

**DIGITAL JUDGMENT: TOWARDS A BLOCKCHAIN-BASED RECOGNITION
SYSTEM**

Avaskhan Z. Asanaliyev*

Cite as: Avaskhan Z. Asanaliyev, *Digital Judgment: Towards a Blockchain-Based Recognition System*, 32 Rich. J.L. & Tech. 287 (2026).

*Avaskhan Asanaliyev is an S.J.D. and International and Comparative Law Research Scholar at the University of Michigan Law School. He holds an LL.M. from Duke University School of Law and has advised on cryptocurrency and blockchain technology matters, including a large-scale cryptocurrency issuance and follow-on placement for a global technology company. He previously practiced at White & Case LLP and Norton Rose Fulbright LLP, where he worked on cross-border transactions in the oil and gas, financial, and mining sectors. His article, *Digital Judgment: Towards a Blockchain-Based Recognition System*, examines how blockchain technology could improve the recognition and enforcement of court judgments by making records more secure, transparent, and efficient. The article reviews legal frameworks governing the recognition of foreign judgments, analyzes how digitalization is reshaping private international law, and argues that blockchain-based judgments should be recognized when they satisfy rigorous standards of authentication, due process, and judicial oversight.

ABSTRACT

Blockchain technology offers judicial systems a transformative opportunity to enhance the efficiency, security, and transparency of court judgments. This article explores how blockchain-based judgment records could streamline recognition and enforcement procedures. Current methods for authenticating and recognizing judgments depend on slow, manual certification processes and state-specific rules. These approaches create administrative delays, expose systems to fraud, and struggle to keep pace with a digital, global legal landscape. In contrast, a decentralized ledger secured by cryptographic verification would deliver near-instant, tamper-proof records. This could significantly expedite cross-jurisdictional enforcement while upholding due process and reliability. The article reviews recent advancements in blockchain dispute resolution and smart contract enforcement, assessing their alignment with existing legal requirements for due process and authentication. It also examines the implications of autonomous, code-based governance mechanisms that operate outside traditional legal frameworks, stressing the need to preserve judicial oversight and discretion. Although U.S. courts currently lack formal recognition for blockchain-based judgments, international developments signal a global shift towards technologically integrated courts. Examples include China's national judicial blockchain platform and Dubai's "smart courts" initiative. In light of these trends, this article argues that courts should recognize cryptographically verified blockchain judgments as authentic and enforceable—*on par* with conventionally certified judgments—provided they satisfy rigorous technical and legal standards for authentication and due process. Key challenges include privacy risks, interoperability across platforms, and balancing automation with human judicial discretion. Ultimately, integrating blockchain into judicial processes promises a more efficient, transparent, and fraud-resistant legal system. Yet this transition must prioritize procedural fairness and resolve tensions between code-based governance and judicial discretion.

Table of Contents

<i>I. INTRODUCTION</i>	292
<i>II. THE LEGAL FRAMEWORK FOR FOREIGN JUDGMENT RECOGNITION AND ENFORCEMENT</i>	298
A. International Regulations and Blockchain-Based Judgments	298
<i>i. The Hague Convention on the Recognition and Enforcement of Foreign Judgments (2019): Relevance and Limitations</i>	298
<i>ii. Enforcement and Recognition Challenges</i>	301
B. Recognition of Foreign Judgments in the U.S.	303
<i>i. Uniform Foreign-Country Money Judgments Recognition Act (UFCMJRA)</i>	303
<i>ii. Due Process Concerns and Judicial Discretion in Recognizing Foreign Judgments</i>	305
<i>iii. Blockchain as a Means to Strengthen Authenticity and Trust in Foreign Judgments</i>	306
<i>III. PRIVATE INTERNATIONAL LAW AND JUDICIAL DIGITALIZATION</i>	308
A. Jurisdiction	308
B. Applicable Law	309
C. Cross-Border Data Integrity and Cooperation	310
D. Digital Identities and Authentication	312
E. Challenges to Established Principles	313
<i>IV. BLOCKCHAIN AS A TOOL FOR JUDICIAL RECORD-KEEPING AND ENFORCEMENT</i>	314

A. How Blockchain Works in Legal Applications.....	315
<i>i. Distributed Ledger Technology and Cryptographic Verification</i>	<i>315</i>
<i>ii. Immutable Court Records: Preventing Fraud and Alterations</i>	<i>316</i>
B. Blockchain Precedents in Legal Systems	318
<i>i. China’s Internet Courts and Blockchain-Based Judicial Records.....</i>	<i>318</i>
<i>ii. Dubai’s Smart Courts Initiative</i>	<i>320</i>
<i>iii. Estonia’s E-Governance Model</i>	<i>323</i>
C. Smart Contracts and Automated Enforcement of Judgments	324
<i>i. Overview of Smart Contracts in Legal Tech</i>	<i>324</i>
<i>ii. Self-Executing Court Orders and Asset Freezing</i>	<i>325</i>
<i>iii. Combining Smart Contracts with Conventional Legal Systems</i>	<i>326</i>
V. CHALLENGES TO INTEGRATING BLOCKCHAIN-BASED JUDGMENTS IN THE	
JUDICIARY.....	327
A. Lex Cryptographica: Autonomous Systems and Their Implications for	
Judicial Review.....	329
B. How Code-Based Protocols May Undermine Judicial Oversight	333
C. Ensuring Human Judicial Review in Automated Enforcement	
Mechanisms	338
<i>i. Designing “Smart Legal Contracts”</i>	<i>338</i>
<i>ii. Incorporating Arbitration and Dispute Resolution within Code</i>	<i>339</i>
<i>iii. Community Governance and “Soft” Oversight.....</i>	<i>340</i>
<i>iv. Legal Accountability for Code Outcomes.....</i>	<i>341</i>
D. Technical and Administrative Challenges	342
<i>i. Standardizing Blockchain Infrastructure Across Courts.....</i>	<i>342</i>

ii. Privacy and Confidentiality Issues in Judicial Data Management ... 344

*iii. Interoperability Between Blockchain Systems and Traditional Court
Databases..... 347*

VI. CONCLUSION..... 351

I. INTRODUCTION

[1] The integration of blockchain technology holds significant potential to enhance the recognition and enforcement of court judgments within judicial systems. In an era of widespread digital innovation, national judiciaries continue to operate under procedural frameworks grounded in manual document certification, court-issued copies, and related rules.¹

[2] Blockchain technology offers a promising solution. Compared to traditional electronic systems, blockchain provides a unique method for data storage.² Its distributed structure, consensus mechanisms (such as proof-of-work), and one-way hashing algorithms render information recorded on the blockchain exceedingly difficult to erase or falsify.³ No single party can unilaterally alter or reverse entries, and smart contracts execute

¹ For instance, despite the rapid pace of digital innovation, the U.S. judiciary still operates under procedural systems based on manual processes and conventional document management. The Supreme Court's rules, for example, state that some records can be submitted in the form of certified copies, while certain situations require receipt and inspection of original documents. See SUP. CT. R. 12.7, *Rules of the Supreme Court of the United States* (2019), <https://www.supremecourt.gov/ctrules/2019RulesoftheCourt.pdf> [<https://perma.cc/TNT5-D8UB>] (last visited Feb. 25, 2025) (explaining how the Supreme Court's rules, for example, state that some records can be submitted in the form of certified copies, while certain situations require receipt and inspection of original documents).

² PRIMAVERA DE FILIPPI & AARON WRIGHT, *BLOCKCHAIN AND THE LAW: THE RULE OF CODE 35* (Harv. Univ. Press 2018) (explaining how in popular blockchain-based networks, the entire blockchain replicates across thousands of computers worldwide, and anyone seeking to change a blockchain must either acquire control of all nodes or pursue a lengthy (and sometimes contentious) process of public consultation to convince other network users to adopt the change as part of the underlying protocol). To alter a blockchain, parties must articulate a rationale for the update and engage with miners (e.g., via social media or direct communication). *Id.*

³ *Id.*

automatically once deployed, unless the code specifies otherwise.⁴ Unlike centralized servers, blockchain systems transcend single-location constraints, delivering two major advantages: broader access and enhanced security.⁵ As electronic court records become increasingly prevalent, courts confront persistent challenges, including unauthorized third-party replication and the absence of reliable mechanisms to ensure accurate reflection of post-judgment amendments.⁶ Blockchain directly addresses these issues by enabling real-time, authenticated updates that extend beyond the confines of a single courthouse.⁷ No matter how many third-party data aggregators access a blockchain-based judgment, the record will invariably reflect the most current and authoritative version.⁸

[3] As a decentralized and immutable record-keeping system, blockchain can generate digitally signed court documents that are resistant to tampering. This capability has the potential to reduce the time for cross-jurisdictional enforcement by eliminating repetitive authentication

⁴ *Id.*

⁵ Di Graski & Paul Embley, *When Might Blockchain Appear in Your Court?*, NAT'L CTR. STATE CTS. (Apr. 11, 2018), <https://courtechbulletin.blogspot.com/2018/04/when-might-blockchain-appear-in-your.html> [<https://perma.cc/YM7X-E7FC>]; *Estonian Blockchain Technology*, E-ESTONIA, https://e-estonia.com/wp-content/uploads/faq_estonian_blockchain_technology.pdf [<https://perma.cc/BCX7-8WK9>] (stating organizations take an average of seven months to detect breaches and manipulations of electronic data, while blockchain solutions enable instantaneous detection); *Cyber Security*, E-ESTONIA, <https://e-estonia.com/solutions/cyber-security/ksi-blockchain/> [<https://perma.cc/JV6R-83ZC>] (showing Estonia, for instance, developed scalable KSI blockchain technology to safeguard data integrity in government repositories against insider threats, and mathematical proof of electronic data renders tampering impossible).

⁶ Di Graski & Embley, *supra* note 5, at 63.

⁷ *See* Graski & Embley, *supra* note 5, at 63.

⁸ *See* Graski & Embley, *supra* note 5, at 63.

processes, thereby redefining how judgment recognition and enforcement can be carried out not only within national boundaries but also in international cases. Current international practices, such as Dubai's smart courts initiative, China's use of blockchain in judicial records, and Estonia's digital court system, show that a growing number of courts and systems have introduced technological judicial platforms. In 2018, the Dubai International Financial Centre (DIFC) Courts communicated the goal of establishing the world's first "Court of the Blockchain."⁹ Based on the existing dispute resolution services, they are examining how to support the verification of court decisions for cross-border enforcement.¹⁰ Blockchain was initially integrated into the operations of China's internet courts, which were first introduced in Hangzhou in 2017 and later expanded to Beijing and Guangzhou.¹¹ These courts have used blockchain as a secure, verifiable way to store and authenticate digital evidence.¹² For example, when a party submits electronic evidence, such as screenshots of transactions, chat logs, or online contracts, the blockchain records a timestamp and a cryptographic hash of the data.¹³ This ensures that the evidence remains unaltered from the moment it is uploaded.¹⁴ Since March 2023, over 3,500 courts in China

⁹ *Thinking Ahead for Businesses of the Future*, COURTS OF THE FUTURE, <https://www.courtsofthefuture.org/#courts-of-blockchain> [<https://perma.cc/Y6Q3-UAJM>] (last visited Feb. 25, 2025).

¹⁰ *Id.*

¹¹ Tian Lu, *The Implementation of Blockchain Technologies in Chinese Courts*, 4 STANFORD J. BLOCKCHAIN L. & POL'Y 102, 112 (Jan. 4, 2021) <https://stanford-jblp.pubpub.org/pub/blockchain-in-chinese-courts/release/1> [<https://perma.cc/L3W2-FFJ2>].

¹² *Id.*

¹³ *Id.*

¹⁴ Blockchain is also used to automate certain procedural aspects of dispute resolution. The courts use "smart contracts," which are self-executing contracts with terms directly written into code, to handle routine matters and reduce human intervention, thereby expediting case processing. *Id.* In May 2022, the Supreme People's Court of China (SPC) issued the Opinions on Strengthening Blockchain Application in the Judicial Field to

have been serving electronic documents that can be verified online through the Judicial Blockchain Platform.¹⁵ It allows courts at all levels to guarantee data security and transparency while storing and verifying judicial information, including electronic evidence, case filings, and enforcement records.¹⁶ Additionally, all documents produced in the courts of Estonia are hashed, signed, and secured by KSI, a blockchain technology embedded across government networks, including the digital justice system, the State Gazette, as well as business, property, succession, and healthcare registries.¹⁷

accelerate digital transformation and promote the development of smart courts. The Opinions aim to create an interconnected “blockchain alliance,” focusing on collaboration between courts and social sectors and integrating blockchain technology into dispute resolution, litigation, trial, and enforcement processes. Xu Jianfeng, *China Leverages the Blockchain to Advance the Development of “Smart Courts,”* WIPO MAGAZINE (Sep. 30, 2022), <https://www.wipo.int/web/wipo-magazine/articles/china-leverages-the-blockchain-to-advance-the-development-of-smart-courts-42824> [<https://perma.cc/GN8Q-SQG2>] (explaining how in May 2022, the Supreme People’s Court of China issued opinions supporting blockchain application in the judiciary to accelerate the development of smart courts).

¹⁵ Yurou Yin, *E-Documents from Chinese Courts can be Verified on Blockchain*, CHINA JUST. OBSERVER (May 8, 2023), <https://www.chinajusticeobserver.com/a/e-documents-from-chinese-courts-can-be-verified-on-blockchain> [<https://perma.cc/E2GZ-Y6KJ>] (explaining that when a bank receives an electronic court document requiring release of a debtor’s deposit to a creditor, the bank may verify the documents’ authenticity through the Judicial Blockchain Platform).

¹⁶ Jianfeng, *supra* note 14.

¹⁷ Ivan Martinovic et al., *Blockchains for Governmental Services: Design Principles, Applications, and Case Studies*, CTR. FOR TECH. & GLOB. AFFS., (Dec. 2017) <https://www.politics.ox.ac.uk/sites/default/files/2022-03/201712-CTGA-Martinovic%20I-Kello%20L-blockchainsforgovernmentalservices.pdf> [<https://perma.cc/859V-58XD>]; see Silvia Semenzin et al., *Blockchain-based Application at a Governmental Level: Disruption or Illusion? The Case of Estonia*, 41 POL’Y & SOC’Y, 386, 386–401 (2022) <https://doi.org/10.1093/polsoc/puac014> [<https://perma.cc/EGW6-4WGP>]; see also Anna-Maria Osula, *Blockchain in Estonia & Project Priviledge H2020: Introduction* (Dec. 2019), <https://northsearegion.eu/media/11757/20191217-guardtime.pdf> [<https://perma.cc/3XGC-HJRP>].

[4] However, the transition to blockchain-based judicial processes raises significant legal challenges. A central question is how such judgments can be made to conform to existing recognition law. In the case of the U.S., while the relevant statutes establish standards for due process,¹⁸ and authentication¹⁹ they do not currently account for cryptographically verified judgments or self-executing smart contracts. The integration of blockchain into judicial functions also presents the complex task of balancing technological efficiency with procedural fairness, especially in light of emerging “rule-by-code” systems, where legal outcomes are enforced automatically through software.²⁰ Despite these concerns, there are notable developments: several U.S. states enacted legislation

¹⁸ See UNIF. FOREIGN-COUNTRY MONEY JUDGMENTS RECOGNITION ACT § 4(b)(1), (c)(8) (2005) [hereinafter UFCMJRA] (permitting nonrecognition where the foreign judicial system or the specific proceeding was incompatible with due process). Additionally, under § 4(c)(8) a court may deny recognition of a foreign-country judgment if “the specific proceeding in the foreign court leading to the judgment was not compatible with the requirements of due process of law.” Unlike the Uniform Enforcement of Foreign Judgments Act (UEFJA) dealing “solely with the *enforcement* of sister-state judgments and other judgments entitled to full faith and credit,” the UFCMJRA also provides for “the *recognition* of foreign-country judgments. The judgment debtor with regard to a sister-state judgment normally does not have any grounds for opposing recognition and enforcement of the judgment. The extremely limited grounds for denying full faith and credit to a sister-state judgment reflect the fact such judgments will have been rendered by a court that is subject to the same due process limitations and the same overlap of federal statutory and constitutional law as the forum state’s courts, and, to a large extent, the same body of court precedent and socio-economic ideas as those shaping the law of the forum state. *Id.* § 6 cmt. 1 (explaining that foreign-country judgments, unlike sister-state judgments, lack the same presumption of fairness and competence).

¹⁹ See generally UNIF. ENF’T OF FOREIGN JUDGMENTS ACT § 2 (1964) [hereinafter UEFJA] (requiring filing of an authenticated copy of a sister-state judgment and providing that the judgment is thereafter treated like a local judgment); see also UFCMJRA § 6 (requiring recognition of a foreign-country judgment to be sought by action or in a pending proceeding); see also FED. R. EVID. 902(3) (governing authentication of foreign public documents).

²⁰ DE FILIPPI & WRIGHT, *supra* note 2, at 9.

recognizing blockchain's legal utility in areas such as electronic transactions, evidentiary authentication, and corporate record-keeping.²¹ This evolving regulatory environment reflects a blockchain-friendly climate that supports further exploration of its role in the judiciary.

[5] This article examines the potential of blockchain technology to enhance the recognition and enforcement of foreign judgments, while also addressing limitations within both international and national frameworks. Part II discusses the international regime, including the 2019 Hague Convention on the Recognition and Enforcement of Foreign Judgments, and explores the ongoing challenges of cross-border enforcement in an increasingly digital legal environment. This Part also reviews the current U.S. legal framework governing cross-border recognition and enforcement of judgments, focusing on the Uniform Foreign-Country Money Judgments

²¹ Between 2016 and 2018, several U.S. states implemented legislative reforms recognizing blockchain technology. For instance, under the Vermont Rules of Evidence, blockchain records are presumed authentic if supported by a qualified person's written statement. 12 V.S.A. § 1913. In 2017, Arizona amended its Electronic Transaction Act to include blockchain records, signatures, and smart contracts, ensuring they cannot be denied legal effect or enforceability, while Delaware updated the Delaware General Corporation Law to allow businesses to maintain records using "distributed electronic networks or databases" (§ 224). Ohio passed similar legislation to Arizona's, recognizing blockchain records and smart contracts. Other states, including Nebraska, Nevada, and Tennessee, amended their Uniform Electronic Transaction Acts to include blockchain-protected documents, and California, Colorado, Florida, and Maryland introduced bills supporting blockchain-based information storage. Illinois took a more expansive approach by enacting the Blockchain Technology Act (BTA), explicitly permitting blockchain use in transactions and legal proceedings. Sylvia Polydor, *Blockchain Evidence in Court Proceedings in China – A Comparative Study of Admissible Evidence in the Digital Age (as of June 4, 2019)*, STAN. J. BLOCKCHAIN L. & POL'Y (Jan. 5, 2020), <https://stanford-jblp.pubpub.org/pub/blockchain-evidence-courts-china/release/1> [<https://perma.cc/TT38-FQH8>]. The BTA also stipulates the responsibilities of authorities overseeing blockchain and smart contract use without restricting their ability to leverage these technologies for official tasks. However, it sets limits on imposing taxes or additional conditions, including licensing, for their use (§ 20). *The Blockchain Technology Act (Illinois)*, HUNTON (Feb. 10, 2020), <https://www.hunton.com/blockchain-legal-resource/the-blockchain-technology-act-illinois> [<https://perma.cc/J7BR-65UB>].

Recognition Act (UFCMJRA). Part III examines how judicial digitalization interacts with key principles of private international law, addressing jurisdictional conflicts, applicable law, and the need for cross-border data integrity and cooperation. This Part explores emerging concepts such as digital identities and cryptographic authentication and assesses how these developments may challenge traditional doctrines. Part IV analyzes the role of blockchain in generating secure and verifiable court records, drawing on international practices and the evolution of smart contracts. The analysis further reviews the tension between algorithmic regulation and judicial authority, examining a model that preserves judicial oversight while leveraging the advantages of automation. Part V addresses the practical and legal challenges of implementing blockchain in the judicial context. Ultimately, the article argues that for blockchain-based judgments to gain legal recognition, courts should adopt a decentralized judicial platform that incorporates cryptographic authentication alongside judicial review to uphold procedural fairness. In doing so, the judiciary can build a system that is not only more efficient and transparent but also consistent with international due process requirements. Part VI concludes.

II. THE LEGAL FRAMEWORK FOR FOREIGN JUDGMENT RECOGNITION AND ENFORCEMENT

A. International Regulations and Blockchain-Based Judgments

i. The Hague Convention on the Recognition and Enforcement of Foreign Judgments (2019): Relevance and Limitations

[6] The Hague Convention on the Recognition and Enforcement of Foreign Judgments in Civil or Commercial Matters²² represents a major step

²² *Convention of 2 July 2019 on the Recognition and Enforcement of Foreign Judgments in Civil or Commercial Matters*, July 2, 2019, HAGUE CONF. ON PRIV. INT'L L. [HCCH], <https://www.hcch.net/en/instruments/conventions/full-text/?cid=137> [<https://perma.cc/V4AW-TN2T>].

toward a global framework for judicial cooperation. The Convention entered into force in 2023 and currently binds the European Union (except Denmark), Ukraine, and Uruguay.²³ The Convention’s goal is to establish a common legal regime for the cross-border circulation of court judgments, reducing the costs and uncertainties of transnational litigation.²⁴ In principle, a blockchain-based judicial system that issues civil judgments would benefit from this Convention by having its decisions recognized and enforced abroad,, similar to traditional court judgments.

[7] However, the Convention’s scope is limited to judgments rendered by a “court of another Contracting State.”²⁵ This definition raises immediate compatibility questions. If a blockchain-based mechanism is not formally part of a state’s judiciary (for example, a decentralized dispute resolution platform or a private digital tribunal), its decisions would likely fall outside the Convention’s scope. Such digital or smart contract-based rulings would not qualify as “judgments” under the Convention, which could preclude their direct recognition internationally. In contrast, if a national court leverages blockchain technology as part of its process—for instance, recording judgments on a blockchain or using smart contracts to execute judgments—the outcome is still a state court judgment and remains within the Convention’s limits. Blockchain does not change the nature of a judgment *per se*; what matters is whether a sovereign court is behind it. Thus, a state-backed blockchain court could have its rulings circulated under the 2019 Convention, whereas a purely private blockchain tribunal currently would not. For instance, the U.S., while not yet a party to the Hague Judgments Convention, may find itself influenced by similar international frameworks and could benefit from recognizing blockchain-based judgments within its own domestic structures. However, U.S. state

²³ *Judgments Convention: Entry into Force and Ratification by Uruguay*, HAGUE CONF. ON PRIV. INT’L L. [HCCH], (Sep. 1, 2023), <https://www.hcch.net/en/news-archive/details/?varevent=936> [<https://perma.cc/3MQS-YYF3>] (last visited Apr. 29, 2025).

²⁴ *Id.*

²⁵ *Convention of 2 July 2019*, *supra* note 22, at Art. 1.

courts could be hesitant to recognize digital judgments from blockchain courts that are not integrated into the formal judicial system.

[8] There are also potential frictions between automated, digital enforcement and the Convention's provisions. The Hague Convention presumes that enforcement of foreign judgments will go through national courts, which can refuse enforcement on specific grounds such as improper notice, fraud, or public policy.²⁶ A blockchain-based judgment encoded in a smart contract might automatically execute (for example, transferring cryptocurrency from a losing party to the winner) without allowing a foreign court to review it. This creates a conflict with the Convention's spirit: parties might circumvent the provisions that allow a requested state to refuse enforcement for fundamental fairness or sovereignty reasons. For example, if an automated judgment transfers assets instantly, a state court loses the chance to ensure the defendant was properly notified or that enforcement does not violate public policy. Such self-enforcement, while efficient, could be viewed as undermining the due process guarantees that international enforcement regimes require. In the long run, this tension may prompt clarifications or protocols to the Convention (or entirely new treaties) to address how self-executing digital judgments should be handled across borders. Such reforms could involve oversight by human judges or arbitrators at key stages.

[9] On the other hand, blockchain technology can also complement the Convention's utility. Recording judgments or case information on a tamper-proof ledger can expedite the recognition process. For instance, if the authenticity and contents of a judgment are verifiable on a blockchain, foreign courts could more quickly trust that the judgment is final and unaltered.²⁷ Indeed, researchers and pilot projects have explored using

²⁶ *Convention of 2 July 2019*, *supra* note 22, at Art. 7.

²⁷ Zhen Er Low, *Execution of Judgements on the Blockchain: A Practical Legal Commentary*, 34 HARV. J. L. & TECH. 1 (2021)
<https://jolt.law.harvard.edu/digest/execution-of-judgements-on-the-blockchain-a-practical-legal-commentary> [<https://perma.cc/A4NY-SZ6S>].

blockchain as a distributed registry of judgments or for transmitting certified copies, to speed up exequatur procedures.²⁸ Dubai’s “Court of the Blockchain” initiative is one example, aiming to use blockchain to authenticate judicial documents internationally. This suggests that, while the Convention sets the legal rules, technology can provide the tools to implement those rules more efficiently. In summary, the 2019 Hague Judgments Convention is highly relevant as a legal backbone for cross-border enforcement. However, its traditional definitions and protections present both challenges and opportunities for blockchain-based judicial mechanisms. Realizing the benefits will likely require innovative interpretations or future agreements that explicitly integrate these new forms of “digital judgment” into the international legal order.

ii. Enforcement and Recognition Challenges

[10] Enforcing judgments through a digital judicial process may also present challenges from the perspective of recognition. If every aspect of a dispute resolution happens on-chain (filings, evidence, decision, and even compliance via smart contracts), it might seem that physical enforcement is no longer needed. However, enforcement often still requires intervention in the offline world, as a losing party may have off-chain assets or resist the outcome. In such cases, a real-world court’s assistance is necessary. Here, the recognition of a digital judgment becomes crucial. As noted, if the outcome does not originate from a recognized state court or arbitral tribunal, there is no straightforward legal mechanism for enforcing it abroad. National courts might treat a blockchain judgment as a private contractual outcome, potentially leading to a new lawsuit on the merits. This poses a significant barrier to the utility of blockchain-based judicial systems in transnational cases. One solution has been to analogize digital proceedings to arbitration. For example, some blockchain dispute resolution platforms, such as Kleros, present their process as arbitration under the parties’

²⁸ *Id.*; Pietro Ortolani, *Recognition and Enforcement of the Outcome of Blockchain-Based Dispute Resolution*, in *BLOCKCHAIN AND PRIVATE INTERNATIONAL LAW* 642, 667 (Andrea Bonomi et al. eds., 2023).

agreement, enabling national courts to enforce the decision under the New York Convention on the Recognition and Enforcement of Foreign Arbitral Awards.²⁹

[11] Indeed, in one instance, a national court enforced an award generated through the Kleros protocol, suggesting that with the right legal framework, even a decentralized ruling can cross national borders.³⁰

[12] In the short term, other national courts could also consider, for recognition purposes, an arbitration model in which traditional arbitrators use decentralized protocols, including Kleros, to determine the substance of the dispute. This approach, which would combine conventional procedures with artificial intelligence, could offer a practical way to address the technical and interoperability challenges discussed in Part V. In the long term, however, if blockchain recognition systems proliferate, nation-states may need to negotiate new agreements (perhaps an “e-Judgment Convention” or an extension of the current one) to specifically address the recognition of digitally rendered judgments that do not fit the traditional

²⁹ *United Nations Convention on the Recognition and Enforcement of Foreign Arbitral Awards*, N.Y. ARB. CONV., <https://www.newyorkconvention.org/english> [<https://perma.cc/YP9Z-UC45>].

³⁰ On September 1, 2020, two parties included an arbitral clause in a Mexican leasing contract, appointing an arbitrator and following traditional New York Convention rules. They innovatively instructed the arbitrator to use the Kleros protocol for the substance of the award, creating a model that combined traditional arbitration with decentralized technology. When a dispute arose, the arbitrator sent a procedural order to Kleros, which issued a decision in favor of the landlord. This decision became the basis for the final arbitral award, issued in the traditional manner. The real test came when the arbitral award was presented for enforcement: the court confirmed that the award complied with local statutes and ordered its enforcement. This marked the first time a Mexican court recognized and enforced an arbitral award governed by the Kleros protocol. Mauricio Virues, *How to Enforce Blockchain Dispute Resolution in Court? The Kleros Case in Mexico*, KLEROS (Jan. 10, 2022), <https://blog.kleros.io/how-to-enforce-blockchain-dispute-resolution-in-court-the-kleros-case-in-mexico/> [<https://perma.cc/3DEU-3ZSA>].

court model. Until then, enforcement may proceed *ad hoc*, relying on parallel legal qualifications (such as treating the outcome as a contract or arbitral award) for enforceability, a legally complex approach that may lead to inconsistent results.

B. Recognition of Foreign Judgments in the U.S.

i. Uniform Foreign-Country Money Judgments Recognition Act (UFCMJRA)

[13] The Uniform Foreign-Country Money Judgments Recognition Act (UFCMJRA) sets the rules on the recognition and enforcement of monetary judgments rendered by foreign countries within the United States. Approved in 2005 as a revision of the 1962 Uniform Foreign Money-Judgments Recognition Act,³¹ the UFCMJRA provides a uniform procedure for the recognition and enforcement of foreign judgments by U.S. courts in thirty states.³² The Act aims to ensure that the enforcement of foreign judgments is consistent and fair, while also protecting against the enforcement of judgments rendered by courts that fail to meet the minimum legal standards.

[14] Under UFCMJRA, U.S. courts may refuse recognition of a foreign judgment if “the judgment was rendered under a judicial system that does not provide impartial tribunals or procedures compatible with the requirements of due process of law.”³³ This provision allows courts to determine if the foreign legal system as a whole observes the fundamental principles of justice, including impartiality, fair notice, and the right to be heard. However, systemic review, where courts refuse to recognize foreign judgments because of perceived deficiencies in the foreign judicial system,

³¹ UFCMJRA, *supra* note 18, (prefatory note).

³² UFCMJRA, *supra* note 18, (prefatory note).

³³ UFCMJRA, *supra* note 18, at § 4(b)(1), (prefatory note).

should be approached with caution. There are examples of U.S. courts denying enforcement of judgments from certain countries, such as China and Indonesia, based on assumptions about corruption or political influence in their judicial systems, without regard to whether the specific proceeding conformed to due process standards.³⁴ The approach noted above may be based on fairly static and outdated assessments of foreign courts, and may fail to take account of reforms, or the nuances of the reality of those legal frameworks.³⁵ It may also be political bias rather than a genuine evaluation of judicial impartiality, eroding the comity and reciprocity principles that underpin international law.

[15] UFCMJRA also provides for case-specific due process violations and allows courts to deny recognition on the ground that “the specific proceeding in the foreign court leading to the judgment was not compatible with the requirements of due process of law.”³⁶ This section provides that although a foreign judicial system may be generally fair, a judgment may still be denied recognition for failure to satisfy the procedural requirements in a particular case, such as a lack of notice or an opportunity for the defendant to present its case. An individualized approach aligns more closely with the goals of due process by concentrating on the actual facts of the judgment under consideration. A fair assessment hinges on whether the

³⁴ *Fox v. Bank Mandiri (In re Perry H. Koplik & Sons, Inc.)*, 357 B.R. 231, 243 (Bankr. S.D.N.Y. 2006) (refusing to accord comity to an Indonesian judgment due to undisputed evidence of pervasive and systemic corruption within the Indonesian judicial system); *Mulugeta v. Ademachew*, 407 F.Supp.3d 569, 583 (E.D. Va. 2019) (declining to recognize Ethiopian judgments, citing that U.S. courts routinely deny comity to courts in countries where the judicial system is well-recognized to be corrupt and lacks impartiality); William S. Dodge, *Against Systemic Review of Foreign Judgments*, 28 Sw. J. INT’L L. 367, 373 (2022) (discussing cases where systemic review led to non-recognition of judgments from China, Nicaragua, and Morocco based on generalizations about impartiality and judicial independence in proceedings rather than case-specific due process violations).

³⁵ See Dodge, *supra* note 34, at 373–74, 382.

³⁶ UFCMJRA, *supra* note 18, at § 4(c)(8).

defendant received adequate notice, had the opportunity to present evidence, and was afforded the right to appeal – factors that stand independent of the broader quality of the foreign legal system.³⁷ By focusing on the specific proceeding rather than the judicial system’s reputation, courts uphold the critical principle that recognition should be based on the fairness of the particular decision. The consequence of potentially unjust, blanket refusals to recognize foreign judgments diminishes cross-border legal cooperation, including through comity and reciprocity, and contradicts the goals of international commercial dispute resolution.³⁸

ii. Due Process Concerns and Judicial Discretion in Recognizing Foreign Judgments

[16] The UFCMJRA’s two-tiered approach, examining both the fairness of a legal system and case-specific due process, grants U.S. courts significant discretion in recognizing foreign judgments. This discretion is important to prevent the enforcement of unjust and invalid judgments obtained through fundamentally unfair processes. Thus, courts have to balance the principles of international comity with constitutional due process requirements.³⁹

³⁷ See *Soc’y of Lloyd’s v. Ashenden*, 233 F.3d 473, 476–77 (7th Cir. 2000); *Najas Cortes v. Orion Secs., Inc.*, 362 Ill. App. 3d 1043, 1048–49 (2005) (emphasizing notice and the opportunity to be heard in foreign proceedings); Dodge, *supra* note 35, at 381–82 (discussing the importance of case-specific review to assess due process on a judgment-by-judgment basis).

³⁸ See *Hilton v. Guyot*, 159 U.S. 113, 164 (1895) (describing the comity of nations that “must necessarily depend on a variety of circumstances which cannot be reduced to any certain rule”). See also Dodge, *supra* note 34, at 374 (arguing that systemic review may lead to unjust blanket refusals of foreign judgments).

³⁹ “‘Comity,’ in the legal sense, is neither a matter of absolute obligation, on the one hand, nor of mere courtesy and good will, upon the other. But it is the recognition which one nation allows within its territory to the legislative, executive or judicial acts of

[17] However, judicial discretion may also lead to uncertainty because the assessment of a foreign court's impartiality or the procedural fairness of a given case may be based on the individual judge's perception. The possibility of inconsistent decisions across jurisdictions may weaken the predictability and effectiveness, diminishing the overall utility of the UFCMJRA. Therefore, it is important to establish clear and reliable criteria to authenticate foreign judgments and assess their conformity with due process requirements.

iii. Blockchain as a Means to Strengthen Authenticity and Trust in Foreign Judgments

[18] The integration of blockchain technology into the process of recognizing foreign judgments offers a good solution capable of enhancing both authenticity and judicial trust. The blockchain's decentralized and immutable ledger can guarantee the recording of court judgments to ensure that the records are easily verifiable as authentic.⁴⁰ This technology could help U.S. courts in several ways by offering a way to confirm the authenticity of judgments and to track their procedural history.

[19] For example, a blockchain-based judicial platform could record critical procedural steps, such as notices received, evidence submitted, and decisions made via a time-stamped and cryptographically secured record that cannot be altered. However, courts may still deny recognition of a foreign judgment based on the overall lack of impartiality in the judicial system. As demonstrated by the pattern of court behavior in the cases discussed above, this may still occur even when the judgment and its associated procedural steps have been authenticated and recorded on a blockchain-based judicial platform. To ensure fairness, courts should

another nation, having due regard both to international duty and convenience..."; Hilton, 159 U.S., at 163–64.

⁴⁰ DE FILIPPI & WRIGHT, *supra* note 2, at 35.

prioritize the specific proceedings at hand rather than assessing the foreign judicial system as a whole, including in cases where recognition is sought for cryptographically-verified court judgments. This would enable U.S. courts to determine, on a case-by-case basis, whether a foreign judgment conformed to due process requirements, thereby reducing the likelihood of subjective interpretations and generalized assumptions about foreign legal systems.

[20] Blockchain technology offers a new strategy for bolstering the authenticity and integrity of foreign judgments to enhance recognition while ensuring compliance with the principles of due process. The integration of blockchain technology in cross-border judgment recognition architecture will help simplify the authentication process, decrease cases of fraud, and provide a more efficient and predictable way of assessing due process compliance. Thanks to blockchain technology's unique characteristics, such as immutability and tamper-proofness, which prevent corruption or unauthorized alterations, a foreign system of blockchain-based records can provide impartial procedures compatible with U.S. due process requirements. When defendants have been heard, represented by counsel, and granted the right to appeal, it should satisfy the basic parameters of due process of law and make the resulting blockchain-based judgment enforceable in commercial matters, even if it originates from a jurisdiction lacking overall judicial independence. In contrast, invoking systemic due process deficiencies as a ground would, by default, result in the non-recognition and non-enforcement of blockchain-based judgments from certain countries in the U.S. This approach may also prevent the recognition and enforcement of potential U.S. blockchain-based judgments in countries accused of having biased judicial systems. For example, China accepts foreign judgments based on the principle of reciprocity,⁴¹ which may be

⁴¹ Dodge, *supra* note 34, at 369, 376. In 2022, the Supreme People's Court of China (SPC) introduced a new *de jure* reciprocity policy, under which reciprocity is established if a Chinese judgment would be recognizable under the laws of a foreign country, even if that country has not previously recognized a Chinese judgment. *Id.* at 376–77. This policy replaces the earlier *de facto* reciprocity standard, which required actual prior recognition of a Chinese judgment by the foreign jurisdiction. *See also* William S. Dodge & Wenliang Zhang, *Reciprocity in China-U.S. Judgments Recognition*, 53 VAND. J.

difficult to maintain if American courts determine that the Chinese judicial system is incapable of producing blockchain-based judgments worthy of recognition. Moreover, beyond China, a recent State Department Country Report highlights issues with judicial independence, corruption, or both in 141 other countries.⁴² Hence, adopting a systemic review may lead to scrutiny of all judgments from countries such as China, including those facilitated by blockchain technology.

III. PRIVATE INTERNATIONAL LAW AND JUDICIAL DIGITALIZATION

[21] Beyond formal enforcement treaties, a blockchain-based recognition system implicates a broad set of private international law (PIL) issues. As judicial processes become digital and decentralized, fundamental PIL questions of jurisdiction, applicable law, and cooperation between legal systems must be re-examined. This section analyzes how blockchain in the judiciary challenges established principles and what modifications might be necessary.

A. Jurisdiction

[22] In a blockchain-enabled dispute resolution, determining which country's courts (if any) have jurisdiction can be complex. Traditional jurisdictional rules rely on territorial connections—such as where a defendant resides or where a transaction took place—criteria that become blurry in a distributed ledger environment. For example, a smart contract may be executed across nodes worldwide with no single location. If a dispute arises, multiple courts might claim jurisdiction or, conversely, courts might all decline jurisdiction (the “floating forum” problem). Parties may attempt to pre-select jurisdiction (or even a specific digital jurisdiction)

TRANSNAT'L L. 1541, 1551–52 (2020). Thus, regarding blockchain-based judgments, it can be assumed that *de jure* reciprocity will exist, if a Chinese blockchain-based judgment would be recognizable under U.S. law.

⁴² Dodge, *supra* note 34, at 369.

in their smart contract, but the enforceability of such clauses remains uncertain. In theory, a blockchain judicial platform could itself be seen as the chosen forum (much as arbitration is a chosen forum), but national courts would have to accept that choice. The absence of clear answers to “which court?” in blockchain disputes has been noted as a pressing concern.⁴³ This lack of clarity risks parallel proceedings or a denial of justice if nobody is willing to hear the case. Going forward, PIL might need to develop new rules (or interpretations of existing ones) to address jurisdiction in “borderless” digital transactions⁴⁴—perhaps by focusing on the parties’ domicile or by recognizing the validity of online forum selection in smart contracts.

B. Applicable Law

[23] Closely tied to jurisdiction is the question of which law governs a blockchain-related dispute. Private international law traditionally uses connecting factors (such as the place of contracting, place of injury, or parties’ residence) to choose an applicable law. With blockchain, these connecting factors are de-territorialized: a contract coded on Ethereum, executed globally, does not have an obvious *lex loci contractus*. Parties can code choice-of-law clauses into smart contracts, but whether courts will uphold those remains uncertain. The current international legal landscape has no consensus on the legal status of blockchain transactions and smart contracts, which creates fundamental challenges for PIL.⁴⁵ For instance,

⁴³ Tonya M. Evans, *The Role of International Rules in Blockchain-Based Cross-Border Commercial Disputes*, 65 WAYNE L. REV. 1, 3 (2019) (suggesting that “due to the transactional, borderless, pseudonymous, and distributed nature of blockchain, [resolution of disputes arising from blockchain-based commercial transactions] clearly necessitate international solutions.”).

⁴⁴ *Id.*

⁴⁷ Anurag Bana & Ammar Osmanourtashi, *Blockchain and Private International Law: Implications for Crypto, Payment Systems, Digital Wallets and Jurisdictional Concerns*, INT’L BAR ASS’N (May 25, 2023), <https://www.ibanet.org/bli-may-2023-blockchain-private-international-law> [<https://perma.cc/6ZC4-TRCM>].

some jurisdictions treat crypto-assets and smart contracts very differently from others, making it hard to predict outcomes in cross-border scenarios. A blockchain-based judicial system might attempt to apply its own rules or a uniform law to all cases, but when enforcement in national courts is needed, conflict-of-law rules will reassert themselves. This could lead to a scenario where a “digital court” decision is valid under its own rules but unenforceable because a national court applies a different substantive law. To enhance legal feasibility, there are calls for harmonizing laws (or at least providing guidance) on digital transactions. For example, the HCCH and UNIDROIT have joint projects studying the law applicable to digital assets.⁴⁶ Such efforts, while focused on commercial law, pave the way for more predictable conflict-of-law rules, which a blockchain judicial system could then build into its design.

C. Cross-Border Data Integrity and Cooperation

[24] A positive aspect of blockchain in a judicial context is the assurance of data integrity across borders. Court records and evidence stored on a blockchain can be identical in every jurisdiction, tamper-evident, and timestamped. This has significant implications for international judicial cooperation. For instance, under existing Hague Conventions (e.g., on evidence or service of process), authorities exchange documents and certifications across countries⁴⁷—a process that can be slow and vulnerable to authenticity doubts. If instead a distributed ledger were used to share and verify these documents, it could increase trust and speed. The Hague

⁴⁸ See *Launch of the HCCH-UNIDROIT Digital Assets and Tokens Joint Project*, HAGUE CONF. ON PRIV. INT’L L. [HCCH], <https://www.hcch.net/de/news-archive/details/?varevent=913> [<https://perma.cc/2TPW-49M9>].

⁴⁹ See *Practical Handbook on the Operation of the 1965 Service Convention*, HAGUE CONF. ON PRIV. INT’L L. [HCCH], <https://www.hcch.net/en/instruments/conventions/specialised-sections/service> [<https://perma.cc/L789-ZL3Q>]; see also *Practical Handbook on the Operation of the 1970 Evidence Convention*, HAGUE CONF. ON PRIV. INT’L L., <https://www.hcch.net/en/instruments/conventions/specialised-sections/evidence> [<https://perma.cc/4Z6Q-CKQP>].

Conference itself has explored using blockchain as a communication protocol for Central Authorities in charge of cross-border judicial requests.⁴⁸ A ledger could provide immediate proof that, say, a summons was delivered or a piece of evidence was submitted, with a secure audit trail. In a blockchain-based recognition system, cross-border data sharing might be built in: every participant (regardless of country) sees the same record of filings, decisions, and compliance. This uniformity supports PIL objectives by minimizing disputes over what happened procedurally in the original forum. It also helps in proving foreign judgments are final and authentic—a prerequisite for enforcement under instruments such as the Hague Convention. That said, this vision requires uniform technical standards and mutual acceptance of a given blockchain’s reliability. This would ensure that when a digital judgment is presented in a foreign court, it can be verified at the click of a button (much like an electronic apostille).⁴⁹

[25] There are also legal concerns around data: if judicial data is stored globally, issues of data protection and sovereignty arise (for example, European privacy laws might conflict with immutable public records of court proceedings). Ensuring cross-border data integrity without violating local laws will be a delicate balance. It may entail permissioned or private ledgers accessible only to courts and parties, and agreements on data governance. In any case, the trend points toward leveraging blockchain to strengthen the connective tissue of international judicial cooperation, even if the core legal rules remain the same.

⁵⁰ Ted Folkman, *Blockchain for Central Authorities?*, LETTERS BLOGATORY (Aug. 23, 2019), <https://lettersblogatory.com/2019/08/23/blockchain-central-authorities/> [<https://perma.cc/BQ5E-F9T4>].

⁴⁹ *E-App*, HAGUE CONF. ON PRIV. INT’L L. [HCCH], <https://www.hcch.net/es/publications-and-studies/details4/?pid=5578> [<https://perma.cc/7XCN-A3ME>]. “Under the e-APP, it is suggested that Competent Authorities use readily available and already widely used PDF technology and digital certificates to issue e-Apostilles . . . The Competent Authority digitally signs the e-Apostille, to which an electronic version of the underlying document is attached so that the two documents form one single PDF file. The single PDF file (i.e., the e-apostillised document) is then sent to the requesting party.” *Id.*

D. Digital Identities and Authentication

[26] A less discussed but crucial component of a digital judicial system is verifying identities across jurisdictions. Courts traditionally rely on passports, notarizations, or diplomatic channels to confirm who is who (for parties, witnesses, judges). In a blockchain-based process, participants could authenticate via digital identity tokens or certificates. Private international law will need to accommodate such methods – for example, by recognizing a foreign litigant’s digital ID as equivalent to official identification. There are already movements in this direction: the European Union’s eIDAS framework and the newer European Blockchain Services Infrastructure (EBSI) aim to enable cross-border recognition of electronic identities and signatures.⁵⁰ This means, in theory, a person identified and verified on one country’s digital identity system could prove their identity in another country’s court without re-verification. Applying this to a blockchain court, one could envision digital identity wallets ensuring that each user of the system has a verified legal identity backed by government-issued credentials, which all participating jurisdictions accept. Such a system would greatly facilitate cross-border proceedings—a user could sign documents or even testify via a secure digital signature that judges in multiple countries trust. It also ties into enforcement: a judgment against a person is only useful if we know exactly who that person is and can link them to assets. If parties in a blockchain trial are pseudonymous and lack verifiable identity, enforcing the outcome in the real world might be impossible. Thus, robust digital identity frameworks are not just an IT convenience but a legal necessity for transnational digital justice. PIL may need to integrate rules on accepting foreign electronic authentications (many countries, including the U.S.,⁵¹ already do for commerce), and to

⁵⁰ Riho Vedler & Machiel Tesser, *Overview of EU eIDAS 2.0 Regulation*, DIGITALTRADE 4.EU (Oct. 23, 2024), <https://www.digitaltrade4.eu/european-digital-identity-eudi-regulation/> [https://perma.cc/XV4A-WZ4A].

⁵¹ See, e.g., Electronic Records and Signatures in Global and National Commerce Act, 15 U.S.C. § 7006 (2018) [hereinafter E-Sign] stipulating the term “electronic signature,” which means “. . . an electronic sound, symbol, or process, attached to or logically

ensure that a judgment document signed with a digital certificate from Country A will be considered duly authenticated in Country B's courts. The integrity of digital identities also has to be protected, as fraud or hacking of identity would undermine the whole system. This calls for continued collaboration on security standards and possibly a supervising international body to accredit identity providers for judicial use.

E. Challenges to Established Principles

[27] The integration of blockchain in judicial processes ultimately forces a re-examination of some bedrock PIL principles. Notably, the territorial sovereignty of courts—the idea that each state's courts have authority within its territory and exclusive say over certain matters—is tested by dispute platforms that are functionally stateless. For example, if a decentralized autonomous organization (DAO) provides a dispute resolution service globally, are state courts willing to defer to that process? This is analogous to, but even more pronounced than, the challenges posed by international arbitration and online dispute resolution. PIL has traditionally adapted by either assimilating new mechanisms (e.g., enforcing arbitral awards via treaties) or by asserting public policy limits.⁵² With blockchain, we might see new quasi-legal orders emerge (some commentators name this *lex cryptographica*)⁵³ which do not map neatly onto nation-states. States may respond by drawing lines: for instance, refusing to recognize any judgment not coming from a sovereign authority (to preserve the Westphalian system), or conversely, by entering agreements that allow a supranational digital forum to function under

associated with a contract or other record and executed or adopted by a person with the intent to sign the record.”

⁵² New York Convention, *supra* note 29, art. V(2)(b); *see also* Edmarverson A. Santos, *Private International Law*, DIPLOMACY & L., <https://www.diplomacyandlaw.com/post/private-international-law> [<https://perma.cc/6WXG-7BUW>].

⁵³ DE FILIPPI & WRIGHT, *supra* note 2, at 9.

agreed rules. Jurisdictional doctrines such as *forum non conveniens*, or principles such as comity, could be stretched when parties argue that a blockchain forum is the most appropriate venue for their dispute. Likewise, the notion of applicable law might shift toward more party autonomy: if parties design a self-executing contract with its own rules, perhaps PIL will increasingly respect that private ordering unless it clashes with fundamental public interests. All these theoretical implications indicate that blockchain could be a catalyst for reshaping PIL, much as the rise of the internet prompted new approaches to cross-border online commerce and torts. The difference here is that blockchain can embed law-like rules (through code) and enforcement directly into transactions, potentially reducing the reliance on national legal processes—a prospect that challenges the traditional monopolies of jurisdiction and enforcement.

IV. BLOCKCHAIN AS A TOOL FOR JUDICIAL RECORD-KEEPING AND ENFORCEMENT

[28] Smart contracts have transformed discussions on legal automation and judicial enforcement of contractual terms. Based on blockchain, smart contracts eliminate the need for intermediaries, accelerating and simplifying the entire process and improving efficiency. However, the increasing use of automated enforcement raises important questions about balancing efficiency with judicial discretion.⁵⁴ While automation in contract execution expedites enforcement, it may also limit the flexibility required in handling complex commercial disputes. The expanding reliance on blockchain-based legal enforcement, including recent advancements in digital judicial systems, highlights both the potential and the challenges of integrating smart contracts into judicial practice.⁵⁵

⁵⁴ See Max Raskin, *The Law and Legality of Smart Contracts*, 1 GEO. L. TECH. REV. 305, 328 (2017).

⁵⁵ DE FILIPPI & WRIGHT, *supra* note 2, at 35.

[29] One of the most significant applications of smart contracts in the judiciary is the automation of order and judgment enforcement, including asset freezing and cross-border enforcement. Experience with blockchain-based judicial systems has demonstrated that digital enforcement can occur in real-time, reducing noncompliance and enhancing financial oversight.⁵⁶

A. How Blockchain Works in Legal Applications

i. Distributed Ledger Technology (DLT) and Cryptographic Verification

[30] At the core of using blockchain in legal systems is Distributed Ledger Technology (DLT). Unlike traditional databases controlled by a central authority, DLT is a secure decentralized system that records transactions across multiple nodes.⁵⁷ The DLT's decentralized system provides transparent recording, verification, and synchronization across networks, which protects entries from unauthorized changes.⁵⁸ The decentralized structure builds trust in judicial and enforcement mechanisms because it removes single points of failure while making verified records unalterable.

[31] As its main feature, cryptographic verification enables the reliability of blockchain-based legal applications. Each transaction or legal record added to the ledger uses secure cryptographic hash functions so that any attempts to modify previous entries become instantly detectable. Smart contracts, which implement self-executing agreements stored on the blockchain, also rely on these cryptographic principles, which enable legal

⁵⁶ Yin, *supra* note 15.

⁵⁷ See Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, BITCOIN.ORG, <https://bitcoin.org/bitcoin.pdf> [<https://perma.cc/7GMF-XBWR>]; DON TAPSCOTT & ALEX TAPSCOTT, *BLOCKCHAIN REVOLUTION: HOW THE TECHNOLOGY BEHIND BITCOIN IS CHANGING MONEY, BUSINESS, AND THE WORLD* (2016).

⁵⁸ *Id.*

obligations to execute automatically without the need for intermediaries. While providing transparent and efficient operations, the integration of legal rules into code automates the enforcement of agreements.

[32] In the context of judicial enforcement, the cryptographic structure of blockchain technology ensures procedural integrity through an auditable system that prevents tampering of legal decisions. Thus, the implementation of DLT in digital court rulings, contract enforcement, and evidentiary record-keeping strengthens the credibility of blockchain-based legal mechanisms, which leads to more efficient and secure dispute resolution processes. However, while DLT offers greater security and efficiency, it also creates significant concerns regarding due process, judicial oversight, and its compatibility with current legal frameworks.

ii. Immutable Court Records: Preventing Fraud and Alterations

[33] One of the most significant applications of blockchain technology in the judiciary involves the creation of immutable court records. Traditional paper-based or digital court record systems face risks of intentional tampering, accidental data destruction, and unauthorized modifications. Blockchain's decentralized ledger system enables the secure storage of judicial records, where each entry is sealed cryptographically to protect it from tampering. Blockchain's cryptographic structure allows data blocks to connect sequentially through hash functions, which makes network consensus necessary to modify previous entries.⁵⁹ This feature provides essential protection for court documents,, including judgments, evidence logs, and procedural filings.⁶⁰ Changing a record requires

⁵⁹ Per Aarvik, *Blockchain as an Anticorruption Tool Case Examples and Introduction to the Technology*, U4 ANTI-CORRUPTION RES. CTR. 3, <https://www.u4.no/publications/are-blockchain-technologies-efficient-in-combatting-corruption.pdf>? [https://perma.cc/4HY7-AGW5].

⁶⁰ *Id.* (illustrating the application of blockchain to maintain the integrity of official records). In 2016, the Republic of Georgia implemented blockchain in its land registry. *Id.* at 16. For this purpose, Bitfury was invited to add a layer of security to the existing

modifications to all subsequent blocks, which becomes computationally impossible in a well-secured blockchain network.⁶¹

[34] While the blockchain-based court record system provides both transparency and accountability, it also prevents fraud. To ensure procedural fairness, the system grants court participants, including judges, attorneys, and litigants, access to case records that display a verifiable history of modifications. It gains additional trustworthiness through digital timestamps and cryptographic signatures, which confirm the identities of record-entry authors. Although blockchain provides immutability benefits, legal systems also need to resolve issues regarding data privacy and error correction. In particular, courts require special procedures to modify their records in rare instances, such as clerical mistakes and court reversals. This could be possible through the implementation of permissioned blockchains in which authorized entities can make modifications via transparent, auditable processes, preserving the integrity of previous records.

[35] The integration of blockchain technology in judicial recordkeeping will help courts reduce their reliance on centralized databases, which are susceptible to cyberattacks and unauthorized changes. This transformation enhances legal certainty while supporting digital innovation efforts aimed at modernizing judicial administration.

digital land ownership registry deploying the Exonum blockchain. *Id.* Consequently, land and property owners gained constant access to cryptographic proof of ownership and transactions. *Id.* Additionally, accompanying notarized documents and contracts were timestamped. *Id.*

⁶¹ *See id.* at 3.

B. Blockchain Precedents in Legal Systems

i. China's Internet Courts and Blockchain-Based Judicial Records

[36] China has taken a leading role in integrating blockchain technology into its judicial system, particularly through the establishment of specialized Internet Courts.⁶² These courts, designed to handle internet-related disputes, utilize blockchain for evidence verification and court record management, marking a shift towards digital legal processes.⁶³

[37] The first of these, the Hangzhou Internet Court, was established in 2017, with similar courts later introduced in Beijing and Guangzhou.⁶⁴ Their primary purpose is to expedite the resolution of disputes involving e-commerce transactions, copyright matters, and other online cases.⁶⁵ In 2018, the Supreme People's Court of China formally recognized blockchain-based evidence, granting it official status in judicial

⁶² In a groundbreaking ruling on June 28, 2018, the Hangzhou Internet Court admitted blockchain-based evidence in a copyright infringement case. Xuhui Fang, *Recent Development of Internet Courts in China*, 2018 (5) 1-2 INT'L J. ONLINE DISP. RESOL.56 (2018), https://www.boomportaal.nl/tijdschrift/IJODR/IJODR_2352-5002_2018_005_102_006 [<https://perma.cc/KE62-56NQ>]. The court recognized the authenticity of electronic data stored via blockchain technology, emphasizing that it is authentic, complete, and cannot be altered. *Id.* A key objective in establishing the Hangzhou judicial blockchain platform was to “solve the credibility and usability problems of electronic evidence from the very beginning.” Lu, *supra* note 11. This involved integrating every stage of electronic evidence collection into the judicial blockchain platform with the entire process recorded in a trusted environment and witnessed by all nodes. *Id.*

⁶³ Fang, *supra* note 62, at 50–51.

⁶⁴ *Id.* at 49.

⁶⁵ Changqing Shi et al., *The Smart Court – A New Pathway to Justice in China?*, INT'L J. COURT ADM'N, <https://iacajournal.org/articles/10.36745/ijca.367#xrn50> [<https://perma.cc/4C8L-DGRJ>].

proceedings.⁶⁶ This approval extended to cases where data collection and storage adhered to specific reliability standards.

[38] China's judicial system incorporates blockchain through structured protocols. Documents such as contracts, transaction records, and copyright claims become immutable when stored on blockchain platforms with timestamping mechanisms.⁶⁷ This method eliminates the need for traditional notarization or expert testimony in verifying electronic records.⁶⁸ For instance, the Hangzhou Internet Court has used blockchain to verify digital contracts and copyright claims, significantly cutting down legal costs and case durations.⁶⁹

[39] Beyond evidence management, blockchain technology now plays a role in enforcing judicial decisions. Chinese courts utilize blockchain networks to oversee court-enforced judgments, ensuring that defaulters cannot evade legal responsibilities. Through smart contracts, legal actions such as financial penalties and asset freezes can be executed automatically, improving enforcement efficiency.⁷⁰

⁶⁶ Lu, *supra* note 11 (Article 11(2) of the SPC Provisions on Several Issues Concerning the Trial of Cases by Internet Courts explicitly affirmed that blockchain evidence may be admitted, provided its authenticity is established, without prejudice to the general rules of evidence, as follows: "Where the authenticity of the electronic data submitted by a party can be proven through electronic signature, trusted time stamp, hash value check, blockchain or any other evidence collection, fixation or tamper-proofing technological means, or through the certification by an electronic evidence collection and preservation platform, the Internet Court shall make a confirmation.").

⁶⁷ *Id.*

⁶⁸ See Fang, *supra* note 62, at 50–51.

⁶⁹ Lu, *supra* note 11.

⁷⁰ See Press Release, Shanghai Maritime Court, SPC Releases Opinions on Strengthening Blockchain Application in the Judicial Field (May 25, 2022), <https://www.shsfy.gov.cn/hsfyywx/hsfyywx/News1354/RelevantNews1482/2022/05/25/09b080ba7f9ca75c018147dbd9047658.html?tm=1676972395290> [<https://perma.cc/8JSY-A2RZ>].

[40] China’s application of blockchain in judicial record-keeping demonstrates how technology can be integrated into legal systems. Despite concerns about state control over blockchain infrastructure and data integrity, this initiative enhances judicial transparency and efficiency while fostering digital trust.

ii. Dubai’s Smart Courts Initiative

[41] Dubai has emerged as a global leader in integrating blockchain technology into its judicial system through its ambitious Smart Courts Initiative. As part of the emirate’s broader “Dubai Blockchain Strategy,” launched in 2016, the initiative aims to leverage distributed ledger technology to enhance efficiency, reduce bureaucratic delays, and improve judicial transparency.⁷¹

[42] The Dubai International Financial Centre (DIFC) Courts have played a leading role in this transformation. In 2018, the DIFC Courts partnered with Smart Dubai to establish the world’s first “Court of the Blockchain,” designed to automate dispute resolution through blockchain-based verification of legal documents and contracts.⁷² This system provides for automatic verification of court judgments without the need in paper duplicates, which has the potential to enhance cross-border judicial cooperation.⁷³

⁷¹ *Dubai Future Foundation Hosts “Keynote 2017” World Blockchain Forum*, DUBAI FUTURE FOUND. (Mar. 6, 2017), <https://www.dubaifuture.ae/latest-news/dubai-future-foundation-hosts-keynote-2017-world-blockchain-forum/> [<https://perma.cc/AW8E-HZ34>].

⁷² *DIFC Courts and Smart Dubai Launch Joint Taskforce for World’s First Court of the Blockchain*, DIFC COURTS (Jul. 30, 2018), <https://www.difccourts.ae/media-centre/newsroom/difc-courts-and-smart-dubai-launch-joint-taskforce-worlds-first-court-blockchain> [<https://perma.cc/PR92-DX6A>].

⁷³ *Id.*

[43] One of the key features of Dubai’s blockchain-based judicial system is its potential integration with smart contracts.⁷⁴ With the integration of legal agreements into blockchain networks, the courts can facilitate self-executing contracts that automatically enforce judicial decisions. This automation may significantly reduce the time required to enforce rulings, particularly in commercial and financial disputes.⁷⁵ Through its immutable ledger system, court documents will maintain their tamper-proof status, with the possibility of permitting authorized stakeholders to access them. This approach further fosters public confidence in the legal system as it addresses concerns over document fraud and data integrity.

[44] Despite its advantages, the Smart Courts Initiative also presents challenges. Legal scholars have raised concerns regarding the enforceability of blockchain-based judgments in jurisdictions that lack sufficient digital infrastructure or a compatible regulatory system.⁷⁶ In such cases, courts may

⁷⁴ Majd A. Kimrakji, *From Code to Court: Advanced Strategies for Securing Smart Contracts in the UAE Legal System*, LinkedIn (Feb. 3, 2025), <https://www.linkedin.com/pulse/from-code-court-advanced-strategies-securing-smart-uae-a-kimrakji-64ucf/> [<https://perma.cc/8D3E-W888>] (“We affirm that smart contracts represent a significant advancement in the UAE legal system, but activating this technology on a wide scale requires legal amendments that keep pace with rapid technological development.”).

⁷⁵ *Emirates Blockchain Strategy 2021*, THE UNITED ARAB EMIRATES, <https://u.ae/en/about-the-uae/strategies-initiatives-and-awards/strategies-plans-and-visions/strategies-plans-and-visions-untill-2021/emirates-blockchain-strategy-2021> [<https://perma.cc/BM8S-LPDN>] (“The blockchain technology will help save time, effort and resources and facilitate people to process their transactions at the time and place that suit their lifestyle and work.”).

⁷⁶ See Andrea Bonomi et al., *Blockchain and Private International Law*, 4 INT’L & COMP. BUS. L. & PUB. POL’Y 1, 667 (2023) (addressing that The decentralized and immutable nature of blockchain technology presents challenges for traditional legal systems, especially when cross-border enforcement is required); see also Ogunsan Isaac, *Blockchain and Legal Systems: Challenges and Opportunities in Regulation*, ResearchGate (Jan. 2025),

struggle to recognize and enforce judgments recorded on a blockchain, particularly in countries with strict evidentiary requirements that do not support digital records. Additionally, varying technological adoption rates across different legal systems may hinder the implementation of blockchain-based court decisions when dealing with international disputes.

[45] Furthermore, questions remain about the potential centralization of blockchain networks controlled by government entities, which could impact the neutrality of the technology.⁷⁷ If a state-run blockchain is subject to governmental oversight, concerns regarding transparency, data manipulation, and restricted access may arise. True decentralization, as the fundamental principle of blockchain technology, may be compromised when a single entity controls network governance and access. Thus, the judicial processes using blockchain technology need a balanced approach that maintains both operational effectiveness and impartial decision-making.

https://www.researchgate.net/publication/388360311_Blockchain_and_Legal_Systems_Challenges_and_Opportunities_in_Regulation [<https://perma.cc/VBE2-AVK5>]
(emphasizing the need for international cooperation to develop cohesive regulatory frameworks, as the decentralized nature of blockchain undermines traditional legal concepts such as jurisdiction and authority).

⁷⁷ Juho Lindman et al., *The Uncertain Promise of Blockchain for Government*, OECD (Nov. 16, 2020), https://www.oecd.org/en/publications/the-uncertain-promise-of-blockchainfor-government_d031cd67-en.html [<https://perma.cc/KUQ6-62QT>] (arguing that despite blockchain's potential for decentralization, government-led implementations may not fully embrace this characteristic); Claudia Biancotti, *Regulating Blockchains While Protecting Decentralization*, PETERSON INST. INT'L ECON. (Oct. 31, 2018), <https://www.piie.com/blogs/realtime-economic-issues-watch/regulating-blockchains-while-protecting-decentralization> [<https://perma.cc/WJN2-DA2Q>] (discussing how government influence over blockchain networks could lead to centralized control, undermining the technology's original decentralized principles).

iii. Estonia's E-Governance Model

[46] Estonia has integrated blockchain technology into its e-governance framework to create one of the world's most advanced digital societies.⁷⁸ Using blockchain technology, it launched a digital transformation strategy to improve data security, system transparency, and operational efficiency across government operations.⁷⁹ The country's e-governance model includes judicial applications that utilize blockchain technology for securing legal records and automating administrative procedures.

[47] The Estonian government implements blockchain governance through KSI (Keyless Signature Infrastructure) technology.⁸⁰ It protects government data integrity through an unalterable ledger system, containing verifiable records for legal documents, court files, and public registries.⁸¹ Through its logging system, the KSI blockchain prevents unauthorized changes, which strengthens trust in Estonia's legal framework.

[48] Estonia's e-Justice system demonstrates practical blockchain application within the judicial domain. Secure real-time access to case files is available for legal professionals through the digitized court proceedings

⁷⁸ *Estonia – the Digital Republic Secured by Blockchain*, PwC (Apr. 2, 2025), <https://www.scribd.com/document/478274557/Estonia-Digital-Republic> [<https://perma.cc/PR9N-A4TR>].

⁷⁹ Mathis Bitton, *The Estonian Miracle: E-Estonia and the Future of Digital Infrastructure*, N.Y.U. SCH. PROF'L STUD., <https://www.sps.nyu.edu/homepage/metaverse/metaverse-blog/the-estonian-miracle-e-estonia-and-the-future-of-digital-infrastructure.html> [<https://perma.cc/Q9CF-DE2V>] (last updated May 27, 2025).

⁸⁰ *KSI Blockchain Provides Truth Over Trust*, E-ESTONIA (Jun. 2, 2022), <https://e-estonia.com/ksi-blockchain-provides-truth-over-trust/> [<https://perma.cc/H29Z-P9GR>].

⁸¹ *Id.*

and case management system.⁸² Smart contracts are also being explored within Estonia's legal system,⁸³ potentially automating judicial decisions and civil dispute resolutions. Additionally, Estonia utilizes blockchain through its digital identity platform to establish secure authentication for citizens and legal professionals who interact with the judiciary.⁸⁴ This platform minimizes identity fraud risks, while providing tamper-proof interactions between court institutions and individuals.⁸⁵

[49] Despite its successes, Estonia's e-governance model may experience certain challenges. As discussed above, concerns arise regarding the ability to enforce blockchain-based judicial decisions across national borders due to potentially incompatible digital infrastructure in other jurisdictions. Further, the long-term scalability of blockchain-based legal frameworks remains uncertain as increasing data volumes may reduce processing efficiency.

C. Smart Contracts and Automated Enforcement of Judgments

i. Overview of Smart Contracts in Legal Tech

[50] Smart contracts are self-executing legal agreements with terms embedded in code, which are activated only when specific conditions are met.⁸⁶ Built on blockchain technology, these contracts eliminate the need

⁸² See generally *e-Justice Factsheet*, E-ESTONIA FACTS & FIGURES, https://e-estonia.com/wp-content/uploads/factsheet_e-justice.pdf [<https://perma.cc/3DJJD-DQE3>].

⁸³ Jesse Anglen, *The Legal Implications of Smart Contracts: Regulations and Compliance*, RAPID INNOVATION, <https://www.rapidinnovation.io/post/the-legal-implications-of-smart-contracts-regulations-and-compliance> [<https://perma.cc/S6XV-FA6R>].

⁸⁴ See generally *e-Identity*, E-ESTONIA: BUILDING A DIGITAL SOCIETY, <https://e-estonia.com/solutions/estonian-e-identity/id-card/> [<https://perma.cc/N5AK-7GPV>].

⁸⁵ *Id.*

⁸⁶ DE FILIPPI & WRIGHT, *supra* note 2, at 74.

for third-party involvement, reducing both costs and time.⁸⁷ However, scholars have raised concerns about the feasibility of integrating smart contracts into the judicial system to streamline court orders and improve the enforceability of judgments.⁸⁸

[51] The integration of rule-by-code systems presents both advantages and challenges for legal implementation.⁸⁹ While smart contracts offer high accuracy, efficiency, and transparency, they may conflict with traditional legal systems, particularly in common law jurisdictions, which emphasize judicial discretion, equity, and flexibility in enforcing contracts. To address this, systems combining smart contracts with traditional legal frameworks can ensure that computerized enforcement remains balanced, fair, and compliant with established legal processes.

ii. Self-Executing Court Orders and Asset Freezing

[52] One of the most promising applications of smart contracts in legal tech is automating court orders, especially for asset freezing and enforcement. With smart contracts on the blockchain, court judgments can be executed in real-time and in a manner that is entirely automatic, preventing debtors from evading enforcement. For example, in a cross-border commercial dispute, a smart contract could freeze assets upon the court's order, ensuring the debtor's digital assets remain inaccessible until the ruling is satisfied. This method eliminates delays associated with manual enforcement procedures.

⁸⁷ Raskin, *supra* note 54, at 315.

⁸⁸ Raskin, *supra* note 54, at 338 (citing Marcella Atzori, *Blockchain Technology and Decentralized Governance: Is the State Still Necessary?*, J. GOVERNANCE & REG. (Dec. 1, 2015), <https://ssrn.com/abstract=2731132> [<https://perma.cc/TVF5-SC9H>] (arguing that smart contracts' benefits can be realized without judicial recognition or enforcement because they have the potential to replace traditional judicial systems operated by a centralized authority)).

⁸⁹ DE FILIPPI & WRIGHT, *supra* note 2, at 72.

[53] China's blockchain-based judicial enforcement system provides an illustrative example of automation in court orders. The Supreme People's Court's judicial blockchain platform enables real-time monitoring of enforcement, ensuring that court decisions are implemented while reducing administrative burdens.⁹⁰ Its integration with financial institutions further facilitates the direct application of asset freezes and financial restrictions, demonstrating how smart contracts can enhance judicial enforcement.⁹¹ However, concerns about due process arise, as automated enforcement may limit the affected parties' ability to seek judicial review before execution. The challenge lies in ensuring fairness and preventing the automation process from leading to unjust outcomes or imposing severe penalties.⁹²

iii. Combining Smart Contracts with Conventional Legal Systems

[54] To mitigate the potential drawbacks of fully automated enforcement, legal systems may explore arrangements that combine smart contract provisions with traditional legal oversight. In these models, smart contracts handle certain clauses, while courts or arbitrators retain the

⁹⁰ See Press Release, Shanghai Maritime Court, SPC Releases Opinions on Strengthening Blockchain Application in the Judicial Field (May 25, 2022), <https://www.shhsfy.gov.cn/hsfywww/hsfywww/News1354/RelevantNews1482/2022/05/25/09b080ba7f9ca75c018147dbd9047658.html?tm=1676972395290> [<https://perma.cc/R3RQ-LYZ9>].

⁹¹ *Id.*

⁹² Khalid Ameen, *Judicial Review of Algorithmic Administrative Systems Legality Evidence and Remedies in the Smart City State*, FRONTIERS IN ARTIFICIAL INTELLIGENCE (Apr. 12, 2026), <https://www.frontiersin.org/journals/artificial-intelligence/articles/10.3389/frai.2026.1802986/full> [<https://perma.cc/LP9U-D4NC>]; Brandon L. Garrett, *Artificial Intelligence and Procedural Due Process*, 27 U. PA. J. CONST. L. 933 (2025), <https://repository.law.upenn.edu/Documents/Detail/artificial-intelligence-and-procedural-due-process/529662> [<https://perma.cc/64L8-CSAA>].

authority to modify or suspend enforcement if necessary.⁹³ For example, a smart contract in commercial arbitration might automatically release funds based on an award, but a court could delay execution if due process concerns arise. This approach allows blockchain-based enforcement to address complex legal issues, such as contractual ambiguities, force majeure events, or public policy considerations.

[55] The development of blockchain-based dispute resolution systems also supports this model. Some blockchain arbitration services already incorporate off-chain adjudication, where human arbitrators make decisions, and smart contracts implement the awards.⁹⁴ This model seeks to combine the efficiency of automation with the fairness and flexibility of traditional legal processes, ensuring that automated outcomes are just.

[56] The adoption of smart contracts in legal enforcement represents a significant shift in the delivery of legal services, offering convenience, clarity, and security. However, concerns about due process, judicial discretion, and flexibility call for a balanced approach. The integration of automated execution with legal oversight promises a gradual evolution towards blockchain-based judicial enforcement that corresponds to core legal principles. As smart contract applications evolve, legislatures and judiciaries will play a crucial role in shaping the future of automated legal enforcement.

V. CHALLENGES TO INTEGRATING BLOCKCHAIN-BASED JUDGMENTS IN THE JUDICIARY

[57] Blockchain technology has given rise to a paradigm often called “*lex cryptographica*,” which is a system of rules enforced not by courts or

⁹³ Raskin, *supra* note 54, at 311.

⁹⁴ DE FILIPPI & WRIGHT, *supra* note 2, at 75.

governments, but by self-executing code.⁹⁵ In this paradigm, smart contracts and decentralized autonomous organizations (DAOs) automatically carry out agreements and governance according to pre-written software logic. Proponents envision this “rule of code” as a new form of law: an autonomous, transnational legal order operating beyond the constraints of nation-states.⁹⁶ These proponents argue that code-based rules can provide incorruptible, transparent enforcement, creating “virtual jurisdictions” where code is the ultimate authority rather than fallible human institutions.⁹⁷ However, this vision raises difficult questions about the relationship between such code-based governance and the traditional rule of law. Can immutable software truly replace judges, or does it undermine fundamental legal principles? This section critically examines *lex cryptographica* and its implications for judicial oversight, emphasizing the tension between automated enforcement and human justice. Just as the advent of arbitration required legal systems to adjust by acknowledging private dispute resolution but keeping courts available as a last resort,⁹⁸ the advent of self-executing code requires a recalibration of dispute settlement. The challenge and opportunity going forward is to craft frameworks where blockchain-based automation and human justice coexist, each augmenting the other. In doing so, the national legal systems can leverage blockchain’s advantages while preserving the core principles of the rule of law and judicial fairness.

⁹⁵ DE FILIPPI & WRIGHT, *supra* note 2, at 5–7; *see also*, *Code is Law*, ETHEREUM CLASSIC (Feb. 22, 2022), <https://ethereumclassic.org/why-classic/code-is-law> [<https://perma.cc/FX8J-6JUQ>].

⁹⁶ *Code is Law*, *supra* note 95.

⁹⁷ DE FILIPPI & WRIGHT, *supra* note 2, at 5–7.

⁹⁸ GARY B. BORN, INTERNATIONAL COMMERCIAL ARBITRATION § 1.02 (Kluwer Law International, 3rd ed. 2021).

A. Lex Cryptographica: Autonomous Systems and Their Implications for Judicial Review

[58] *Lex cryptographica* refers to the emerging body of rules and norms administered through blockchain-based code—essentially, law encoded in software. It may also be described as “a set of rules administered through smart contracts and decentralized organizations, whereby complex networks of smart contracts establish self-executable rules among participants.”⁹⁹ In simpler terms, code is used to “rewrite the rules of the game” by enforcing commitments automatically without relying on courts or other centralized authorities.¹⁰⁰ As blockchain adoption grows, scholars predict the expansion of this code-based legal subset, with more interactions governed by software rather than conventional law.¹⁰¹ Concurrently, widespread deployment of blockchain may lead to expansion of *lex cryptographica*, potentially reducing the ability of governments and traditional legal systems to control or shape the behavior of individuals.¹⁰² This prospect raises profound implications for judicial review and state authority.

[59] *Lex cryptographica* is characterized by its autonomy and transnational character. Because blockchain networks are decentralized and borderless, the rules encoded in them operate independently of any single jurisdiction. Code running on a public blockchain does not respect geographic boundaries. It executes uniformly for all users worldwide, meaning autonomous blockchain systems can effectively create a legal

⁹⁹ Joe Tirado & Gabriela Cosio, *Lex Cryptographia: Guidelines for Ensuring Due Process in Transnational Blockchain-Based Arbitration*, INTL’L BAR ASS’N (Mar. 4, 2022), <https://www.ibanet.org/lex-cryptographia-due-process-blockchain-based-arbitration> [<https://perma.cc/4T2T-TERQ>].

¹⁰⁰ *Id.*

¹⁰¹ DE FILIPPI & WRIGHT, *supra* note 2, at 7.

¹⁰² *Id.*

order that “emancipates itself from three essential dimensions of law: language, territory, and the body.”¹⁰³ Unlike traditional laws, which are written in natural language, tied to a territory, and enforced upon human actors, blockchain’s rule of code is expressed in programming languages, applicable globally, and executed by machines. This independence from territory poses a jurisdictional challenge for courts that may struggle to assert authority over rules that exist “in the wild” of a decentralized network. Further, the decentralized nature of *lex cryptographica* inherently “limits the effects of national and international laws” when it comes to ensuring due process.¹⁰⁴ In other words, if an autonomous smart contract spans the globe, it may be unclear whether national courts can step in when something goes wrong. The traditional linkage between law and sovereign territory may be disrupted.

[60] Moreover, *lex cryptographica*’s self-executing autonomy can sideline the role of human judgment. Decisions that would ordinarily be subject to judicial oversight, such as whether a contract was performed correctly, or whether an outcome is fair, are pre-determined by software logic. Blockchain enthusiasts often tout the ideal of “code is law,” meaning the software code alone defines the rights and obligations of the parties, leaving no room for external interpretation or intervention.¹⁰⁵ This phenomenon should be approached with caution as “this code, or architecture, sets the terms on which life in cyberspace is experienced,” functioning as an invisible regulator that can threaten liberty if

¹⁰³ Katrin Becker, *Blockchain Matters – Lex Cryptographia and the Displacement of Legal Symbolics and Imaginaries*, 33 L. & CRITIQUE 113, 113–115, 118, 120 (Jan. 6, 2022), <https://link.springer.com/article/10.1007/s10978-021-09317-8> [<https://perma.cc/48S5-5QGT>].

¹⁰⁴ Tirado & Cosio, *supra* note 99.

¹⁰⁵ See *Code is Law*, *supra* note 95.

unchecked.¹⁰⁶ In the blockchain context, the code-is-law ethos is embraced as a feature: advocates claim it removes human fallibility and bias from the equation, ensuring that agreements are enforced exactly as written.¹⁰⁷ For example, the Ethereum Classic community (which split from Ethereum in 2016) explicitly upholds “Code is Law” as its guiding principle. They envision future “virtual jurisdictions” governed purely by software, believing that “for the first time, humanity can operate under *actual*, as opposed to the guise of, Rule of Law, codified not in esoteric and misinterpretable legal texts, but in pure mathematics.”¹⁰⁸ Under this view, code-based rules are seen as more transparent and incorruptible than traditional legal systems, which can be slow, costly, or subject to manipulation.

[61] However, the rise of *lex cryptographica* directly implicates judicial review because it calls into question who, if anyone, can review or overturn the decisions made by autonomous systems. In a conventional legal system, any exercise of power or enforcement of a contract is ultimately reviewable by an independent judiciary to ensure it comports with the law and justice. The U.S. legal system is structured to ensure that disputes are reviewed by impartial judges who interpret the law and balance competing interests in the context of fairness and equity.¹⁰⁹ If a contract is unfair or executed improperly, its courts can void it or provide a remedy. By contrast, in a blockchain-based system, enforcement is automatic and presumed final. The “judgment” is effectively rendered by code at the moment conditions

¹⁰⁶ Michael Jünemann, *Can Code Be Law?*, BIRD & BIRD (Aug. 9, 2021), <https://www.twobirds.com/en/insights/2021/germany/can-code-be-law> [<https://perma.cc/3MRA-5TST>].

¹⁰⁷ *Code is Law*, *supra* note 95.

¹⁰⁸ *Code is Law*, *supra* note 95.

¹⁰⁹ See *Goldberg v. Kelly*, 397 U.S. 254, 271 (1970) (requiring an impartial decisionmaker); *Hecht Co. v. Bowles*, 321 U.S. 321, 329–30 (1944) (describing equitable discretion in judicial decision-making).

encoded in the smart contract are triggered. Some commentators suggest that if traditional law proves ineffective at regulating blockchain activity, we may witness the full emergence of a *lex cryptographica* ecosystem where technology itself, rather than the state, “ensures the protection of fundamental rights” within the blockchain realm.¹¹⁰

[62] This would represent a dramatic shift: the guarantor of rights and fairness in a transaction would be the software’s design, not a constitution or court. Indeed, certain fundamental values might be encoded differently, or not at all, in such systems. For instance, blockchain networks by design prioritize transparency and immutability, which means that once data is recorded it cannot be easily removed. This has led observers to note that in a *lex cryptographica* environment, freedom of speech (i.e., the ability to publish information immutably) could prevail over privacy (the ability to remove or hide information), because technology inherently favors recording and broadcasting data over concealing it.¹¹¹ Such an outcome might conflict with the delicate balance of rights that courts and lawmakers attempt to maintain in society. It underscores that when code, rather than law, dictates outcomes, the usual mechanisms for balancing competing values, such as a court weighing free expression against privacy concerns, may not operate. The implications for judicial review are therefore significant: courts could find themselves either bypassed entirely or forced to grapple with *fait accompli* results produced by autonomous code.¹¹²

[63] *Lex cryptographica* offers a provocative model of autonomous rule-making through software. It holds promises for more efficient and incorruptible transactions, but it also challenges the foundations of legal oversight. Courts would need to be able to interact with decentralized systems in a way that allows for the enforcement of legal rights and

¹¹⁰ Tirado & Cosio, *supra* note 99.

¹¹¹ Tirado & Cosio, *supra* note 99.

¹¹² Garrett, *supra* note 92, at 948–52.

remedies when these systems fail to meet standards of fairness and equity. This is a crucial barrier to incorporating blockchain-based dispute resolution within national judiciaries, as there is currently no framework that bridges the gap between the automated execution of code and judicial oversight. The next subparts explore how these code-based protocols might undermine judicial oversight, and what can be done to ensure human review remains integral even as automated enforcement becomes more prevalent.

B. How Code-Based Protocols May Undermine Judicial Oversight

[64] Smart contracts and blockchain protocols, by their very design, can undercut traditional judicial oversight in multiple ways. One fundamental issue is the immutability and self-enforcement of code. Once a smart contract is deployed on a decentralized network, its operations are typically irreversible and unstoppable; it will execute exactly as coded, no matter how circumstances change or whether the outcome is unjust.¹¹³ This threatens to bypass the role of courts, which ordinarily can halt or unwind transactions that violate the law or equity. Legal scholars have pointed out that in the realm of smart contracts, “the hands of the court are tied to a large extent.”¹¹⁴ Even if a judge wanted to intervene, for example by issuing an injunction or ordering the blockchain ledger to be rectified, “the blockchain cannot be changed subsequently” in most cases.¹¹⁵ In effect, a software protocol may carry out an agreement in a way that a court—applying ordinary law—would consider invalid or voidable, yet the court cannot easily undo it. Parties who opt into a blockchain transaction may even be deemed to have “implicitly or explicitly agreed to operate in a technical,

¹¹³See Sushmita Rashid & Alejandro Mena, *Understanding How to Write Upgradeable Smart Contracts*, META MASK (Oct. 3, 2024), <https://metamask.io/news/understanding-how-to-write-upgradable-smart-contracts> [<https://perma.cc/3BUP-YSNB>].

¹¹⁴Jünemann, *supra* note 106.

¹¹⁵*Id.*

trustless environment” with its own internal rules, possibly superseding the relevant private law rules of the jurisdiction.¹¹⁶

[65] The result is a scenario where the normal authority of judicial decisions is weakened. Where even if legal norms indicate one result, if the code delivers a different result, there may be no practical mechanism to enforce the legal outcome on-chain.

[66] A vivid illustration of this tension came with The DAO incident in 2016. “The DAO” was a decentralized autonomous organization on Ethereum, essentially a crowd-sourced investment fund governed by smart contracts. When an attacker exploited a loophole (recursive withdrawal bug) to siphon off one-third of The DAO’s funds, a fierce debate ensued over how to respond.¹¹⁷ On one side were those who held a strict code-is-law view: since the smart contract’s code allowed the exploit, the attacker’s actions were legitimate by the rules of the system. The purported hacker even argued that any attempt to reverse the transfers “would amount to seizure of [his] legitimate and rightful ether, claimed legally through the terms of a smart contract.”¹¹⁸ In other words, from his perspective the software code itself was the ultimate authority, and adhering to it was more important than any external notions of fairness or intent. On the other side, many in the Ethereum community felt that this outcome, an apparent theft, was fundamentally unjust and would destroy trust in the platform.¹¹⁹ Lacking any court to appeal to (since the DAO was stateless and autonomous), the community took the extraordinary step of hard-forking the blockchain to reverse the exploit. This meant manually altering the code

¹¹⁶ *Id.*

¹¹⁷ *Client Alert: “Code is Law”*, QUINN EMANUEL URQUHART & SULLIVAN, LLP, <https://www.quinnemanuel.com/the-firm/publications/code-is-law/> [<https://perma.cc/4EV7-BEPU>].

¹¹⁸ *Id.*

¹¹⁹ *Id.*

and ledger to undo the attacker's transactions, effectively overriding the "law" of the smart contract with a one-time, human-driven intervention. The fallout was significant: Ethereum's network split into two (the majority that executed the fork, and a minority that refused, now known as Ethereum Classic).¹²⁰ The episode demonstrated both the power and the peril of autonomous code. On one hand, the normal legal recourse (suing the thief, freezing assets, etc.) was impractical: the attacker was pseudonymous, the funds were in a smart contract, and no court order could have been enforced on the decentralized network. On the other hand, the community's *ad hoc* solution showed that pure code outcomes could still be subverted by collective human action when deemed necessary. However, that "solution" was governance by community vote, not by a neutral judiciary, serving as a reminder that blockchain networks have their own politics that may or may not align with rule-of-law values.¹²¹

[67] Beyond that, there are more systematic ways in which code-based protocols challenge judicial oversight. One issue is the elimination of interpretative flexibility. Traditional legal contracts are written in natural language, which allows courts to interpret clauses in context, apply equitable doctrines, or void contracts for reasons such as duress, illegality, or unconscionability. Smart contracts, in contrast, execute literal code; they lack the nuanced understanding of context that a judge or jury can bring. As a result, a smart contract might enforce an agreement even when a real-world contingency arises that would justify non-enforcement under law (for instance, a force majeure event or a fundamental mistake by the parties). The software lacks the ability to show mercy or adjust for unexpected circumstances. This rigidity means parties could be locked into outcomes that a court would have relieved them from. Further, no possibility of appeal exists within the smart contract's operation – there is no automated mechanism to pause execution, assess fairness, or call for revision. The Ethereum Classic philosophy embraces this rigidity: it states plainly that,

¹²⁰ *Id.*

¹²¹ DE FILIPPI & WRIGHT, *supra* note 2, at 58–60.

“if a contract is poorly written or contains a mistake, it is not the responsibility of the wider network to ‘make whole’ parties who are not happy with a given outcome. In short, there are no do-overs, bailouts or refunds, unless pre-programmed.”¹²² This shows a stark departure from the traditional rule of law, where courts can provide remedies or second chances in the interest of justice. For example, in the U.S., contract law allows courts to void or modify contracts in certain circumstances, including duress, mistake, or fraud. Under a strict rule-of-code regime, no external corrective is available when the code’s outcome diverges from what is just or socially acceptable.

[68] Another challenge is the lack of a clear accountable entity for courts to confront. In many blockchain arrangements, there is no single party in control; the code runs autonomously or the decision is made by a distributed set of users (as in a DAO). If something goes wrong or a rule needs to be challenged, who do you sue or summon to court? The traditional model of judicial oversight assumes an identifiable defendant or authority that can be ordered to act or refrain from acting. Code, especially when truly decentralized, does not respond to subpoenas. For example, if a self-executing lending contract automatically liquidates a borrower’s collateral in a cryptocurrency loan, and the borrower believes this was done in error or was predatory, a court could in theory render a judgment against the lender. But if the “lender” is just a program or a DAO with no legal personality, the judgment may be futile.¹²³ In short, code-based protocols

¹²² *Code is Law*, *supra* note 95.

¹²³ An echo of this problem can be seen in the recent Tornado Cash case. Tornado Cash is a decentralized software protocol (a “crypto mixer”) with no central operator, consisting of immutable smart contracts on Ethereum. *See Joseph Van Loon v. Dep’t of the Treasury*, 122 F.4th 549, 553 (5th Cir. 2024). In 2022, the U.S. Treasury attempted to sanction Tornado Cash by adding it to its sanctions list, treating the software as an entity. *See id.* at 560–561. This led to a legal challenge, and in 2024 the U.S. Fifth Circuit Court of Appeals ruled that “immutable smart contracts are not ‘property’” under the sanctions law (International Emergency Economic Powers Act (IEEPA)), essentially because they are “unownable, uncontrollable, and unchangeable” pieces of code. *See id.* at 565–566. The court noted further that such autonomous code is not even a contract in the legal sense since it lacks mutual agreement between parties. *See id.* at 568. The result was that

can undermine judicial and regulatory oversight simply by existing in a zone that law was not designed to reach: they execute power (transferring value, enforcing rules) without a readily accountable human actor or attachable “property” that courts can order to be turned over.

[69] Finally, code-based systems may undermine the spirit of the rule of law by prioritizing strict rule compliance over principles of equity and proportionality. The rule of law is not just about rules being enforced, but about those rules being subject to reasoned interpretation and conformed to societal values. A system that enforces literal code above all else risks enabling exploits and injustices under the banner of formal correctness. The DAO attacker’s stance, that exploiting the contract was legitimate since the code permitted it, reveals this danger. It elevates form over substance in a way most courts would reject (analogous to abusing a loophole in a contract, which equity might prevent). If participants come to believe that no oversight or appeal is possible, they may lose trust in the system’s fairness or avoid using it for anything but the simplest transactions. Thus, even as code-based protocols remove some inefficiencies (no need to go to court for enforcement), they introduce new oversight risks: errors or abuses that cannot be readily rectified. This has prompted calls to find ways to integrate human judgment and legal protections into or alongside these automated systems.¹²⁴

the sanctions could not directly apply to the code itself. From one perspective, this was a victory for the idea that code lies outside certain legal constraints, “a significant victory for decentralized finance advocates,” limiting the reach of regulators such as the Treasury’s Office of Foreign Assets Control (OFAC). See *Fifth Circuit Limits OFAC’s Authority Over Immutable Smart Contracts*, TODAY’S GENERAL COUNSEL (Jan. 17, 2025), <https://todaysgeneralcounsel.com/fifth-circuit-limits-ofacs-authority-over-immutable-smart-contracts/> [<https://perma.cc/G3R9-XDAM>]. From another perspective, it underscores a gap in oversight: if harmful or illicit activity is facilitated by an autonomous protocol, the traditional legal tools (e.g., asset freezing or sanctions) may prove ineffective. Regulators may be forced to pursue indirect routes – for instance, going after individuals (developers, users) or intermediaries (exchanges, front-end web hosts), which is a step removed from the source of the problem.

¹²⁴ Garrett, *supra* note 92; Ameen, *supra* note 92.

C. Ensuring Human Judicial Review in Automated Enforcement Mechanisms

[70] Despite the autonomous and self-executing nature of smart contracts, human judicial review may be essential as a backstop for justice. In practice, completely removing human review is neither feasible nor desirable. A comprehensive study on smart contracts concluded that, for all their self-enforcing power, “smart contract self-enforcement mechanisms will not be able to supplant completely the need for judicial review and enforcement procedures.”¹²⁵ There will almost always be scenarios (known in the U.S. as fraud, mistake, illegality, unforeseen hardship, etc.) where parties seek relief that only a court or comparable tribunal can provide. In fact, current legal systems often guarantee the availability of judicial review. For example, when creditors breach the peace to repossess collateral, a U.S. judge may limit their right to self-help.¹²⁶ Such legal principles make clear that automation cannot entirely close the courthouse doors. In theory and practice, multiple approaches are emerging to ensure that automated enforcement mechanisms remain synchronized with broader legal systems.

i. Designing “Smart Legal Contracts”

[71] One approach is to embed legal protocols into smart contracts or to pair code with natural-language contracts. Rather than relying on code alone, parties can agree that their smart contract is subject to an accompanying text contract or statute. Hence, if the code produces an outcome that is disputed, a court can interpret the human-readable terms to decide if the outcome should be adjusted. In other words, the smart contract handles routine execution, but ultimate interpretive authority still lies with

¹²⁵ Smart Contracts Alliance, *Smart Contracts: Is the Law Ready?*, CHAM. DIG’L COMM. 32 (Sept. 2018), <https://lowellmilkeninstitute.law.ucla.edu/wp-content/uploads/2018/08/Smart-Contracts-Whitepaper.pdf> [<https://perma.cc/7L8A-3643>].

¹²⁶ *Id.* at 32, n.87.

legal principles. For instance, if each of the elements of ordinary contract law (offer, acceptance, consideration, etc.) is satisfied, a smart contract should be legally binding under U.S. law.¹²⁷ From this standpoint, smart contracts are seen not as a separate legal universe but as a new medium for agreements – one that courts can work with by treating the code as embodying an agreement between parties. If something goes wrong, traditional remedies (e.g., damages or injunctions) can still be pursued in court against one of the contracting parties, even if the code has been executed. Courts could also have the authority to freeze blockchain transactions or modify the terms of a contract if they are deemed to violate fundamental legal principles or due process. In practice, this requires careful drafting (e.g., a clause stating “the parties agree that the smart contract at address XYZ is part of this contract and that in case of discrepancy, the natural language terms prevail”). While this might slow down the pure automation, it ensures that legal fallbacks exist.

ii. Incorporating Arbitration and Dispute Resolution within Code

[72] Another strategy gaining traction is building alternative dispute resolution (ADR) mechanisms into blockchain systems themselves. Projects such as Kleros¹²⁸ and Aragon Court¹²⁹ are representative examples of this approach. These are decentralized arbitration services where human jurors (often token-holders in the system) can be called upon to resolve disputes arising from smart contracts. For example, Kleros allows parties to write an arbitration clause into a smart contract, specifying that if a dispute

¹²⁷ *Smart Contracts*, *supra* note 125, at 18.

¹²⁸ *The Justice Protocol*, KLEROS, <https://kleros.io/> [<https://perma.cc/W3AS-JVE3>] (“Kleros is a decentralized arbitrations service for the disputes of the new economy.”).

¹²⁹ *What is Aragon Court*, ARAGON, <https://legacy-docs.aragon.org/products/aragon-court/aragon-court> [<https://perma.cc/3WE9-C4DM>] (“Aragon Court is a dispute resolution protocol that handles subjective disputes that cannot be solved by smart contract.”).

arises, the contract will refer the matter to the Kleros DApp. Kleros then randomly selects a panel of jurors who review evidence and render a decision, which the smart contract will automatically enforce.¹³⁰ Notably, Kleros has built-in due process features: the protocol automatically provides notice to the parties, selects jurors, and enables evidence exchange via smart contract functions, ensuring that even though the process is digital, it is subject to fundamental fairness criteria.¹³¹ This kind of on-chain arbitration brings a human element into the loop before irreversible actions are taken. If a buyer and seller have a dispute over an online transaction, a smart contract escrow might hold the funds and call an arbitrator (human) if either party contests the outcome, rather than releasing the funds automatically. Such systems can be faster and more global than traditional courts, yet still introduce judgement and context where pure code cannot. They represent a middle ground between total automation and traditional litigation or arbitration.

iii. Community Governance and “Soft” Oversight

[73] As seen in the Ethereum DAO example, blockchain communities themselves can act as a form of oversight through governance mechanisms. Many decentralized finance (DeFi) platforms have administration keys or governance tokens that allow humans to intervene in protocol parameters.¹³² For instance, some smart contract platforms include pause or emergency stop functions that developers or governance token-holders can trigger if a bug or hack is detected—essentially a “circuit breaker” to halt automated processes before they do more damage. While not a judicial review in the

¹³⁰ Tirado & Cosio, *supra* note 99.

¹³¹ *Id.*

¹³² ORG. FOR ECON. CO-OPERATION & DEV. (OECD), *Why Decentralised Finance (DeFi) Matters and the Policy Implications* 45 (2022), https://www.oecd.org/content/dam/oecd/en/publications/reports/2022/01/why-decentralised-finance-defi-matters-and-the-policy-implications_5f54ead/109084ae-en.pdf [<https://perma.cc/55BD-9BAM>].

formal sense, this process introduces accountability and the possibility of correction. It echoes how, in U.S. corporate law, internal governance and boards provide oversight in addition to external regulation. Similarly, blockchain networks with on-chain voting allow participants to change the code (upgrade contracts, reverse transactions in extreme cases, etc.) when the community consensus deems it necessary for the health of the system.¹³³ Some may view this as a proto-judicial function: the community deliberates and reaches a decision to remedy a problem, akin to a collective court. However, community governance may lack the impartiality and rights-conscious approach of real courts, so it is not a complete substitute. It can be biased towards the majority or those with more tokens, for example. Nonetheless, it provides an additional layer of oversight to purely automatic execution: a safety valve when code behaves in an unforeseen or unacceptable way.

iv. Legal Accountability for Code Outcomes

[74] Another pillar of ensuring oversight is clarifying how existing law applies to actions taken by smart contracts. Courts may not be able to rewrite blockchain history, but they can attach legal consequences to those outcomes in the off-chain world. For example, if a smart contract wrongfully transfers assets, a court might still impose liability on the recipient (if identifiable) under unjust enrichment or other tort theories, effectively ordering them to compensate the victim even if the on-chain transfer cannot be reversed. Scholars note that many self-help mechanisms in commerce, including repossessing collateral, exist but are “judicially supervised” to prevent abuse.¹³⁴ The same concept can extend to smart contracts: they might execute automatically (like a self-help remedy), but if they do so in a way that breaches legal duties, the parties can be hauled into court afterwards. For example, legislators could introduce policies that mandate high-stakes smart contracts used for dispute resolution in regulated

¹³³ Quinn Emanuel URQUHART & SULLIVAN, LLP, *supra* note 117.

¹³⁴ *Smart Contracts*, *supra* note 125, at 32, n.87.

sectors (e.g., financial services, healthcare) to have an explicit path for judicial appeal, providing parties with the right to challenge or modify automated decisions. This ensures that, despite blockchain's ability to execute code-based decisions autonomously, there is a forum (courts or arbitration) to hear claims.

D. Technical and Administrative Challenges

i. Standardizing Blockchain Infrastructure Across Courts

[75] Implementing a blockchain-based recognition system faces the fundamental obstacle to standardization across disparate courts and jurisdictions. In the United States, courts operate under various state and federal systems with their own legacy databases and processes, making a one-size-fits-all blockchain infrastructure difficult to achieve. Without common standards, one court's blockchain solution may not be compatible with another's, undermining the goal of seamless information sharing. By contrast, some countries have pursued top-down standardization: for example, China's Supreme People's Court (SPC) built a unified judicial blockchain platform accessible by courts at all levels nationwide.¹³⁵ This centralized approach allows all Chinese courts to share a tamper-proof ledger for evidence, filings, and judgments. Similarly, Dubai's judiciary has explored a "Court of the Blockchain" initiative to connect different courts on a single network, aiming to eliminate manual data silos and duplicative record-keeping by enabling decentralized information exchange.¹³⁶ These efforts show that achieving interoperability requires consensus on technical standards, governance, and infrastructure across the judiciary. In jurisdictions such as the U.S. where court systems are autonomous,

¹³⁵ Jianfeng, *supra* note 14.

¹³⁶ Wolfie Zhao, *Dubai Plans to 'Disrupt' Its Own Legal System with Blockchain*, COINDESK, <https://www.coindesk.com/markets/2018/07/30/dubai-plans-to-disrupt-its-own-legal-system-with-blockchain> [<https://perma.cc/T38D-SG9R>] (last updated Sep. 13, 2021, at 04:13 ET).

establishing such uniformity is a technical and administrative challenge. Stakeholders would need to agree on which blockchain platform or protocol to use and how to integrate it with existing case management systems before leveraging the benefits of a connected, transparent record system.

[76] Real-world examples reveal both the promise and complexity of standardization. Internationally, Estonia’s e-justice system uses a blockchain-based KSI technology to secure court records, illustrating that smaller jurisdictions can implement nationwide solutions.¹³⁷ India has also piloted a “Judiciary Chain” under its National Informatics Centre, with a total of 665 judiciary documents verified on it as of October 21, 2025.¹³⁸ These cases show that standardizing blockchain in courts is feasible with strong central coordination. However, adopting a uniform blockchain in the U.S. would entail unprecedented coordination between federal and state courts. Courts would need to reconcile different data formats, privacy rules, and procedures under a common technical umbrella. As the National Center for State Courts has noted, “justice partners will also need to consider carefully the implications of a variety of architectural decisions . . .” before blockchain can be effectively deployed in court technology.¹³⁹ Without an agreed-upon framework, there is a risk of fragmentation with each court or state implementing its own incompatible ledger, which could recreate the very silos that blockchain is meant to break down. In summary, standardization is a crucial yet difficult prerequisite for a blockchain-based recognition system, requiring both policy consensus and technical coordination across the judicial branch.

¹³⁷ See Semenzin et al., *supra* note 17; see also Osula, *supra* note 17.

¹³⁸ *National Blockchain Network, Strengthening Governance Through Blockchain Technology*, PIB, GOV’T OF INDIA (Oct. 24, 2025), <https://www.pib.gov.in/PressNoteDetails.aspx?NoteId=155672&ModuleId=3®=3&lang=2> [<https://perma.cc/3H42-NUQ9>].

¹³⁹ Graski & Embley, *supra* note 5, at 66.

ii. Privacy and Confidentiality Issues in Judicial Data Management

[77] Courts handle sensitive information, including personal data, confidential evidence and sealed records, that must be protected even as blockchain promises transparency and immutability. This creates a tension between openness and privacy. A key concern is that once data is recorded on a blockchain, it becomes extremely difficult to remove or alter.¹⁴⁰ In many U.S. jurisdictions, however, laws require certain records to be sealed or expunged, meaning hidden from public view or destroyed entirely (for instance, juvenile records or criminal convictions after a set period).¹⁴¹ A “truly immutable” blockchain would conflict directly with these requirements as an append-only ledger does not allow for data to be deleted or hidden. Adding a new block to note that a prior record was expunged does not solve the problem either; the underlying sensitive data would remain accessible on-chain, defeating the purpose of sealing and expungement.¹⁴² Thus, strict immutability, one of blockchain’s defining features, becomes a liability in the context of legal data confidentiality. Because of the privacy laws, a completely immutable blockchain database for court records “may not be the best approach” unless it is designed with some flexibility or off-chain mechanism.¹⁴³

[78] Beyond expungement, there are broader data protection concerns. Court records often include personally identifiable information (addresses,

¹⁴⁰ Peter Leasure, *A Comment on the Potential Utilization of Blockchain Technology for Criminal Record Databases*, RICH. J.L. & TECH. (Oct. 27, 2022), <https://jolt.richmond.edu/2022/10/27/a-comment-on-the-potential-utilization-of-blockchain-technology-for-criminal-record-databases> [https://perma.cc/2Y6Y-VWHF].

¹⁴¹ *Id.*

¹⁴² *Id.*

¹⁴³ The author argues that, “[g]iven these points, a hybrid, private, or consortium blockchain may be best suited for a blockchain-based criminal record database.” *Id.*

financial details, health records in injury cases, etc.), which if stored on a public blockchain could be exposed to anyone. Even on a permissioned (private) blockchain, all participating nodes might see data that should be restricted. This runs up against data privacy regulations. For example, the European Union's GDPR grants a "right to be forgotten," which clashes with blockchain's inalterability.¹⁴⁴ One corporate law analysis noted that once personal data is on a blockchain and cannot be easily altered or erased, "this clearly has implications for data privacy."¹⁴⁵ To reconcile blockchain with confidentiality, technologists are exploring solutions, including encryption, zero-knowledge proofs, and off-chain storage.¹⁴⁶ In practice, courts would likely avoid putting full-text sensitive information on-chain. Instead, a blockchain system might store hashes or digital fingerprints of documents, with the actual files stored securely off-chain in traditional databases or encrypted repositories. This approach maintains an immutable proof of a document's existence and integrity without exposing the content. For example, a blockchain-based evidence platform could record a hashed reference to a piece of evidence, while the evidence itself is kept in a secure server so that any tampering with the server file would be detectable via hash mismatch on the blockchain. Some commentators caution, however,

¹⁴⁴ European Union, *General Data Protection Regulation (GDPR)* Art. 17, Regulation (EU) 2016/679, 2016 O.J. (L 119) 1 (EU), <https://gdpr-info.eu/> [<https://perma.cc/DXG3-F7JD>].

¹⁴⁵ John McKinlay et al., *Blockchain: Background, Challenges and Legal Issues*, DLA PIPER (Feb. 2, 2018), <https://www.dlapiper.com/en/insights/publications/2020/12/blockchain-background-challenges-legal-issues> [<https://perma.cc/94DL-DHFV>].

¹⁴⁶ For instance, zero-knowledge proofs allow one party to prove to another that they know a value without revealing the value itself. Judith Etugbo, *Why Zero-Knowledge Proofs Are the Future of Blockchain Security*, BUILT IN (Mar. 25, 2025), <https://builtin.com/articles/zero-knowledge-proof-blockchain-security> [<https://perma.cc/3HTN-JD9H>].

that even storing hashes of personal data on-chain could in theory violate privacy norms if those hashes can be linked back to individuals.¹⁴⁷

[79] Another confidentiality issue is role-based access. In traditional judicial proceedings, not every participant can see all available information. For instance, jurors may not see sealed motions, while the public cannot access certain victim identities.¹⁴⁸ A blockchain for courts would need specific access controls layered on top of it, determining who can read or add each transaction. Achieving this on a distributed ledger can be complex. Permissioned blockchain networks address part of this by limiting participation to trusted entities (courts, prosecutors, defense counsel, etc.), but within that network further restrictions are needed. Smart contract-based access control or encryption keys can enforce some confidentiality, but managing keys and permissions adds administrative overhead. Further, one of blockchain's selling points is that data is verifiable and auditable by all nodes, yet judicial data often demands confidentiality and even anonymity for parties. As a result, any court blockchain must be designed as a private/consortium ledger with robust privacy-preserving techniques, rather than a fully public blockchain. This inherently limits transparency to the invited participants and reintroduces a degree of centralized trust (since someone must vet and authorize participants and oversee access rights).¹⁴⁹

¹⁴⁷ See *Using Algorand for Criminal Justice Database*, ALGORAND (Mar. 2024), <https://forum.algorand.co/t/using-algorand-for-criminal-justice-database/11592> [<https://perma.cc/GWY6-BJ26>].

¹⁴⁸ 18 U.S.C. § 3509(d)(2) (protecting confidentiality of victim identities); *Nixon v. Warner Commc'ns, Inc.*, 435 U.S. 589, 598 (1978) (recognizing limits on public access to judicial records); *Press-Enterprise Co. v. Superior Court*, 478 U.S. 1, 9 (1986) (allowing restrictions to protect fairness and privacy).

¹⁴⁹ See Michael Wilson, *Permissioned Blockchain: Top Tips for Setting It Up*, BLOCKCHAIN COUNCIL (Sept. 29, 2025), <https://www.blockchain-council.org/blockchain/permissioned-blockchain-setup-tips> [<https://perma.cc/HA93-VA5U>]; *Private Blockchain Networks*, NADCAB LABS (Jun. 6, 2025) (explaining that participation and access are controlled by administrators), <https://www.nadcab.com/blog/private-network-in-blockchain> [<https://perma.cc/95V9-W75M>].

Privacy and confidentiality requirements present a significant practical barrier: courts adopting blockchain must carefully engineer solutions that uphold secrecy where required (such as sealed cases) while still leveraging the ledger's integrity. Getting this balance right is fundamental to protect litigants' rights and comply with laws, and it often means trading off some of blockchain's openness to meet real-world legal privacy standards.¹⁵⁰

iii. Interoperability Between Blockchain Systems and Traditional Court Databases

[80] Courts will not be able to abandon their existing IT systems overnight in favor of blockchain. Decades' worth of case files, electronic document management systems, and public access portals are already in place. Thus, a blockchain-based recognition system would have to interoperate smoothly with traditional court databases during any transition and likely long after. Interoperability here means two things: connecting blockchain platforms with legacy systems, and ensuring different blockchain implementations (if multiple are adopted) can communicate or at least exchange data reliably. Both pose challenges.

[81] First, integration with legacy databases is technically complex. Traditional court case management systems (CMS) often run on relational databases and have their own data schemas. If a blockchain is introduced (for example, to log all evidentiary filings or to record judgments), the data on the chain must sync or reconcile with the court's primary database to avoid inconsistencies.¹⁵¹ Without integration, courts might face duplicate

¹⁵⁰ McKinlay et al., *supra* note 145.

¹⁵¹ HYPERLEDGER FIREFLY (noting that enterprise blockchain applications require coordination between off-chain data flows and on-chain transactions), https://hyperledger.github.io/firefly/latest/overview/key_components/flows/ [<https://perma.cc/H9C2-RJLR>]; see also Wuqi Zhang et al., *Detecting On-Chain–Off-Chain Synchronization Bugs in Decentralized Applications*, CORNELL U. (Jun. 17, 2021) (stating that failure to synchronize on-chain and off-chain data leads to inconsistencies), <https://arxiv.org/abs/2106.09440> [<https://perma.cc/N9P9-R5CA>].

data entry. For instance, clerks might enter information into the old system and into the blockchain, which is inefficient and prone to error. A recent Colorado investigation into court data sharing showed how, currently, each court maintains its own siloed records and there is “no data sharing system” between them, leading to duplicate work and inconsistencies.¹⁵² The goal of that effort is to enable read-only data exchanges so that information entered in one court’s system can be seen by others, preventing scenarios such as multiple courts unknowingly working on cases involving the same individual.¹⁵³ While Colorado’s study did not mention blockchain, it underscores the importance of interoperability for efficiency. Thus, introducing blockchain without robust integration could exacerbate silos (i.e., what happens if some case data would be on the blockchain, while the other is on the old database, with no single source of truth).

[82] To achieve interoperability, courts would likely need to develop Application Programming Interfaces (APIs)¹⁵⁴ or middleware¹⁵⁵ that bridge

¹⁵² *Data Sharing Task Force Investigation, Options, and Recommendation: House Bill 23-1132 Final Presentation*, COLO. JUD. BRANCH, <https://www.coloradojudicial.gov/sites/default/files/2024-05/House%20Bill%2023-1132%20Final%20Presentation.pdf> [<https://perma.cc/8TUT-9948>].

¹⁵³ *Id.*

¹⁵⁴ API Gateway is a service that sits between clients and backend services, acting as a reverse proxy to accept incoming requests from clients, perform various operations such as routing, authentication, and rate limiting, and then forward those requests to the appropriate backend services. It serves as a single entry point for clients to access multiple services, providing a unified interface and abstracting the complexities of the underlying architecture. *Difference Between API Gateway and Middleware*, GEEKS FOR GEEKS, <https://www.geeksforgeeks.org/system-design/difference-between-api-gateway-and-middleware/> [<https://perma.cc/3AGG-SHN7>] (last updated July 23, 2025).

¹⁵⁵ Middleware is software that acts as a bridge between different systems, applications, or components. It enables communication and data exchange between these disparate elements, allowing them to work together seamlessly. Middleware abstracts the complexities of communication protocols, data formats, and platform differences, making it easier for developers to integrate different software components. *Id.*

the blockchain and existing systems. For example, if a court's CMS queries the status of a case, the middleware should retrieve relevant updates from the blockchain (e.g., a timestamped filing or payment recorded on-chain) and present it in the CMS interface. Conversely, if data is entered into the legacy system (perhaps for parts of the process not yet on blockchain), that data might need to be anchored to the blockchain via hashed entries or transaction logs. Although designing and maintaining such two-way connectors appears to be resource-intensive, failure to do so may lead to incompatibilities and cause data to not translate correctly between systems.

[83] Interoperability challenges also arise if multiple blockchains are in play. In the absence of one standard platform (as discussed earlier), one court might use a Hyperledger-based ledger¹⁵⁶ while another uses an Ethereum-based chain,¹⁵⁷ for instance. If a case spans jurisdictions (common in criminal or family law), how will the two systems exchange information? Cross-chain interoperability protocols are still an evolving technology. It may require cross-authentication mechanisms or third-party "oracle" services to transfer data from one chain to another securely,¹⁵⁸

¹⁵⁶ A Hyperledger-based ledger refers to a distributed ledger built on one of the open-source blockchain frameworks developed under the Hyperledger umbrella, hosted by the Linux Foundation. These frameworks are designed for enterprise use to ensure privacy, control, and permissioned access. Tracy Kuhrt, *LF Decentralized Trust: FAQ*, HYPERLEDGER, <https://hyperledger.atlassian.net/wiki/spaces/HYP/pages/19595483/FAQ> [<https://perma.cc/4WMN-KXK3>] (last updated (Mar. 20, 2024)).

¹⁵⁷ An Ethereum-based chain is a blockchain network that utilizes the Ethereum protocol, enabling the creation and execution of smart contracts, tokens, and decentralized applications (dApps). Ethereum is a decentralized software platform that allows developers to build and deploy thousands of dApps without relying on a central authority. *Ethereum*, ALCHEMY, <https://www.alchemy.com/dapps/ethereum> [<https://perma.cc/YRK4-EZH5>].

¹⁵⁸ Cross-authentication enables different blockchain networks to authenticate and verify transactions across chains, ensuring secure data transfer. Yue Yu & Shibin Zhang, *A Cross-Chain Identify Authentication Scheme Based on Blockchain*, in *PROCEEDINGS OF THE 2022 INTERNATIONAL CONFERENCE ON E-COMMERCE AND INFORMATION TECHNOLOGY* 637, 635–643 (Z. Zeng et al. eds., 2023), <https://www.atlantis->

adding another layer of complexity and potential points of failure. By contrast, the ideal scenario is a unified network where all courts either share the same blockchain or use interconnected instances of it. Dubai's blockchain taskforce hinted at this ideal by aiming to let "different courts share information in a decentralized manner," thereby reducing manual duplication.¹⁵⁹ The premise is that if all relevant judicial bodies are nodes on one network, any authorized party can access the needed data without complex bridges. However, until such unity is achieved, hybrid environments may persist.

[84] During a likely lengthy transition period, courts would run blockchain systems in parallel with legacy systems. This raises operational challenges: ensuring consistency between the two, training staff to use both, and deciding which is the authoritative record in a discrepancy. If an error is entered in one system but not the other, reconciliation protocols are needed. In addition, legacy systems have established business continuity plans, such as backups and disaster recovery. Mirroring those for blockchain (which by design replicates data across nodes) requires careful planning. For instance, if a blockchain node fails, the network can continue, but if the integration layer fails, data may not flow to the old system. All these factors mean that interoperability is not just a technical add-on, but a core requirement for any practical blockchain deployment in courts. It demands both technological solutions and institutional coordination (e.g., agreements on data sharing across courts, which in some cases may even implicate legislative changes if data currently cannot be shared). Until interoperability is solved, blockchain risks becoming an isolated pilot project rather than a fully embedded part of judicial administration.

press.com/article/125976508.pdf [<https://perma.cc/NJN4-ZRQG>] Oracles are services that provide external data to smart contracts, enabling them to interact with real-world information. *What Are Blockchain Oracles? A Complete Guide*, NERVOS FOUND. (Mar. 15, 2024), [https://www.nervos.org/knowledge-base/what_are_oracles_\(explainCKBot\)](https://www.nervos.org/knowledge-base/what_are_oracles_(explainCKBot)) [<https://perma.cc/7S89-EG9X>].

¹⁵⁹ Zhao, *supra* note 136.

VI. CONCLUSION

[85] Integrating blockchain technology into judicial processes through tools such as smart contracts and blockchain dispute resolution platforms holds significant promise for greater efficiency and transparency, but it also demands careful oversight and legal reform to preserve due process guarantees. International developments, including China's blockchain courts and Dubai's smart court initiative, demonstrate global interest in leveraging distributed ledger technology to modernize case management and enforcement. To realize this potential sustainably, innovative digital judgments subject to recognition and enforcement must conform to established legal frameworks, such as drawing on principles from the UFCMJRA for cross-border recognition, to ensure interoperability and legitimacy across jurisdictions. Utilizing blockchain's benefits alongside robust oversight, data privacy measures, and respect for fundamental fairness would enable modernization of judicial systems without compromising core legal principles.