LEDGER
ledgerjournal.org

ISSN 2379-5980 (online)
DOI 10.5195/LEDGER.2025.392

An Invitational Research Article from the INATBA Blockchain Horizons Academic and R & D Forum 2024

Blockchain for Democratic Justice: Innovating the Service of Judicial Documents to Uphold the Rule of Law

Ioannis Revolidis,* Marica Ciantar,† Joshua Ellul‡

Abstract. The service of judicial documents is fundamental to ensuring access to justice, as outlined in Article 47(2) of the Charter of Fundamental Rights. This paper explores the evolving legal framework for serving judicial documents in the EU, with a particular focus on the Recast Service of Documents Regulation. The Regulation introduces the possibility of electronic service, addressing inefficiencies in traditional methods. However, challenges remain due to varying national procedural laws and technological limitations. This paper examines how blockchain technology could enhance the electronic service of judicial documents, offering a more secure, efficient, and interoperable solution across Member States. By leveraging blockchains' decentralised and immutable characteristics, the service process could become more reliable, particularly in cross-border disputes, thus strengthening procedural guarantees within the EU.

1. Introduction

The service of judicial documents lies at the heart of the right of access to justice as per Article 47 of the Charter of Fundamental Rights of the EU.[1] The right of access to justice encompasses multiple procedural dimensions that aim to entrench the principles of the rule of law during civil litigation.[2] It guarantees access to remedies, a fair judicial hearing, effective redress, and effective judicial protection.[3]

The legal regime regulating the service of judicial documents plays a pivotal role in delivering the procedural guarantees established under Article 47(2). It establishes a delicate equilibrium between the procedural positions of the opposing litigating parties, the plaintiff and the defendant.[4] For the plaintiff, who seeks judicial redress and aims to change the current legal and factual status quo of a legal relationship, access to justice means initiating the litigation process and the appointment of a natural judge to oversee the satisfaction of their legal rights within the lawsuit's parameters. For the defendant, the service of documents is the primary act informing

* I. Revolidis (ioannis.revolidis@um.edu.mt) is a resident academic within the Faculty of Laws and the Centre for DLT at the University of Malta, Malta.

† M. Ciantar (marica.ciantar.17@um.edu.mt) is an MSc graduate in Blockchain and Distributed Ledger Technologies from the University of Malta's Centre for DLT and an Independent Legal Practitioner.

‡ J. Ellul (joshua.ellul@um.edu.mt) is an Associate Professor within the Department of Computer Science and the Centre for DLT at the University of Malta, Malta.

them of a procedural attack, allowing them to understand the litigation's details and prepare their defence. Due process is fundamental here, as the defendant must be afforded a fair opportunity to participate in litigation without compromising their ability to mount a defence.[5]

The importance of proper service of judicial documents becomes even more critical in international litigation, where the procedural adversaries are domiciled in different states. In such situations, the vulnerability of the rights of the litigating parties becomes more pronounced.[6] The plaintiff risks not obtaining access to justice if the international service of judicial documents is ineffective. The defendant must learn about a legal action pending in courts outside their domicile or residence within appropriate time and circumstances. They face additional judicial challenges, as they will likely need to engage with a foreign legal and procedural system, adding burdens such as double representation, increased litigation costs, and language and cultural barriers. Thus, in international litigation, the legal framework regulating the service of judicial documents must balance the plaintiff's right to quick and effective remedies and the defendant's right to a fair defence. In the EU, this balance is guaranteed by the Recast Service of Documents Regulation, which traditionally protects the procedural rights of litigant parties in cross-border proceedings within the common judicial area.[7]

One might argue that such procedural guarantees are unnecessary in digital spaces, especially blockchain environments, where the rule of code ostensibly ensures the rights and obligations of stakeholders. However, these procedural guarantees become even more important in an increasingly digitised and interconnected world where fundamental rights are constantly at stake. Blockchain spaces are no exception. By introducing new economic, social, and financial models and facilitating engagement with digital assets, blockchains create vibrant transactional spaces where rights and obligations are rapidly exchanged. Although the architecture of blockchains provides critical guarantees for smooth stakeholder transactions, such as decentralised and immutable provenance and automatic enforcement of obligations, they are not free from frictions and disputes. While blockchains effectively address the double-spending problem, they cannot guarantee that malicious actors will not feed the blockchain with faulty input (*e.g.*, regarding the ownership of digital assets) or attempt to defraud unsuspecting users by hacking their digital assets. Thus, access to justice and effective service of the relevant judicial documents remain imperative.[8]

Blockchains have the capacity to influence the process of serving documents in multiple ways.[9] The European Parliament and the Council have decided that digital means can be deployed in the service of judicial documents within the common EU judicial area, particularly when service is to be effected against a defendant with a known identity and address in the EU.[10] In that sense, it is worth exploring whether blockchains can enhance the procedural guarantees of such electronic service.

The deployment of blockchain technology in the realm of digital service of documents within the EU has largely remained unexplored. This paper aims to close that gap by exploring the relationship between blockchains and the service of judicial documents under the Recast Service of Documents Regulation. Specifically, it will examine whether blockchains can contribute constructively to the digitisation of the process of serving judicial documents between EU Member States. While disputes become increasingly digitised, the service of documents is primarily conducted through traditional means. The Recast Service of Documents Regulation marks a step towards deploying digital means, and blockchains might offer a technological

ISSN 2379-5980 (online)
DOI 10.5195/LEDGER.2025.392

solution that elevates the procedural guarantees introduced by the EU legislature.

To achieve this goal, the paper is structured as follows: Section 2 introduces and explores the Service of Documents Regulation, focusing on the digitisation initiatives undertaken by the European Parliament and the Council, their underlying purposes, controversies, and limits. Section 3 builds on section 2, using its findings on the digitisation of the service of judicial documents under the Recast Service of Documents Regulation to present a conceptual framework on how blockchains might contribute to this process. The final part concludes and points to topics that merit further research.

2. The Digitisation of the Service of Judicial Documents Under the Recast Service of Documents Regulation

2.1. The Service of Judicial Documents in the EU, A General Appraisal—To ensure the procedural rights of EU litigants as outlined in the introduction, the European Parliament and the Council have intervened in the process of serving judicial documents in cross-border disputes within the EU. This intervention, in its current iteration, is embodied in the Recast Service of Documents Regulation, which was enacted relatively recently to address the limitations of the previous regime established under Regulation 1393/2007. Despite the changes introduced by the Recast Service of Documents Regulation, the basic mode of operation remains similar to that in Regulation 1393/2007.

It is important to note that the Recast Service of Documents Regulation applies only when litigant parties need to serve documents from one EU Member State to another, typically when the parties are domiciled in different Member States.[11] The Regulation provides various methods to effect such service, with no hierarchical relationship between them; they all stand on equal footing.[12] However, until the enactment of the Recast Service of Documents Regulation, this process was conducted through traditional, often unreliable, cumbersome, and time-consuming means.

The traditional method of service is established in Article 8 of the Regulation, namely, service via the transmitting and receiving authorities. Under this arrangement, Member States designate national authorities responsible for transmitting judicial documents abroad and receiving such documents from other EU jurisdictions. If a plaintiff in Member State A (which is normally the person responsible for service) wishes to serve a document to a defendant in Member State B (which is normally the addressee of such service), the plaintiff, after filing their lawsuit as required by the procedural law of Member State A, submits the documents to the transmitting agency in Member State A. The agency acknowledges receipt, which bears significant legal consequences as it marks the point at which the plaintiff meets certain procedural obligations, including critical deadlines regarding their claims. The agency then transmits the documents to the receiving authority in Member State B, typically sending the physical documents of the lawsuit via postal services. Upon receipt, the receiving authority in Member State B attempts to locate the defendant, which usually involves verifying their identity and inquiring about their premises. If successful, the documents are delivered to the defendant in Member State B.[13]

The European Commission has acknowledged that, in the context of service through transmitting and receiving agencies, Member States have traditionally been hesitant to deploy digital tools. The processing of requests, the transmission of documents, and the communication between the

ISSN 2379-5980 (online)
DOI 10.5195/LEDGER.2025.392

agencies were based on traditional, mostly paper-based, communication methods. This approach has severe limitations.[14]

Empirical data gathered during the preparation of the Recast Service of Documents Regulation indicate that serving documents abroad continues to encounter significant delays. The cumulative time required for the designated transmitting and receiving agencies to complete their actions often extends to several months.[15] Such extended waiting periods can be detrimental to the rights of litigant parties, as access to justice becomes available only after the service process is completed. If parties must wait months for the service process to be completed, the overall processing time of their actual case can become untenable. While these delays in the traditional method of service via transmitting and receiving agencies can be attributed to multiple factors,[16] it must be stressed that the efficient conduct of legal proceedings within an integrated European Union requires the swift service of judicial documents. Prolonged delays undermine the effectiveness of legal processes and the right to timely justice.

One might expect that alternative service methods could prove more effective. Postal service, as per Article 18 of the Recast Service of Documents Regulation, presents an interesting alternative. Indeed, postal service can be more straightforward as it does not involve the transmitting and receiving agencies. If the plaintiff in Member State A knows the address of the defendant in Member State B, they can send the judicial documents via the postal services available to them. Processing time can generally be shorter than when the transmitting and receiving agencies are involved. Nevertheless, postal service comes with its own limitations.[17] Postal delivery is not always reliable or successful. There are also no common delivery standards across EU postal services, meaning the certification of service is not always considered adequate when presented in foreign proceedings. Issues also arise when the addressee is not present during the postal delivery, raising the question of whether delivery to other persons present is sufficient.

Similar limitations exist for other alternative methods. For example, direct service via the authorities available in the Member State of service under Article 20 of the Regulation should have been the most straightforward option. However, this solution has proven ineffective in practice, as it is not mandatory and depends on the discretion of Member States, many of which have been reluctant to allow it. Furthermore, not all Member States facilitate the direct service of documents on the initiative of the parties. While in countries like Belgium, France, and Greece, service is effected by bailiffs who can be employed by foreign litigants, other Member States, such as Germany, do not provide for service via bailiffs, minimising the provision's usefulness.[18]

Given these limitations, it is crucial to explore solutions that contribute to reducing these delays and minimise the overall inefficiencies of the service system. While the Recast Service of Documents Regulation attempted to address the deficiencies of existing methods of service,[19] the most interesting developments involve the exploration of digital solutions and tools.

By leveraging digital technologies, it may be possible to streamline the process, minimise errors, and expedite the overall service time, ensuring more efficient and effective legal proceedings across Member States. The Recast Regulation attempts to do so on two distinct levels. Firstly, the regulation aims to digitise communication between transmitting and receiving agencies via the decentralised e-CODEX platform.[20] Secondly, and most importantly for the purposes of this paper, the regulation provides, for the first time, the possibility of effecting service directly between litigant parties via electronic means. The next subsection will explore the strengths and limitations of direct electronic service of documents in the EU under the Recast Service of

ISSN 2379-5980 (online)
DOI 10.5195/LEDGER.2025.392

Documents Regulation.

2.2. The Digitisation of the Service of Judicial Documents in the EU Under the Recast Service of Documents Regulation—The introduction of direct electronic service of judicial documents within the common EU justice area was a focal point of the Recast Service Regulation.[21] In its impact assessment for the Proposal of the Recast Service of Documents Regulation, the Commission noted that the previous Regulation was inadequately adapted to the technological advancements already implemented at the national level.[22] Electronic service of documents was recognised as an emerging method in civil proceedings across Member States, with national procedural codes increasingly accommodating this possibility. However, the types of cases and categories of recipients eligible for this method varied (and still do so) significantly among Member States.[23]

To address these challenges, the European Commission's original Proposal for the Recast Service of Documents Regulation introduced electronic service of documents as an additional alternative method of direct service, elevating it to the same status as postal service. This innovative approach provided two primary alternatives for electronic service.[24]

Firstly, litigant parties could be served judicial documents electronically at any procedural stage of the litigation via Qualified Electronic Registered Delivery Services (QERDS), as defined by the Electronic Identification, Authentication and Trust Services (eIDAS) Regulation.

Secondly, following the commencement of legal proceedings, the court or authority in charge could use any "user account" designated by the addressee for the electronic service of judicial documents relevant to the ongoing proceedings. This provision offered a more streamlined and efficient process, reducing the reliance on traditional, often cumbersome methods of service. However, this flexibility was limited to service after the commencement of litigation, thereby excluding its applicability for the initial service of documents that institute the proceedings.

Most importantly, these modes of direct electronic service were designed to be autonomously available to EU litigants, bypassing the need for recourse to the national procedural laws of their respective Member States.

The original Commission proposal was not fully endorsed by the European legislators, as reflected in the current (and final) form of Article 19 of the Recast Service of Documents Regulation. The final provision does not establish a purely autonomous EU electronic service regime. Instead, Article 19 stipulates that direct electronic service can only be effected by electronic means available for domestic service under the national procedural law of the Member State of the person effecting the service.[25] In simpler terms, direct electronic service of judicial documents under the Regulation is only permissible if electronic service is provided for under the national procedural law of the Member State of the forum where proceedings have been initiated by the party or authority responsible for such service.

This cautious approach by the EU legislation creates an uneven landscape, considering the divergence in the adoption of electronic service methods across Member States. While some Member States facilitate electronic service, others do not.[26] Consequently, litigants from Member States where electronic service is not permitted cannot benefit from the introduction of electronic service methods under the Regulation. Such litigants are unable to serve documents electronically within their home jurisdiction and, therefore, cannot serve electronically abroad. However, they may still be served electronically if the litigation is initiated in a Member State where the court, authority, or party responsible for the service is allowed to serve electronically.

ISSN 2379-5980 (online)
DOI 10.5195/LEDGER.2025.392

Article 19 provides two alternative methods for electronic service, assuming the national procedural law permits electronic service in general. National procedural law is only decisive when it comes to whether electronic service is possible or not; as soon as national procedural law allows electronic service, the methods of service are provided by Article 19 of the Recast Service Regulation. These methods are, similarly to the original Proposal of the Commission, service via QERDS (Article 19(1)(a) Recast Service of Documents Regulation) or service via email (Article 19(1)(b) Recast Service of Documents Regulation). Unlike the original Proposal of the Commission, however, the current text of Article 19 does not differentiate between the two methods based on the procedural stage. While some commentators argue that service via email should only be available after the commencement of litigation,[27] this interpretation is not fully supported by the current formulation of Article 19, which is more open and flexible than the original proposal.[28] It is also worth noting that there is no hierarchical relationship between the two alternative direct electronic service methods outlined in Article 19; both stand on equal footing, representing equivalent options.

Regarding the requirements for the deployment of the two alternative methods of electronic service, both require the consent of the addressee, albeit under different conditions. Service under Article 19(1)(a) can be justified by the general consent of the addressee for the use of QERDS for any legal action within a legal relationship. Conversely, under Article 19(1)(b), service via email requires specific consent for the service of judicial documents related to a specific legal action. Additionally, when service is effected by email, the addressee must acknowledge receipt by signing and returning an acknowledgment of receipt or by returning an email from the address provided for service. The acknowledgment of receipt can also be signed electronically.

There is a notable difference in the levels of assurances provided by the two service methods. Service under Article 19(1)(a) requires the use of QERDS,[29] which offer several benefits over traditional email, including guaranteed delivery, increased security through verification of sender and receiver identities, detection of data changes, and timestamps. These features help safeguard the integrity and confidentiality of the data. Additionally, QERDS provide highly interoperable data sharing, reduced routing errors, and the ability to send large amounts of data, with elevated security standards managed by the provider.

Despite these assurances, QERDS face strong limitations, especially if the goal is to expand and popularise electronic service methods. Despite the fact that QERDS providers can obtain a trusted service certification in line with the eIDAS Regulation, they are not accessible on an EU-wide basis, as most QERDS providers operate locally within specific Member States, limiting their usefulness in cross-border situations.[30] Additionally, QERDS have a limited user base, which undermines their viability. Experience in certain Member States shows that they have generally failed to attract enough interest to remain a viable option.[31] While this trend may change in the long term—particularly as broader EU initiatives in the digitisation of justice advance, including the ongoing training of legal professionals on digital solutions—the current limitations of QERDS make them a rather impractical option.

Email service, on the other hand, seems to be a more accessible option. Despite offering lower levels of assurances compared to QERDS, email is widely accessible to all EU citizens. It operates on widely interoperable protocols that transcend borders between Member States and is the default mode of digital communication for most businesses and individuals in the EU. To partially address the assurance gap in email communication, Article 19(2) of the Regulation

ISSN 2379-5980 (online)
DOI 10.5195/LEDGER.2025.392

allows Member States to set stricter requirements for service via email. Such requirements could address issues such as the identification of the sender and recipient, the integrity of the documents sent, and protection against outside interference.[32] Some Member States have already introduced these stricter requirements.[33]

Blockchains could provide the extra assurances envisioned by the European Parliament and the Council for service via email.[34] In the next section, we will explore a framework of design choices to demonstrate how deploying blockchain technology could enhance the service of judicial documents via email.

3. An Exploration of Design Choices for a Blockchain-Based Judicial Document Service Solution

In this section we explore different blockchain-based solutions towards providing a more robust judicial document service framework with the aim of providing higher levels of assurances to involved stakeholders within the context of Article 19(1)(b) of the Recast Service of Documents Regulation. In Section 3.1, we explore a blockchain-based solution to be used when servicing addressees that are not (necessarily) blockchain/crypto-native users, assuming commonly available technological infrastructure is used. In Section 3.2, we briefly touch on a few important requirements for the application of such a solution. Then, in Section 3.3 we introduce how supra/national infrastructure, such as EU's Digital Identity Wallet (EUDIW) could augment such solutions.[35]

3.1. Servicing of Addressees That Are Not Blockchain/Crypto-Natives with Commonly Available Existing Technological Infrastructure—Blockchain- and crypto-native users represent a small portion of society, and therefore solutions beyond those that target crypto-natives (alone) are required. Therefore, we start with demonstrating a solution that targets non-blockchain- and crypto-natives. An overview of the process required to initiate download of judicial documents is depicted in Figure 1, that will now be discussed. The process mainly involves the two parties, *i.e.,* the *party responsible for service* and the *addressee*. With respect to technology used, such a solution should not require users (as much as possible) to install any specific software (beyond that of commonly available technology). The *addressee*, in this specific implementation of the use-case, is only required to make use of their usual web browser (and email services). The *party responsible for service* will need to make use of a platform that provides the automation required—which could be outsourced to a private entity, be infrastructure provided by the state, or even be run by themselves. We'll now go through each step that the process involves, highlighting particular solutions and challenges.

The party responsible for service, or some delegate thereof, initiates the process of "servicing" judicial documents and other necessary forms (depicted as step 1) by inputting the email address of the addressee (that they are aware of).[36] The system would then send a notification email to the addressee with details regarding the judicial documents to be served, for which the addressee can consent (or not—as according to the law) to receive the documents (depicted as step 2). Within the email sent to the addressee, a "tracking pixel image" could be embedded which may allow for a signal to be sent to the platform once the email is viewed (depicted as step 3) and thereafter a log to be kept that indicates that the addressee—or rather someone that owns the email address provided by the party responsible for service—had viewed the initial

ISSN 2379-5980 (online)
DOI 10.5195/LEDGER.2025.392

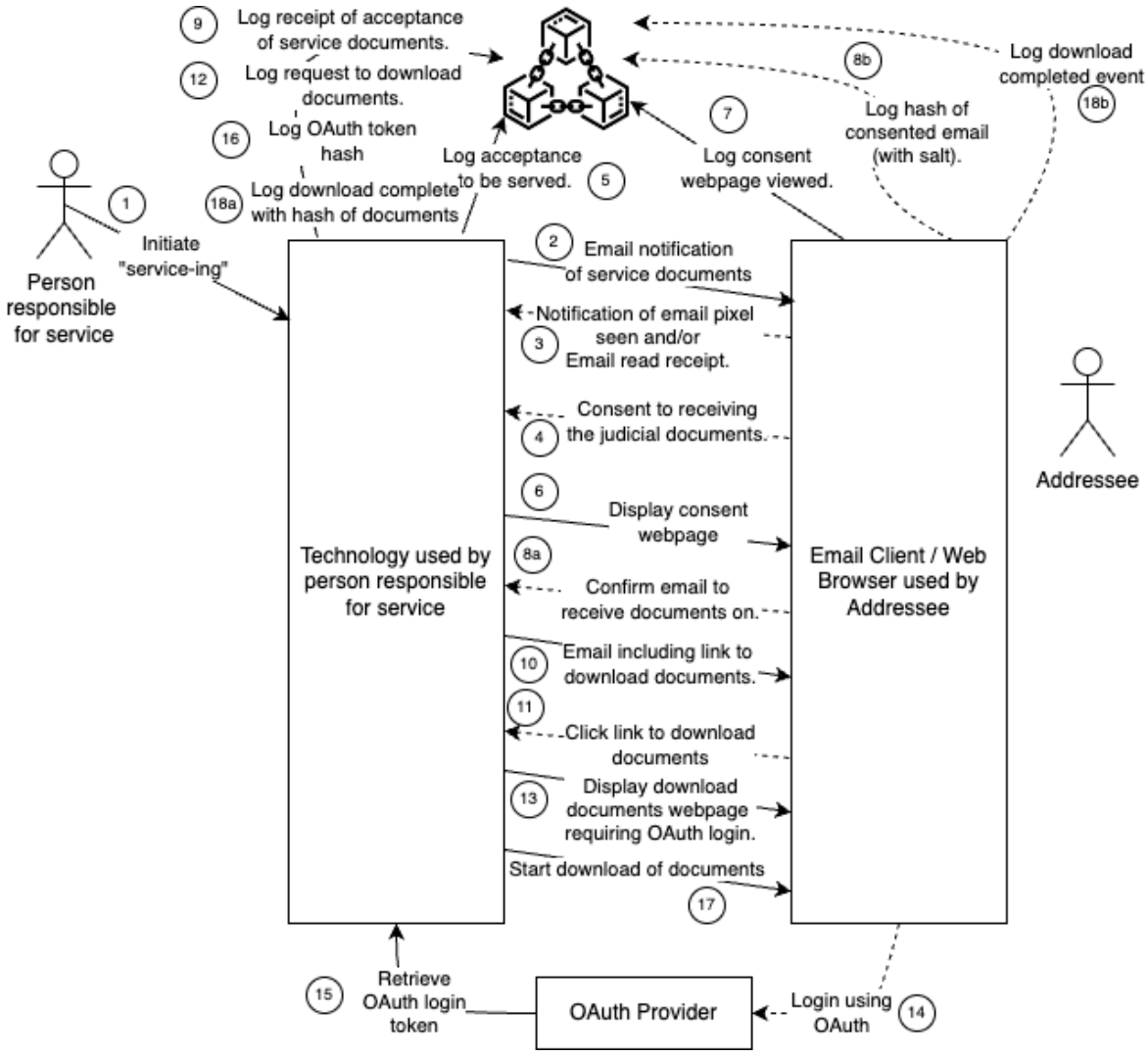

Fig. 1. Depiction of the process involved to initiate download of judicial documents.

ISSN 2379-5980 (online)
DOI 10.5195/LEDGER.2025.392

notification email. It is important to highlight that whilst most email services, by default, load and display images embedded in emails (which would allow for this notification of viewing an email to work), some users may disable the automatic viewing of embedded images. In a similar vein, the email could also have a request for a read receipt—though, yet again, users can stop the read receipt from being sent.

As discussed above, users have the legal right to either consent (or not) to receiving the documents. If a user does not consent to receiving the documents, the process would end here—at which point the party responsible for service could opt to get in touch with the addressee in a different manner if they choose. If the addressee consents to receiving the judicial documents (by clicking on text indicating that they consent to receiving the documents), then the email client would make (an HTTP) request (depicted as step 4) to retrieve the consent form. Upon doing so, the platform would keep a log of the fact that the addressee has requested to fill in the consent form, and also log this same event onto a blockchain (depicted as step 5). It is important to note that the platform provider could attempt to fake the event that the addressee has requested the consent form and still write the log onto a blockchain—yet this event could be corroborated by requesting the relevant internet service provider's logs to provide further evidence supporting that the consent page may very well have been requested. By adding the log onto a blockchain, an anchor is created to a point in time that cannot thereafter be changed.

The consent form webpage is sent (depicted as step 6) to the addressee, which would display (amongst any required details to the documents) a field allowing for the addressee to input the email address which they would like to receive the judicial documents in, and a button (or checkbox or other method) that allows for the addressee to indicate that they consent to receiving the judicial documents (on the inputted email address). The platform should support OAuth (or other forms of email services that allow for authentication—as will be discussed further below). Code could be embedded into the consent form webpage that would trigger a log being written to a blockchain (depicted as step 7) indicating that the addressee has viewed the consent form. When users interact with blockchain systems, they are (on most platforms) required to pay for that interaction—this transaction fee is referred to as "gas" in the Ethereum blockchain domain.[37] Given that this gas is typically required to be paid when uploading data to a blockchain, such an implementation would ideally make use of a mechanism that allows for the log to be paid by the platform and not by the addressee—since paying for gas may be non-trivial for non-crypto natives as it involves: (i) setting up a cryptocurrency wallet; (ii) purchasing cryptocurrency; (iii) transferring the purchased cryptocurrency to the wallet; and (iv) interacting with the platform in question whilst making use of the wallet (typically through a browser extension). Methods to get around this may include account abstraction, reverse gas,[38] some other mechanism such as relying on a proxy (or the platform) to finalise payment and submission of the transaction, or even embedding the private key into the code. Indeed, there is a risk that once the addressee receives the webpage content (in Step 6), they may withdraw the gas fees if a private key containing the said gas fees is exposed; however, in and of itself that may be supporting evidence that the addressee has viewed the webpage in question—though the addressee may argue that they were not responsible for withdrawing the said fees (yet again corroboration through IP logs could be sought). Other distributed ledger technologies (DLT), such as IOTA (which is implemented as a directed acyclic graph, *i.e.*, an alternative to a blockchain structure) could allow for fee-less uploading of the data—though there are concerns regarding the long-term availability of

ISSN 2379-5980 (online)
DOI 10.5195/LEDGER.2025.392

data stored.[39] Alternatively, "layer 2" DLTs offering cheaper transactions (costing a few USD cents) could be used, or lesser decentralised platforms offering potentially offering free/cheaper solutions—*e.g.*, the European Blockchain Services Infrastructure (EBSI),[40] Bloxberg,[41] or others.

Once (and if) the addressee consents to receiving the judicial documents (on the email address they input), simultaneously the consent will be sent to the platform (depicted as step 8a) and also the consent will be stored on the blockchain—through logging of a hash of relevant case details, the email address input along with sufficient salt (*i.e.*, random data added to input data used to make it harder to decipher the input data) to ensure details cannot be inferred (depicted as step 8b). The platform will, upon receiving consent, also log receipt of the acceptance onto the associated blockchain (depicted as step 9).

Thereafter, an email will be generated including links to download the judicial documents and sent to the email address indicated by the addressee (depicted as step 10). The email sent to the addressee, similar to that discussed for step 2, can embed a "tracking pixel image" with the same caveats discussed. The addressee can then choose to download the judicial documents by clicking on the download links made available in the email (depicted as step 11). Once (and if) the addressee clicks the link to download the judicial documents, since the link click results in a (HTTP) request directly to the platform, a log of the download being initiated can be stored centrally on the platform—and furthermore, this event can be logged onto the blockchain in a privacy-preserving manner (as depicted as step 12). Upon doing so, the platform will send the "download webpage" to the client (depicted as step 13) that requires the addressee to login using the OAuth based email which provides evidence that addressee indeed did authenticate the download themselves—or more specifically that the addressee's OAuth-based email address was used to download the documents. The platform will receive the addressee's OAuth login and notarise the event on the blockchain (depicted as steps 14, 15 and 16). The download will thereafter immediately start (depicted as step 17), and upon the download being completed, once the platform transfers the last amount of data associated with the documents it will log the event on the blockchain (depicted as step 18a) and simultaneously the code embedded in the "download webpage" will also log a similar event (from the client-side) on the blockchain as well (depicted as step 18b)—in a manner similar to that discussed for step 8b.

Once the documents have been downloaded, an email would be generated by the platform requesting that the addressee accepts or refuses the judicial documents (as is their legal right).[42] This email, like other emails discussed above, would have an embedded "tracking pixel image" and a read receipt request and would allow for logging of whether the addressee viewed the email (and the image was loaded and/or the read receipt responded to). To lodge their response, the addressee would need to authenticate themselves using their OAuth email addresses—so as to provide support that it was indeed the *addressee* that lodged the response. The addressee's response (*i.e.*, acceptance or refusal) would be logged onto the blockchain—both from embedded client-side code (in a similar manner to that discussed above) as well as from the platform once it receives the addressee's response.

The proposed system described in this section provides a solution that, except for the judicial document service-ing platform, relies on infrastructure and technology that is commonly available, and therefore does not impose large barriers towards its adoption. Whilst a solution could be provided that relies solely on emails, some jurisdictions currently do not deem email only solutions to provide the assurances required—and the solution discussed above provides higher

ISSN 2379-5980 (online)
DOI 10.5195/LEDGER.2025.392

levels of assurances with respect to processes followed, provenance of some data points, and the inability to tamper with data once logged into a blockchain. Furthermore, the solution provides more granular insight with respect to what information and steps in the process an addressee has seen.

As per the addressee's right of refusal according to Article 12 of the Recast Service of Documents Regulation, the addressee may, after downloading the documents, choose to refuse them on linguistic grounds (as per Article 12) either at the time of service or promptly thereafter, but in any case, no later than two weeks after service has been effected via the platform.[43] The proposed system will also allow for the exercise of the right of refusal within two weeks of service being effected and will register logs on the blockchain when such refusals are initiated.

If the *addressee* disputes certain actions made, *e.g.*, if they originally accept the judicial documents and then claim that they never did, various parts of the logs could be corroborated through OAuth's authentication mechanism, whilst other aspects may require ISP corroboration. The addressee may also argue that the authentication provided through OAuth (and the input email address) does not reasonably identify them, and further proof would need to be gathered to provide evidence that the email address indeed belongs to them.

3.2. Court Access to Logs Generated—With such a detailed account of actions including acceptance/refusal being logged immutably on a blockchain, it is crucial that the logs can be easily and efficiently accessed by the courts and any parties that should have rights to such details. Therefore, the platform should expose the appropriate technological interface adequate for the particular court of relevance. We envisage the following options to cater for different requirements (and resources):

3.2.1. User Credentials Provided to Judges/Courts—Access to the logs could be made available to courts, judges, and any other party (*e.g.*, court experts) that should have access to such logs through user credentials issued to them, or alternatively by linking their access to existing identity solutions (such as OAuth and/or supra/national infrastructure discussed in Section 3.3). Once a user is authenticated, they would be able to view and (if necessary) print the logs generated.

3.2.2. Provision of an API—For courts/jurisdictions that may already have in place technological infrastructure that is used to support court procedures, an Application Programming Interface (API) could be exposed allowing for existing technological infrastructure to directly interface with the platform proposed herein, to automatically extract generated logs that can be exposed through system that courts/jurisdictions already have in place.

3.2.3. Hard-Copies of Logs—For courts/jurisdictions that are less tech-savvy, hard copies of logs could be provided via: (i) requiring involved parties to print logs (via the platform); (ii) through formal requests made to the platform operator to provide printed copies; or (iii) printing of logs by an appointed individual (as discussed in Section 3.2.1).

3.3. Augmentation with Supra/National Infrastructure—To circumvent disputes from addressees mentioned above, supra- and national digital identity infrastructure could be used—so as to provide definitive support with respect to the fact that it was indeed the addressee that interacted with the platform. A European solution to providing this assurance may include integrating an EU Digital Identity Wallet (EUDIW) solution (instead of or augmented with OAuth).[35] As per the Regulation (EU) 2024/1183 which amends Regulation (EU) 910/2014 to establish the European Digital Identity Framework, EUDIWs implemented should "offer all

ISSN 2379-5980 (online)
DOI 10.5195/LEDGER.2025.392

natural persons the ability to sign by means of qualified electronic signatures by default and free of charge."[44] This means, that using EUDIWs, any citizen will be able to digitally sign a document, which besides providing legal validity across the EU to such digital signatures (or more specifically qualified electronic signatures), provides computational measures towards providing guarantees with respect to ensuring that such (digital) signatures were really made by the owner of the respective EUDIW. Since it is not the scope of this paper to delve into the technological underpinnings that provide these guarantees, we direct the reader to further material on encryption, hashing and digital signatures—to delve deeper into how such techniques provide this guarantee.[45]

Furthermore, if it were ever desirable to service documents to individuals whilst not disclosing their identity to other involved parties, bridging techniques such as those proposed by Biedermann *et al*. (2025) could be explored.[46]

4. Conclusions

This paper explored the intersection of blockchain technology and the service of judicial documents within the framework of the Recast Service of Documents Regulation. Our analysis has focused on whether blockchains can play a constructive role in digitising and improving the process of serving judicial documents across EU Member States, with particular attention given to electronic service via email.

The Recast Service of Documents Regulation marks a significant step towards incorporating digital tools into the judicial process. However, the application of these tools remains uneven, with varying levels of adoption and legal integration across Member States. Among the digital service methods provided by the Regulation, email emerges as the most accessible and widely used. Despite its accessibility, the level of assurances provided by email is generally considered weaker by comparison to QERDS according to the EU legislature. This is where blockchain technology presents a compelling solution.

Blockchains, with their secure and immutable ledgers, offer a way to enhance the procedural guarantees associated with email service. One of the critical challenges in electronic service is verifying the various steps required for effective service, including ensuring the addressee's consent to receive documents via email and confirming the addressee's acknowledgment of receipt. Blockchain technology can address these issues by providing a transparent and tamper-proof record of each transaction in the service process. For example, when a litigant consents to service via email, this consent can be recorded on the blockchain, ensuring that it is both verifiable and immutable. Similarly, when the addressee acknowledges receipt of the judicial documents, this action can also be logged on the blockchain, creating an incontrovertible record that the documents were received and when they were received.

This capability of blockchains to verify and securely document each step of the service process could significantly enhance the reliability and legal certainty of email service. It addresses concerns about the integrity and security of email communication, providing a higher level of assurance that the service has been completed correctly and in compliance with procedural requirements. The current paper demonstrated some of the design choices that underpin a blockchain-based judicial document service solution within the framework of Article 19(1)(b) of the Recast Service of Documents Regulation.

ISSN 2379-5980 (online)
DOI 10.5195/LEDGER.2025.392

However, the scope of this paper is confined to exploring digital service methods as provided by the Recast Service of Documents Regulation. It does not extend to a full analysis of all possible technical implementations where blockchains could be deployed for the service of judicial documents, a field that undoubtedly merits further research. Moreover, while we have focused on enhancing service via email, the relationship between blockchains and QERDS, particularly as outlined in Article 19(1)(a) of the Regulation, remains an intriguing area for future investigation.

Additionally, the paper does not explore the potential for direct electronic service via blockchain and NFTs which could be a useful solution when the identity and address of the addressee are unknown. This area, rich with implications for the fundamental rights of litigant parties, deserves thorough examination in the context of EU and national human rights and civil procedural law.

Author Contributions

IR conceived the central idea for the paper and was responsible for sections 1, 2 and 4 with the support of MC. JE was responsible for the technological contributions made in section 3. All authors reviewed the work.

Conflict of Interest

The authors declare that they have no known conflicts of interest as per the journal's Conflict of Interest Policy.

Notes and References

[1] Article 47 of the Charter of Fundamental Rights reads as follows: "Everyone whose rights and freedoms guaranteed by the law of the Union are violated has the right to an effective remedy before a tribunal in compliance with the conditions laid down in this Article. Everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal previously established by law. Everyone shall have the possibility of being advised, defended and represented. Legal aid shall be made available to those who lack sufficient resources in so far as such aid is necessary to ensure effective access to justice." European Parliament, Council of the European Union, European Commission. "Charter of Fundamental Rights of the European Union." *Official Journal of the European Union* **C326** (2012) (accessed 5 June 2025) https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:12012P/TXT.

[2] On how Article 47 of the Charter of Fundamental Rights establishes the rule of law during the process of the administration of justice see Galera, S. "The Right to a Fair Trial in the EU: Lights and Shadows." *Revista de Derecho Político* **87** 49-76 (2013) https://doi.org/10.5380/rinc.v2i2.44509; and Barents, R. "EU Procedural Law and Effective Legal Protection." *Common Market Law Review* **51.5** 1437–1461 (2014) https://doi.org/10.54648/cola2014112.

[3] For the procedural guarantees of Article 47 see Eser, A. "Artikel 47." In *Charta der Grundrechte der Europäischen Union*. Baden-Baden: Nomos Verlag 667-668 (2014).

[4] See CJEU. "Götz Leffler v Berlin Chemie AG." Case C-443/03 (2005) ECLI:EU:C:2005:665 paragraphs 64-67 https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62003CJ0443; and Hess, B. *Europäisches Zivilprozessrecht*. Berlin: De Gruyter 596-597 (2021).

[5] See in that regard CJEU. "Andrew Marcus Henderson v Novo Banco SA." Case C-354/15 (2017) ECLI:EU:C:2017:157 paragraph 51 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62015CJ0354, where the Court stated: "... While the main aim of Regulation No 1393/2007 is to improve the efficiency and speed of judicial procedures and to ensure the proper administration of justice,

ISSN 2379-5980 (online)
DOI 10.5195/LEDGER.2025.392

the Court has held that those objectives cannot be attained by undermining in any way the rights of the defence of the addressees of the documents in question . . . ".

[6] See in detail Hess, B. *Europäisches Zivilprozessrecht*. Berlin: De Gruyter 596-598 (2021).

[7] European Parliament, Council of the European Union. "Regulation (EU) 2020/1784 of the European Parliament and of the Council of 25 November 2020 on the Service in the Member States of Judicial and Extrajudicial Documents in Civil or Commercial Matters (Service of Documents) (Recast)." *Official Journal of the European Union* **63.L405** 1–39 (2020) http://data.europa.eu/eli/reg/2020/1784/oj.

[8] For the necessity for access to justice also in blockchain spaces see in detail Revolidis, I. "On Arrogance and Drunkenness - A Primer on International Jurisdiction and the Blockchain," *Lex & Forum* **2.2** 349-396 (2022) https://doi.org/10.2139/ssrn.4234569.

[9] Blockchain-related disputes have already pushed the limits of established norms on the service of documents. Common law jurisdictions have encountered instances where the inherent characteristics of blockchains tested the adequacy of traditional litigation systems in handling such fast-paced and unique disputes. Cases such as D'Aloia v Persons Unkown and Others,[47,48] Osbourne V. Persons Unknown And Others,[49] and LCX AG vs John Doe Nos. 1-25,[50] demonstrate that applying the rule of law in purely blockchain-based disputes can be challenging, as the identity of the counterparty and their domicile may not always be identifiable. While these situations fall outside the realm of EU law and, therefore, also of the current paper, they raise interesting questions about the procedural autonomy of Member States in finding practical solutions and defending the rule of law.

[10] See Article 19 of the Recast Service of Documents Regulation (Note 7, above).

[11] See Article 1(1) of the Recast Service of Documents Regulation (Note 7, above).

[12] See in that regard CJEU. "Plumex v Young Sports NV." Case C-473/04 (2006) ECLI:EU:C:2006:96 paragraphs 19-22 https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62004CJ0473.

[13] For a description of the basic functioning of the traditional method of service of documents via the transmitting and receiving agencies see Stürner, M. "Article 8-Transmission of Documents." In *The European Service Regulation - A Commentary*. Cheltenham: Edward Elgar Publishing 88-89 (2023).

[14] See European Commission. "Impact Assessment Accompanying the Proposal for a Regulation of the European Parliament and of the Council Amending Regulation (EC) No 1393/2007 of the European Parliament and of the Council on the Service in the Member States of Judicial and Extrajudicial Documents in Civil or Commercial Matters (Service of Documents)." SWD(2018) 287 Final (2018) (accessed 1 April 2025) 14-15 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018SC0287.

[15] See European Commission. "Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee on the Application of Regulation (EC) No 1393/2007 of the European Parliament and of the Council on the Service in the Member States of Judicial and Extrajudicial Documents in Civil or Commercial Matters (Service of Documents)." COM(2013) 858 Final (2013) (accessed 1 April 2025) 8-9 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013DC0858.

[16] Firstly, there is the issue of misaddressed requests. When a request is incorrectly sent to an inappropriate agency, additional time is required to redirect it to the correct receiving agency, introducing significant delays. Secondly, and more critically, a substantial portion of these delays is due to the linguistic limitations of the agencies involved. Many agencies lack proficiency in the languages specified by their Member States as acceptable for receiving documents. This linguistic barrier hampers their ability to process requests efficiently and accurately. Additionally, the agencies often lack sufficient knowledge of the relevant procedural rules and regulations, further complicating the service process. Moreover, delays are also reported due to inadequate equipment and infrastructure within the central bodies responsible for handling these requests. Insufficient technological resources and outdated systems within the administrations of Member States significantly slow down the process, leading to extended waiting times.

[17] See European Commission Report on the Application of Regulation (EC) No 1393/2007 (Note 15, above), 13-14.

[18] For the operation and limitations of Article 20 see Ulrici, B. "Artikel 20 - Unmittelbare Zustellung." In *Europäisches Zivilprozess- und Kollisionsrecht EuZPR/EuIPR, Band II-II: Die neue EU-Zustellungsverordnung.* Cologne: Otto Schmidt 368-373 (2023).

ISSN 2379-5980 (online)
DOI 10.5195/LEDGER.2025.392

[19] For a general assessment of the improvements introduced by the Recast Service Regulation see Stein, A. "The European Service Regulation: Introduction." In *The European Service Regulation - A Commentary*. Cheltenham: Edward Elgar Publishing 3-5, 7-15 (2023).

[20] See Articles 5 and 6 of the Recast Service Regulation (Note 7, above).

[21] For the same assessment see Stein (Note 19, above), who notes that the issue of direct electronic service has been "one of the most hotly debated issues in the negotiations of the Recast Service Regulation".

[22] See European Commission Impact Assessment of the Proposal Amending Regulation (EC) No 1393/2007 (Note 14, above), 15-16.

[23] For a general overview of Member State digitalisation initiatives in the area of service of documents see Simoni, A., Pailli, G. *Final Report—Study on the Service of Documents—Comparative Legal Analysis of the Relevant Laws and Practices of the Member States*. JUST/2014/JCOO/PR/CIVI/0049 94-121 (2014).

[24] See article 15a of European Commission. "Proposal for a Regulation of the European Parliament and of the Council Amending Regulation (EC) No 1393/2007 of the European Parliament and of the Council on the Service in the Member States of Judicial and Extrajudicial Documents in Civil or Commercial Matters (Service of Documents)." COM(2018) 379 Final (2018) 22-23 (accessed 1 April 2025) `https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018PC0379`.

[25] See Ulrici, B. "Artikel 19 - Elektronische Zustellung." In *Europäisches Zivilprozess- und Kollisionsrecht EuZPR/EuIPR, Band II-II: Die neue EU-Zustellungsverordnung.* Cologne: Otto Schmidt 352 (2023). See also Anthimos, A. "Article 19 - Electronic Service." In *The European Service Regulation - A Commentary*. Cheltenham: Edward Elgar Publishing 181 (2023).

[26] For an overview of the diverging positions with regards to electronic service in different Member States see the information communicated on the e-justice portal (accessed 1 April 2025) `https://e-justice.europa.eu/topics/taking-legal-action/european-judicial-atlas-civil-matters/serving-documents-recast_en?clang=en`.

[27] See Ulrici on Article 19 (Note 25 above) and Stein (Note 19, above).

[28] For a similar assessment, see Anthimos (Note 25, above).

[29] See Articles 43 and 44 of European Parliament, Council of the European Union. "Consolidated Text: Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market and Repealing Directive 1999/93/EC." *EUR-Lex* 02014R0910-20241018 `http://data.europa.eu/eli/reg/2014/910/2024-10-18`.

[30] The limited success of QERDS was already pointed out in the evaluation of the eIDAS Regulation performed by the European Commission, where it was concluded that, at the time of the evaluation, QERDS providers operated in only seven Member States. See European Commission. "Commission Staff Working Document Accompanying the Document Report from the Commission to the European Parliament and the Council on the Evaluation of Regulation (EC) No 910/2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market (eIDAS)." SWD (2021) 130 Final (2021) 15-16 (accessed 1 April 2025) `https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52021SC0130`; where the Commission concludes that QERDS have by far been the least successful trust service established by the eIDAS Regulation. The same trend persists today. A review of the trusted services list maintained by the European Commission confirms that QERDS remain operational in only 11 out of 27 Member States, highlighting their failure to achieve mass adoption across the EU. See the information posted on the eIDAS Dashboard (accessed 1 April 2025) `https://eidas.ec.europa.eu/efda/home`. Furthermore, an examination of the websites of listed service providers reveals significant scaling difficulties. Many of these services are only available in the language of their country of origin (*e.g.*, `https://doreczeniaelektroniczne.pl/` (accessed 1 April 2025), while others require a national ID from their country of establishment to grant access to their service (*e.g.*, `https://mein.bitkasten.de/register` (accessed 1 April 2025), effectively excluding users from other Member States. These severe limitations render QERDS practically inaccessible for cross-border service of judicial documents. In stark contrast, email has achieved near-universal adoption, offering immediate, barrier-free communication that is vastly more accessible and effective for digital service.

ISSN 2379-5980 (online)
DOI 10.5195/LEDGER.2025.392

[31] On the various limitations and the limited prospects of QERDS with regards to the electronic service of documents see Deters, H., Elsner, N. "Digitalisierungselemente in der EuZVO und EuBVO 2020." In *Göttinger Kolloquien zur Digitalisierung des Zivilverfahrensrechts, Band 3*. Göttingen: Universitätsverlag Göttingen 51 (2024), where they document the failures of the German variant of QERDS with much detail.

[32] See Recital 33 of the Recast Service of Documents Regulation (Note 7, above) which provides that: "... In order to guarantee the security of transmission, Member States could specify additional conditions under which they will accept electronic service by email where their law sets stricter conditions in respect of service by email or where their law does not allow such service by email. Such conditions could address issues such as the identification of the sender and the recipient, the integrity of the documents sent and the protection of the transmission against outside interference...".

[33] This is the case according to the e-justice portal, for example, in Belgium (accessed 1 April 2025) `https://e-justice.europa.eu/topics/taking-legal-action/european-judicial-atlas-civil-matters/serving-documents-recast/be_en#article-19--electronic-service` and France (accessed 1 April 2025) `https://e-justice.europa.eu/topics/taking-legal-action/european-judicial-atlas-civil-matters/serving-documents-recast/fr_en#article-19--electronic-service`. It is also worth noting that some Member States have exhibited an arguably unjustified hostility towards service by email. While Article 19(2) of the Recast Service of Documents Regulation permits Member States to impose stricter requirements than those outlined in Article 19(1)(b) for electronic service via email, it certainly does not authorise them to outright ban or severely restrict this method of service. However, Germany has done precisely this, contravening Article 19 of the Recast Service Regulation. Specifically, §1068 of the German Civil Procedural Code (ZPO) mandates that addressees in Germany can only be served electronically via QERDS as stipulated in Article 19(1)(a) of the Recast Service Regulation, effectively prohibiting service by email as provided for in Article 19(1)(b). In its explanatory memorandum, the German legislator defended this decision by arguing that, since only QERDS are provided for national service within Germany, the same standard should apply to services conducted in EU-related disputes. As stated in Bundestag, Drucksache 20/1110 from 21 March 2022 (accessed 15 August 2024) `https://dserver.bundestag.de/btd/20/011/2001110.pdf` page 30: "...Da die Zustellung elektronischer Dokumente in der Bundesrepublik Deutschland nach § 173 Absatz 1 ZPO in der seit dem 1. Januar 2022 geltenden Fassung immer einen sicheren Übermittlungsweg voraussetzt, wird die Zustellung nach Artikel 19 Absatz 1 Buchstabe b EuZVO in der Bundesrepublik Deutschland nicht durchgeführt. Vielmehr wird nach § 1068 ZPO-E nur die elektronische Direktzustellung gemäß Artikel 19 Absatz 1 Buchstabe a EuZVO zulässig sein. Dies dient der Sicherheit bei der elektronischen Übermittlung. ...". This interpretation, however, neither reflects the letter nor the spirit of Article 19(2) of the Recast Service Regulation. Article 19(2) does not empower Member States to deprive EU citizens of electronic service methods guaranteed by EU law. While the permissibility of electronic service is indeed conditional upon Member State law, as long as such service is permissible, EU citizens should be entitled to utilise any of the methods available under Article 19(1) of the Recast Service Regulation. Member States may only increase the level of assurances required for service via email under Article 19(1)(b), not exclude this method of service altogether. This level of hostility towards service by email highlights a significant rift in the application of the Regulation (raising serious concerns about discrimination against EU litigants by certain Member States), which in turn justifies the research undertaken in this paper into how blockchain technology could enhance the level of assurances for service by email. By potentially addressing the concerns Member States have regarding this method, blockchain could offer a solution that mitigates objections and promotes more consistent adherence to EU law.

[34] Blockchains may also offer an elegant solution for the deployment of a QERD system. Indeed, blockchains inherently possess many of the attributes that make QERDS an attractive option for the service of documents. It is also worth noting that Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024, which amends Regulation (EU) No 910/2014 regarding the establishment of the European Digital Identity Framework, has now incorporated electronic ledgers within the eIDAS ecosystem (see Articles 45k and 45l thereof).[44] While the intricate relationship between electronic ledgers and QERDS lies beyond the scope of this paper, it remains an appealing subject for further research, especially in the context of electronic service. This paper focuses on service by email, which, as mentioned in the main text, is the most accessible and widely available method of the two envisaged by Article 19 of the Recast Service of Documents Regulation. Email is also more in need of additional assurances than QERDS.

[35] See No Author. "EU Digital Identity Wallet." (accessed 5 June 2025) `https://ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET/EU+Digital+Identity+Wallet+Home`.

ISSN 2379-5980 (online)
DOI 10.5195/LEDGER.2025.392

[36] According to Article 12 of the Recast Service of Documents Regulation, the addressee may refuse to accept a document for service if it is not written in, or is not accompanied by a translation into, either a language that the addressee understands or the official language of the Member State addressed. If the Member State has multiple official languages, the document must be in the official language or one of the official languages of the place where service is to be effected. Pursuant to Article 12(6) of the Recast Service Regulation (Note 7, above), this right also applies to service effected through alternative methods, as outlined in Section 2 of the Regulation. Most significantly for the purposes of this paper, the right of refusal extends to electronic service in accordance with Article 19 of the Regulation. This right is designed to safeguard the addressee's ability to prepare an effective defence in legal proceedings and is triggered when the documents to be served are not in a language the addressee understands. The right to refuse service is strictly limited to instances where the addressee does not understand, or cannot reasonably be expected to understand, the language in which the judicial documents are drafted. It does not, therefore, permit refusal on any other grounds. At the time of service, the addressee must be informed of their right to refuse acceptance and the deadline for exercising this right. The right may be exercised either immediately upon service or within two weeks of the date on which service was effected. To invoke this right, the addressee may either complete Form L (as set out in Annex I of the Recast Service Regulation) or submit any written declaration stating that they refuse to accept the document due to the language in which it was served. The party responsible for service must inform the addressee of their right of refusal and provide them with Form L. In light of this, where the party responsible for service is required to notify the addressee of their right of refusal under Article 12——particularly in cases where there are reasonable doubts as to the addressee's ability to understand the language of the documents——they must ensure that, along with the judicial documents to be served, the addressee receives information regarding their right of refusal as well as Form L. The system will thus enable the party responsible for service to furnish the necessary information and documentation where circumstances so require.

[37] While many different blockchain ecosystems rely on some form of transaction fee, one of the most complete explanations of the concept comes from the Ethereum blockchain. In Ethereum, as is the case in many other blockchains, transaction fees, in this case known as "gas," power activity across the network. Because they are so small, gas fees on the Ethereum network are denominated in "Gwei," or units of one one-billionth of one ether (0.000000001 ETH = 1 Gwei). The primary purpose of gas is to regulate how much computational effort a transaction can consume, especially since these operations are executed simultaneously across a decentralised global network of nodes. Because Ethereum and other blockchains enable unrestricted (Turing-complete) computation, it's necessary to implement a mechanism like gas to prevent misuse—such as malicious or unintentionally infinite transactions that could drain system resources. In 2021, EIP-1559 (the "London Upgrade") changed the way gas fees were calculated and distributed to the "miners" that operate the Ethereum network. For more details, see: Buterin, V., Conner, E., Dudley, R., Slipper, M., Norden, I., Bakhta, A. "EIP-1559: Fee Market Change for ETH 1.0 Chain." *Ethereum Improvement Protocols* (accessed 4 June 2025) `https://eips.ethereum.org/EIPS/eip-1559`.

[38] See the DFINITY Team's whitepaper: Camenisch, J. *et al*. "The Internet Computer for Geeks." *Cryptology ePrint Archive* **2022/087** (accessed 5 June 2025) `https://eprint.iacr.org/2022/087`.

[39] Traditionally, Blockchain ecosystems face the problem of speed and scalability. Modern blockchain platforms try to improve their speed and scalability by using new consensus methods, like proof-of-stake instead of proof-of-work. As explained earlier in this subsection, in these systems, users often have to pay gas or other fees to get their transactions processed. These fees usually go to the network participants (like miners or validators) who confirm and order the transactions. As demand increases, so do the costs. In an attempt to address both of these problems—scalability and transaction costs—some newer distributed ledger technologies are moving away from the traditional chain model and adopting a different structure called a Directed Acyclic Graph (DAG). In a DAG, transactions are not grouped into blocks or lined up one after another. Instead, each transaction can directly approve others, forming a web-like structure. This allows many transactions to be processed in parallel, which not only improves speed but also removes the need for middlemen like miners. As a result, there are usually no gas fees, making the system arguably more scalable and cost-efficient. For an overview of Directed Acyclic Graph arrangements vis-a-vis more traditional linear Distributed Ledger applications see Kahmann, F., Honecker, F., Dreyer, J., Fischer, M., & Tönjes, R. "Performance Comparison of Directed Acyclic Graph-Based Distributed Ledgers and Blockchain Platforms." *Computers* **12.12** 257 (2023) `https://doi.org/10.3390/computers12120257`.

[40] No Author. "Introducing EBSI." *EBSI European Blockchain* (accessed 5 June 2025) `https://ec.europa.eu/digital-building-blocks/sites/display/EBSI/Home`.

ISSN 2379-5980 (online)
DOI 10.5195/LEDGER.2025.392

[41] No Author. "Bloxberg Block Explorer" (accessed 5 June 2025) https://https://blockexplorer.bloxberg.org/.

[42] In order to facilitate the exercise of the right of refusal as per Article 12 of the Recast Service Regulation (Note 7, above) the email will include the information accompanying form L as per Annex I of the Regulation.

[43] See Article 12(3) of the Recast Service of Documents Regulation (Note 7, above), which sets the deadline for exercising the right of refusal to a maximum of two weeks after service has been effected.

[44] European Parliament, Council of the European Union. "Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 Amending Regulation (EU) No 910/2014 as Regards Establishing the European Digital Identity Framework." *EUR-Lex* 32024R1183 (accessed 5 June 2025) http://data.europa.eu/eli/reg/2024/1183/oj.

[45] For the less tech-savvy, see Cobb, C. (2004). *Cryptography for Dummies*. Hoboken: John Wiley & Sons (2004); and for the more tech-savvy, see: Wong, D. *Real-World Cryptography*. Shelter Island: Manning Publications Co. (2021).

[46] Biedermann, B., Scerri, M., Kozlova, V., & Ellul, J. "Aggregating Digital Identities through Bridging." *Distributed Ledger Technologies: Research and Practice* (February 2025) https://doi.org/10.1145/3719661.

[47] No Author. "D'Aloia v Person Unknown & Others." (2022) EWHC 1723 (Ch) https://www.bailii.org/ew/cases/EWHC/Ch/2022/1723.html.

[48] No Author. "Fabrizio D'Aloia v (1) Persons Uknown Category A (2) Binance Holdings Limited (3) Polo Digital Assets Inc. (4) Gate Technology Corp (5) Aux Cayes Fintech Co Ltd (6) Bitkub Online Co Ltd (7) Persons Unknown Category B." (2024) EWHC 2342 (Ch) https://www.bailii.org/ew/cases/EWHC/Ch/2024/2342.html.

[49] No Author. "Lavinia Deborah Osbourne v (1) Persons Unknown Category A (2) Fiona Cowton Persons Unknown Category B (3) Thembani Dube." (2023) EWHC 340 (KB) https://www.bailii.org/ew/cases/EWHC/KB/2023/340.html.

[50] No Author. "LCX AG v John Doe Nos. 1-25, 1.274M U.S. Dollar Coin, and Circle Internet Financial LLC and Centre Consortium LLC." Supreme Court of the State of New York, Commercial Division, Part 48, 154644/2022 https://www.nycourts.gov/Reporter/pdfs/2022/2022_32834.pdf.

SSN 2379-5980 (online)
DOI 10.5195/LEDGER.2025.392