describes challenges related to blockchain interoperability. Section 8 provides a high-level overview of blockchain industry concerns related to the EU Data Act. Section 9 reports related work. Section 10 concludes the paper.

2. European Union Data Act

The EU Data Act is a document composed of 11 chapters and 50 articles on *harmonised rules on fair access to and use of data*. As reported by official channels [4], the EU Data Act also introduces measures to protect European businesses from unfair contractual practices, thereby fostering fairer negotiations and boosting the confidence of small and medium-sized enterprises in the digital market.

The European Union Data Act has been in force since 11 January 2024 [4], and its application is scheduled for 12 September 2025 [1, Article 50]. According to the European Commission [5], the EU Data Act complements the *Data Governance Act* [6, 7] and clarifies who can create value from data and under which conditions, where data means *"any digital representation of acts, facts or information and any compilation of such acts, facts or information, including in the form of sound, visual or audio-visual recording"* [1, Article 2, point (1)]. It also derives from the *European Data Strategy* [8, 9] and aims to position Europe as the leader in the data economy by harnessing the potential of the ever-increasing amount of industrial data to benefit the European economy and society [9].

Although the EU Data Act amends a previous directive [10] and regulation [11], it is not intended to replace all other previous directives and regulations such as the well-known *General Data Protection Regulation* [12] (GDPR). Indeed, EU Data Act *"is without prejudice to Union and national law on the protection of personal data, privacy and confidentiality of communications and integrity of terminal equipment, which shall apply to personal data processed in connection with the rights and obligations laid down herein [...], including the powers and competences of supervisory authorities and the rights of data subjects"* [1, Article 1 (5)]. For instance, compared to the GDPR, the EU Data Act is more comprehensive and is applied to both personal and non-personal data, including the relevant metadata[1] necessary to interpret and use such data. At the same time, the GDPR is focused only on personal data. However, the definitions of personal and non-personal data reported in the EU Data Act [1, Article 2, points (3) and (4)] explicitly refer to those defined into the GDPR [12, Article 4, point (1)]. Moreover, no provision of the EU Data Act should be applied or interpreted in such a way as to diminish or limit the right to the protection of personal data or the right to privacy and confidentiality of communications [1, Whereas point (7)].

3. DLT and Blockchain

Traditionally, a ledger is a physical book or document where *transactions* are manually recorded to keep track of data changes. An electronic ledger, also known as a *digital ledger*, is a digitalized version of a traditional ledger that leverages information technology to create, store, and manage records in digital format. A *distributed ledger* is a type of electronic ledger distributed across multiple locations or participants in a network. Unlike traditional centralized electronic ledgers, typically controlled by a single entity or organization, distributed electronic ledgers are also decentralized and often maintained by a network of computers or nodes. Note that transactions do not necessarily have a financial purpose or require transaction fees.

[1] In EU Data Act, metadata is *"a structured description of the contents or the use of data facilitating the discovery or use of that data"* [1, Article 2, point (2)].

In recent years, DLT has received growing attention for its suitability to a large number of application fields (e.g., finance [13], supply chain management [14], IoT [14], healthcare [15], scientific data dissemination [16], ...). The most well-known form of DLT is undoubtedly the blockchain. In a nutshell, it is a shared abstract data structure composed of a chain of blocks and based on a distributed ledger. Typically, each block contains a certain bounded amount of data records (new data, data changes, ...), the *hash* of the previous block, the *hash* of the block itself, and a creation *timestamp*, where a *hash* is a number obtained by applying a collision-free function [17] to the content of a block. The idea is to concatenate each block with its predecessor to obtain a chain of linked blocks that preserve the integrity of data and the chronological order of changes, using the hash information and timestamp information respectively. Verifying the integrity of data stored in the blockchain thus boils down to recomputing the chain of hashes, and checking if it corresponds to the ones stored in the blockchain. In this way, tampering a block will cause a mismatch between the hashes stored in the blocks and the recomputed ones, making it immediately clear that the chain has been altered. In addition, this data structure is typically shared in a peer-to-peer network located in a heterogeneous geographical area, where peers can keep a redundant copy (full or partial) and approve transaction requests to add new data through a consensus mechanism based on a reward/disincentive systems (e.g., *Proof-of-Work*, *Proof-of-Stake*, ...), to reach a consensus on a single state within the network. The anti-tampering data structure combined with the redundant copies collected by peers belonging to a heterogeneously geolocalized network and the consensus mechanism makes the data stored into the blockchain *immutable*, *distributed* and *decentralized*. The consensus mechanism also allows the blockchain to be byzantine fault tolerant [18], and to be applied in *trustless*[2] contexts without being required to trust third-party intermediaries or individual peers.

Typically, blockchain networks are divided into *permissioned* and *permissionless*. The distinction is due to how the network is designed based on access, visibility, restriction, and consensus validation criteria. In the case of permissioned blockchain, access to the network and the ability to participate in the consensus process are restricted to a specific group of participants, and it is possible to perform operations through network governance. Moreover, this subset of peers also typically has the power to propose a plan for modifying, stopping, and restarting the blockchain with updated software, carefully migrating the state of the previous version [19]. Typically, permissioned blockchains are widely used in the industrial context to create private and consortium blockchains. A notable example of a permissioned blockchain is Hyperledger Fabric [20, 21]. In the case of permissionless blockchain, anyone can access and join the network, validate transactions, and participate in the consensus process without needing prior approval or identity verification/authentication. However, in this case, maintenance can only be performed on-chain, as no high-level entity governs the entire blockchain, and each request must go through the consensus mechanism. Permissionless blockchains are commonly used for cryptocurrencies and decentralized finance (DeFi). Notable examples of permissionless blockchains are Bitcoin [13, 22] and Ethereum [23, 24].

Blockchain can also support *smart contracts*, i.e., computer programs that can be deployed, even immutably, and deterministically executed within the blockchain thanks to transaction requests recorded in the ledger. Smart contracts can be exploited in a wide variety of use cases. For instance, a smart contract can automate tasks, implement business and application logic, create and manage a decentralized autonomous organization (DAO), or move economic assets.

In 2008, Bitcoin [13, 22] proposed the first blockchain smart contracts. They are written in a Turing-incomplete low-level language that specifies Bitcoin's transactions, that can be seen as a limited scripting language for smart contracts. In 2013, Ethereum [23, 24] introduced a Turing-complete bytecode for smart contracts for developing decentralized applications. Ethereum smart contracts can be programmed in high-level domain-specific languages, with Solidity being the most popular one, and run on the Ethereum virtual machine. The creation of a Turing-complete language is a milestone as smart contracts can achieve the complexity and potential of modern programming languages. Subsequently,

[2]Trustless does not mean complete removal of trust, but rather its distribution in a type of economy that encourages specific behaviors and punishes others.

the blockchain industry also moved to the implementation of smart contracts with general-purpose languages, although they introduced additional issues [25].

4. Blockchain Strategy of the European Commission

The blockchain is considered a strategic technology by the European Commission, that wants Europe to become a leader in blockchain technology and home to significant platforms, applications, and companies [3]. In this regard, the European Commission designed a blockchain strategy [3] to meet these goals, supporting a *"gold standard"* for blockchain technology in Europe that embraces European values and ideals in its legal and regulatory framework. The objectives of this standard have different purposes (i.e., *environmental sustainability*, *data protection*, *digital identity*, *cybersecurity*, and *interoperability*) and the European Commission strongly supports blockchain on the policy, legal and regulatory, and funding fronts. The Commission's strategy include *building a pan-European public services blockchain*, *promoting legal certainty*, *increasing funding for research and innovation*, *promoting blockchain for sustainability*, *supporting interoperability and standards*, *supporting blockchain skills development*, and *interacting with the community*.

5. Benefits and Pitfalls of Blockchain for the EU Data Act

According to the European Commission, blockchain technology should be compatible with, and where possible support, Europe's strong data protection and privacy regulations [3]. However, it is necessary to investigate the limits and potential of this technology to avoid misusing it and incurring penalties [1, Article 40]. For this reason, in this section, we highlight the benefits and pitfalls of blockchain in the context of the EU Data Act and the European Blockchain Strategy.

5.1. Benefits

In the following, we explore the benefits and advantages of leveraging blockchain technology for EU Data Act compliance solutions.

Data Transparency, Integrity, Auditability and Accountability Blockchain technology immutably records transactions or data that are transparently shared between peers in the network. This transparency can improve compliance with the GDPR's principles of accountability and transparency [12, Articles 13, 14, and 24]. Moreover, immutability allows the integrity of the data to be maintained, avoiding data corruption. Hence, the blockchain can also serve as an audit trail [12, Article 28], providing a transparent and tamper-proof record of data processing activities by allowing data subjects to verify how their personal data is processed or moved, such as documenting data processing activities and demonstrating compliance with data protection principles.

Trustlessness According to the European Commission [3], blockchain technology allows people and organizations who may not know or trust each other to collectively agree on and permanently record information without a third-party authority. By creating trust in data in ways that were not possible before, blockchain has the potential to revolutionize how we share information and carry out transactions online.

Selective Disclosure of Information Blockchain technology can be compatible with zero-knowledge proofs [26] and other privacy-enhancing techniques. These features may require a lot of effort and the introduction of off-chain components into the system. However, they can bring various benefits such as enabling users to prove certain statements about data without revealing the underlying data itself, thus reducing the exposure of sensitive information and avoiding leaking any private transaction data. This principle can be implemented, for instance, through new digital identity paradigms such

as *self-sovereign identity* [27], where people and organizations have complete control over their data, allowing them to manage and share their identity information without relying on centralized authorities or intermediaries and without disclosing the sensitive data. Not by chance, the design of a *"gold standard"* by the European Commission includes blockchain compatibility with electronic signature regulations, such as eIDAS, and support for a reasonable, pragmatic, decentralized, and self-sovereign identity framework [3].

Automatic Payments and Cost Reduction The EU Data Act includes providing reasonable compensation for costs incurred to make data available [1, Article 9], such as technical costs (e.g., for data reproduction, dissemination, ...) and costs of facilitating concrete data sharing (e.g., data processing for data availability, data formatting, ...). Compensation is also provided in case of exceptional need, and it shall cover the technical and organizational costs incurred to comply with the request, including, where applicable, costs of anonymization, pseudonymization, aggregation, and technical adaptation and a reasonable margin [1, Article 20]. Moreover, the EU Data Act suggests the use of smart contracts to reduce the costs in regular or repetitive transactions in business relationships for long-term arrangements between data holders and data recipients [1, Whereas point (47)].

Blockchain technology offers several benefits in this context. Blockchain payments can significantly reduce transaction costs by eliminating intermediary fees related to banks or payment processors. Every transaction is provided in a transparent and immutable way since all payment activities can be recorded on the distributed ledger. Blockchain-based payment systems can also facilitate almost instantaneous transactions, operating 24 hours a day, allowing users to send and receive instant payments at any time without taking days to settle, as it happens with traditional banks or international wire transfers. Moreover, self-executing blockchain smart contracts with the terms of the agreement directly written into code can automate payment processes based on predefined conditions. This eliminates the need for manual intervention and reduces the risk of errors, delays, and disputes in payment settlements.

However, exchanged assets for payments require to be compliant with the *Cryptocurrency Markets Regulation* [28] (MiCA) and the smart contracts need to be compliant with the EU Data Act definition (see Section 6).

5.2. Pitfalls

We now delve into the potential pitfalls of integrating blockchain technology with EU Data Act compliance solutions.

Data Minimisation EU Data Act recalls the principles of data minimization and data protection by design and by default of GDPR [12, Articles 5 and 25], when processing involves significant risks to the fundamental right of individuals [1, Whereas point (8)]. However, as reported in Section 2, the EU Data Act is broad and not limited to personal data only. Furthermore, it requires avoiding *"unnecessary copying of the raw or structured data"* [1, Whereas point (8)]. The data minimization principle may not align with blockchain technologies, potentially limiting its scope. Indeed, the blockchain needs to distribute the data in redundant copies between different network peers. Such copies could not adapt to the claim *"unnecessary coping"* provided by the EU Data Act if not motivated by the fact that the greater the number of copies and peers, the more the integrity and availability of the data is preserved. Therefore, depending on the use case, there may be a different trade-off between the level of security required and the number of redundancy copies in the network.

Data Erasing EU Data Act provides that a third party or data recipient shall comply, without undue delay, to erase data made available by the data holder and any copies thereof in specific circumstances (unlawfully disclosed data, provided false information to a data holder, data usage for unauthorized purposes, ...) [1, Article 11, paragraphs 2 and 3]. In addition, a cornerstone of the processing of personal data is the *right to erasure* [12, Article 17] (aka *"right to be forgotten"*). Then, the EU Data Act must grant individuals the right to have their data erased under these circumstances. However, given blockchain's

data immutability, this could pose a conflict in real scenarios that make it challenging to comply with the right to erasure.

Data Responsabilities Different actors are involved in data protection and data sharing processing. The EU Data Act requires separating the different roles of actors involved in the data-sharing workflow. However, in the blockchain network, the decentralized nature blurs these distinctions, making it challenging to identify the entities responsible for complying with obligations. According to Finck [29, 30], to identify the actors determining the purposes and means of data processing in a specific use case, it is not only necessary to consider the specificities of that use case and how personal data is handled, but moreover to carefully examine the governance design of a given blockchain. Indeed, permissioned and permissionless blockchains differ on this aspect. In the first case, there is generally a determined legal entity (such as a company or a consortium) that determines the means and in many cases also the purposes of personal data processing [29, Section 4.3.1]. In the second case it becomes necessary to determine controllership at the infrastructure level, contextualizing case-by-case, and it is challenging. According to Finck [29], it is important to stress that the identity of the data controller depends on the perspective that is adopted. For instance, Finck [29, Section 4.3.2] suggests that, from a macro-level, the purpose of processing is to *"provide the associated service"* (such as a Bitcoin transaction) whereas the *"means"*" related to the software used by nodes and *miners*[3] [31]. From a micro-perspective (that is to say the individual transaction) the purpose of processing is *"to record a specific transaction onto a blockchain"* whereas the means refer *"to the choice of the blockchain platform"* [31]. Arguably, the micro-level is the more appropriate approach as data protection law deals with specific items of personal data [31].

Data Disclosure outside the European Economic Area For personal data transferring, restrictions can be applied to countries outside the European Economic Area (EEA) that do not ensure an adequate standard of data protection [12, Chapter 5]. Hence, ensuring compliance with these restrictions can be complex if a blockchain network is too heterogeneously geolocalized or globally distributed. Moreover, it also depends on where users access the data. For instance, in permissioned settings, these issues can be solved or mitigated since subjects that operate the nodes decides where to put them and the governance system can apply access restrictions to users and blockchain peers. However, in permissionless settings, it is not possible to have guarantees on the location of the nodes, which is also irrelevant since data can be accessed from anywhere by anyone and, depending to the blockchain, also in an anonymous way.

6. Blockchain and EU Data Act Smart Contracts

According to Antonopoulos [24], the term *smart contract* has been used to describe a wide variety of different concepts. In this section, we analyze three definitions of smart contracts:

Definition 6.1 (Traditional Smart Contract)**.** A smart contract is *"a set of promises, specified in digital form, including protocols within which the parties perform on the other promises"* [24, 32].

Definition 6.2 (Blockchain Smart Contract)**.** A smart contract is a *"computer program that can be deployed, even immutably, and deterministically executed within the blockchain thanks to transaction requests recorded in the ledger"* (see Section 3).

Definition 6.3 (EU Data Act Smart Contract)**.** A smart contract is *"a computer program used for the automated execution of an agreement or part thereof, using a sequence of electronic data records and ensuring their integrity and the accuracy of their chronological ordering"* [1, Article 2 point (39)].

Their original meaning of agreement between the parties suggested by the definition 6.1 is nowadays blurred, given the genericity of the software within modern blockchains, especially after adopting

[3] Actors involved in Proof-of-Work consensus (e.g. adopted in Bitcoin). A miner competes with other miners to append blocks and mine new currency, each miner experiencing a success probability proportional to the computational effort expended.

Turing-complete languages for blockchain smart contracts. Indeed, the definition 6.2 generalizes the concept to computer programs without adding parties or promises to the meaning. Regarding to the definition 6.2, EU Data Act claims that it is *technologically neutral* [1, Whereas point (104)] (see Section 8). However, definition 6.2 is close both to definition 6.1 and definition 6.3. Indeed, both definitions 6.1 and 6.3 recall interactions with parties, while definitions 6.2 and 6.3 refer to computer programs and require ensuring the integrity and chronological order of records. In particular, blockchain ensures integrity thanks to its tamper-proof construction, and it also collects the timestamps of blocks when contracts are deployed or executed through transaction requests recorded in the ledger. Moreover, the legal component is absent in the three definitions. Therefore, in the blockchain context, smart contracts that can comply with the EU Data Act definition are only a subset of all the possible contracts that developers can create: only the ones where there is a prior agreement between parties.

However, the main challenge for blockchain smart contracts to fit EU Data Act compliance is not in its definition but rather in the essential requirements that must be met for executing data sharing agreements [1, Article 36, paragraph 1]. In the EU Data Act, requirements are reported as follows:

1. ***robustness and access control***, to ensure that the smart contract has been designed to offer access control mechanisms and a very high degree of robustness to avoid functional errors and to withstand manipulation by third parties;
2. ***safe termination and interruption***, to ensure that a mechanism exists to terminate the continued execution of transactions and that the smart contract includes internal functions which can reset or instruct the contract to stop or interrupt the operation, in particular to avoid future accidental executions;
3. ***data archiving and continuity***, to ensure, in circumstances in which a smart contract must be terminated or deactivated, that there is a possibility to archive the transactional data, smart contract logic, and code in order to keep the record of operations performed on the data in the past (auditability);
4. ***access control***, to ensure that a smart contract is protected through rigorous access control mechanisms at the governance and smart contract layers;
5. ***consistency***, to ensure consistency with the terms of the data-sharing agreement that the smart contract executes.

We focus the discussion of the first requirement on *robustness* only, as we will discuss *access control* with the fourth requirement. We recall that smart contracts typically become immutable after being deployed in the blockchain, and therefore, they are resistant to manipulation by third parties. However, program development is an error-prone process, and if immutable programs are not adequately checked, this may lead to errors, bugs, and vulnerabilities that are immutable as well. For this reason, the adoption of blockchain is not sufficient to guarantee robustness completely, and a strong component of program verification techniques is required. In particular, program static analysis can help programmers detect issues early in code development, before deployment (and thus before it becomes immutable). Moreover, it can be combined with formal methods (see, for instance, [33], [34], [35]) to provide mathematical guarantees on the analyzed programs, such as ensuring the absence of functional errors in the context of data sharing.

Concerning the second requirement, we recall that the halting problem [36] is undecidable in computer science for non-trivial programs written in Turing complete languages. That is, for all possible inputs of a program, one cannot precisely determine whether the execution will end or not. Thus, it is not possible to generally prove *safe termination* without specific mechanisms or conditions. In the blockchain context, the concept of *gas* is typically used to ensure the termination of smart contracts: when a contract is executed, it also sets an amount of gas consumed while executing its instructions. If the gas is depleted before the execution is completed, then termination is forced, leading to a failure error and roll-back of the blockchain state before execution. The correct functioning of the gas mechanism and the absence of gas issues can be proven with formal techniques. For instance, it is possible to ensure the termination of smart contracts executions concerning the gas model [37], to infer sound bounds

on gas consumption [38], and also to detect *out-of-gas* behavior due to gas limit caps related to smart contract execution [38]. Regarding the requirements for interruption or a temporary stop of an ongoing transaction, since each transaction is executed atomically, it is impossible to revert it after its approval. However, some workarounds permit code inside a contract to specify exceptions to its execution. For what regards *interruption* or reset operations to avoid accidental executions, there are already blockchain smart contracts [39, 40] that support these concepts or that can be exploited to create a *"kill switch"*, but there exist no standards or official European guidelines yet.

Regarding the third requirement, *data archiving and continuity*, a blockchain is based on a distributed and decentralized network where each peer keeps a redundant copy of the blockchain. Then, data is accessible from different peers in different locations that keep records of past data operations, avoiding the problem of single points of failure. In addition, blockchain can also be enriched with off-chain data storage, or can exploit sidechains [41].

Concerning the fourth requirement, *access control* can always be enforced at the smart contract layer, by adding conditional statements that are satisfied only when executed by specific users, or with conditions that can be changed over time. Governance strictly depends on the type of blockchain network. In permissioned blockchains, it is explicitly possible to set up governance on different levels, for instance, by setting up a consortium [42], sub-networks, or private collections [43] for transmitting sensitive data. Instead, in the case of permissionless blockchains, given its nature, there are no permissions or restrictions to the use of the blockchain, and there is no governance layer for the entire blockchain. Indeed, in permissionless setting, this is only relevant for *write access* since reading is allowed anyway without resorting to smart contracts.

Finally, *consistency* is the fifth requirement. The terms of the agreement can be thought of as requirements that must be satisfied by the smart contract code to be compliant. According to Chechik et al. [44], writing requirements in a formal notation permits automatic assessment of properties such as ambiguity, consistency, and completeness. For instance, formal notions can be digested by theorem-provers [35, 45] to check if the contract implies a property, or model-checking [46] can be applied to check properties via state exploration to highlight the access on unsafe and unexpected states (e.g., if an agreement term cannot be satisfied or fully satisfied).

7. Blockchain and Interoperability

A topic of great interest covered by both the EU Data Act [1, Chapter VIII] and the European blockchain strategy [3] is certainly interoperability. For interoperability, EU Data Act means *"the ability of two or more data spaces or communication networks, systems, connected products, applications data processing services or components to exchange and use data in order to perform their functions"* [1, Article 2 point (40)]. Hence, blockchains should be interoperable between themselves and with legacy systems in the outside world [3], and the development of interoperability standards should enhance the ease of data flow across the European Union [4].

However, an increase in interoperability poses new challenges, both technical for data sharing and ethico-legal for data privacy. We identified three points of discussion on this matter: (i) interoperability between smart contracts in the same blockchain, (ii) interoperability of blockchains, and (iii) interoperability with blockchain-external data and applications.

The interoperability of the first point has already been achieved. Since the first blockchain solutions, instructions (aka *delegate calls*) have been designed that could invoke other contracts [24, 47]. Depending on the blockchain solution, they can give rise to new transaction requests or execute functions of other smart contracts without needing a transaction. In this scenario, some of the main problems are to guarantee the security of the software by preventing contracts from being improperly called from other contracts (e.g., re-entrancy [48], untrusted cross-contract invocations [49, 50], …) and to guarantee the integrity and consistency of data where the blockchain solutions (e.g., Hyperledger Fabric) allows different programming languages with different semantics and types (e.g., leading to truncation of values, overflows, …). However, this also implies new non-trivial verification challenges.

For the second point, there needs to be more standardization for smart contracts, and different blockchain platforms use different programming languages and consensus mechanisms. Moreover, it is required a standardization also for token definitions and token exchanges. Indeed, although, the ERCs [51] (e.g. ERC-20, ERC-721, ERC-777, ERC-1155) are well known standards for Ethereum community, they are currently only adopted by a few other blockchains [52, 53, 54, 55, 56]. In addition, they might be affected by potential problems with uncontrolled data localization. Moreover, different blockchains may operate under different legal and regulatory frameworks, and interoperability solutions must account for these differences to ensure compliance, making the design of standards a challenging task.

The last point concerns external data and applications [57]. Regarding integration between smart contracts and external software, it is important to consider both of inbound (to blockchain) and outbound (from blockchain) data directions. In the case of inbound data, smart contracts often need to be parameterized, i.e., to change their behavior depending on external data sources. This can be achieved using *oracles* that provide data to a smart contract. However, deciding whether an oracle is trustworthy and reliable without ad-hoc mechanisms might be challenging. Instead, in the case of outbound data, they require to access data coming from blockchains and trust the code that runs inside it. A typical scenario are token marketplaces, where external software manages the graphical user interface and application logic, while the creation and exchange of a large number of tokens (without prior coordination with token creators) are delegated to smart contracts within the blockchains. For instance, this can be achieved providing standards about tokens [51].

8. Concerns in the Blockchain Industry

During the negotiation phase of the EU Data Act, the blockchain industry expressed several concerns about the potentially limiting, harmful, or deficient content and terminologies contained in the proposals[4]. The most critical aspects are highlighted in an open letter [58, 59, 60] proposed by leading organizations in the blockchain sector. For instance, the blockchain industry pushed for technological neutrality to leave freedom of choice, refrain from imposing the use of any specific technology, and safeguard the regulations from obsolescence by ensuring their applicability regardless of the technology used. Furthermore, the blockchain industry has investigated the impact of applying some articles in conjunction, which may cause countless existing smart contracts deployed on public blockchains to be considered in breach of law. The blockchain industry is also concerned that the broad interpretation of the proposed definitions of smart contracts used in agreements to make data available could be extended to include those smart contracts enabling the exchange of digital assets. Such an outcome would pose significant operational and compliance challenges, also causing the EU Data Act to conflict with the requirements of the MiCA.

9. Related Work

The EU Data Act only came into force a few months before the writing of this manuscript. To the best of our knowledge, we have yet to find any related work dealing with the final document of the EU Data Act and addressing blockchain challenges. However, there is some preliminary work on the official proposals of the EU Data Act. For instance, Casolari et al. [61] suggest recommendations on addressing smart contracts to improve the EU Data Act. Unfortunately, it does not analyze how existing technologies can be applied to satisfy the proposal. Our previous work [62] focused on smart contracts and performed a brief investigation to start to fill the gap related to existing technologies. However, the main issue of proposals is that since they are not the version of the final text, the analysis of the text contains parts that are no longer valid (e.g., the definition of smart contract has changed in favor of a more technologically neutral one, while it previously referred to an electronic ledger explicitly) or lacks

[4]Proposals are documents of the European Parliament and the Council officially published before the final in force version and used in the negotiation phases.

fundamental contents added only later (e.g., the number of essential requirements for smart contracts increased in the final version).

Regarding personal data compliance only, Haque et al. [63] provide a systematic literature review regarding blockchain and GDPR compliance. Their finding indicates that studies about these topics have been rising. In particular, data deletion and modification seem to be blockchain's most discussed compliance issues. They also observed that IoT and healthcare domains are the most discussed research areas in this literature. Molina et al. [64] design principles for GDPR-compliant blockchain solutions, identifying and discussing the challenges of GDPR requirements.

Program verification is required for smart contract compliance. To the best of our knowledge, only Tauqeer et al. [65] dealt with this topic, proposing a solution based on knowledge graphs and semantically modeled informed consent [66] for GDPR compliance of smart contracts. However, other existing tools and techniques based on formal methods for traditional software could be adapted to the blockchain context [67, 68, 69].

10. Conclusion

Blockchain technology offers numerous benefits regarding data transparency, security, and decentralization. However, it is challenging to implement solutions compliant with the EU Data Act and that can fit within the European blockchain strategy. Addressing these challenges requires careful consideration and the development of new frameworks or solutions that reconcile the benefits of blockchain technology with the requirements of data protection regulations such as the GDPR. In the coming years, i.e., before the actual implementation of the EU Data Act, new standards will be developed and adopted thanks to the European blockchain strategy. Also, privacy-enhancing techniques will be designed and implemented, such as zero-knowledge proofs or off-chain data storage, and governance mechanisms will be established to ensure compliance with data protection regulations.

Acknowledgments

Luca Olivieri, Luca Negrini, Pietro Ferrara: Work partially supported by SERICS (PE00000014) and iNEST (ECS 00000043) projects funded by PNRR NextGeneration EU.
Luca Pasetto: This work was supported by the Luxembourg National Research Fund (FNR) (INTER/DFG/23/17415164/LODEX).

References

[1] European Parliament and the Council, Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act), 2023. Document 32023R2854. PE/49/2023/REV/1 OJ L, 2023/2854, 22.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2854/oj.

[2] Directorate-General for Communication, Data Act enters into force: what it means for you, 2016. NEWS ARTICLE - 11 January 2024 https://commission.europa.eu/news/data-act-enters-force-what-it-means-you-2024-01-11_en Accessed 03/2024.

[3] C. European Commission Directorate-General for Communications Networks, Technology, Policies -Blockchain Strategy | Shaping Europe's digital future, 2023. Last update 27 February 2023 https://digital-strategy.ec.europa.eu/en/policies/blockchain-strategy Accessed 03/2024.

[4] Publications Office of the European Union, The EU Data Act: A new era in data economy and open data integration, 2024. Publication Date 11/01/2024 on the official portal for European data. URL: https://data.europa.eu/en/news-events/news/eu-data-act-new-era-data-economy-and-open-data-integration-0.

[5] European Commission, Data Act: Commission welcomes political agreement on rules for a fair and innovative data economy, 2023. PRESS RELEASE, 18 June 2023, Brussels, https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3491 Accessed 03/2024.

[6] European Parliament and the Council, Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) (text with EEA relevance), 2022. Document 32022R0868. PE/85/2021/REV/1 OJ L 152, 3.6.2022, p. 1–44 ELI: http://data.europa.eu/eli/reg/2022/868/oj.

[7] C. European Commission Directorate-General for Communications Networks, Technology, Policies -European Data Governance Act | Shaping Europe's digital future, 2024. Last update 27 February 2024 https://digital-strategy.ec.europa.eu/en/policies/data-governance-act Accessed 03/2024.

[8] European Parliament and the Council, COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS A European strategy for data, 2020. Document 52020DC0066. COM/2020/66 final https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0066.

[9] C. European Commission Directorate-General for Communications Networks, Technology, Policies - A European strategy for data, 2024. Last update 4 March 2024 https://digital-strategy.ec.europa.eu/en/policies/strategy-data Accessed 03/2024.

[10] European Parliament and the Council, Consolidated text: Directive (EU) 2020/1828 of the European Parliament and of the Council of 25 November 2020 on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/ec (Text with EEA relevance), 2020. Document 02020L1828-20240217. ELI: http://data.europa.eu/eli/dir/2020/1828/2024-02-17.

[11] European Parliament and the Council, Regulation (EU) 2017/2394 of the European Parliament and of the Council of 12 December 2017 cooperation between national authorities responsible for the enforcement of consumer protection laws and repealing Regulation (EV) No 2006/2004 (text with EEA relevance), 2017. Document 02017R2394-20220101. ELI: http://data.europa.eu/eli/reg/2017/2394/2022-01-01.

[12] European Parliament and the Council, Consolidated text: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/ec (General Data Protection Regulation) (Text with EEA relevance), 2016. Document 02016R0679-20160504. ELI: http://data.europa.eu/eli/reg/2016/679/2016-05-04.

[13] S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008. https://bitcoin.org/bitcoin.pdf Accessed: 06/2023.

[14] W. F. Silvano, R. Marcelino, Iota tangle: A cryptocurrency to communicate internet-of-things data, Future Generation Computer Systems 112 (2020) 307–319. doi:https://doi.org/10.1016/j.future.2020.05.047.

[15] C. C. Agbo, Q. H. Mahmoud, J. M. Eklund, Blockchain technology in healthcare: A systematic review, Healthcare 7 (2019). URL: https://www.mdpi.com/2227-9032/7/2/56. doi:10.3390/healthcare7020056.

[16] V. Bonnici, V. Arceri, A. Diana, F. Bertini, E. Iotti, A. Levante, V. Bernini, E. Neviani, A. Dal Palù, Biochain: towards a platform for securely sharing microbiological data, in: Proceedings of the 27th International Database Engineered Applications Symposium, IDEAS '23, Association for Computing Machinery, New York, NY, USA, 2023, p. 59–63. URL: https://doi.org/10.1145/3589462.3589501. doi:10.1145/3589462.3589501.

[17] I. B. Damgård, Collision free hash functions and public key signature schemes, in: Workshop on the Theory and Application of of Cryptographic Techniques, Springer, 1987, pp. 203–216.

[18] L. Lamport, R. Shostak, M. Pease, The Byzantine Generals Problem, ACM Trans. Program. Lang. Syst. 4 (1982) 382–401. doi:10.1145/357172.357176.

[19] L. Olivieri, F. Tagliaferro, V. Arceri, M. Ruaro, L. Negrini, A. Cortesi, P. Ferrara, F. Spoto, E. Talin, Ensuring determinism in blockchain software with golisa: an industrial experience report, in: L. Gonnord, L. Titolo (Eds.), SOAP '22: 11th ACM SIGPLAN International Workshop on the State

Of the Art in Program Analysis, San Diego, CA, USA, 14 June 2022, ACM, 2022, pp. 23–29. URL: https://doi.org/10.1145/3520313.3534658. doi:10.1145/3520313.3534658.

[20] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. De Caro, D. Enyeart, C. Ferris, G. Laventman, Y. Manevich, S. Muralidharan, C. Murthy, B. Nguyen, M. Sethi, G. Singh, K. Smith, A. Sorniotti, C. Stathakopoulou, M. Vukolić, S. W. Cocco, J. Yellick, Hyperledger fabric: a distributed operating system for permissioned blockchains, in: Proceedings of the Thirteenth EuroSys Conference, EuroSys '18, Association for Computing Machinery, New York, NY, USA, 2018, pp. 1–15. URL: https://doi.org/10.1145/3190508.3190538. doi:10.1145/3190508.3190538.

[21] IBM, Hyperledger achieves huge milestone: Introducing Hyperledger Fabric 2.0, 2023. Https://www.ibm.com/blog/hyperledger-achieves-huge-milestone-introducing-hyperledger-fabric-2-0/ (Accessed 01/2024).

[22] A. M. Antonopoulos, Mastering Bitcoin: Programming the open blockchain, " O'Reilly Media, Inc.", 2017.

[23] G. Wood, et al., Ethereum: A secure decentralised generalised transaction ledger, Ethereum project yellow paper (2014).

[24] A. M. Antonopoulos, G. Wood, Mastering ethereum: building smart contracts and dapps, O'reilly Media, 2018.

[25] L. Olivieri, L. Negrini, V. Arceri, F. Tagliaferro, P. Ferrara, A. Cortesi, F. Spoto, Information Flow Analysis for Detecting Non-Determinism in Blockchain, in: K. Ali, G. Salvaneschi (Eds.), 37th European Conference on Object-Oriented Programming (ECOOP 2023), volume 263 of *Leibniz International Proceedings in Informatics (LIPIcs)*, Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl, Germany, 2023, pp. 23:1–23:25. URL: https://drops.dagstuhl.de/opus/volltexte/2023/18216. doi:10.4230/LIPIcs.ECOOP.2023.23.

[26] X. Sun, F. R. Yu, P. Zhang, Z. Sun, W. Xie, X. Peng, A survey on zero-knowledge proof in blockchain, IEEE Network 35 (2021) 198–205. doi:10.1109/MNET.011.2000473.

[27] A. Preukschat, D. Reed, Self-sovereign identity, Manning Publications, 2021.

[28] European Parliament and the Council, Consolidated text: Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/eu and (EU) 2019/1937 (Text with EEA relevance), 2023. Document 02023R1114-20240109. ELI: http://data.europa.eu/eli/reg/2023/1114/2024-01-09.

[29] Michèle Finck, Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law?, 2019. PE 634.445 – July 2019. This study was written by Dr Michèle Finck at the request of the Panel for the Future of Science and Technology (STOA) and managed by the Scientific Foresight Unit, within the Directorate-General for Parliamentary Research Services (EPRS) of the Secretariat of the European Parliament. Study: https://www.europarl.europa.eu/stoa/en/document/EPRS_STU(2019)634445 Accessed 04/2024. Project Report: https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf Accessed 04/2024.

[30] M. Finck, Blockchain Regulation and Governance in Europe, Cambridge University Press, 2018.

[31] J. Bacon, J. D. Michels, C. Millard, J. Singh, Blockchain demystified: a technical and legal introduction to distributed and centralized ledgers, Rich. JL & Tech. 25 (2018) 1. https://jolt.richmond.edu/files/2018/11/Michelsetal-Final-1.pdf.

[32] N. Szabo, Smart contracts: building blocks for digital markets, EXTROPY: The Journal of Transhumanist Thought,(16) 18 (1996) 28.

[33] P. Cousot, R. Cousot, Abstract interpretation: A unified lattice model for static analysis of programs by construction or approximation of fixpoints, in: Proc. of the 4th Symposium on Principles of Programming Languages, 1977, ACM, 1977, pp. 238–252.

[34] E. M. Clarke, Jr., O. Grumberg, D. A. Peled, Model Checking, MIT Press, Cambridge, MA, USA, 1999.

[35] J. H. Gallier, Logic for computer science: foundations of automatic theorem proving, Courier Dover Publications, Mineola, NY, USA, 2015.

[36] H. G. Rice, Classes of Recursively Enumerable Sets and Their Decision Problems, Transactions of the American Mathematical Society 74 (1953) 358–366. doi:10.1090/s0002-9947-1953-0053041-6.

[37] T. Genet., T. Jensen., J. Sauvage., Termination of ethereum's smart contracts, in: Proceedings of the 17th International Joint Conference on e-Business and Telecommunications - SECRYPT, INSTICC, SciTePress, 2020, pp. 39–51. doi:10.5220/0009564100390051.

[38] E. Albert, J. Correas, P. Gordillo, G. Román-Díez, A. Rubio, Don't run on fumes—parametric gas bounds for smart contracts, Journal of Systems and Software 176 (2021) 110923. doi:https://doi.org/10.1016/j.jss.2021.110923.

[39] J. Chen, X. Xia, D. Lo, J. Grundy, Why do smart contracts self-destruct? investigating the selfdestruct function on ethereum, ACM Trans. Softw. Eng. Methodol. 31 (2021). doi:10.1145/3488245.

[40] OpenZeppelin, Pausable, 2023. https://docs.openzeppelin.com/contracts/2.x/api/lifecycle#pausable (Accessed 09/2023).

[41] A. Singh, K. Click, R. M. Parizi, Q. Zhang, A. Dehghantanha, K.-K. R. Choo, Sidechain technologies in blockchain networks: An examination and state-of-the-art review, Journal of Network and Computer Applications 149 (2020) 102471.

[42] O. Dib, K.-L. Brousmiche, A. Durand, E. Thea, E. B. Hamida, Consortium blockchains: Overview, applications and challenges, Int. J. Adv. Telecommun 11 (2018) 51–64.

[43] S. Wang, M. Yang, Y. Zhang, Y. Luo, T. Ge, X. Fu, W. Zhao, On private data collection of hyperledger fabric, in: 2021 IEEE 41st International Conference on Distributed Computing Systems (ICDCS), 2021, pp. 819–829. doi:10.1109/ICDCS51616.2021.00083.

[44] M. Chechik, J. Gannon, Automatic analysis of consistency between requirements and designs, IEEE Transactions on Software Engineering 27 (2001) 651–672. doi:10.1109/32.935856.

[45] D. W. Loveland, Automated theorem proving: A logical basis, Elsevier, 2016.

[46] E. M. Clarke, Model checking, in: Foundations of Software Technology and Theoretical Computer Science: 17th Conference Kharagpur, India, December 18–20, 1997 Proceedings 17, Springer, 1997, pp. 54–56.

[47] KC Tam, Cross-Chaincode Invoking in Hyperledger Fabric, 2024. https://kctheservant.medium.com/cross-chaincode-invoking-in-hyperledger-fabric-8b8df1183c04 Accessed 03/2024.

[48] N. Atzei, M. Bartoletti, T. Cimoli, A survey of attacks on ethereum smart contracts (sok), in: Principles of Security and Trust: 6th International Conference, POST 2017, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2017, Uppsala, Sweden, April 22-29, 2017, Proceedings 6, Springer, 2017, pp. 164–186.

[49] L. Olivieri, T. Jensen, L. Negrini, F. Spoto, Michelsonlisa: A static analyzer for tezos, in: 2023 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops), 2023, pp. 80–85. doi:10.1109/PerComWorkshops56833.2023.10150247.

[50] L. Olivieri, L. Negrini, V. Arceri, T. Jensen, F. Spoto, Design and implementation of static analyses for tezos smart contracts, Distrib. Ledger Technol. (2024). URL: https://doi.org/10.1145/3643567. doi:10.1145/3643567, just Accepted.

[51] Ethereum.org, Ethereum Development Standard, 2024. https://ethereum.org/en/developers/docs/standards/ Accessed 04/2024.

[52] Hyperledger, ERC-20 Token Scenario, 2022. https://github.com/hyperledger/fabric-samples/tree/main/token-erc-20#erc-20-token-scenario Accessed 04/2024.

[53] Hyperledger, ERC-721 Token Scenario, 2022. https://github.com/hyperledger/fabric-samples/tree/main/token-erc-721#erc-721-token-scenario Accessed 04/2024.

[54] M. Koscina, M. Lombard-Platet, P. Cluchet, PlasticCoin: An ERC20 Implementation on Hyperledger Fabric for Circular Economy and Plastic Reuse, in: IEEE/WIC/ACM International Conference on Web Intelligence - Companion Volume, ACM, 2019, pp. 223–230.

[55] M. Crosara, L. Olivieri, F. Spoto, F. Tagliaferro, Re-engineering erc-20 smart contracts with efficient snapshots for the java virtual machine, in: 2021 Third International Conference on

Blockchain Computing and Applications (BCCA), 2021, pp. 187–194. doi:10.1109/BCCA53669.2021.9657047.

[56] M. Crosara, L. Olivieri, F. Spoto, F. Tagliaferro, Fungible and non-fungible tokens with snapshots in java, Cluster Computing 26 (2023) 2701–2718. doi:10.1007/s10586-022-03756-3.

[57] S. Porru, A. Pinna, M. Marchesi, R. Tonelli, Blockchain-oriented software engineering: Challenges and new directions, in: 2017 IEEE/ACM 39th International Conference on Software Engineering Companion (ICSE-C), 2017, pp. 169–171. doi:10.1109/ICSE-C.2017.142.

[58] European Crypto Initiative, Blockchain4Europe, Digital Currencies Governance Group, European Blockchain Association, INATBA, IOTA, et al., Open Letter, 2023. Published 15/06/23. URL: https://data-act.info/wp-content/uploads/2023/06/Open-Letter-About-Concerns-No-Logos-4.pdf Accessed 03/2024.

[59] European Crypto Initiative, Blockchain4Europe, Digital Currencies Governance Group, European Blockchain Association, INATBA, IOTA, et al., Open Letter Summary, 2023. https://data-act.info Accessed 03/2024.

[60] European Crypto Initiative, OPEN LETTER ON DATA ACT, 2023. https://eu.ci/open-letter-on-data-act Accessed 03/2024.

[61] F. Casolari, M. Taddeo, A. Turillazzi, L. Floridi, How to improve smart contracts in the European Union Data Act, Digital Society 2 (2023) 9.

[62] L. Olivieri, L. Pasetto, Towards compliance of smart contracts with the european union data act, in: CEUR Workshop Proceedings, volume 3629, 2024, p. 61 – 66. URL: https://ceur-ws.org/Vol-3629/paper10.pdf, 5th Workshop on Artificial Intelligence and Formal Verification, Logic, Automata, and Synthesis (OVERLAY 2023).

[63] A. B. Haque, A. K. M. N. Islam, S. Hyrynsalmi, B. Naqvi, K. Smolander, Gdpr compliant blockchains–a systematic literature review, IEEE Access 9 (2021) 50593–50606. doi:10.1109/ACCESS.2021.3069877.

[64] F. Molina, G. Betarte, C. Luna, Design principles for constructing gdpr-compliant blockchain solutions, in: 2021 IEEE/ACM 4th International Workshop on Emerging Trends in Software Engineering for Blockchain (WETSEB), 2021, pp. 1–8. doi:10.1109/WETSEB52558.2021.00008.

[65] A. Tauqeer, A. Kurteva, T. R. Chhetri, A. Ahmeti, A. Fensel, Automated gdpr contract compliance verification using knowledge graphs, Information 13 (2022). URL: https://www.mdpi.com/2078-2489/13/10/447. doi:10.3390/info13100447.

[66] T. R. Chhetri, A. Kurteva, R. J. DeLong, R. Hilscher, K. Korte, A. Fensel, Data protection by design tool for automated gdpr compliance verification based on semantically modeled informed consent, Sensors 22 (2022). URL: https://www.mdpi.com/1424-8220/22/7/2763. doi:10.3390/s22072763.

[67] P. Ferrara, F. Spoto, Static analysis for GDPR compliance, in: CEUR Workshop Proceedings - Proceedings of ITASEC '18, volume 2058, 2018, pp. 1–10.

[68] P. Ferrara, L. Olivieri, F. Spoto, Tailoring Taint Analysis to GDPR, in: Privacy Technologies and Policy - 6th Annual Privacy Forum, APF 2018, Barcelona, Spain, June 13-14, 2018, Revised Selected Papers, volume 11079 of *Lecture Notes in Computer Science*, Springer, 2018, pp. 63–76. doi:10.1007/978-3-030-02547-2_4.

[69] P. Ferrara, L. Olivieri, F. Spoto, Static Privacy Analysis by Flow Reconstruction of Tainted data, Int. J. Softw. Eng. Knowl. Eng. 31 (2021) 973–1016. doi:10.1142/S0218194021500303.