Oñati Socio-Legal Series (ISSN: 2079-5971)
Oñati International Institute for the Sociology of Law
Avenida Universidad, 8 – Apdo. 28
20560 Oñati – Gipuzkoa – Spain
Tel. (+34) 943 783064 / opo@iisj.net / https://opo.iisj.net

Blockchain evidence versus the State: RAIMUNDO as a case study

OÑATI SOCIO-LEGAL SERIES FORTHCOMING
DOI LINK: HTTPS://DOI.ORG/10.35295/OSLS.IISL.2202
RECEIVED 24 NOVEMBER 2024, ACCEPTED 14 APRIL 2025, FIRST-ONLINE PUBLISHED 9 MAY 2025

SEBASTIÁN RIVERO SILVA*

Abstract

RAIMUNDO is an innovative decentralized application (DApp) designed for the legal sector, leveraging Ethereum's sustainable blockchain technology (now based on Proof of Stake) to certify documents. By using a dual-hash system, it enables attorneys to produce tamper-proof "blockchain evidence," eliminating the need for state intermediaries. This empowers legal professionals, especially in regions with authoritarian regimes or corruption, to independently certify documents. However, judicial acceptance of blockchain evidence varies. Common law systems increasingly recognize it as valid, while civil law jurisdictions, with formal and state-centric traditions, often prioritize public certification over private digital methods. Factors such as blockchain's anonymity and the strict public certification duties of European notaries contribute to this divide. Although technically compatible with notarial roles in civil law, the integration of blockchain into regulatory frameworks remains uncertain, highlighting the need for ongoing evaluation of its evidentiary value compared to traditional public documents.

Key words

Blockchain evidence; common law; court admission; DApp; Ethereum

Resumen

RAIMUNDO es una aplicación descentralizada orientada al sector jurídico que utiliza la blockchain de Ethereum (actualmente basada en Proof of Stake) para certificar documentos mediante un sistema de doble hash. Esta tecnología permite a los abogados generar evidencia digital inalterable sin intervención estatal, facilitando la autonomía profesional en contextos de debilidad institucional, autoritarismo o corrupción. No obstante, la validez probatoria de dicha evidencia varía según el sistema jurídico. En el common law, su admisión judicial es creciente. En contraste, en los sistemas de derecho civil, prevalece la formalidad documental y la centralidad del notariado, lo cual dificulta

* Sebastián Rivero Silva. Licensed practicing lawyer in Spain. PhD student at the School of Architecture and Technology of Universidad San Jorge, within the research line "Global change and sustainable development". Email: sebastian.riverosilva@gmail.com

la incorporación de herramientas descentralizadas. Factores como el anonimato de la blockchain y la regulada función pública del notario europeo refuerzan esta tensión. Aunque existe compatibilidad técnica entre blockchain y funciones notariales, su incorporación efectiva en marcos normativos aún es incierta. Todo ello subraya la necesidad de una evaluación sobre su valor probatorio frente a los documentos públicos tradicionales.

Palabras clave

Evidencia blockchain; derecho anglosajón; admisión judicial; DApp; Ethereum

Table of contents

1. Explaining the blockchain evidence and other preliminary issues

In an increasingly digitalized world, concerns such as the integrity and traceability of electronic documents and digitized physical documents present particular importance, especially regarding their evidentiary capacity before courts and tribunals, as well as for use before public non-judicial administrations (Kumar *et al.* 2023). Document certification — understood as the capability to issue exact copies and authenticate signatures, traditionally vested in state-designated individuals such as notaries and registrars — now faces an unprecedented transformation due to the advent of decentralized technologies like blockchain. Initially popularized for speculative uses in the cryptocurrency context, blockchain technology has proven to be a versatile tool capable of revolutionizing sectors as diverse as public administration and the legal field. In this context, blockchain-based document certification presents new opportunities for the private legal sector to ensure the integrity of both electronic and digitized physical documents, as well as the accuracy of a specific copy and its issuance date, thereby reducing reliance on the state and ensuring transparency throughout the certification process (Falbo and Di Castelnuovo 2019).

Document certification (encompassing both originally electronic documents and digitized physical documents) is fundamental in judicial and administrative procedures, where document validity can determine the outcome of a particular claim. In legal practice, comprehensive document certification has historically remained within the domain of state power, leading to various limitations, including cost, delay, data sharing with other state agencies, and, in some cases, vulnerability to fraud, especially in so-called "fragile democracies" or in jurisdictions with widespread corruption (Issacharoff 2006). These constraints can lead to a decline in service quality for citizens, infringe upon rights to independent legal defense, and even cause loss of opportunities due to the inability to certify documents promptly. Here, blockchain technology, with its inherent capability to ensure data immutability through a distributed network, emerges as a technological solution that not only enhances security and privacy but also has the potential to expedite and reduce the costs of these certification processes.

Blockchain technology enables document certification through the use of a public, transparent digital ledger — commonly referred to as a "libro mayor" in Spanish — which, based on current technological standards, prevents alteration without leaving evident traces (Wu *et al.* 2021). In this regard, Professor Jiménez-Gómez (2023a, 64) defines a ledger as "a place to record all transactions that occur in the system. It is similar to (…) a record of transactions carried out, which acts like a database with the information organized in a certain way."

Each certified document inserted into the blockchain through its entry in the aforementioned ledger, is identified by a unique hash, functioning as a singular, immutable "digital fingerprint." This hash is stored on the network functioning in the manner of a "private note" within an Ethereum transaction. Any attempt to modify the original document results in a hash alteration, which would invalidate the certification itself and alert users to potential tampering. As a secondary safeguard, the document hash certification occurs through a blockchain transaction between two digital wallets. This transaction is recorded with a second, equally unchangeable and auditable hash. Therefore, the system provides dual security verification: (a) the hash of the certified

document and (b) the hash of the transaction between the digital wallets, all publicly audited by tens of thousands of independent, anonymous nodes that operate in exchange for a fee (gas fee) paid by the interested party, without requiring the involvement of a public official. The final record is noted in the ledger of the network itself, also public and subject to audit (Stančić 2018). The Ethereum network, one of the most widely used in decentralized application development, has been pivotal in implementing certification systems using blockchain technology due to its flexibility and capacity to execute a wide range of smart contracts specifically designed for this purpose.

In this context, RAIMUNDO emerges as a document certification system based on blockchain technology, developed as a DApp that directly interacts with the Ethereum network. Leveraging the Ethereum ecosystem, RAIMUNDO utilizes a consensus mechanism among validator nodes known as Proof of Stake (PoS). Under this model, instead of executing complex mathematical operations to earn gas fee rewards as in the traditional Proof of Work (PoW) model, validator nodes stake cryptocurrency for the right to verify the document hash transaction and ''claim the reward''. This paradigm offers a more energy-efficient alternative to traditional Proof of Work (PoW) systems, which will be discussed later in chapter three of this article. Consequently, RAIMUNDO not only guarantees the integrity and blockchain timestamping of digital documents independently and without state oversight, but also positions itself as a sustainable solution — especially relevant in an era where digital technologies face increased scrutiny for their environmental impact. PoW models, in which validator nodes require powerful hardware to solve mathematical operations and compete to verify information, have been criticized in scholarly circles for their high energy consumption, particularly in large networks like Bitcoin (Wendl *et al.* 2023, 2). By contrast, PoS-based networks, such as Ethereum following its 2022 migration known as "The Merge," dramatically reduce energy consumption without sacrificing, *prima facie*, document security or integrity of the process.

RAIMUNDO's adoption of the PoS (Proof of Stake) consensus mechanism, native to the Ethereum network, is particularly significant given that various scholars have underscored the network's notable energy efficiency (Fernández-Caramés and Fraga-Lamas 2024, 7). Indeed, the "Green Blockchain" doctrine is gaining traction among developers of blockchain solutions such as RAIMUNDO. If the aim is to endow blockchain certification with a quasi-public function, it is evident that embracing systems ensuring the sustainability of its operations is imperative.

The environmental impact of blockchain technology has been a growing focus in academic and legal discussions, particularly with the increased use of PoW networks that consume significant amounts of electricity as well as generate a significant amount of hardware e-waste due to the need for nodes to use hardware capable of mining cryptocurrency and the continuous wear and tear on these systems, which are generally set up as ''rigs'' and are 24 hours a day, 7 days a week in operation (Miraz *et al.* 2021, 54-59). Recent studies estimate that, should extensive PoW systems remain in use, blockchain technology could contribute to global warming with an increase of between 0.26 and 0.43 degrees Celsius by 2120 (Shi *et al.* 2023). In response to these concerns, RAIMUNDO and other PoS-based systems offer a more environmentally friendly

solution, reducing both energy consumption, e-waste generation and the associated environmental impact. In this regard, it is worth noting that certain authors (Jiménez-Gómez 2023b, 677) have pointed out that, although awareness of the issue exists, there is currently no effective and binding regulatory framework to mandate reductions in the energy consumption of blockchain technology when applied to specific sectors, such as financial markets

In the legal domain, blockchain certification also presents challenges worth examining. Although this technology provides a notably high level of security and transparency (contingent, of course, on the various consensus mechanisms that will be discussed further), its widespread adoption in judicial and administrative processes still faces clear regulatory barriers, particularly in civil law systems rooted in Roman law, as opposed to the Anglo-Saxon common law systems. In many Roman law jurisdictions like Spain or Mexico, private documents require public certification to be fully valid in judicial proceedings (Krstinic and Zarubica 2021, 42), raising a key question: can blockchain document certification be equated in evidentiary quality to traditional state certification systems? The answer largely depends on jurisdiction. This issue is significantly influenced by each country's legal framework and, crucially, whether it follows a civil or common law system. While some jurisdictions, like the United States and several common law jurisdictions (former British colonies), have adopted a favorable stance toward blockchain certification (Wang *et al.* 2024), others, such as Spain, Mexico and most Roman-derived legal systems, accept blockchain evidence as private documentation only — with some probative advantages — which limits its efficacy in judicial and administrative proceedings (Ibáñez 2017).

Indeed, the Article 5 of the Spanish Commercial Registry Regulation notably restricts the official registry validity of various legal acts unless they are authorized before a Notary. However, this legal prohibition against the registration of private documents in public registries is not absolute. Some scholars highlight the internal inconsistency of Spanish law whereby certain registries accept private documents accompanied by a duly legitimized notarial signature, while others insist on the submission of a public instrument — particularly given that the Spanish public registries share the same legal nature (Jiménez-Gómez 2024, 33). In this same context, the academic doctrine points out that in Mexico, the strict reserve of the notarial function, incompatible with other professions such as the legal profession and even with certain commercial businesses, serves a social function and must be criminally punished in case of breach (Barba 2014, 42).

Given this background, the RAIMUNDO system aims to position itself at the forefront of technological innovation in document certification, not only for its sustainability benefits but also for its focus on delivering high-quality evidentiary support that is (a) transparent, (b) low-cost, (c) accessible to private legal practitioners, and (d) decentralized, free from political control and scrutiny. Additionally, RAIMUNDO seeks to enable interoperability between document certification systems across different jurisdictions, allowing blockchain-certified documents to be recognized and validated in various legal contexts. With respect to RAIMUNDO's low-cost nature, it is important to note that this refers to the system being provided free of charge, as it is not operated by a commercial entity and therefore does not impose any fees. Consequently, the only cost

involved is the minimum Ethereum transaction fee required for a transfer between two wallets.

2. Nature and functioning of the RAIMUNDO system

The RAIMUNDO system, as previously mentioned, is a Decentralized Application (DApp) currently in its playground (pre-beta) phase, developed for document certification via the Ethereum network to ensure the integrity and timestamping of both electronic documents and digitized physical documents. It is important to first note the limitations of RAIMUNDO, which, due to specific legal barriers, is not yet able to verify the authenticity of a copy of a document issued, for example, by a public official. However, it can issue authentic copies of a digital file, ensuring that the copy has not deviated from the original document, whether the file was originally digital or later digitized. This capability has already been acknowledged as feasible by academic literature (Aldwairi *et al.* 2023, 253). In the future, RAIMUNDO aims to implement a digital electronic signature authority, enabling not only the issuance of authentic copies but also the legitimization of users' authentic signatures. In this regard, the identity verification capability conferred by qualified electronic signature systems under Article 25 of Regulation (EU) No 910/2014 (Schwalm and Alamillo-Domingo 2021, 90-91) serves as an ideal complement to the proposed blockchain-based evidence.

In this context and considering the decentralized nature of RAIMUNDO as a DApp, we can define this concept as a type of software that operates in a distributed manner (through independent, anonymous nodes not controlled by the State) on a blockchain network, rather than relying on centralized servers of a public or private entity subject to political authority. This means that the evidentiary quality of RAIMUNDO's certifications depends on the specific blockchain network community with which it interacts, such as the Ethereum network. DApps leverage the fundamental characteristics of blockchain technology — immutability, transparency, and security of process — to offer services, as in RAIMUNDO's case, for document certification. This technology can yield numerous benefits in terms of privacy compared to "traditional" document certifications overseen by the State.

Following the classification proposed by Professor Jiménez-Gómez (2020, 288), RAIMUNDO is, in its current phase, entirely public and permissionless. Indeed, anyone can use the script, which interacts with the user's private MetaMask on the ETHEREUM network and may even modify or adapt it if they wish. In the future, there are plans to restrict its use to attorneys, but such a measure could compromise the intended anonymity, particularly in countries where practicing law is dangerous. Consequently, the project's direction must allow, when necessary, a "masked" certification wherein the attorney's identity is withheld and, instead, the entity managing RAIMUNDO is identified. In any case, it would be worthwhile to see adaptations of RAIMUNDO emerge for specific professional associations or groups that might integrate it into their daily operations.

This advantage is particularly useful for nations closely related to Spain, such as Cuba, Venezuela, and Nicaragua, which are classified as dictatorships in the Freedom House index (Carpio Cervantes 2021, 297) and are well-known for subjecting uncooperative entrepreneurs and, more generally, political opposition members to state scrutiny

through public officials, including judges, notaries, and registrars (Briones and Quispe 2019, 4). The possibility for an independent attorney to certify the authenticity of a copy or the validity of a digital signature without reporting it to the State creates spaces for freedom and security in legal transactions. This also facilitates the free practice of law in countries where law licenses are limited to professionals who do not serve the political opposition or non-cooperative business under the regime. It may also provide an effective option to bypass the widespread corruption among certain public officials (Gehlot and Dhall 2022). It should be noted that in countries where corruption rates are lower, the State's interest may lie more in maintaining access to key information for the Public Treasury and the financial intelligence units responsible for combating money laundering. In other words, preventing the loss of vital tax-related data ordinarily supplied by civil law notaries. In this regard, it is important to remember that under Article 2 of Spanish Law 10/2010 (April 28), on the prevention of money laundering and terrorist financing, notaries are considered "obligated entities." to provide information. Likewise, attorneys enjoy a partial and limited exemption according to Article 22 of the same statute.

RAIMUNDO thus presents itself as a blockchain tool that, on one hand, enables private attorneys to certify documents — within the aforementioned limits and subject to jurisdictional variation — and, on the other, generates a technical report that may be submitted to a national or foreign court, providing dual assurance of both "tamper-proof" (protection against alteration) and "proof of existence" (evidence of the file's timestamp) (Shawn *et al.* 2021, 301). It is important to clarify that this process does not validate the legal act within the document (a function still reserved for public officials in Spain and Mexico), but rather affirms the document's date of existence and integrity — and soon, as mentioned, the signature on the document itself.

With these points clarified, we proceed to explain the operation of RAIMUNDO, which functions as follows:

The attorney accesses the RAIMUNDO web platform (currently in pre-beta phase: https://maroon-rigorous-crepe.glitch.me/public/). This platform was conceptualized in 2023 and developed in 2024 within the context of the author's doctoral dissertation, with the aim of demonstrating the technical feasibility of generating blockchain-based evidence that has transnational utility and is compatible with public documents. Therefore, it remains an experimental product derived from academic research. It currently does not have a white paper, nor will further development proceed until the certification system and the intuitive, automated verification capability for judicial bodies are perfected.

Once the user accesses RAIMUNDO, a user-friendly interface allows the input of essential information, such as professional affiliation, bar association membership, identification number, and the type of document to be certified. RAIMUNDO then performs the following tasks automatically:

(a) First, using the JavaScript Node.js library, a cryptographic hash of the "document to be certified" is generated using the SHA-256 algorithm. A hash is essentially a logarithmic function that produces a unique, unrepeatable "digital fingerprint" for a digital file (Gupta and Kumar 2014, 1). Just as each human has a unique fingerprint, each contract, notification, and, in general, digital file possesses its own distinctive,

immutable hash. Calculating the hash of the same contract multiple times (provided the same digital file is used) will yield the same unique alphanumeric code each time. There are various algorithms for calculating a document's hash, the most common being the aforementioned SHA-256 algorithm, developed by the United States National Security Agency (NSA), which assigns a unique, unrepeatable 64-character string to each digital file (Prasanna and Premananda 2021, 246-250).

For example, if a barely perceptible white mark is added to the white background of a document's margin — virtually invisible to the human eye — the hash generated by the SHA-256 algorithm would change significantly. This provides a high degree of certainty regarding document integrity, as simply calculating the SHA-256 hash for two seemingly identical documents will reveal any modifications or differences between them (Roussev 2009, 50-53, Almansa Arévalo 2024). The current technological state enables each document to be uniquely and irreplaceably identified, thereby allowing verification of whether one digital copy is exactly identical to another purported digital copy. In this regard, it is worth highlighting the Instruction of December 20, 2019, issued by Spain's General Directorate of Registries and Notaries (now the General Directorate of Legal Security and Public Faith), which states:

"One may seek alternatives to the incorporation into the notarial protocol of the voluminous documentation submitted by the bank, such as establishing — in the same free-of-charge notarial act — a deposit of said documentation in the notary's file, via an electronic file identified by its Hash. In so doing, one ensures both the preservation of the electronic file and the possibility of verified, conclusive proof of the file's content for the issuance of subsequent copies of the act, either incorporating the deposited document or converting it to paper."

Indeed, it can be observed that some Spanish notaries already openly discuss the remarkable qualities offered by hashing technology in the context of document security (Brancós 2024).

(b) Second, through the JavaScript library known as ethers.js, RAIMUNDO interacts with Metamask, a general-purpose digital wallet, or "crypto wallet" in specialized terminology. Metamask allows users to conduct transactions (both sending and receiving cryptocurrency) across various blockchain networks, including Ethereum, and to include relevant information within each transaction (Lee 2023), such as a document hash as described in section (a) for RAIMUNDO's purposes. In this context, the ethers.js JavaScript library functions as an API — a type of "connection guide" — facilitating the interconnection between RAIMUNDO and METAMASK to operate on Ethereum. It is an almost essential library for any DApp developer working within blockchain environments (Saian *et al.* 2024).

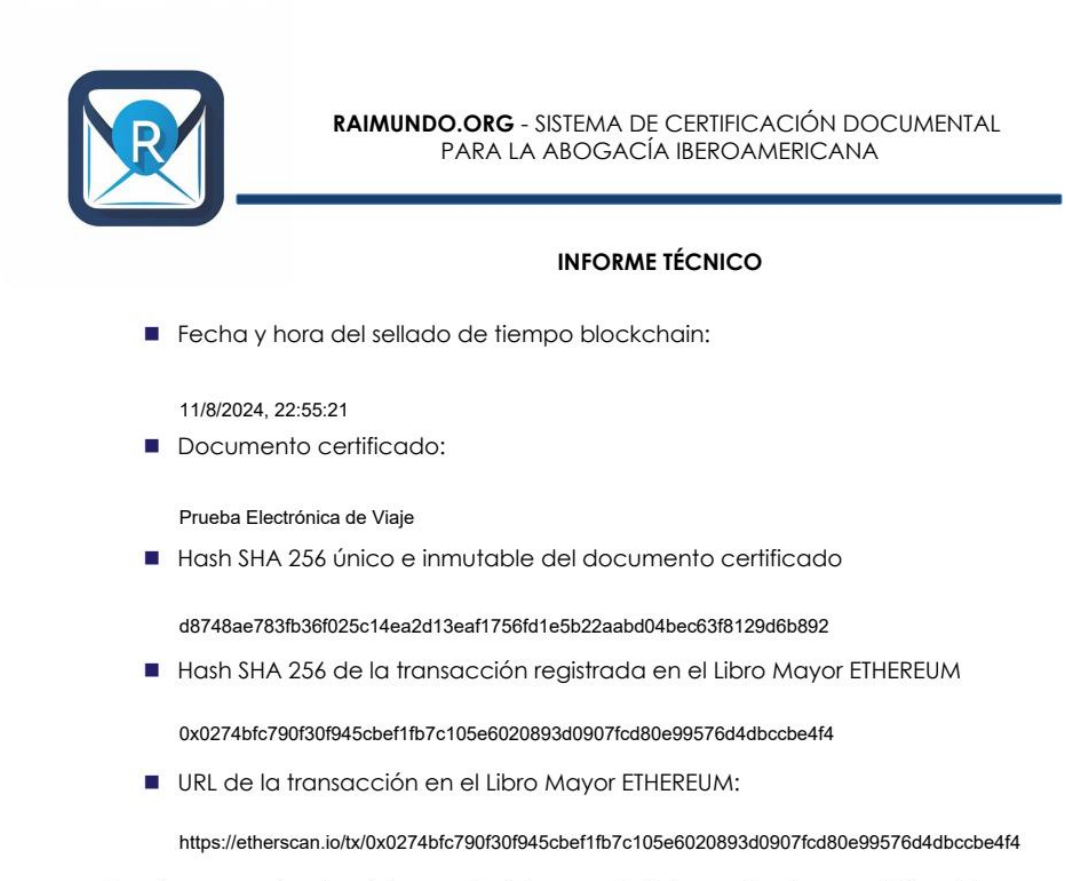
(c) Third, RAIMUNDO uses the aforementioned ethers.js library to execute a cryptocurrency transaction on the Ethereum network from the user's account connected with Metamask back to the same account. This transaction records the verified information as both an input and output on the Ethereum Ledger, with the SHA-256 hash of the certified document (as mentioned in section (a)) included as a "private note" within the blockchain auto-transaction data. RAIMUNDO then awaits transaction confirmation on the Ethereum blockchain. Once confirmed, the user interface communicates the success of the operation and provides a copy of the blockchain

transaction hash, along with a generated Etherscan URL for viewing transaction details. Etherscan is Ethereum's blockchain explorer, functioning as a viewer for the network's Ledger.

(d) Fourth, RAIMUNDO updates the interface with the document hash, the transaction hash, the blockchain timestamp, and the associated Etherscan portal URL for the transaction. Additionally, a QR code is generated with the Etherscan portal URL using the JavaScript library qrcode.js. To conclude, RAIMUNDO uses the JavaScript library pdf-lib to add the SHA-256 hash to the upper margin of each page of the uploaded PDF. As a final step, the modified PDF is saved, and a download link is provided to the user.

(e) Additionally, the user can download a "Technical Report" containing all the aforementioned information: the certified document hash, the Ethereum transaction hash, timestamp data, and a QR code linking to the Etherscan portal, which provides access to the Ethereum Ledger. The automatically generated technical report by RAIMUNDO is included as Figure 1 and a copy of the Ethereum Ledger transaction executed by RAIMUNDO as Figure 2.

FIGURE 1



RAIMUNDO.ORG - SISTEMA DE CERTIFICACIÓN DOCUMENTAL PARA LA ABOGACÍA IBEROAMERICANA

INFORME TÉCNICO

- Fecha y hora del sellado de tiempo blockchain:

  11/8/2024, 22:55:21

- Documento certificado:

  Prueba Electrónica de Viaje

- Hash SHA 256 único e inmutable del documento certificado

  d8748ae783fb36f025c14ea2d13eaf1756fd1e5b22aabd04bec63f8129d6b892

- Hash SHA 256 de la transacción registrada en el Libro Mayor ETHEREUM

  0x0274bfc790f30f945cbef1fb7c105e6020893d0907fcd80e99576d4dbccbe4f4

- URL de la transacción en el Libro Mayor ETHEREUM:

  https://etherscan.io/tx/0x0274bfc790f30f945cbef1fb7c105e6020893d0907fcd80e99576d4dbccbe4f4

Puede comprobar los datos contenidos en este informe técnico en el Libro Mayor ETHEREUM a través del siguiente código QR:

Sobre RAIMUNDO.ORG:

RAIMUNDO.ORG es un sistema de certificación documental para la Abogacía Iberoamericana, que se basa en tecnología blockchain, a través de la interacción con la red ETHEREUM.

RAIMUNDO.ORG calcula el hash único e inmutable del documento a certificar y lo incluye en una transacción ETHEREUM, quedando ésta registrada en el Libro Mayor de la red ETHEREUM, por naturaleza inalterable.

La tecnología criptográfica no permite generar un hash documental sin que exista el propio documento. De igual modo, cualquier modificación, por mínima que sea, en el documento certificado arrojará un hash totalmente distinto. De este modo, RAIMUNDO.ORG permite certificar la fecha de existencia de un documento así como la integridad de los datos en él contenidos a la fecha de existencia certificada.

Figure 1. Automatically generated technical report by RAIMUNDO.

FIGURE 2

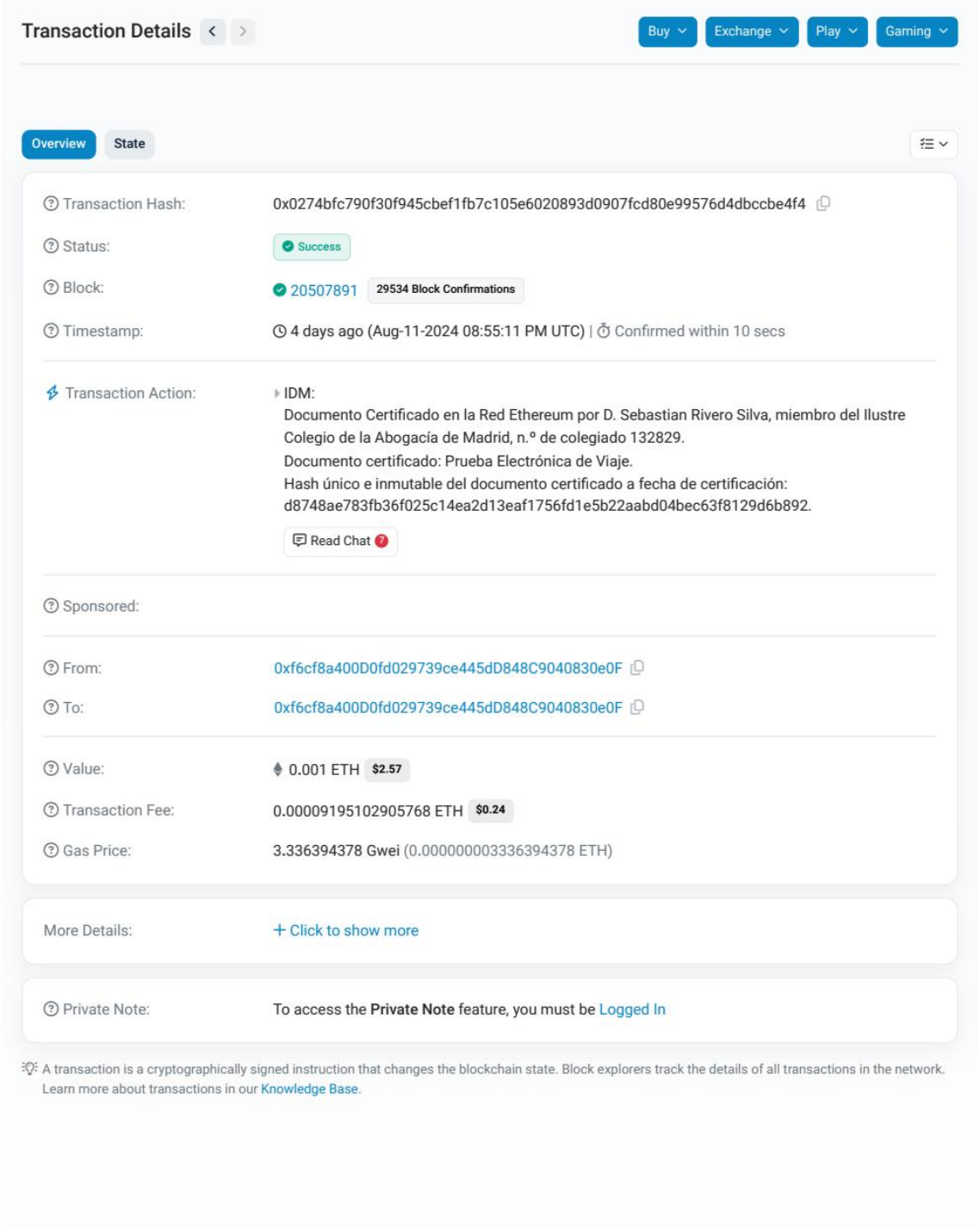


Figure 2. Copy of the Ethereum Ledger transaction executed by RAIMUNDO.

What practical use does a document certification issued by an attorney through RAIMUNDO serve? To address this question, we must first examine the probative quality of blockchain technology, in general terms, before a court or tribunal. In this

context, Spanish Magistrate Yolanda Ríos (2021, 3) defines blockchain technology as "a decentralized database, based on Distributed Ledger Technology (DLT), in which multiple nodes or users, through a peer-to-peer system, validate the information recorded in each block using a consensus formula, where majority agreement is sufficient for the information to be considered reliable and authentic."

In practical terms for this article, to understand the evidentiary validity of RAIMUNDO's technical process as previously described, we can say that a blockchain network essentially consists of a group of computers or computing systems, coordinated in a decentralized manner as "nodes." These nodes transfer and validate information amongst themselves, competing to earn a fee for performing this task. The final entry of the information validated by the majority of nodes is recorded in an almost automatic manner within the so-called ledger of the respective blockchain network, which is by nature immutable, unique, and transparent. This creates what can be termed a "tunnel effect," enabling any information — including hashed documents — to be digitized and timestamped, thus recording the document's existence date and the integrity of its contents as of that date, as per the final ledger entry (Sabry 2021).

In other words, once a document has been hashed and included in a blockchain network, we can assert that the document has been (a) audited in its content by tens of thousands of anonymous nodes, all independent of one another and, logically, of the attorney that is using RAIMUNDO, (b) recorded with its date of existence in the blockchain network's Ledger, and (c) documented with the SHA-256 hash code — discussed further below — which allows verification of the document's integrity within the blockchain. From this author's perspective, information certified by tens of thousands of anonymous computing systems should, at the very least, be evidentially equivalent to information certified by a public official working alone in an office. However, a significant legal obstacle remains unresolved: the restrictive interpretation of the concept of a public document. From this perspective, it becomes evident that the technological innovation introduced by RAIMUNDO cannot be fully leveraged for citizens' benefit, because the State (to varying degrees, depending on its civil law or common law tradition) retains the exclusive privilege of issuing "public documents." These public documents enjoy certain prerogatives, such as a presumption of authenticity, and are typically required for specific administrative procedures. Consequently, although RAIMUNDO generates highly reliable certificates that are publicly endorsed by the ETHEREUM community, from a legal standpoint, such certificates remain private documents and therefore carry less evidentiary weight than notarial certifications.

Under Spanish jurisdiction, which defines public documents through a closed and exhaustive list in Article 317 of the Civil Procedure Act (Ley de Enjuiciamiento Civil), "blockchain evidence" would not be considered a public document. Neither would it be in accordance with Art. 795 of the Mexican Federal Labor Law (section on documentary evidence). In other words, it would not be presumed inherently truthful as a public deed issued by a notary would be. Instead, blockchain evidence would fall under the category of "probative private document," subject to contradiction and challenge within judicial proceedings. This does not mean that evidence generated by RAIMUNDO would be "invalid" in court proceedings; rather, in evidentiary terms, it ranks one step below documents issued by State officials. Notably, the Spanish Supreme Court Judgment No.

326/2019, dated June 20, briefly touches upon the probative value of Bitcoin — which, in certain respects, shares fundamental characteristics with blockchain technology — even though the Supreme Court has not explicitly ruled on blockchain technology as such – (Monteagudo and García 2019). In Mexico, Judiciary Power has simply stated that cryptocurrencies are not money in legal terms, without further consideration of their evidentiary value (Melero and González 2019).

Thus, the judicial "validity" of RAIMUNDO is relative. Each jurisdiction has a degree of discretion — with the limits imposed by applicable international treaties — to accept "blockchain evidence" in court and, moreover, to assign it a greater or lesser probative value in comparison to traditional certification systems, such as standard document notarization or the signature of a public official. In this context, both Spain and Mexico have additional probative categories, such as the "compulsa," a certified copy issued by certain institutions, like universities, exclusively for their own documents, such as academic diplomas or transcripts (Zapatero Lourinho 2011, 327-331).

In this context, in civil law jurisdictions, which have a tradition of high legal certainty and are descendants of the codified system of the Roman Empire, consensus-based blockchain evidence has not been generally accepted as a public document, as this concept is classically associated with a function reserved to the State and delegated public officials. Historically, civil law systems have been known for their strict formalism and ritualism (Lambert and Wasserman 1929), a characteristic often at odds with technological innovations like blockchain. It is notable that in this "Roman" legal tradition, public documents generally carry the highest presumption of veracity and, therefore, the highest probative value (Abel Lluch 2010). Accordingly, "Roman" jurisdictions such as Spain and many Ibero-American jurisdictions like Mexico, continue to elevate the probative effectiveness of documents signed by a public official in an office over that of a document certified by tens of thousands of nodes in a transparent manner. This perspective, contrasted with that of other Anglo-Saxon common law jurisdictions, is by no means arbitrary. It stems from a State-based skepticism toward the consensus-based system upon which blockchain technology operates and to which all DApps are inextricably bound. By way of example, in the United Kingdom, the Digital Architecture and Cyber Security division at Her Majesty's Courts and Tribunals Service (HMCTS) proposed a pilot system for document archiving and certification using blockchain technology, intended for use in all UK courts (BCAS 2020). In a similar vein, during a symposium organized by the Bank of England on the economic development offered by blockchain technology, the Master of the Rolls remarked: "The advantages of the blockchain are so obvious that they will inevitably be taken up over time. The curve plotting the growth of DLT usage closely tracks the growth of the internet, and DLT is now about where the internet was in the mid-1990s" (Vos 2022).

Following a similar approach, in the case of *D'Aloia v. Unknown*, the High Court of England and Wales, in 2022, allowed a claim to be served via an NFT token sent to the defendant's blockchain wallet (Palacio Castiblanco *et al.* 2023, 347-348). Likewise, in the Supreme Court of the State of New York in 2022, the case *LCX AG v. John Doe Nos. 1–25* also permitted service of a claim through an NFT token (*LCX A.G. v. John Doe Nos. 1–25*, 2022, 9). Finally, in 2024, the High Court of Hong Kong — another jurisdiction that adheres to the common law tradition — accepted service of a civil claim via an NFT

token in the case *A – Plus World Wide Limited v. Unknown* (Yun 2025), mirroring the approach taken previously in the United Kingdom and the United States. Any practicing attorney in Spain would confirm that no Spanish judge would even contemplate serving a summons on an unknown party by means other than the court's official notification service or the relevant police authority.

The aforementioned examples of blockchain-based service of process in judicial settings attest to the recognition — in common law jurisdictions — of this technology's utility, traceability, and security for litigation purposes. In the same vein, some authors have argued that the evidentiary framework of common law systems, owing to its flexibility compared to that of Roman law systems, is more conducive to the adoption of blockchain technology for evidentiary purposes (Wang *et al.* 2024, 2). Such use, however, would not be permitted in civil law systems so long as their national legislation does not explicitly acknowledge the judicial validity of blockchain evidence. This is precisely the problem at hand: the restrictive definition of a public document, established by a numerus clausus regime that does not allow variations, as codified in Article 317 of Spanish Law 1/2000, of January 7, on Civil Procedure.

Certain authors have suggested that this distrust may also stem from the State's attempt to retain control over the highest probative effectiveness (i.e., notarial certification) and to counter legal transactions and operations outside of state oversight (Chambers 2019, 13). That is, the State is unwilling to relinquish its exclusive authority to issue public documents, the only instruments granted full evidentiary value. In my view, a key factor here is the reduction in the flow of commercial and financial information that the State typically obtains through civil law notarial services, a point of particular relevance to public revenue authorities and the prevention of money laundering in what are commonly referred to as developed countries. Furthermore, in jurisdictions marked by authoritarian rule or corruption, there may be a vested interest in exercising oversight over the legal affairs of business leaders, prominent figures, and political adversaries.

In contrast to the formalism of civil law regimes, it is worth citing the 2016 Vermont Blockchain Enabling Act, which grants blockchain evidence an exceptional probative quality by recognizing the security and immutability of the process, as previously discussed. Similarly, Delaware's 2017 amendments to its General Corporation Law allow for the full effectiveness of share transactions executed via blockchain (Caytas 2017). For instance, in Spain, share transfers in limited liability companies are only valid if executed before a notary public, as stipulated by Article 106.1 of the Spanish Companies Act (Ley de Sociedades de Capital). It is true that this development does not amount to Delaware courts recognizing so-called "blockchain evidence" as equivalent to a public document, but it nonetheless represents a significant precedent that would be unimaginable under Spain's civil law system. Ultimately, it demonstrates that the State is according credibility and legitimacy to the traceability, security, and public nature of blockchain technology.

In any case, it seems evident that Anglo-Saxon jurisdictions would be less inclined to exercise this type of control over private blockchain certifications., particularly because, in such jurisdictions — and notably in the United States — any individual can become a notary with only the basic requirements of literacy and, in some stakes, a one week course. Likewise, in the United Kingdom, it is well known that almost any legal

professional may issue, at their own risk, a "true copy" provided they are of "good standing" within their community (The Law Society 2024, HM Government 2025). In this regard, individuals who are recognized as both reputable and trustworthy by those around them are deemed to be in "good standing." In other words, Anglo-Saxon jurisdictions do not have as much at stake, as the notarial sector is largely liberalized, and there is no direct interconnection between the certifier and state agencies. In fact, in many U.S. states, notaries are not even required to maintain an up-to-date record book; such a practice is merely a recommendation.

The fact remains that, despite the high evidentiary value commonly acknowledged by international academia — albeit to varying degrees — within judicial proceedings (Li *et al.* 2021), a document certified by tens of thousands of nodes in a blockchain network is also subject to the acknowledgment that the consensus system, underlying such certification is not infallible and remains vulnerable to manipulation. This particular aspect will be examined further in the following section.

3. On the blockchain consensus system as the key to its evidentiary validity

Having understood RAIMUNDO's general functioning and the role of nodes as independent verifiers within the blockchain transaction, we must now examine the consensus among the nodes themselves. The "magic" by which blockchain technology delivers its core characteristics of immutability, traceability, and security is embedded precisely in the mechanism through which tens of thousands of nodes reach agreement on a particular verification.

Each blockchain network operates under its own consensus logic, pursuing specific primary objectives, whether a particular emphasis on security, energy efficiency, or mechanisms for rewarding the most "active" nodes or those contributing the most resources to the network. Regardless of the goal of the consensus logic, it is clear that the more secure the consensus protocol of the blockchain network on which a certification DApp operates, the higher the quality and weight of that DApp's blockchain evidence.

Ironically, while consensus logic builds trust among some users, it remains controversial in jurisdictions that hesitate to treat blockchain evidence as equivalent to state-issued public documents, issued by a state official, who — unlike blockchain nodes — is neither anonymous nor unsupervised, and is held accountable under disciplinary and regulatory frameworks (Llopis 2016). The function of the consensus system, wherein the blockchain nodes reach "agreement" to validate the data integrity of a transaction, is indeed critical to the evidentiary quality of blockchain evidence. As previously noted, RAIMUNDO adheres to the Proof of Stake (PoS) consensus model used by the Ethereum network (Buterin 2016, 3-10).

Reflecting a growing interest in environmental sustainability, the Ethereum blockchain network did not always operate under the PoS model. As recently as 2020, Ethereum was still utilizing the Proof of Work (PoW) model, during which time the so-called "Beacon Chain" was introduced — a secondary blockchain to Ethereum initially operating under PoS (Cassez *et al.* 2022, 167-171). Serving as a foundational layer, the Beacon Chain enables sharding — a "Green blockchain" strategy intended to reduce environmental impact by subdividing blocks into smaller "shards." Each shard operates as a full block, allowing partial, parallel verification rather than relying on a single, linear

addition. Coordinated through the Beacon Chain, this approach significantly reduces energy consumption (Luu *et al.* 2016).

In 2022, a significant event known as "The Merge" took place: the absorption merger of the Ethereum blockchain network, still operating under PoW, with the parallel Beacon Chain blockchain network already using PoS. This merger resulted in Ethereum adopting the PoS model in place of PoW, aiming for greater network sustainability (Mancino *et al.* 2023). Consequently, RAIMUNDO operates on one of the few networks that have specifically adopted the PoS model and apply "Green Blockchain" techniques to achieve better energy efficiency and a reduced environmental impact (Wang *et al.* 2023). This is why PoS-based blockchain networks are significantly less polluting than those operating under PoW algorithms and are central to the doctrinal debate advocating a shift towards more efficient models.

In this regard, various authors (Kohli *et al.* 2023) have claimed that the PoS algorithm, depending on its specific variation, can reduce a blockchain network's energy consumption by as much as 99.98% compared to traditional PoW. While it is true that this consensus model raises both ethical and technical concerns — since PoS relies on "staking" cryptocurrency to qualify as the "primary verifier" and thus earn gas fees or "rewards" in exchange for the verification services — the certification capability no longer resides in the computational power of the node (as in PoW) but instead depends on the "wealth" of the node (as in PoS). Regardless of these ethical aspects, in terms of sustainability, it is the opinion of this author that, should attorneys begin to use this technology as evidentiary support in court proceedings, they should employ blockchain networks operating under the Proof of Stake algorithm, such as Ethereum, Cardano, or Tezos. This would help sustain the system's eco-friendly benefits without negating the positive effects of reducing paper usage and combating deforestation.

Within the PoS and PoW binary, various alternative consensus models exist that could serve as potential alternatives or even undergo a new "Merge," similar to the Beacon Chain. Several scholars have explored these alternatives (Yadav *et al.* 2023). Nonetheless, with the advent of DApps, many blockchain networks have adopted PoS-based consensus mechanisms to address the distinct security requirements of individual communities. In this context, a number of relatively innovative approaches have emerged, aiming to implement additional security safeguards and attack-prevention mechanisms while also considering sustainability issues and minimizing barriers to node participation or transaction execution. Some solutions, for example, involve raising the costs of becoming a node or enhancing oversight of trusted nodes. The overarching goal remains the protection of transaction traceability, security, and transparency. Below is a concise overview of the most relevant options:

(i) Within the PoS model, two distinct sub-models exist: (a) the "Chain-based" format and (b) the "Committee-based" format (Xu *et al.* 2023). The first, the classic Ethereum PoS model, is based on staking, as previously discussed. The second, an adaptation of the Chain-based system, incorporates a group of "security nodes" that can be democratically selected and have the ability to verify and protect the network in the event of an attack, as they are considered "high-quality" nodes. This mechanism is crucial in cases of "poisoned branches" attempting to falsify the blockchain ledger. The so-called "committee" operates under a system known as secure multiparty

computation, which is intended to enhance network security; however, a compromised "committee" could wield considerable power in trimming "poisoned branches" from the ledger, making it a double-edged sword.

(ii) Alternatives to the PoS (in both Chain-based and Committee-based variations) and PoW consensus mechanisms include several variants, such as (a) Delegated Proof of Stake (DPoS), (b) Proof of Burn (PoB), and (c) Proof of Activity (PoA) (Rebello *et al.* 2022).

The DPoS model was developed with two main goals: to provide greater security and to be more energy-efficient. This approach invites us to reconsider whether we must choose between security and efficiency, as DPoS potentially meets both needs. DPoS can be seen as a variant of PoS in its Committee-based form. Under DPoS, the nodes verifying transactions are selected not randomly as in a committee but via an internal voting system based on reliability. In other words, the most reliable nodes — those staking the most cryptocurrency on correct certification — are tasked with verifying and recording data on the Ledger, monitored closely by other nodes, and subsequently distributing gas fees proportionally according to actual work performed. Since transactions are verified only by designated nodes rather than the entire network, they are completed almost 50% faster than with the original PoS model, with an annual energy consumption estimate of 0.0012 TWh (Bada *et al.* 2021, 506).

In contrast, PoB does not involve staking (as in PoS) or solving mathematical problems (as in PoW) to compete for validation. Instead, participants "burn" a portion of their cryptocurrency — a quantity, obviously, less than the expected gas fee or reward. Finally, PoA was expressly designed to mitigate 51% or Sybil attacks. It is a hybrid of PoS and PoW, initially operating as PoW and transitioning to PoS a few blocks into transaction verification. While PoA does not prioritize sustainability, some authors have proposed Redefined Proof of Activity (RPoA), a less energy-intensive variation, though it is still unable to match DPoS in terms of efficiency (Kamali *et al.* 2022).

Ultimately, the strength and reliability of the consensus mechanism determine the probative quality of blockchain evidence within judicial proceedings or when presented to a public authority. Each network can implement its own unique consensus logic, which influences the risk of data corruption as well as environmental and ethical considerations. Some authors argue that, beyond theoretical risk, there remains a tangible possibility of a consensus logic failure or a successful attack on a particular blockchain (Haugum *et al.* 2022). For this reason, certain jurisdictions remain steadfast in their refusal to substitute notaries or registrars — public officials trained in law and subject to strict regulatory regimes — for blockchain networks.

A public official is typically personally identifiable and bears direct personal liability — both civil and criminal — for any negligence or fraud in document certification. Blockchain nodes, by contrast, operate anonymously and currently lack comparable mechanisms for personal accountability. This distinction does not inherently dictate which system is more reliable, but rather highlights the different ways in which accountability and trust are established in each model.

Thus, if a blockchain network's consensus logic succumbed to a Sybil or 51% attack (Del Haro Olmo 2024, 2), the certification would be invalidated, and no individual could be

held liable. While many methods currently exist for detecting such attacks (Swathi *et al.* 2019), blockchain technology cannot, at least as of today, be deemed infallible.

In my view, blockchain evidence can coexist with the State's notarial function — whether more or less restrictive — to provide a spectrum of choices without limiting citizens' options for document certification. In this regard, it is worth reflecting on the potential incompatibility between the notarial function and certification through RAIMUNDO. In some countries, such as Spain or Mexico, the notarial function — i.e., the issuance of public documents — is reserved for certain officials, with explicit restrictions on compatibility with the practice of law. In this regard, some authors have noted that the liberalization of notarial functions in certain European Union countries may lead to a decline in service quality (Murray 2020, 49).

However, as some scholars note, other countries in the region, such as Portugal or Italy, permit partial and highly limited compatibility for functions like signature authentication and issuance of authentic copies (Rivero 2024). In contrast, the model in the United States and UK, as previously discussed, is fully open and compatible with the practice of law. Ultimately, there does not appear to be a Reason of Imperative General Interest (RIIG), in the strictest sense (Álvarez and Martínez 2018), that would justify prohibiting the use of blockchain technology for certifying data integrity and document timestamping in civil law jurisdictions. Moreover, Article 3 of Spanish Law 6/2020 of November 11, regulating certain aspects of electronic trust services, permits the coexistence between the notarial function and the use of private digital documents in Spain. Thus, if "blockchain evidence" is deemed private documentation under State law, it does not conflict in any way with the notarial function. On the other hand, Mexican law has not pronounced itself on this aspect, expressly allowing the judicial effects of electronic signatures (Argüelles 2016).

In any case, particularly regarding the potential shift within civil law jurisdictions, it is worth concluding this final section with a remark by Professor Jiménez-Gómez (2024, 1004). She observes that "without the help of all these professions (referring to notaries and registrars), a change of system is not possible." In other words, we can assert that those professional groups currently vested with the authority to issue public documents in civil law jurisdictions will have a decisive role in liberalizing that sector and, by extension, in securing the full legal validity of blockchain evidence.

4. Conclusions

This paper concludes with an examination of the implications of blockchain technology, specifically its application in the legal domain, and the questions it raises regarding its utility in judicial and administrative proceedings. The emergence of blockchain technology — and, more specifically, its application in the legal domain — raises questions regarding its utility within judicial and administrative proceedings. In this context, document certification through DApps like RAIMUNDO will need to be assessed on a jurisdiction-by-jurisdiction and court-by-court basis to determine the evidentiary quality of what is referred to as "blockchain evidence."

While it is true that, prima facie, common law jurisdictions, such as the United States, which tend to be more open to innovation, are granting significant probative value to blockchain evidence. Other civil law jurisdictions, like Spain or Mexico, traditionally

more formalistic, are reluctant to move away from the "public document" as the primary evidentiary tool in judicial and administrative contexts. This tendency is closely tied to the strict regulatory framework governing the European notarial system — incompatible with other offices, legal practice, and possessing near-exclusive authority in terms of public trust — contrasted with the more flexible North American and Anglo-Saxon systems, in which notarial roles can be combined with virtually any occupation, without even requiring intensive legal qualifications. In these common law jurisdictions, like United Kingdom, true copies may be issued by any "good standing" community member. In other words, Anglo-Saxon jurisdictions have no reserved or exclusive notarial authority to protect, making them more compatible with this type of disruptive technology. Nonetheless, regardless of the evidentiary quality attributed by each jurisdiction, blockchain evidence, as a form of private documentation, is entirely compatible with a State-reserved exclusivity for the creation of public documents, as far as we are clear about blockchain evidence not being a public document.

Accordingly, RAIMUNDO's aim is to enable blockchain-generated evidence to be used universally across jurisdictions, irrespective of the probative quality or public or private nature assigned by each. This leads to a second conclusion regarding the role of blockchain consensus logic in the evidentiary quality of RAIMUNDO's work. The reliability of blockchain evidence — and, indeed, the fundamental characteristics of this technology, such as transaction traceability and security — depends almost entirely on the community of nodes comprising a given blockchain network. More specifically, it depends on how these nodes, which verify the data in a blockchain transaction, reach an agreement in this verification, which is ultimately recorded in the network's Ledger.

In this context, the existence of "consensus mechanisms" and their potential for failure or exposure to attacks is, in my opinion, one of the reasons certain jurisdictions are still reluctant to accept blockchain evidence as a public document. A public official is identifiable and subject to civil and criminal liability in the event of document fraud, whereas a node could simply malfunction or fail without liability for any party.

In general, there are dozens of consensus mechanisms, most of which are derived essentially from two models: Proof of Work (PoW) and Proof of Stake (PoS). The first is characterized by high energy consumption and greater security, as verifying nodes must perform complex mathematical operations to earn gas fees. Therefore, establishing an infrastructure to attempt to infect or impersonate 51% of nodes and thereby alter verification outcomes is prohibitively expensive and highly improbable. The second model, by contrast, relies on a cryptocurrency staking system among verifying nodes to earn gas fees. Although it does not require as resource-intensive a process, it would still require a substantial amount of cryptocurrency to overcome 51% of the remaining nodes. In any case, the inherent nature of this technology would allow fraudulent activity within the consensus system to be automatically identified.

In this way, environmental impact and sustainability are central considerations in legal doctrine regarding the choice of a particular consensus mechanism. It is generally argued that the more environmentally impactful PoW model is more secure than PoS, as it is less vulnerable to attack. Consequently, in developing dApps like RAIMUNDO, a debate emerges between sustainability and security, with the risk of undermining the utility of blockchain evidence if a model favoring reduced environmental impact is

chosen at the expense of network security. In this context, PoS has been shown to be up to 99.98% less polluting than PoW. Despite this, there is a broad consensus in legal doctrine that new dApps should be developed using more sustainable models than PoW, as demonstrated by the Ethereum network after adopting the PoS model through The Merge.

As a final reflection, the full integration of RAIMUNDO and other similar DApps will require time for various jurisdictions to determine the extent to which they will allow blockchain evidence to enter a domain traditionally reserved for the public notarial function within civil law systems. Nonetheless, until that point is reached, DApps like RAIMUNDO have the potential to create new freedom spaces for citizens, supporting the free exercise of the legal profession and enhancing transactional security in diverse contexts, particularly within authoritarian or highly corrupt state environments.

References

Abel Lluch, X., 2010. Valoración de la prueba del documento público. *In:* X. Abel Lluch and A. Picó i Junoy, *La prueba documental.* Barcelona: J.M. Bosch, 531-547.

Aldwairi, M., Badra, M., and Borghol, R., 2023. DocCert: Nostrification, Document Verification and Authenticity Blockchain Solution. *Fifth International Conference on Blockchain Computing and Applications (BCCA)* [online], 652-657. https://doi.org/10.1109/BCCA58897.2023.10338908

Almansa Arévalo, D.E., 2024. Hashing: Types, Benefits and Security Issues. *Benefits and Security Issues* [online], 7 February. https://dx.doi.org/10.2139/ssrn.4718938

Álvarez Suárez, M., and Martínez Guerra, M., 2018. Los principios de la Ley de Unidad de Mercado como fuente de competencia y regulación eficiente de las actividades económicas. *Anuario de la competencia* [online], (1), 79-102. https://portal.mineco.gob.es/RecursosArticulo/mineco/economia/gum/articulos/LosprincipioLeyunidadmercadofuentecompetencia.pdf

Argüelles Arellano, M.D.C., 2016. Challenges of cyber law in Mexico. *Computación y Sistemas* [online], 20(4). https://doi.org/10.13053/cys-20-4-2515

Bada, A.O., *et al*., 2021. Towards a green blockchain: A review of consensus mechanisms and their energy consumption. *17th international conference on distributed computing in sensor systems (DCOSS)* [online], 503-511. https://doi.org/10.1109/DCOSS52077.2021.00083

Barba Álvarez, R., 2014. La invasión notarial y su justificación penal como mecanismo de protección notarial: estudio de la legislación local de Jalisco, México. *Prolegómenos* [online], 17(34), 42-52. https://doi.org/10.18359/dere.794

BCAS, 2020. *Blockchain court evidence* [Blog post] (online). 23 April. https://blog.bcas.io/blockchain_court_evidence#_ftn28

Brancós, E., 2024. Blockchain, función notarial y registro. *El Notario del Siglo XXI* [online]. https://www.elnotario.es/academia-matritense-del-notariado/7325-blockchain-funcion-notarial-y-registro

Briones Aguirre, R.J., and Quispe Gaibor, J.S., 2019. Análisis ético de la crisis humanitaria en Venezuela frente a la dictadura del presidente Nicolás Maduro y la migración de venezolanos hacia el Ecuador. *Revista Caribeña de Ciencias Sociales (RCCS)* [online], 4. https://dialnet.unirioja.es/servlet/articulo?codigo=9104718

Buterin, V., 2016. Ethereum: platform review. *Opportunities and challenges for private and consortium blockchains* [online], 45, 1-45. https://www.smallake.kr/wp-content/uploads/2016/06/314477721-Ethereum-Platform-Review-Opportunities-and-Challenges-for-Private-and-Consortium-Blockchains.pdf

Carpio Cervantes, E., 2021. La democracia latinoamericana del siglo XXI. *Andamios* [online], 18(46), 297-329. https://doi.org/10.29092/uacm.v18i46.847

Cassez, F., Fuller, J., and Asgaonkar, A., 2022. Formal verification of the ethereum 2.0 beacon chain. *In:* D. Fisman and G. Rosu, eds., *Tools and Algorithms for the Construction and Analysis of Systems. TACAS 2022. Lecture Notes in Computer Science, vol 13243* [online]. Cham: Springer. https://doi.org/10.1007/978-3-030-99524-9_9

Caytas, J., 2017. Blockchain in the US regulatory setting: Evidentiary use in Vermont, Delaware, and elsewhere. *Columbia Science & Technology Law Review* [online]. https://ssrn.com/abstract=2988363

Chambers, C., 2019. Money + markets: Blockchain isn't just a new technology, it is a political disrupter that takes away the state's monopoly on money. try as they might, governments won't be able to legislate it away. *Engineering & Technology,* 14(7/8), 13-13.

Del Haro Olmo, F.J., 2024. Ataque del 51% en blockchain: Golpe a la democracia digital. *Scientia Omnibus Portus* [online], 4(7), 2. https://iescelia.org/ojs/index.php/scientia/article/view/28

Falbo, S., and Di Castelnuovo, F., 2019. *Nuevas tecnologías aplicadas a la función notarial.* Buenos Aires: Di Lalla.

Fernández-Caramés, T.M., and Fraga-Lamas, P., 2024. *A Comprehensive Survey on Green Blockchain: Developing the Next Generation of Energy Efficient and Sustainable Blockchain Systems* [online]. https://doi.org/10.48550/arXiv.2410.20581

Gehlot, S., and Dhall, A., 2022. Cryptocurrencies And Blockchains: Will It Be The Vaccine Against Corruption?. *Journal of Positive School Psychology* [online], 6(8), 10146-10155. https://journalppw.com/index.php/jpsp/article/view/12605/8169

Gupta, P., and Kumar, S., 2014. A comparative analysis of SHA and MD5 algorithm. *International Journal of Computer Science and Information Technologies* [online], 5(3), 4492-4495. https://www.ijcsit.com/docs/Volume%205/vol5issue03/ijcsit20140503398.pdf

Haugum, T., *et al.*, 2022. Security and privacy challenges in blockchain interoperability-A multivocal literature review. *Proceedings of the 26th International Conference on Evaluation and Assessment in Software Engineering* [online], 347-356. https://doi.org/10.1145/3530019.3531345

HM Government., 2025. *Certifying a document* [online]. https://www.gov.uk/certifying-a-document

Ibáñez Jiménez, J.W., 2017. Cuestiones jurídicas en torno a la cadena de bloques («blockchain») ya los contratos inteligentes («smart contracts»). *ICADE. Revista de la Facultad de Derecho* [online], (101). https://doi.org/10.14422/icade.i101.y2017.003

Issacharoff, S., 2006. Fragile democracies. *Harvard Law Review* [online], 120(6), 1405. https://harvardlawreview.org/print/vol-120/fragile-democracies/

Jiménez-Gómez, B.S., 2020. Risks of blockchain for data protection: a European approach. *Santa Clara High Technology Law Journal* [online], 36(3), 281. https://digitalcommons.law.scu.edu/chtlj/vol36/iss3/2.

Jiménez-Gómez, B.S., 2023a. Blockchain as an opportunity to upgrade the right to vote in listed companies. *InDret* [online], 1, 61–97. https://www.doi.org/10.31009/InDret.2023.i1.03

Jiménez-Gómez, B.S., 2023b. Distributed Ledger Technology in Financial Markets. The European Union Experiment. *Cuadernos de Derecho Transnacional* [online], 15(2), 677. https://doi.org/10.20318/cdt.2023.8073

Jiménez-Gómez, B.S., 2024. La tecnología TRD y el derecho: una relación necesaria para la seguridad jurídica. *Cuadernos de Derecho Transnacional* [online], 16(2), 1000-1013. https://doi.org/10.20318/cdt.2024.8956

Kamali, S., *et al*., 2022. *RPoA: Redefined Proof of Activity* [online]. https://doi.org/10.48550/arXiv.2210.08923

Kohli, V., *et al*., 2023. An analysis of energy consumption and carbon footprints of cryptocurrencies and possible solutions. *Digital Communications and Networks* [online], 9(1), 79-89. https://doi.org/10.1016/j.dcan.2022.06.017

Krstinic, D., and Zarubica, S., 2021. Enforcement of Public Notary Documents. *Law Theory & Practice* [online], 38(1), 42. https://doi.org/10.5937/ptp2101042K

Kumar, D., Kumar, S., and Joshi, A., 2023. Assessing the viability of blockchain technology for enhancing court operations. *International Journal of Law and Management* [online], 65(5), 425-439. https://doi.org/10.1108/IJLMA-03-2023-0046

Lambert, E., and Wasserman, M.J., 1929. The case method in Canada and the possibilities of its adaptation to the civil Law. *Yale Law Journal* [online], 39(1), 1-21. https://doi.org/10.2307/790333

LCX A.G. v. John Doe Nos. 1–25 [online]. Supreme Court of the State of New York 2022. https://www.hklaw.com/-/media/files/generalpages/lcx-ag-v-doe/nyscef22amcompl.pdfrev=21aff6cbbca346bd872a5bab408cc272&sc_lang=en&hash=B6060BEF8FED081C6141A5D275C042B3

Lee, W.M., 2023. Using the MetaMask crypto-wallet. *In:* W.M. Lee, *Beginning Ethereum Smart Contracts Programming: With Examples in Python, Solidity, and JavaScript* [online]. Berkeley: Apress, 111-144. https://doi.org/10.1007/978-1-4842-9271-6

Li, M., *et al.*, 2021. LEChain: A blockchain-based lawful evidence management scheme for digital forensics. *Future Generation Computer Systems* [online], 115, 406-420. https://doi.org/10.1016/j.future.2020.09.038

Llopis, J.C., 2016. Blockchain y la profesión notarial. *El Notario del Siglo XXI* [online]. https://www.elnotario.es/hemeroteca/revista-70/7106-blockchain-y-profesion-notarial

Luu, L., *et al*., 2016. A secure sharding protocol for open blockchains. *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security* [online], 17-30. https://doi.org/10.1145/2976749.2978389

Mancino, D., *et al*., 2023. *Exploiting Ethereum after" The Merge": The Interplay between PoS and MEV Strategies* [online]. ITASEC 2023: The Italian Conference on CyberSecurity, May 03–05, 2023, Bari, Italy. https://ceur-ws.org/Vol-3488/paper24.pdf

Melero, V.I., and González, E.S., 2019. Banco de México y sus facultades respecto de las instituciones de tecnología financiera en materia de criptoactivos. *Jurídica Ibero. Revista Semestral del Departamento de Derecho de la Universidad Iberoamericana*, (7), 43-70.

Miraz, M.H., Excell, P.S., and Rafiq, M.K.S.B., 2021. Evaluation of green alternatives for blockchain proof-of-work (PoW) approach. *Annals of Emerging Technologies in Computing (AETiC)* [online], 54-59. https://doi.org/10.33166/AETiC.2021.04.005

Monteagudo, M., and Javier García, F., 2019. La primera sentencia sobre bitcoins de nuestro Alto Tribunal: comentario a la Sentencia del Tribunal Supremo (Sala de lo Penal, Sección 1.ª) número 326/2019, de 20 de junio. *Actualidad Jurídica Uría Menéndez* [online], 52, 128-135. https://www.uria.com/documentos/publicaciones/6681/documento/foro10.pdf?id

Murray, P.L., 2020. Valoración desde USA del sistema europeo de justicia preventiva basado en el notariado. *Anales de la Academia Matritense del Notariado* [online], 60, 19-53. http://www.cnotarial-madrid.org/nv1024/paginas/TOMOS_ACADEMIA/060-01-PETER_L_MURRAY.pdf

Palacio Castiblanco, M.L., Cespedes Suárez, J.S., and Caraballo Ramírez, H.J., 2023. Eficacia de la implementación de los NFT'S como medio de notificación judicial en procesos de arbitraje. *Derecho global. Estudios sobre derecho y justicia* [online], 9(25), 345-365. https://doi.org/10.32870/dgedj.v9i25.697

Prasanna, S.R., and Premananda, B.S., 2021. Performance analysis of md5 and sha-256 algorithms to maintain data integrity. *2021 International Conference on Recent Trends on Electronics, Information, Communication & Technology (RTEICT)* [online], 246-250. https://doi.org/10.1109/RTEICT52294.2021.9573660

Rebello, G.A.F., *et al*., 2022. A security and performance analysis of proof-based consensus protocols. *Annals of Telecommunications* [online], 1-21. https://doi.org/10.1007/s12243-021-00896-2

Ríos López, Y., 2021. Blockchain, Smart contracts y administración de justicia. *Blockchain Intelligence* [online], enero, 2-12. https://blockchainintelligence.es/wp-content/uploads/2021/02/BLOCKCHAIN-SMART-CONTRACTS-Y-ADMINISTRACION-DE-JUSTICIA_YOLANDA-RIOS.pdf

Rivero, S., 2024. Certificación documental, ¿nueva función para la Abogacía? *Revista de Derecho Mercantil* [online], 58. https://www.sepin.es/revistas-digitales/revista.asp?cde=61&id=77143

Roussev, V., 2009. Hashing and data fingerprinting in digital forensics. *IEEE Security & Privacy* [online], 7(2), 49-55. https://doi.org/10.1109/MSP.2009.40

Sabry, F., 2021. *Libro Mayor Distribuido: Poniendo la riqueza y la fe en un marco matemático, libre de políticas y errores humanos (Vol. 1).* One Billion Knowledgeable.

Saian, S.D.S., Sembiring, I., and Manongga, D.H., 2024. A Prototype of Decentralized Applications (DApps) Population Management System Based on Blockchain and Smart Contract. *JOIV: International Journal on Informatics Visualization* [online], 8(2), 845-853. http://dx.doi.org/10.62527/joiv.8.2.1861

Schwalm, S., and Alamillo-Domingo, I., 2021. Self-sovereign-identity & eIDAS: a contradiction? Challenges and chances of eIDAS 2.0. *Wirtschaftsinformatik* [online], 58, 247-270. https://doi.org/10.1365/s40702-021-00711-5

Shawn, L.W.M., *et al.*, 2021. Blockchain-based proof of existence (POE) framework using Ethereum Smart Contracts. *Proceedings of the Eleventh ACM Conference on Data and Application Security and Privacy* [online], 301-303. https://doi.org/10.1145/3422337.3450319

Shi, X., *et al*., 2023. Confronting the carbon-footprint challenge of blockchain. *Environmental science & technology* [online], 57(3), 1403-1410. https://doi.org/10.1021/acs.est.2c05165

Stančić, H., 2018. New technologies applicable to document and records management: blockchain. *Lligall*. *Revista Catalana d'Arxivística*. *Noves perspectives en matèria de gestió documental* [online], 41, 56-72. https://arxivers.com/wp-content/uploads/2018/10/1.3_Dossier-HStancic.pdf

Swathi, P., Modi, C., and Patel, D., 2019. Preventing sybil attack in blockchain using distributed behavior monitoring of miners. *2019 10th international conference on computing, communication and networking technologies (ICCCNT)* [online], 1-6. https://www.doi.org/10.1109/ICCCNT45670.2019.8944507

The Law Society, 2024. How should I certify a copy of an original document? *The Law Society* [online], 15 March. Available at: https://www.lawsociety.org.uk/contact-or-visit-us/helplines/practice-advice-service/q-and-as/how-should-i-certify-a-copy-of-an-original-document

Vos, G., 2022. *[Keynote speech: The economic value of English law in relation to DLT and digital assets]* (online). Digital Assets Symposium: Challenging Legal Frontiers, Bank of England, 25 July. https://www.judiciary.uk/speech-by-the-master-of-the-rolls-the-economic-value-of-english-law-in-relation-to-dlt-and-digital-assets/

Wang, P., *et al.*, 2023. Energy-Efficient Distributed Learning and Sharding Blockchain for Sustainable Metaverse. *IEEE Wireless Communications* [online], 30(5), 128-134. http://dx.doi.org/10.1109/MWC.015.2300107

Wang, X., Wu, Y.C., and Ma, Z., 2024. Blockchain in the courtroom: exploring its evidentiary significance and procedural implications in US judicial processes. *Frontiers in Blockchain* [online], 7, 1306058. https://doi.org/10.3389/fbloc.2024.1306058

Wendl, M., Doan, M.H., and Sassen, R., 2023. The environmental impact of cryptocurrencies using proof of work and proof of stake consensus algorithms: A systematic review. *Journal of Environmental Management* [online], 326(part A), 116530. https://doi.org/10.1016/j.jenvman.2022.116530

Wu, K., *et al.*, 2021. A first look at blockchain-based decentralized applications. *Software: Practice and Experience* [online], 51(10), 2033-2050. https://doi.org/10.1002/spe.2751

Xu, J., Wang, C., and Jia, X., 2023. A survey of blockchain consensus protocols. *ACM Computing Surveys* [online], 55(13s), 1-35. https://doi.org/10.1145/3579845

Yadav, A.K., *et al.*, 2023. A comparative study on consensus mechanism with security threats and future scopes: *Blockchain. Computer Communications* [online], 201, 102-115. https://doi.org/10.1016/j.comcom.2023.01.018

Yun, Y., 2025. Hong Kong court serves tokenized legal notice to illicit Tron wallets. *Cointelegraph* [online], 15 January. https://cointelegraph.com/news/hong-kong-tokenized-legal-notice-tron

Zapatero Lourinho, A.S., 2011. Cotejo y compulsa de los documentos, responsabilidades asumidas por los ciudadanos en la tramitación electrónica de los procedimientos administrativos. *In:* J.A. Martínez, J.C. Marcos and J.M. Sánchez, eds., *Información y documentación: investigación y futuro en red* [online]. Universidad Complutense de Madrid, 327-335. https://hdl.handle.net/20.500.14352/45853