The oracle problem in smart contracts: data privacy, security, and solutions*

Sharmin N. Chougule - Luigi Cantisani

Abstract

In the process of improving traceability and equipping supply chains with contract automation, smart contracts based on blockchains are being explored by the industry and even somewhat indicated by the EU legislator (see Data Act). But smart contracts in turn require data sources known as "oracles". The oracle problem in smart contracts poses significant challenges to data privacy and security. This article explores the various risks associated with the oracle problem within supply chains and discusses potential solutions to enhance the security and privacy of smart contracts. The oracle problem encompasses data privacy risks, data manipulation risks, trust in oracle operators, data leakage, and regulatory compliance concerns. Among the solutions aimed at mitigating these risks are Privacy-preserving oracles, decentralised oracle networks, and reputation-based models which nonetheless are not foolproof, and each approach has its limitations. Hybrid approaches and cross-chain solutions are also discussed. The article emphasises the dynamic nature of the blockchain space and the importance of keeping up with the latest developments to address the oracle problem effectively.

Table of contents

Keywords

Smart Contracts – Oracle Problem – Data Privacy – Supply Chains – Blockchain Security

1. Introduction to the context and the core issue

As technology advances, new ways of creating and sharing value along the supply chain emerge. In particular, personal and non-personal data could be the gold of the current

* L'articolo è stato sottoposto, in conformità al regolamento della Rivista, a referaggio "a doppio cieco".

millennium[1], as it contains information that any economic operator involved in the supply chain could benefit from to maximise its service performance and focus the production based on the customers' preferences. The European Union is aware of that, and as a first step to cope with innovation, a legislative intervention occurred with the adoption of Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation, hereinafter: GDPR). We would like to emphasise "free movement" to underline that the legislator understands the role of data sharing and «the importance of creating the trust that will allow the digital economy to develop across the internal market»[2]. This regulation provides a framework of rights and obligations for those involved in the processing of personal data, with a vision aimed at not restricting the development of business and technology, rooted in the principle of accountability[3]. For this reason, it is often said that this regulation adopts a risk-based approach[4].

Risk-based regulations have the advantage of not imposing one-size-fits-all measures, as they leave it up to companies to determine their own "do's" and "don'ts" based on the processing carried out and the existing risks. On the other hand, it also has the disadvantage of making many provisions of the legislative text ambiguous, especially those that refer to areas that are themselves very heterogeneous and multi-layered such as automation and automated decision-making. Let us exemplify this by referring to a much-discussed topic, that is artificial intelligence (hereinafter referred to as: AI): GDPR allows the development of AI and big data applications that successfully balance data security and other social and economic interests, but it provides limited guidance on how to achieve this goal. The Panel for the Future of Science and Technology of the European Parliamentary Research Service in its study in June 2020 asserted that «no major changes to the GDPR are needed to address AI»[5]. However,

[1] That has been argued on several occasions by leading economics media outlets or representatives of relevant corporations. See, among the others, The Economist, *The world's most valuable resource is no longer oil, but data*, 6 May 2017, in *economist.com*; CNN, *The data rush: How information about you is 21st century gold*, 13 November 2014, in *edition.cnn.com*; the Urban Unit CEO K. Sherdil according to whom "*Data is the new gold or oil for 21st century*" as reported by Shahram Haq in The Express - Tribune, *Data is the new gold for 21st century*, 9 February 2020, in *tribune.com.pk*; as well as Siemens CEO Joe Kaeser, as reported Shannon Tellis in The Economic Times - Panache, *"Data is the 21st century's oil", says Siemens CEO Joe Kaeser*, 24 May, 2018, in *economictimes.indiatimes.com*.

[2] Recital 7 of the GDPR. Also see, among the others, Recital 6 according to which «Technology has transformed both the economy and social life, and should further facilitate the free flow of personal data within the Union and the transfer to third countries and international organisations, while ensuring a high level of the protection of personal data».

[3] On the role of accountability within the GDPR, see, among others, C.D. Raab, *Information Privacy: Ethics and Accountability*, in *ssrn.com,* 2016.

[4] With regard to the risk-based approach in general, see B.M. Hutter, *What Makes a Regulator Excellent? A Risk Regulation Perspective*, Paper Prepared for the Penn Program on Regulation's Best-in-Class Regulator Initiative, June 2015, in *law.upenn.edu*. With regard to the application of the risk-based approach to data protection, see Working Party 29 Statement 14/EN WP 218 on the role of a risk-based approach to data protection legal frameworks, adopted on 30 May 2014. Working Party 20, hereinafter referred to as "WP29" was the joint working group of national supervisory and data protection authorities replaced by the EDPB on 25 May 2018.

[5] The impact of the General Data Protection Regulation (GDPR) on artificial intelligence, Panel for

it identified that many AI-related data-protection issues are not explicitly addressed in the GDPR. This could in turn lead to uncertainties and costs, and unnecessarily hinder the development of AI applications. To fill these as some other regulatory gaps concerning AI, the EU Parliament finally passed the AI Act on 18 March 2024[6]. However, the risk-based approach of the GDPR still results in a sort of vagueness posing significant challenges for other technologies - such as the ones discussed in this work - that have not benefited yet from dedicated pieces of legislation, *i.e.* smart contracts.

The vagueness of the GDPR can be seen in certain open-ended provisions such as arts. 13, para. 2, lit. f) and 14, para. 2, lit. g), of the GDPR which establish right of data subjects to be informed about personal data processing activities involving automated decision-making, but leave many questions open as to how to inform users (see, for instance, largely interpretable wording such "meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject" by both the aforementioned articles). In a similar manner, art. 22, para. 3, requires that where the data subject is affected by an automated decision necessary for entering into, or performance of, a contract between the data subject and a data controller, or based the data subject's explicit consent, the data controller shall implement "suitable measures" to safeguard the data subject's rights and freedoms and legitimate interests, but the provision give no clue about what a suitable safeguarding measure is, apart from the possibility of expressing one's point of view and contesting it before a human being . Same goes with art. 25 on the appropriateness of the technical and organisational measures for data protection by design and by default, as the provision never explains what an appropriate measure is (although a few specific examples aimed at security are given under art. 32). In sum, in the presence of new technologies, it may be difficult for controllers to determine whether the processing they envisage meets these widely open-to-interpretation criteria.

This problem has to be reconciled with not unreasonably restricting the free movement of data, to enable the development of the data economy, which is also part of the GDPR's scope as outlined above. It is no coincidence that the legislator's second major intervention concerning data circulation was enacting the Data Act[7], a regulation that acknowledges the economic value of data[8], aims at removing barriers to data sharing by imposing obligations concerning portability and interoperability[9], and

the Future of Science and Technology of the European Parliamentary Research Service, in *europarl.europa.eu*.

[6] "AI Act" means the final approved version of the Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain union legislative acts.

[7] "Data Act" means 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).

[8] See Recital 1, which states «High-quality and interoperable data from different domains increase competitiveness and innovation and ensure sustainable economic growth. The same data may be used and reused for a variety of purposes and to an unlimited degree, without any loss of quality or quantity».

[9] Recital 2 highlights such barriers ("Barriers to data sharing prevent an optimal allocation of data for the benefit of society") and Chapter 3 is entirely devoted to laying down obligations relating to

governs the modalities for data sharing. These innovations, where combined, should leverage the possibilities offered by, among others, the Internet-of-Things technology (hereinafter: "IoT technology" or simply "IoT"). Specifically, the Data Act aims at "Connected products that obtain, generate or collect, by means of their components or operating systems, data concerning their performance, use or environment and that are able to communicate those data via an electronic communications service, a physical connection, or on-device access"[10]. Hence, IoT is understood as a concept encompassing many technologies, including devices, appliances, and sensors, interconnected with each other via the Internet to facilitate communication and data sharing. Given that the Data Act finally brings rules and thus presumably legal certainty to a segment of the IoT sector, adoption of this technology could experience a significant increase, and supply chain management could be one of the areas benefiting the most from the adoption. This, in turn, can be hypothesised on the basis that IoT has enabled significant advancements in supply chain management, allowing for real-time tracking and monitoring of goods and assets[11].

However, it is worth noting that data processed via IoT systems could include personal data, which creates tension between, on the one hand, empowering businesses and removing obstacles to the data-driven economy in line with the EU regulatory goals, and on the other hand, complying with the mandatory personal data privacy obligations under the GDPR.

References to devices meant for consumers that could be empowered by blockchain technology can be found in early major literature contributions. For instance, De Filippi and Wright illustrated a wide range of use potential and existing use cases, referred to as Blockchain of Things, including washing machines able to automatically order and pay for new detergent from an online service when the detergent supply is low[12]. The functioning of such a feature requires monitoring the user and its consumption habits, collecting payment data of the user, as well as the address to deliver new supply, albeit the cited work does not directly engage with the GDPR implications of IoT-devices using blockchain technology. A recent study, still in progress, highlights how "smart fridges", meaning advanced IoT refrigerators that based on current EU new regulations would fall within the meaning of "connected products" set forth in the Data Act, given their features (communicating with software and devices managed by different stakeholders operating in the food industry), could make it possible for companies to learn about consumers' food consumption habits, and create a network of digital relationships and data sharing involving IoT-sensors producers, consumers, supermarkets, suppliers, and, last but not least, the technology company that sells the

business-to-consumer and business-to-business data sharing.

[10] Recital 14, Data Act.

[11] S. Taj-A. Imran-Z. Kastrati-S. Daudpota-R. Memon-J. Ahmed, *IoT-based supply chain management: A systematic literature review*, in *Internet of Things*, 24, 2023; Also see, R. Abderahman-J. G. Keogh-H. Treiblmaier, *Leveraging the Internet of Things and Blockchain Technology in Supply Chain Management*, in *Future Internet,* 11(7), 2019.

[12] P. De Filippi-A. Wright, *Blockchain and the Law: The Rule of Code,* Cambridge (MA), 2018, 156 ss.

smart fridge[13]. To fulfil its purpose, such a system would require processing important personal data concerning the end-users, potentially including special categories of sensitive data within the meaning of art. 9 of the GDPR.

The foundational elements and concerns raised so far could be then summed up as ensuring data protection under the GDPR by applying its risk-based rules to new technologies and contract automation contexts, considering the data sharing and growth of the digital economy, in the context of the potential advantages brought by IoT to supply chains. Based on that, this work raises the question of how to reconcile GDPR with IoT-based supply chains that make use of other disruptive technologies such as distributed ledger technology (hereinafter: "DLT") and smart contracts. Specifically, this work focuses on the risk and opportunities deriving from implementing said technologies in supply chains that pose *per se* challenges due to underpinning IoT infrastructures. To be fair, addressing such an issue in its entirety would probably require an entire book jointly written by lawyers and technologists, so for the purposes of this smaller contribution we want to focus on a single but crucial aspect of the triangular relationship between IoT, DLT, and smart contracts with respect to data privacy, a sort of problem within a problem, which is that of the oracles.

As we will see in detail in the next chapter, smart contracts as intended in the DLT field are not tools based on AI and therefore they are less "smart" than it is generally believed[14]. Smart contracts can merely execute a predetermined set of operations[15], and to do that they require information from trusted sources, which in industry jargon are referred to as "oracles". Oracles act as intermediaries between blockchain-based smart contracts and external data sources, yet their involvement introduces risks related to data integrity and trustworthiness. Oracles determine whether or not the smart contract will execute a given operation and ultimately what information will be recorded on a given distributed ledger. Some authors highlight the tension between decentralisation and reliance on oracles, as oracles could be vulnerable to security breaches or manipulation[16], errors, or data breaches, emphasising the need for trusted oracles and regulatory oversight to address these issues[17]. This exacerbates concerns around

[13] S. M. Caravaca-L. Cantisani, *The Fridge: Charting the Course for AI-Integrated Predictive Systems and Their Legal Paradigms*, a not yet published work which was previewed at the "Lawtomation Days" of September 2023, at the IE University, in Madrid (access granted by the authors).

[14] In the context of DLT technology, smart contract technology came to light and was presented with the advent of the blockchain "Ethereum". In the Ethereum white paper, "smart contracts" are defined as "systems which automatically move digital assets according to arbitrary pre-specified rules". See, V. Buterin, *Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform*, in *ethereum.org*, 2014.

[15] *Ibidem*.

[16] P. Hacker-I. Lianos-G. Dimitropoulos-S. Eich, *Regulating Blockchain: Techno-Social and Legal Challenges*, Oxford, 2019.

[17] P. De Filippi-A. Wright. *Blockchain and the Law,* cit.; see also M. Finck, *Blockchain Regulation and Governance in Europe*, Cambridge, 2018. Michèle Finck explores the regulatory challenges posed by blockchain technologies, including the oracle problem in smart contracts. Finck identifies oracles as critical intermediaries that feed external data into smart contracts, but she highlights their vulnerability to manipulation and inaccuracies. The decentralised nature of blockchain is compromised by the need to trust oracles, which can introduce risks related to data integrity and security. Finck argues that effective governance mechanisms and regulatory frameworks are essential to ensure the reliability of

data privacy and the reliability of the information that smart contracts depend on.

Now, imagine combining the possibilities offered by IoT with DLT and smart contracts. IoT would connect devices for data collection and analysis, enhancing efficiency and automation. DLT would offer secure, transparent, and immutable transaction recording. Smart contracts would automate processes based on predefined conditions. That would result in a complex network of software and devices, sharing a huge amount of data, and having such data processed by oracles. What would be the risks for privacy protection where the processing of personal data is involved in such a huge network where oracles operate?

This paper aims to explore the novel challenges[18] and opportunities arising at the intersection of these three technological realms, shedding light on their growing significance and their profound impact on industries worldwide. We are aware of the already existing literature[19] discussing the issue of trust in oracles[20], as well as the delicate relationship between DLT and the GDPR. Building on the work of the distinguished authors who preceded us, this paper focuses on a very specific angle, and questions what problems oracles pose for privacy in the context of supply chains that simultaneously make use of IoT, DLT, and smart contracts, where the processing of personal data is involved. The objective is to contribute, from a legal standpoint, to the debate around the development of secure, efficient, and privacy-preserving IoT-driven supply chain solutions that use DLT and smart contracts. That has practical applications in industries such as food safety, trade finance, inventory management, logistics, healthcare, and manufacturing, where supply chain management (hereinafter also shortly referred to as "SCM") is key. For instance, VeChain is a blockchain platform that focuses on SCM and business processes and has partnered with Walmart China to create a food safety traceability platform[21]. Skuchain is another blockchain platform that facilitates trade finance, inventory management, and logistics for cross-border transactions, and has collaborated with Mitsubishi to streamline the financing and delivery of metal products[22]. Provenance is a blockchain platform that provides transparent and verifiable information about the origin, journey, and impact of products, and has partnered with Co-op UK to track the provenance and sustainability of fresh produce[23].

The following chapters will therefore be devoted to examining this issue in more detail, trying to indicate possible solutions that comply with the GDPR[24].

oracles, thus protecting data privacy and the security of smart contracts in blockchain ecosystems.

[18] Authors, for instance P. Hacker, *Regulating Blockchain,* cit., focus on the legal challenges of blockchain technologies, particularly in the context of data privacy and security and have made a beautiful attempt to address regulatory concerns and technical dependencies in blockchain

[19] M. Finck, *Blockchain Regulation*, cit.,

[20] See para. 2.2, and the literature therein referred to.

[21] *Far More Than Walmart China — How VeChain Leads Blockchain Adoption in the Food Industry Around the Globe*, in *Medium*, June 16, 2021.

[22] M. White, *Skuchain and Mitsubishi launch blockchain platform ECO for metals and mining*, in *Global Tech Review*, August 10, 2020, /.

[23] *Blockchain: the solution for transparency in product supply chains*, in *provenance.org*, September 21, 2015.

[24] We are aware that the aforementioned Data Act contains important provisions for the IoT world and rules on how smart contracts should be designed for the purposes of data sharing among businesses

2. Issues: risks and trust

This chapter is dedicated to further unpacking the issues teased in the introduction, which in turn requires illustrating at least the basic elements of DLT and smart contracts.

2.1. The basics to understand DLT and smart contracts

DLT is a term that encompasses electronic ledgers that reject the idea of central management in favour of decentralisation, meaning that information and transactions are not stored, accessed, and processed by a central server but by several computer devices, belonging to different network participants, that make computational power available to the network (in the industry jargon referred to as "nodes")[25]. The paradigm benchmark when talking about DLT is Bitcoin, the first distributed ledger in the modern sense and in particular the first "blockchain", a subcategory of distributed ledger that, through cryptographic techniques, converts the identification data of a transaction into ashes (although the identification codes of the e-wallets that executed the transaction remain readable in plain text), packs these hashes into data blocks, which linked together in chronological order to form a chain, and where the next block always contains a hash of the information contained in the previous block to ensure the consistency of the history of the transactions tracked by the ledger[26]. Bitcoin's blockchain is administered on a peer-to-peer basis by the nodes, meaning that anyone can access and read the ledger (public), and anyone meeting the computing power requirements fixed in the code can act as a node (permissionless)[27]. Moreover, nodes validate transactions in a fully automated way (for Bitcoin, this mechanism is named

and consumers (see art. 36 of the Data Act), however, for reasons of focus on the research question, we will avoid digressions on the technical requirements of "smart contracts" under the DSA, which in any case apply only in the context of data sharing agreements involving connected devices, and we will mainly deal with more general privacy issues, and thus with the rules under the GDPR.

[25] See S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, in **bitcoin.org,** 2008, 1-4, for a proper introduction to Bitcoin's ledger. For a more comprehensive overview, see B. Anthony, *Deployment of distributed ledger and decentralised technology for transition to smart industries*, Environ Syst Decis, 2003, 298 ss.

[26] *Ibidem*. S. Nakamoto while he discusses how blocks are linked together in chronological order and how each block contains a hash of the previous one to ensure the integrity and immutability of the transaction history, it does not delve into the terminology of "paradigm benchmark"

[27] *Ibidem*. In S. Nakamoto's paper, the concepts of public accessibility and permissionless participation are central to the design of Bitcoin's blockchain. Nakamoto describes the Bitcoin blockchain as a public ledger where all transactions are recorded and can be viewed by anyone, ensuring transparency and enabling participants to verify transactions independently.
The white paper outlines that Bitcoin operates on a decentralized peer-to-peer network, meaning there is no central authority; instead, each node maintains a copy of the blockchain and contributes to transaction validation. Nakamoto emphasizes that anyone can join the network and act as a node, provided they meet the computational power requirements set in the code, making Bitcoin a permissionless system. This design enhances security, reduces reliance on a single entity, and promotes inclusivity in the maintenance and governance of the network. Nakamoto may not explicitly use the terms "public" and "permissionless" in the same way contemporary discussions might, the concepts are integral to the design and function of Bitcoin as outlined in his paper.

"proof-of-work")[28], and information recorded cannot be changed or misrepresented unless otherwise decided by many nodes representative of the majority of the computational power running the ledger. Should a majority vote in favour of a change, said change would be visible to the users, because the continuation of the ledger would not be displayed as a continuation consistent with the past, but rather as an inconsistent deviation referred to in the industry jargon as a "fork". Due to these features and the increased level of transparency that comes with them, Bitcoin has been presented as a solution for replacing trust in humans with technology in the realm of e-payment execution and record-keeping[29].

However, Bitcoin had several limitations, mainly consisting of the following: a) it was designed as a mere electronic payment system, meant to solely transact the native cryptocurrency Bitcoin; b) replicating that design for use cases that require recording more information, would lead to "scalability" issues, meaning information overload that could slow down the entire system[30]; c) proof-of-work is an automatic validation mechanism, which rewards those who provide more and more computational power with the allocation of newly generated Bitcoin, but to prevent the currency from inflating, for each newly generated Bitcoin, the demanded computational power increases, which results in a "sustainability" issue[31].

Due to such limitations, new examples of DLT came to light. Ethereum for instance

[28] S. Nakamoto, cit. It may also be noted that Byzantine Fault Tolerance (BFT) for Consensus Mechanisms filters faulty and dishonest information which is different from other nodes. In this way also accesses some part of information on other blocks but may not always be the personal data. While S. Nakamoto's white paper does not explicitly refer to traditional BFT algorithms, it introduces a novel Consensus Mechanism that addresses the same underlying problem in a different way. Satoshi Nakamoto's Bitcoin white paper addresses the Byzantine Generals' Problem, a classic issue in achieving consensus in distributed systems with potential faulty or malicious nodes. Instead of using traditional BFT algorithms, which work in smaller, permissioned networks, Nakamoto introduces a new approach called "Nakamoto Consensus" based on Proof of Work (PoW). Nakamoto Consensus achieves consensus by having nodes compete to solve cryptographic puzzles, with the majority's computational power ensuring network security. It provides probabilistic finality, meaning the likelihood of transaction finality increases as more blocks are added. This approach is suitable for decentralized, permissionless networks, unlike classical BFT, which tolerates up to one-third malicious nodes and offers instant, deterministic finality. Thus, Nakamoto Consensus can be viewed as a form of "probabilistic BFT" suited for large-scale, decentralized environments like Bitcoin.

See also, F. Rahman-C. Titouna-F. Naït-Abdesselam, *Asymmetric Byzantine Quorum Approach to Resolve Trust Issues in Decentralized Blockchain Oracles*, International Conference on Software, Telecommunications and Computer Networks (SoftCOM), Split, Croatia, 2023, 1-6.

[29] «A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution», as stated by Satoshi Nakamoto, *Bitcoin,* cit.*,* 1. Precisely, Sakamoto advocates the need for "cryptographic proof" rather than trust, meaning the proof of work. That is a concrete application of the ideology promoted by the "cypherpunk" movement during the eighties, and in particular, by the Crypto Anarchy Manifesto, which endorsed the role that cryptography can play in disintermediating many roles traditionally played by institutions, companies, or other public or private entities, with the end goal of achieving more economic and trade freedom.

[30] A. Asmaa-H. Noor-A. Fiza, *A Systematic Review on Blockchain Scalability*, in *International Journal of Advanced Computer Science and Applications*, 14(9), 2023.

[31] A. Hani-N. Islam-D. Syed-A. Sulaiman-M. Saleh Al Reshan-K. Rajab-A. Shaikh-J. Shuja-Uddin-A. Soomro, *Sustainability in Blockchain: A Systematic Literature Review on Scalability and Power Consumption Issues*, in *Energies*, 16(3), 2023, 1510.

debuted in 2014 along with the innovative feature named "smart contracts"[32], which is software meant to automate contractual relationships more complex than mere electronic payments[33]. To resolve the scalability issue Ethereum recently moved to a multi-chain structure, meaning that there are several blockchains, each one dedicated to a given industry or set of online applications, usually referred to as "side-chains" or "shard chains", and on top of them there is the main blockchain where hashes of the transaction processed by the side-chains are in turn summarised as hashes as well. In other words, it is a matter of allocating computational workload on several ledgers connected to a main one to avoid overloading. Also, proof-of-work has been replaced with an efficient "proof-of-stake"[34], a governance model of the ledger where anyone wishing to act as a node must deposit a given amount of cryptocurrency on the blockchain in question, which can resemble shareholder's *pro quota* governance rights in the world of corporate governance[35].

Aside from Ethereum, other types of blockchains emerged, some of which largely diverge from the paradigm of Bitcoin. Bitcoin and Ethereum, for instance, are public and permissioned ledgers, but other ledgers are referred to as "private" and "permissioned", usually meaning that: a) all the nodes belong to the same legal entity or a group of legal entities (where more entities are involved, the blockchain is referred to as "federated"); b) the managing entity or group grants the users with authorisations to access and/or validate transactions, thus essentially deciding who can respectively be a mere user and who can be a node. Hyperledger Fabric is an example of that concept: this ledger is managed by the Hyperledger Consortium which is a group of entities, and it is considered permissioned as the Fabric platform assigns different access levels to nodes based on their role within the organisation. Recent research on these permissioned DLTs brings about that Hyperledger Fabric and Corda are more suitable for enterprise use cases.[36] Issues like scalability, energy efficiency, and interoperability have been under scrutiny. Moreover, the emergence of hybrid DLT solutions, combining public and private networks, shows promise in addressing these issues. An emphasis here is also made on the importance of smart contract security audits, as vulnerabilities can lead to substantial losses of various natures. It identifies the effort of security assessment of blockchain applications by evaluating exploited vulnerabilities of smart contracts.

[32] Taking note that the reflections on Nick Szabo's work are already made later in this paper. Smart Contracts came in way before in 1994 but the current implementations are Ethereum and Electro-Optical System.

[33] See also footnote 13.

[34] C. T. Nguyen-D. T. Hoang-D. N. Nguyen-D. Niyato-H. T. Nguyen-E. Dutkiewicz, *Proof-of-stake consensus mechanisms for future blockchain networks: fundamentals, applications and opportunities*, IEEE Access, 2019, 7, 85727 ss.

[35] The first functioning implementation of a proof-of-stake cryptocurrency was Peercoin, introduced in 2012. Other cryptocurrencies, such as Blackcoin, Nxt, Cardano, and Algorand followed.

[36] S. De Angelis, *Cybersecurity in Blockchain Technology: A Comprehensive Study*, Ph.D. dissertation, Department of Computer Science, University of Southampton, Southampton, U.K., 2022. 36, 132.
S. De Angelis, G. Zanfino, L. Aniello, F. Lombardi, and V. Sassone, *Evaluating Blockchain Systems: A Comprehensive Study of Security and Dependability Attributes*, in Proceedings of the 10th International Conference on Blockchain Technology (ICBT), vol. 3166, 2022.

By contrast, the previously mentioned VeChain is a hybrid blockchain described as public and permissioned, given that anyone can join the network as a mere user, but only certain nodes are authorised to run certain operations, including validating transactions.

This distinction is important since, as we will see in the next chapters, not only do certain blockchains fit better with supply chain implementations, but they also facilitate compliance with the GDPR. In this regard, to preview the upcoming discussion, we anticipate the following compliance issues rooted in the functioning of DLT as outlined so far:

- In a peer-to-peer network, such as a blockchain or other ledgers belonging to the DLT family, it might not be easy to identify who carries the rights and the obligations set forth in the GDPR. GDPR distinguishes between data controllers (entities that determine data processing purposes and means) and data processors (entities that process data on behalf of controllers). In a decentralised smart contract network, these roles may not be clearly defined. Who is the data controller? Who is the data processor? Are these distinctions applicable to DLT to begin with[37]?
- How to guarantee the "right to rectification" and the "right to be forgotten" where personal data recorded on the ledger can be neither changed nor erased? A change to the ledger would require consensus from the majority of the nodes, which would affect the integrity of the DLT and undermine its credibility before users' eyes;
- GDPR mandates that personal data must be collected for specific, explicit, and legitimate purposes (purpose limitation). Additionally, only the minimum amount of data that is necessary for the envisioned purpose should be processed (data minimization). Given that a smart contract is a contract or is supposed to be a contract (smartly) deployed on the DLT if the parties change their minds how possible would it be to exercise these rights?
- How to comply with the GDPR provisions for pseudonymisation or anonymisation of data? It may not always be possible to anonymise data to avoid the applicability of the GDPR, therefore pseudonymisation could be considered as an alternative without hampering the principles of data accuracy and purpose limitation.
- How to ensure compliance with GDPR which regulates the transfer of personal data outside the European Economic Area (EEA) in the context of data stored on a public blockchain, considering the potential for cross-border data transfer issues arising from the global accessibility of the blockchain?
- Where transaction validation is fully automated, would it be possible to comply with art. 22, which poses strict limitations to automated decision-making regarding data subjects?

Before answering these questions, we need to visualise the broad picture and get to the

[37] It is worth noting that the CNIL has stressed in relation to relation to smart contracts that the developer of the software can be a simple external provider but, if they actively participate in the data processing they can also be found to be a processor or joint controller, depending on their role in the determination of the purposes of processing (note that also here, the CNIL mainly looks towards the purposes, not the means, of processing to determine controllership). Commission Nationale Informatique et Libertés, *Premiers Éléments d'analyse de la CNIL: Blockchain*, September 2018, 3.

core of the issue under consideration, which is the oracles.

2.2. Focus on smart contracts: unpacking the oracles issue

In the previous section, we focused on DLT, and we gave smart contracts only a brief introduction. This is because understanding DLT as ledgers subject to different rules on which transactions are executed, is usually the first step to a correct and gradual understanding of the decentralisation realm. Smart contracts can be understood as the software that executes operations that are then recorded on the distributed ledgers. Specifically, smart contracts are software programmed according to a logic "if, then", meaning that when certain conditions occur, the software executes a given pre-programmed operation. Due to their functioning, smart contracts are deemed to be "self-executing contracts" which, along with DLT, could contribute to disintermediation by replacing the untrustworthy "middleman" with trustworthy automated processes. However, scholars have already questioned and demystified certain hype-driven assumptions about smart contracts[38].

Like they say in the blockchain industry, smart contracts are "neither smart nor contracts"[39], they are software that under certain circumstances may have the value of a legal contract and that upon the meeting of a precondition (the so-called "trigger event")[40], produce results, *e.g.* move a sum from a buyer to a seller. In particular, these contracts are not "smart" because - to date - they are not powered by artificial intelligence[41], but merely execute transactions based on information received from external sources. Since their conceptualisation in 1994, well before the first blockchain came to light[42], Nick Szabo argued that the most compelling applications of smart contracts require access to data about real-world state and events[43]. Szabo's prediction turned out to be true with the advent of Ethereum in 2014, the first blockchain designed to support smart contracts, which requires data sources to unleash the full potential of smart contracts as stated by some of its founders.[44] These sources are referred to in blockchain industry jargon as "oracles", and can be categorised as machine-based oracles, meaning fully automated sources in the form of software, databases, or robots, and human-based oracles, which imply assessments by trusted persons, entities, or

[38] See A. U. Janssen-F. P. Patti, *Demistificare gli smart contracts*, in *Osservatorio del Diritto Civile e Commerciale*, 1, 2020, 31 ss.

[39] This expression is widely used in the blockchain industry, albeit it is unknown who first said it.

[40] See A.U. Janssen-F.P. Patti, *Demistificare gli smart contracts,* cit., 34.

[41] C. Jacobs -C. Lange-Hausstein*, Blockchain und Smart Contracts: zivil- und aufsichtsrechtliche Bedingungen*, IT-Rechts-Berater, 2017, 10, especially 13. M. Kaulartz-J. Heckmann, *Smart Contracts – Anwendung der Blockchain-Technologie*, in *Computer und Recht*, 2016, 618.

[42] Bitcoin debuted in 2008.

[43] N. Szabo, *Smart Contracts*, 1994, in *szabo.best.vwh.net*. See also G. Wood, *Ethereum: A Secure Decentralised Generalised Transaction Ledger*, Ethereum Project Yellow Paper, 2014.

[44] V. Buterin, *Ethereum: A Next-Generation Smart Contract and Decentralised Application Platform*, 2014, in *github.com.*

bodies. An automated source could be a database that communicates a stock price to a financial instrument managed by smart contracts on a blockchain[45], as well as a database that communicates a flight delay to a smart contract to process compensation for delays in favour of customers[46].

If the trustworthiness of a smart contract depends on the sources it is powered by, it means that the problem of trust does not disappear, but has to be analysed by turning elsewhere, that is, to oracles. Dealing with the problem of trust in oracles implies, first and foremost, dealing with information reliability[47]. For instance, in the context of commerce, what could be a reliable source to determine whether or not a force majeure event occurred objectively and prevented the seller from fulfilling its obligations towards the buyer? Certain authors suggest that in this kind of situation, where a form of evaluation is required, trusted third-neutral parties should provide assessments as opposed to automated data sources[48].

That said, assuming that for certain use cases, it is possible to find viable and reliable oracles, be they machines or humans when the information provided by the oracles and received by smart contracts include personal data, additional questions arise as to the adequacy of these technologies to ensure data privacy and minimise security issues[49].

Issues pertaining to trust and GDPR compliance are two sides of the same coin, in the sense when it comes to entrusting oracle operators or any other service providers with sensitive data, it is important to consider various factors and potential risks. We argue that some of the key aspects of data privacy and security risks and trust in Oracle operators lie in operators often handling sensitive data, making potential threats a significant concern. Risks encompass the possibility of data breaches where unauthorised access could lead to data theft, financial losses, and damage to an organisation's reputation. Inadequate encryption of data during transmission or storage can render it vulnerable to malicious actors. Insider threats, such as employees mishandling data intentionally or accidentally, pose another risk. Non-compliance with data protection regulations like GDPR can result in legal consequences and fines. Furthermore, the issue of data ownership and control must be clearly defined when entrusting oracle

[45] F. Zhang-E. Cecchetti-K. Croman-A. Juels-E. Shi, *Town Crier: An Authenticated Data Feed for Smart Contracts*, in Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS'16) (Association for Computing Machinery, New York, NY, USA, 2016) 270.

[46] Compensation for flight delays or cancellation under Regulation (EC) no. 261/2004 of the European Parliament and of the Council of 11 February 2004 is a use case often referenced by scholars. Specifically, we refer to A. U. Janssen-F. Paolo Patti, *Demistificare gli smart contracts*, cit., 37, which in turn refers to the following sources: C. Buchleitner-T. Rabl, *Blockchain und Smart Contracts*, in *ecolex*, 2017, 7; M. Fries, *Schadensersatz ex machina*, in *Neue Juristische Wochenschrift*, 2019, 90.

[47] Lack of reliable data feeds is often cited as an obstacle to make certain use cases feasible. For instance, see G. Greenspan, *Why Many Smart Contract Use Cases Are Simply Impossible*, in *coindesk.com,* April 17, 2016.

[48] T.F.E. Tjong Tjin Tai*, Force Majeure and Excuses in Smart Contracts*, in *European Review of Private Law*, 26, 2018, 787.

[49] In addition, the outcome processed by a smart contract could feed another connected smart contract, and so the smart contract serves in turn as an oracle to another smart contract, which is often the case in decentralised finance applications.

operators with data, ensuring the data subject can concretely exercise the rights to access, modify, and delete its own personal data.

2.3. Further down the rabbit hole: from a basic use case, to supply chain management

As we know, personal data protection is centred around the duties to be fulfilled by the "data controller", meaning the subject who determines the purposes and means of the processing of personal data. Partly similar, partly different duties also rest with the "data processors", meaning the individuals or entities that process personal data on behalf of the controller. The "data subject", the identified or identifiable natural person whose personal data is processed[50], is the protected party under the GDPR and should therefore always be taken into account when building a network of contractual relationships and data sharing, along with an IT infrastructure to support this network.

Based on this premise and the roles within the data protection realm, to further understand the issues posed by oracles, consider a basic example of a smart contract, such as "Fizzy". Fizzy was developed by Axa, launched in 2017, and supported until 2019, and designed to manage insurance and compensation against airline flight delays or cancellations in compliance with Regulation (EC) 261/2004; in other words, a sort of "smart insurance". The project, which perhaps arrived too ahead of its time, is reportedly discontinued by Axa due to obstacles to mass adoption but still serves well as a case study. The first version of Fizzy relied on smart contracts fed by data provided by Axa itself. Given this context, the flight would qualify as a data subject, while Axa, the company directly selling the insurance to the customer, would be the data controller within the contractual relationship. As Axa used its database to feed the smart contracts, no proper oracle existed, and therefore no other controller or processor would have been involved in this processing of customers data[51].

However, in 2019, recognising the need for trusted neutral data sources, Axa moved to FlightStats to data feed the smart contracts. In this case, we had a real machine-based oracle, but since no personal data was sent by FlightStats to Axa's smart contract, and *vice versa* no customer's personal data was sent by Axa's smart contract to FlightStats, apparently this data sharing process did not trigger any obligation under the GDPR. However, one must consider the implications under art. 22 of the GDPR, which governs automated decision-making and provides that «the data subject shall have the right not to be subject to a decision based solely on automated processing» and that «the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision». Where could human intervention take place within Fizzy's

[50] For the precise definitions refer to art. 4, nos. 1 and 7, of the GDPR.

[51] Under art. 4, no. 8, "processor" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

scheme? If Fizzy 2017 left some room for human intervention as the smart contract was fed by Axa itself, Fizzy 2019 evolved into a system where an external data source directly fed the smart contract. It is arguable whether or not this system left room for human intervention. Moreover, the subject matter handled by Fizzy pertained to a delicate and longstanding consumer protection issue, that is right to reimbursements under Regulation (EC) 261/2004. Could consumers' rights be overridden by automated decision-making? In our opinion, Axa deployed a fascinating tool, yet quite controversial given its capability to impact the rights of individuals through automated decision-making. If the project had not been dismissed, maybe further measures should have been considered to avoid a data processing activity in breach of art. 22 of the GDPR.

That said, Fizzy presents us with a concrete opportunity to ponder more about the questions raised at the end of Chapter 2.1 as to the adequacy of DLT and smart contracts to ensure privacy. Fizzy ran on the Ethereum blockchain, which is public and permissionless, and consequently makes transparent and readable to anyone any transaction recorded on the ledger, including flight reimbursements processed by Fizzy. It is worth noting that the Ethereum ledger does not contain any information that allows to directly identify parties to transactions; however electronic wallet numbers could in theory open the door to an indirect identification of parties. Specifically, Axa, the data controller, collected data other than the wallet numbers and was therefore in a position to identify the customers. In addition, consider that Ethereum was designed to make immutable any information therein recorded. How could Axa ensure the right to be forgotten and the right to rectification? About the deletion of data, Axa could have deleted the data allowing direct identification that it kept outside the blockchain, to prevent the wallet tracked on the blockchain from being traced back to a precise individual; while for the rectification of data, for instance in the case of errors, the doubt still remains. Immodifiability of data, especially in cases of errors in the processing of refunds, further exacerbates the previously discussed problem of automated decision-making under art. 22.

In sum, the Fizzy case, even though it did not involve personal data sharing by Axa to other players, already manifested the issues inherent with the use of DLT, smart contracts, and oracles. Now, imagine a wider mechanism, where personal data sharing occurs among different data controllers and to track and manage via blockchain a wide range of contractual obligations, which could be the case within a supply chain. Consider the fashion industry. End-users may place clothes purchase orders in person at the store or remotely via an online application, and the seller could gradually collect information about the customers' preferences. Then this information could be shared through an IoT-based system with the players involved in the supply chain so that each supplier could manage production following the aggregated market demand. In turn, the end-user could read information about the products and the suppliers involved and - for instance - make the conscious decision to purchase only clothes that adhere to certain sustainability criteria, but the economic players of the supply chain could as a result learn more about the buyer's ideology, which could qualify as a processing of sensitive data under art. 9 GDPR. The system as a whole could rely on the use of DLT, and all the features that come with it, including smart contracts and oracles. As we mentioned in the introduction to this work, examples of that technological convergence already exist within certain blockchain ecosystems that got traction due to their suitability for supply chain management, such as VeChain.

Similar scenarios may be envisioned for growing sectors, such as smart fridges, IoT health devices, and smart cars, which by design would collect sensitive personal data of the users.

3. Advanced solutions to the oracles issue

We introduced the elements of the technology at the centre of our analysis in Chapter 1 and highlighted some of the general key issues of making technology trustworthy and compliant with the GDPR. In Chapter 2 we provided more information on DLT, smart contracts and oracles, explaining the problems these technologies can bring for GDPR principles when used in multi-party contexts, such as typical SCM situations. The next step is to indicate potential solutions to such issues. We reiterate that the scope of this paper is to examine a fraction of a larger matter, that is trust towards oracles and privacy protection in the context of the supply chains that use DLT and smart contracts, thus requiring oracles. Accordingly, the solutions we are going to propose pertain to this specific phenomenon.

Starting with the legal grounds to deploy such technologies, it is worth noting that the Data Act does not introduce any new legal basis, as highlighted by provisions such as art. 4, para. 12, and art. 5, para. 7, which refer to the GDPR, precisely art. 6 on the legal bases for processing in general, and art. 9 for the special rules concerning sensitive data. This interpretation is expressly given under Recital 7 of the Data Act, according to which «This Regulation does not constitute a legal basis for the collection or generation of personal data by the data holder». Therefore, the legal bases remain exclusively the ones we have become accustomed to under the GDPR. Which of these legal bases should be adopted is, however, another matter. Identifying a legal basis is a case-by-case process, which requires looking at the specific activities, purposes and means of a given processing. Mapping all potential case studies is actually out of the scope of this work. However, for the purpose of further research, we suggest that consent could be the legal basis to be privileged, given the following arguments. Firstly, IoT is evolving with a view at contract automation, and regardless whether this future will be dominated by AI, deterministic blockchain-based smart contracts, a mix of both, or something totally new yet to come, where automated decision-making is involved in personal data processing activities, art. 22 of the GDPR applies apart from a few exceptions indicated by that same article. Secondly, it is reasonable to imagine that in a network of economic players traced via IoT, having the end-user and its data at the centre, contractual performance could not be invoked as a basis for covering all possible interests and purposes of data processing, which makes the exception under art. 22, para. 2, lit. a), non applicable. Last but not least, one should consider concrete human behaviours, and so the possibility of data subjects inadvertently transmitting data falling within the sensitive categories outlined in art. 9, which reinforces the idea that consent should be the primary basis for any data collection meant to feed the SCM.

Coming to the focus of our work, which is reconciling the oracle issue with GDPR in the context of SCM based on IoT and DLT, our guiding beacon in this mist is art. 25 of the GDPR, which expresses two pillar principles of data protection:

- "privacy by design", according to which both at the time of the determination of the means for processing and at the time of the processing itself, the data controller shall implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation;
- "privacy by default" according to which the controller shall implement appropriate technical and organisational measures for ensuring that only personal data which are necessary for each specific purpose of the processing are processed.

In other words, it is a matter of considering privacy since the design phase of a personal data processing activity and processing only the personal data necessary for the purpose. Both principles categorise the "appropriate measures" as technical and organisational. For the purpose of this work centred on reconciling law with technology, we will focus on technical measures, which consist of certain advanced solutions available to enterprises. It is worth noting that this rule is mirrored by art. 32, concerning security of processing, which expressly indicates among the measure that, *inter alia*, could ensure a level of security appropriate to the risk, pseudonymisation and encryption of personal data, which are foundational pillars of the blockchain technology. This suggests that, in principle, blockchains should not be seen as an obstacle to the implementation of privacy. On the contrary, this technology, or rather, the cryptography behind it, was envisaged since the days of the cypherpunks movement in the 1980s and 1990s as a way to preserve individuals' privacy. The GDPR today confirms the possibility of this synergy between law and technology; it is therefore a matter of accommodating the pro-privacy aspects already present by design and by default in the blockchains, while working around the aspects conflicting with the GDPR. The next sections of this work are meant to address such aspects.

3.1. Trust and privacy since the foundations

To effectively engage with the issues that oracles pose to privacy, one should firstly consider the technical framework on which oracles operate. As explained throughout Chapters 1 and 2, oracles provide information to the smart contracts, and as a result some information are recorded on the distributed ledger on which the smart contracts run. In other words, DLT and smart contracts are the foundations of the ecosystem where oracles operate. That is true for any use case, including supply chains[52]. There-

[52] We mean that, regardless of the use case, which may be providing an online platform or tracking a supply chain, smart contracts on Ethereum are all designed and executed through the Ethereum Virtual Machine (EMV), a kind of virtual computer decentralised according to peer-to-peer logic that is used to deploy smart contracts on Ethereum and other blockchains designed to support this machine and

fore, before even considering the involvement of oracles in the data processing activities, enterprises interested in tracking their supply chains via DLT and smart contracts should select means that are adequate, by design and by default, to preserve privacy.

In the previous Chapters we have highlighted certain disadvantages in terms of privacy deriving from the use of DLT, we must therefore indicate certain measures to mitigate the risks. We have anticipated that not all distributed ledgers are the same and that not all are public and permissioned. In this respect, we point out that in the context of a supply chain, a federated blockchain where companies or *consortia* of companies are the nodes, could be a fitting solution both in terms of increasing trust and mitigating privacy risks. Having as nodes exclusively parties that are presumably interested in the trustworthiness of the ledger is positive because, in principle, it should create a context in which all parties are either supervisors and supervisees of each other, without interference by other players. Where there is an interest of the business parties in making information available to the customer base (consider the possibility of the customer tracking the provenance of the product and the raw materials used for the production) certain data could be made public, while maintaining the authorisation to validate operations on a permissioned basis. In addition, to make the distributed ledger governance more agile, and facilitate the achievement of a majority that can take action to rectify data or delete data that could indirectly identify individuals, enterprises should consider proof-of-authority as a consensus mechanism, rather than the previously mentioned proof-of-work and proof-of-stake. Proof-of-authority is, in simple terms, a mechanism where each node stakes its authority and credibility within the ecosystem, and where decision-making is weighted in proportion to these parameters. All this might sound blasphemous to decentralisation and Bitcoin purists, but one has to consider that there are different problems and different goals at stake and that one size does not fit all. Bitcoin was designed to disintermediate financial systems. Solutions such as those suggested here for supply chains do not aim at removing intermediaries, but rather at establishing conditions of mutual trust and traceability, with ultimate benefits for businesses and customers.

Moreover, one should remember that the DLT family is wide and includes solutions other than blockchains, such as Tangles, among which we mention the IOTA protocol, a Tangle specifically designed for supply chains and IoT, as the name already evokes[53]. In other words, depending on the type of supply chain and the needs of the supply chain tracking project, stakeholders should consider the most appropriate type of DLT to strike the balance between business agenda, trust, and privacy protection. In this regard, it is worth remembering that DLT offers not only privacy disadvantages but also advantages. For instance, pseudonymisation dominates in the world of DLT, which is a good measure to preserve users' privacy and is expressly invoked by the principle of privacy by design in art. 25, para. 1, of the GDPR. We have also mentio-

benefit from smart contracts. Without smart contracts and without a blockchain supporting them, which means, namely without the EVM, there would be no manner for said oracles to communicate affect operations tracked on decentralised ledgers. More information on the EVM is available at the official website of Ethereum.

[53] See S. Popov, *The Tangle*, April 30, 2018.

ned that DLT raises problems of overload. In this regard, we note that the necessity of minimising the number of data recorded on the ledger reconciles nicely with the principle of data minimisation. Thus, a supply chain tracking project based on DLT and smart contracts should aim at reducing the data recorded on the ledger to the essential minimum. For instance, an on-ledger recording could be limited to hashes of operations and identification codes of the wallets, while personal data storage could rely on separate centralised and traditional databases that do not present problems in terms of a right to rectification and right to be forgotten. This way, there can be a bridging of the gap between the technical world, which brings solutions, and the legal world, which protects rights and imposes obligations to safeguard those rights.

Measures relating to smart contracts also deserve a mention. Since we are dealing with a context where companies will presumably share data, based on data-sharing agreements, the smart contracts used in supply chains to execute these agreements should meet the requirements of art. 36 of the Data Act. As we said, this analysis is focused on data protection, and therefore the GDPR is the primary source we are analysing, but there are important reasons to mention this article:

- The requirements laid down by the Data Act apply to agreements among businesses to make data available, and since the legislator did not specify "non-personal data" as it did in other provisions, one should conclude that said rules also apply to smart contracts that make personal data available. This leads to the conclusion that art. 36 in a sense complements the GDPR;
- Among the requirements listed by art. 36, the obligation to provide a "kill switch" function for the smart contract, to stop it where needed stands as a rule of primary importance to rectify mistakes, as well as to rectify or delete data, with benefits both in terms of trustworthiness and privacy-preservation[54].

3.2. Solutions specifically addressed to oracles

Having explained how the risks associated with the foundations of the framework on which oracles operate - i.e. DLT and smart contracts - can be mitigated and privacy preserved, it is time to explore some of the technical measures that could be fruitfully applied to oracles themselves. Specifically, this section delves into decentralised oracle networks and advanced solutions. Elements deemed pivotal for stimulating the security of sensitive supply chain information in the dynamic realm of contemporary supply chain management like reputation-based assessment, and privacy-preserving techniques, external adjudication, data authentication, and data integrity are delved into. The intricate landscape of decentralised technologies is considered to seek to contextualise these findings within the broader domain of cutting-edge solutions. The seamless fusion of a comprehensive literature review with contextual insights forms the bedrock of our approach, enriching our understanding of the dynamic interplay

[54] Precisely, the requirement is explained under art. 36, para. 1, lit. b) of the Data Act as follows: «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».

between oracles and advanced technologies in supply chain management.

That said, we will either have solutions aimed at the problem of trust, and solutions aimed at privacy preservation, highlighting the interplay between them where present. Reputation-based assessment, facilitated by Oracle's reputation scoring mechanisms, is a cornerstone of evaluating the trustworthiness of supply chain entities based on their historical performance and interactions[55]. This approach relies on Oracle's reputation scoring mechanisms, which are likely algorithms or systems developed by Oracle to analyse and quantify the reputation of various entities involved in the supply chain. In practical terms, Oracle's reputation scoring mechanisms may take into account factors such as the entities' track record, adherence to contractual agreements, on-time deliveries, quality of products or services, and overall reliability[56]. The goal is to assign a numerical or qualitative score that reflects the level of trust that can be placed in each supply chain participant[57] .This reputation-based assessment is crucial for decision-making processes within the supply chain[58]. It helps stakeholders, such as manufacturers, distributors, and retailers, make informed decisions about which entities to engage with based on their past performance and reliability. By leveraging Oracle's reputation scoring mechanisms, the assessment aims to provide a standardised and data-driven approach to evaluating and ensuring the trustworthiness of supply chain partners[59].

This approach is complemented by privacy-preserving techniques, including encryption and tokenization, which safeguard sensitive information and ensure authorised access. Encryption involves converting information into a code to prevent unauthorised access. Encryption ensures that even if someone gains access to the data, they cannot understand or use it without the proper decryption key. In the context of supply chain management, sensitive information such as customer details, financial transactions, or proprietary data can be encrypted to protect it from unauthorised viewing or tampering[60]. Tokenization is a process where sensitive data is replaced with unique

[55] S., Radivojevic-K., Nabrzyski *et al.*, Persona preserving reputation protocol (P2RP) for enhanced security, privacy, and trust in blockchain oracles, in *Cluster Comput*, 2024.
Another paper with a deeper insight on the existing blockchain-based reputation systems, provides a model harnessing an intrinsically economically incentivized approach to bolster agent integrity. See, H. Wen-T. Huang-D. Xiao, *An Intrinsic Integrity-Driven Rating Model for a Sustainable Reputation System*, Ithaca, 2023.

[56] See this in the thesis of A. Gucciardi*, Trustless contract management: a study on the benefits of blockchain-based smart contracts,* 2023, Politecnico di Torino, Master's Degree in Engineering and Management.
Also see A. Rijanto, *Blockchain technology adoption in supply chain finance*, in *Journal of Theoretical and Applied Electronic Commerce Research*, 16(7), 2021, 3078 ss.

[57] K. Almi'Ani-Y. C. Lee-T. Alrawashdeh-A. Pasdar, *Graph-Based Profiling of Blockchain Oracles*, 11, 2023, 24995 ss.

[58] *Ibid.*

[59] Y. Wu-Y. Zhang, *An integrated framework for blockchain-enabled supply chain trust management towards smart manufacturing*, in *Advanced Engineering Informatics*, 51, 2022, 101522 ss.; Also see, J. M. Jorquera Valero-P. M. Sánchez-M. Gil Pérez-A. Huertas Celdrán-G. Martínez Pérez, *Toward pre-standardization of reputation-based trust models beyond 5G*, in *Computer Standards & Interfaces*, 81, 2022.

[60] O. L. Van Daalen, *The Right to Encryption: Privacy As Preventing Unlawful Access*, in *Computer Law & Security Review*, 49, 2023, 105804 ss.; another great reference on Encryption is P. Loshin's, *Simple Steps to Data Encryption,* in *Syngress*, 2013.

identifiers called tokens[61] (this process should not be confused with the homonymic crypto-asset creation process generally associated with the blockchain sector). These tokens are typically random and hold no meaningful information by themselves. The actual sensitive data is securely stored in a separate location, and only authorised parties with the proper authentication can retrieve and use it. Tokenization helps in minimising the exposure of sensitive information, reducing the risk of data breaches[62]. By implementing encryption and tokenization, the supply chain system aims to enhance the overall security of the data it handles[63][64]. This ensures that sensitive information is kept confidential and can only be accessed by authorised individuals or systems, thereby mitigating the risk of data breaches or unauthorised use.

External adjudication, involving third-party entities and leveraging DLT-based smart contracts or blockchain technology, further enhances trust in the supply chain. An additional layer of trust and transparency is introduced into the supply chain management system. This is achieved through external adjudication, which involves the participation of third-party entities. Furthermore, this process is facilitated by the utilisation of DLT-based smart contracts or blockchain technology. The involvement of independent third-party entities or organisations is in resolving disputes, validating transactions, or ensuring compliance within the supply chain[65]. Having external entities oversee certain aspects of the supply chain, it adds an impartial and objective perspective, contributing to increased trust among participants[66].

Concurrently, data authentication, implemented through digital signatures or certificates, verifies data integrity across the supply chain, supported by features like checksums and audits in Oracle's advanced solutions to maintain accuracy and consistency[67]. It outlines yet another aspect of ensuring trust within the supply chain. Data Authentication involves verifying the authenticity of data to ensure that it has not been altered or tampered with during transmission or storage. This is achieved through the use of digital signatures or certificates, which provide a secure way to confirm the origin and integrity of the data. Checksums and Audits in Oracle's Advanced Solutions incorporate additional measures such as checksums (a mathematical value derived from the data) and audits to maintain the accuracy and consistency of data. Checksums help detect errors or discrepancies in data, while audits provide a systematic review of processes to ensure compliance and reliability[68].

[61] S. Ahmad-S. Paul-A.P. Singh, *Tokenization based service model for cloud computing environment*, International Conference on Inventive Computation Technologies (ICICT), Coimbatore, India, 2016.

[62] *Ibid.*

[63] B. Vagadia, *Data Integrity, Control and Tokenization*, in *Digital Disruption. Future of Business and Finance*, Cham, 2020.

[64] J. Xia-H. Li-Z. He, *The Effect of Blockchain Technology on Supply Chain Collaboration: A Case Study of Lenovo,* in *Systems* 11, 2023, 299 ss.

[65] S. D. Levi-A.B. Lipton, *An Introduction to Smart Contracts and Their Potential and Inherent Limitations*, in *Harvard Law School Forum on Corporate Governance*, 2008.

[66] S. Penzo-N. Selvadurai, *A hard fork in the road: developing an effective regulatory framework for public blockchains*, in *Information & Communications Technology Law*, 31(2), 2022, 240 ss.

[67] Oracle, Security Guide for Release 3.0.1 Security Features for Oracle Private Cloud Appliance.

[68] *Ibid.*

Despite the manifold benefits of these advanced solutions, challenges in their implementation and maintenance persist. Reputation-based assessment, which aids decision-making, faces difficulties in accurately evaluating entities' reputations, particularly when relying on historical data. Fluctuations in performance and changes in business practices may not be immediately reflected, posing a challenge to real-time trustworthiness assessments. The implementation of privacy-preserving techniques may introduce complexity in data sharing and collaboration, necessitating a delicate balance between data security and seamless collaboration, especially with multiple stakeholders involved. Relying on external adjudication introduces dependencies on third-party entities, and delays in dispute resolution or issues with the external validation process may impact the timely flow of data, potentially causing operational disruptions.
While data authentication is crucial, managing the infrastructure for digital signatures and certificates requires careful planning. Issues related to key management, certificate expirations, or compromised keys can undermine the effectiveness of these authentication mechanisms. Maintaining data integrity faces challenges related to the volume and diversity of data in supply chains, necessitating continuous monitoring and adjustment to ensure consistency across various data sources and formats, particularly in a rapidly changing environment.

4. Conclusions

Throughout this work we have tried to convey that while smart contracts on DLT platforms could offer transparency and automation, integrating them effectively with IoT devices for supply chain management poses either risks or opportunities.
Trying to summarise our findings about risks, it is worth highlighting that blockchains and smart contracts were conceived to disintermediate and replace trust in intermediaries with automation; however, the need for oracles brings into the equation new types of intermediaries for data-feeding purposes. Paraphrasing the brilliant conclusions expressed by Janssen and Patti, the more oracles are added to the equation, the more the automation is reduced as a result of the intermediate steps performed by the oracles before "self-execution" occurs[69]. We add that the more oracles are involved, the more privacy could be undermined where principles such as data minimisation, limitation of purpose, and privacy by design and by default are not concretely applied. However, risks could be mitigated by applying the principles laid down in the GDPR. Some basic examples of how these principles could be fruitfully applied (and data security increased as a result) include not sharing personal data with oracles unless this is strictly necessary for the purpose of the smart contract, not processing personal data for purposes other than the execution of the contractual relationship, thus avoiding profiling and marketing activities to which the data subject has not expressly and freely consented. On this basis, businesses should adopt only IT infrastructure made of DLT, smart contracts, oracles, that offer or allow the implementation of and technical measures that are adequate to comply with the principles of privacy by design and by

[69] A.U. Janssen-F. P. Patti, *Demistificare gli smart contracts*, cit., 41.

default.

We also suggest that, based on the needs of the considered supply chain, the SMC via DLT and smart contracts should be carried out with a vision aimed at limiting the involvement of human-based oracles in data processing operations, and favouring the use of machine-based oracles in operations involving the processing of non-personal data, in order to seek a balance between the need to limit the sharing of personal data among multiple players from the GDPR compliance perspective, and the ambition to maximise the possibilities of disintermediation and automation offered by DLT from the business perspective.

In terms of opportunities, in the context of the supply chain, leveraging DLT-based smart contracts or blockchain technology could enhance trust by creating a tamper-resistant and transparent system. This is meant to lead to more efficient and reliable execution of contracts, transactions, and data management.

Also, with regard to opportunities, the vagueness of the GDPR and the open interpretation of the risk-based approach, which we highlighted as a critical point at the beginning of this work, could be turned into an opportunity for significant experimentation and innovation. This means that what is not expressly prohibited should be considered as permitted, and what is not expressly mandated should not necessarily be implemented, as long as companies adhere to the principles of the regulation. Regarding prohibitions, it is worth noting that no provision of the EU legal framework sets out limitations on the use of DLT, smart contracts, and the consequent involvement of oracles. Regarding mandatory requirements, we cite the obligation to include a kill-switch function set forth in art. 36 of the Data Act, which in our opinion should be considered something limited to the scope of application of that very regulation and article, without application by analogy to any data processing activity based on smart contracts that could occur in SMC.

In conclusion, bringing together the points expressed so far, we believe that interpretations that prioritise data protection over the free movement, which is also part of the balance as suggested by the full title of the GDPR itself, may ultimately limit the EU's role as a hub of technological innovation, especially considering that so far this region has shown a greater inclination towards regulation rather than innovation. If the integration of IoT, DLT, and smart contracts into SMCs were to pose more practical challenges than benefits, it would be reasonable for companies to spontaneously abandon them and redirect their efforts towards the new trends of the moment, but the law should not be the cause of such an abandonment. And if and when such change of trends occurs, then we, legal scholars, will be there again questioning the replacing technologies and their implications for the law, and history will repeat itself.