

ARTICLE

SMART CONTRACTS AND PRIVATE INTERNATIONAL LAW: CLAIMANT-CENTERED JURISDICTION AND APPLICABLE LAW

*Amir Bushansky**

I. INTRODUCTION.....	62
II. CONFIGURATIONS OF SMART CONTRACTS AND THEIR TERRITORIAL CONNECTIONS	67
A. Autonomous Interaction of Computer Programs.....	68
B. The Default Configuration	69
C. The Default Bilingual Configuration	71
D. The Traditional-Virtual Configuration.....	72
E. The Hybrid Configuration.....	73
III. PSEUDONYMITY OF THE PARTIES AND ITS IMPLICATIONS.....	75
IV. COMPARATIVE RESPONSES TO JURISDICTIONAL CHALLENGES IN DIGITAL TRANSACTIONS	80
A. Public Harmonization.....	81
B. Private Ordering and Technological Self-Regulation	82
V. IDENTIFYING THE APPROPRIATE FORUM IN SMART CONTRACTS	84
A. The Place of Contracting	85

* Amir Bushansky, LL.B., Bar-Ilan University (*cum laude*); M.A. in Law, Technology, and Business Innovation, Harry Radzyner Law School, Reichman University (*summa cum laude*); Ph.D., Harry Radzyner Law School, Reichman University. I am grateful to Professor Celia Fassberg for her insightful comments and guidance during the preparation of this work. I also thank Professor Eyal Zamir and Professor Lior Zemer, Dean of the Harry Radzyner Law School, for their support and encouragement throughout the research process.

B. The Place of Performance and Non-Performance.....	88
C. The Place of Intermediaries.....	91
VI.APPLICABLE LAW IN SMART-CONTRACT DISPUTES.....	93
A. The Place of Contracting	94
B. The Place of Negotiation	95
C. The Place of Performance and Non-Performance.....	95
D. The Location of the Contractual Subject Matter.....	96
E. The Territorial Affiliations of the Parties	97
F. Additional Smart-Contract-Specific Connecting Factors	98
1. Tax Liabilities.....	98
2. Technologically Generated Connecting Factors.....	99
VII.CHOICE-OF-LAW AND FORUM-SELECTION CLAUSES IN SMART CONTRACTS.....	100
VIII.THE CLAIMANT AS THE PRIMARY CONNECTING FACTOR.....	105
IX.CONCLUSION.....	111

I. INTRODUCTION

This Article examines the compatibility of private international law with smart contracts operating on blockchain networks and explores the need for doctrinal adaptation. In the digital environment, anonymous parties increasingly engage in agreements written in computer code, commonly referred to as smart contracts.¹ Over the past decade, such contracts have evolved into a significant socio-economic phenomenon, with applications across various sectors, including finance, insurance, supply chains, and real estate.²

1. See Amir Bushansky, *From Presumed Intent to Programmed Performance: Smart Contracts and the Future of Contract Law*, 74 CLEV. ST. L. REV. 297, 298–99, 318 (2026).

2. See, e.g., Mark Fenwick & Erik P.M. Vermeulen, *A Primer on Blockchain, Smart Contracts & Crypto-Assets: How Distributed Ledger Technologies Solve the World's Most*

Smart contracts represent a significant development in the evolution of digital commerce. Their distinctive features—deriving from both their technological architecture and mode of operation—distinguish them from conventional contracts.³ These autonomous, self-executing agreements, deployed on blockchain infrastructure,⁴ promise increased efficiency, greater automation, and reduced reliance on intermediaries.⁵

The environment in which smart contracts operate—a decentralized and borderless blockchain network—creates a unique contractual setting.⁶ Unlike traditional online transactions or electronic commerce, smart contracts minimize reliance on centralized intermediaries and often involve pseudonymous parties with no identifiable connection to a specific territorial

Pressing Economic, Social, and Humanitarian Problems 3 (Lex Rsch. Topics in Corp. L. & Econ., Working Paper No. 2019-3, 2019), <https://ssrn.com/abstract=3379443> [<https://perma.cc/4CY5-58BX>]; DON TAPSCOTT & ALEX TAPSCOTT, BLOCKCHAIN REVOLUTION: HOW THE TECHNOLOGY BEHIND BITCOIN AND OTHER CRYPTOCURRENCIES IS CHANGING THE WORLD 280 (2016) (“As we wrote at the beginning of this tome, ‘It appears that once again the technological genie has been unleashed from its bottle . . . now at our service for another kick at the can—to transform the economic power grid and the old order of human affairs. If we will it.’ Like the first generation of the Internet, the Blockchain Revolution promises to upend business models and transform industries. But that is just the start. Blockchain technology is pushing us inexorably into a new era, predicated on openness, merit, decentralization, and global participation.”); *see also* Bushansky, *supra* note 1, at 299 (“Over the past decade, smart contracts have evolved from a theoretical concept into significant socio-economic phenomenon.”).

3. *See* Bushansky, *supra* note 1, at 322.

4. Blockchain is a type of decentralized, secure, and immutable database that operates without the involvement of a central controlling authority. *See generally* Paul Catchlove, *Smart Contracts: A New Era of Contract Use* 1 (Dec. 1, 2017) (unpublished manuscript), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3090226 [<https://perma.cc/CUU2-BB3A>].

5. *See, e.g.*, Kevin Werbach, *Trust, but Verify: Why the Blockchain Needs the Law*, 33 BERKELEY TECH. L.J. 487, 499 (2018) (“The magic of distributed ledgers is to make certain activities trustworthy without the need to trust anyone in particular.”); Max Raskin, *The Law and Legality of Smart Contracts*, 1 GEO. L. TECH. REV. 305, 309 (2017) (“They are designed to automatically enforce obligations without the need for human intervention, thereby reducing the flexibility traditionally associated with contract enforcement.”).

6. *See* PRIMAVERA DE FILIPPI & AARON WRIGHT, BLOCKCHAIN AND THE LAW: THE RULE OF CODE 33–35 (2018); *see also* Kevin Werbach & Nicolas Cornell, *Contracts Ex Machina*, 67 DUKE L.J. 313, 332 (2017) [hereinafter *Contracts Ex Machina*] (“And, because blockchains run on a distributed network of independent nodes, with no central control point, a litigant seeking to enjoin performance of a smart contract has no one to sue.”).

jurisdiction.⁷ As a result, fundamental elements of contractual activity—formation, performance, and breach—may occur within a virtual, non-territorial space.⁸

These characteristics pose a significant challenge to private international law.⁹ On the one hand, smart contracts facilitate transactions that readily transcend territorial boundaries,¹⁰ increasing the likelihood that disputes will involve multiple legal systems. The decentralized and geographically dispersed nature of many smart-contract transactions may therefore render disputes international in character, generating uncertainty regarding both the applicable law governing the agreement and the appropriate forum for adjudication.

On the other hand, the decentralized and frequently pseudonymous nature of blockchain-based smart-contract transactions may complicate the identification of traditional connecting factors, such as the parties' domicile, the place of contracting, or the place of performance.¹¹ This difficulty is further

7. LAW COMM'N, SMART LEGAL CONTRACTS: ADVICE TO GOVERNMENT, 2021, CP 563, Law Com No 401, at 167, ¶ 7.5 (UK) [hereinafter LAW COMM'N (2021)] (footnote omitted) ("As such, we think that smart legal contracts are more likely to give rise to a variety of connections to various legal systems, than they are to be completely connected to just one jurisdiction. When a smart legal contract dispute with a foreign element comes before a court in England and Wales, the first question that will arise is whether the court has jurisdiction to adjudicate the dispute.").

8. *Id.* at 173, ¶ 7.24 ("For solely code smart legal contracts that are formed by the autonomous interaction of computer programs, there is an even greater degree of uncertainty, and a greater variety of possibilities.").

9. *Id.* at 193, ¶ 7.113 ("The difficulties inherent in identifying a place of performance are indicative of the broader challenges of determining jurisdiction in relation to contracts that do not involve real world performance. We think that this is also indicative of a general observation: the further the factual scenarios are from traditional contractual settings, the greater the difficulty in applying existing legal rules and principles to those new scenarios.").

10. See Anna Duke, *What Does the CISG Have to Say About Smart Contracts? A Legal Analysis*, 20 CHI. J. INT'L L. 141, 176 (2019) ("Furthermore, smart contract technology has the potential to promote international trade by reducing transactional costs, and confirming smart contracts as a valid alternative to traditional contracts would increase their use, an outcome that is consistent with the goal of the creation of the Convention.").

11. See LAW COMM'N (2021), *supra* note 7, at 170, ¶ 7.14 (footnote omitted) ("As we discuss in Chapter 3, the pseudonymous nature of some technological systems, such as DLT systems, may make it comparatively more common for a party to enter into a smart legal contract without knowing the real identity of their counterparty. As such, there are likely to be situations where the parties to a smart legal contract do not know, and may not

exacerbated by the attenuated territorial links of many blockchain-based transactions and the pseudonymous nature of decentralized networks. In some cases, uncertainty may arise not only as to the identity and location of the contracting parties, but also as to the location of the blockchain infrastructure through which the transaction is executed, including the validating nodes responsible for maintaining the distributed ledger.¹² As a result, traditional connecting factors may be difficult to identify and, in certain cases, may fail to provide a clear territorial anchor.

Private international law does not operate through a single rigid rule, but through a combination of connecting factors, jurisdictional principles, and discretionary doctrines. Although jurisdiction has traditionally been associated with the defendant's forum (*actor sequitur forum rei*), that principle operates within a broader framework characterized by considerable flexibility.¹³ In common-law systems, jurisdictional questions are frequently influenced by the doctrine of *forum non conveniens*, under which courts consider whether another forum is clearly more appropriate for the resolution of the dispute.¹⁴ This discretionary and fact-sensitive inquiry, however, depends upon the existence of meaningful territorial connections capable of linking the dispute to a particular legal system.¹⁵

The limitations of traditional territorial approaches to private international law became apparent with the rise of internet-based transactions. The geographically diffuse nature of online activity has long challenged jurisdictional frameworks that rely upon

be able to discover, each other's identities. This poses problems for questions of presence and domicile.").

12. *Id.* at 189, ¶ 7.93 ("Other factors suggested, such as the identities, habitual residences, and domiciles of the parties, or the location of the nodes running the smart legal contract, may be trickier to apply (or less relevant) in the smart legal contract context, as we discuss above."); *see id.* at 194, ¶ 7.115 ("[T]he location of the nodes does not correlate with the location of the parties or place of performance and therefore it does not seem to be appropriate to locate jurisdiction of the contract on this basis.").

13. *See* Trevor C. Hartley, *Basic Principles of Jurisdiction in Private International Law: The European Union, the United States and England*, 71 INT'L & COMP. L.Q. 211, 213 (2022).

14. *Id.* at 222 ("The principle on which it is based is that hard-and-fast rules should be avoided: all relevant circumstances must be taken into account and the court should do what justice requires.").

15. *See* ADRIAN BRIGGS, CIVIL JURISDICTION AND JUDGMENTS 411, 419–23 (7th ed. 2021); *Spiliada Mar. Corp. v. Cansulex Ltd.* [1987] AC 460 (HL) 476–78 (appeal taken from Eng.).

identifiable territorial connections.¹⁶ Courts and scholars have responded by developing alternative approaches, such as effects-based and targeting doctrines, that seek to anchor jurisdiction in the territorial effects of online activity.¹⁷ Yet, these approaches continue to depend upon the existence of a meaningful territorial connection, notwithstanding sustained scholarly criticism of territorially based models of jurisdiction.¹⁸

The difficulty, therefore, lies not only in the potential absence of clear territorial connecting factors, but also in the possibility that digital transactions may generate multiple competing connections to different legal systems. In the absence of clear jurisdictional rules, both the indeterminacy and the multiplicity of territorial connections in digital environments may lead to increased uncertainty and unpredictability in the resolution of cross-border disputes.¹⁹

Accordingly, this Article asks whether existing private international law frameworks provide an adequate normative response to the jurisdictional and choice-of-law difficulties posed by smart contracts, or whether doctrinal adaptation is required. It argues that where traditional connecting factors are indeterminate, absent, or dispersed across multiple jurisdictions, a more structured approach is desirable. Specifically, the Article proposes a claimant-centered model that aligns jurisdiction and choice of law, thereby promoting greater certainty, predictability, and coherence in the resolution of disputes arising from decentralized digital transactions.

16. See JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET? ILLUSIONS OF A BORDERLESS WORLD 50–55, 149 (2006) (“[T]he global Internet is becoming a collection of nation-state networks.”).

17. See, e.g., *Calder v. Jones*, 465 U.S. 783, 789–90 (1984); *Zippo Mfg. Co. v. Zippo Dot Com, Inc.*, 952 F. Supp. 1119, 1124 (W.D. Pa. 1997).

18. See DAN JERKER B. SVANTESSON, SOLVING THE INTERNET JURISDICTION PUZZLE 13–56 (2017).

19. See LAW COMM’N (2021), *supra* note 7, at 200, ¶ 7.145 (“We agree that the problem of digital location – that is, the difficulty of ascribing real-world locations to digital actions and digital objects – is amongst the most significant challenges that private international law will have to overcome in relation to emerging technology, including smart legal contracts.”); see also *id.* at 200, ¶ 7.146 (“We will consider these issues and potentially propose solutions as part of our future project on conflicts of laws in the context of emerging technology.”).

The proposed framework is grounded both in the distinctive characteristics of smart contracts and the procedural realities of smart-contract disputes. By anchoring both jurisdiction and applicable law in the claimant's forum, this framework seeks to reduce reliance on broad judicial discretion and ensure that the certainty and predictability associated with smart-contract execution are not undermined by uncertainty at the level of jurisdiction and applicable law. The proposed approach further reflects the practical reality that, where corrective relief becomes necessary, the burden of initiating proceedings will ordinarily fall upon the claimant.

The Article proceeds in seven parts. Part II maps the principal configurations of smart contracts and assesses the degree to which each configuration maintains a territorial connection to the physical world. Part III examines the pseudonymity of blockchain participants and its implications for service of process, identification of parties, and effective access to remedies. Part IV situates the problem within broader comparative responses to jurisdictional challenges in digital transactions, focusing on public harmonization and private ordering. Part V analyzes the difficulties involved in identifying the appropriate forum in smart-contract disputes, with particular attention to the place of contracting, performance, non-performance, and intermediaries. Part VI considers the corresponding choice-of-law problems and evaluates both traditional and smart-contract-specific connecting factors. Part VII addresses the role and limits of choice-of-law and forum-selection clauses in smart-contract environments. Part VIII develops the Article's central normative proposal: a claimant-centered connecting-factor framework that aligns jurisdiction and applicable law in order to promote certainty, predictability, coherence, and access to justice in disputes arising from decentralized digital transactions.

II. CONFIGURATIONS OF SMART CONTRACTS AND THEIR TERRITORIAL CONNECTIONS

While the operational mechanism of smart contracts is fundamentally uniform, the scholarly literature identifies multiple configurations that reflect their diverse applications across

various sectors.²⁰ These configurations differ in their structure, the degree of their territorial connections, and the legal implications that follow—particularly with respect to the identification of connecting factors, jurisdiction, and applicable law.

Mapping these configurations is essential, as they give rise to distinct legal consequences. In particular, the degree of each configuration's territorial connections directly affects the ability to identify the connecting factors on which private international law is grounded. As these connections diminish, the difficulty of identifying such factors correspondingly increases. Accordingly, it becomes necessary to assess whether existing doctrinal frameworks remain adequate, or whether doctrinal adaptations—or even the development of novel connecting factors—are required.

This Part examines the various configurations of smart contracts according to their degree of territorial connection to the real world, ranging from the weakest to the strongest territorial connection.

A. *Autonomous Interaction of Computer Programs*

The first configuration, which may be described as the autonomous interaction of computer programs, represents the weakest connection to the physical world. In this scenario, each party deploys a computer program onto a blockchain-based platform, and the programs autonomously interact with one another.²¹ Offer and acceptance are generated and executed entirely through code, without any direct human involvement at the moment of contract formation.²²

A prominent example is the Singapore Court of Appeal decision in *Quoine Pte Ltd. v. B2C2 Ltd.*, in which the court recognized that binding contractual obligations may arise from the autonomous operation of trading algorithms interacting on a cryptocurrency platform.²³ The court held that both offer and

20. See LAW COMM'N (2021), *supra* note 7, at 22–33, ¶¶ 2.51–2.96.

21. See Bushansky, *supra* note 1, at 309.

22. *Id.*

23. *Quoine Pte Ltd. v. B2C2 Ltd.* [2020] SGCA(I) 2, [1] (Sing.).

acceptance may be concluded through computer programs, even in the absence of direct human intervention.²⁴

In this configuration, where contractual relationships are conducted exclusively between computer programs within a blockchain environment, the identification of traditional connecting factors—such as the parties’ domicile, the place of contracting, the place of performance, or the place where non-performance produces legal effects—becomes particularly difficult, thereby posing a significant challenge to the application of private international law.

B. *The Default Configuration*

The second and most prevalent configuration, often referred to as the default configuration, involves a unilateral smart contract deployed on a blockchain network.²⁵ In this scenario, one party publishes an offer in the form of code, which becomes visible to all network participants.²⁶ A counterparty may accept the offer through conduct—typically by transferring digital assets or cryptocurrency in accordance with the coded terms.²⁷

This configuration is frequently described in the literature as a “glass-box” smart contract, reflecting the transparency of both the contractual terms and the associated digital assets.²⁸ It constitutes the dominant model in contemporary blockchain applications,²⁹ including transactions involving digital assets, non-

24. *Id.* at [96].

25. See *Contracts Ex Machina*, *supra* note 6, at 343 (“Smart contracts, on Ethereum and presumably on other platforms, are by default unilateral, because only one party places them on the blockchain.”).

26. See Bushansky, *supra* note 1, at 307–08.

27. See *Contracts Ex Machina*, *supra* note 6, at 368.

28. See Gregory Klass, *How to Interpret a Vending Machine: Smart Contracts and Contract Law*, 7 GEO. L. TECH. REV. 69, 101 (2023) (“The more common type of glass-box smart contract will be software whose code is available to non-programming users.”).

29. *Id.* at 73 (“More common will be transactions in which one user program a smart contract and then invites others to interact with it or in which two users purchase smart contract software from a third-party vendor.”).

fungible tokens (“NFTs”),³⁰ and decentralized finance (“DeFi”) platforms.³¹

Its defining feature is the absence of any direct connection between the parties in the physical world. The entire contractual relationship is encapsulated within the blockchain environment, and the parties are not required to disclose their identities or establish interpersonal trust.³² Instead, reliance is placed on the technological reliability and automated execution of the system.³³ Moreover, because the agreement is expressed exclusively in code rather than in natural language, it lacks the linguistic features that might otherwise serve as a connecting factor to a particular legal system.³⁴

From the perspective of private international law, this configuration raises acute difficulties. The pseudonymous nature of the parties and the absence of a clearly identifiable territorial locus complicate the identification of relevant connecting factors,

30. A token is a digital asset transferred via blockchain. Unlike fungible cryptocurrencies, unique tokens represent specific rights and are inherently non-interchangeable, making them non-fungible. See Lital Helman & Ofer Tur-Sinai, *Bracing Scarcity: Can NFTs Save Digital Art?*, 51 FLA. ST. U. L. REV. 183, 191 (2023) (explaining that NFTs possess unique characteristics that make them non-interchangeable, unlike fungible cryptocurrency tokens); see also Emily Tonelli, *NFT Marketplace OpenSea Hits \$10B in Total Volume*, DECRYPT (Nov. 8, 2021), <https://decrypt.co/85507/nft-marketplace-opensea-hits-10b-total-volume> [<https://perma.cc/ZX4Z-EK3L>]. See generally OPENSEA, <https://opensea.io> [<https://perma.cc/9V8S-ZSA9>] (last visited June 10, 2026).

31. See Bushansky, *supra* note 1, at 307–08 (discussing applications of the default configuration in NFT marketplaces and DeFi platforms, including Compound); see also Rakesh Sharma, *Understanding Decentralized Finance (DeFi): Basics and Functionality*, INVESTOPEDIA (June 13, 2026), <https://www.investopedia.com/decentralized-finance-defi5113835> [<https://perma.cc/MNQ5-RPUL>]. See generally COMPOUND, <https://compound.finance> [<https://perma.cc/3NKA-BF62>] (last visited June 10, 2026).

32. See LAW COMM’N (2021), *supra* note 7, at 170, ¶ 7.14 (footnote omitted) (“As we discuss in Chapter 3, the pseudonymous nature of some technological systems, such as DLT systems, may make it comparatively more common for a party to enter into a smart legal contract without knowing the real identity of their counterparty. As such, there are likely to be situations where the parties to a smart legal contract do not know, and may not be able to discover, each other’s identities. This poses problems for questions of presence and domicile.”); see also *Contracts Ex Machina*, *supra* note 6, at 372.

33. *Id.*

34. See HAGUE CONF. ON PRIV. INT’L L., PRINCIPLES ON CHOICE OF LAW IN INTERNATIONAL COMMERCIAL CONTRACTS 47, ¶ 4.14 & illus. 4–9 (2015) (“In the absence of other circumstances, the use of the particular language would not be sufficient to establish a tacit choice of law.”).

particularly where the entire transaction is conducted within a decentralized virtual environment.

Crucially, however, this configuration differs from the autonomous interaction of computer programs in that it still involves an act of human acceptance. The offeree, acting in the physical world, executes acceptance—typically through the use of a private key to transfer digital assets—thereby introducing a limited but legally significant territorial connection that may serve as a connecting factor to a particular legal system.³⁵

C. *The Default Bilingual Configuration*

A variation of the default configuration arises where the smart-contract code is accompanied by a natural language description of its terms and operation. While contractual performance remains governed by code, the existence of a parallel natural language representation introduces an additional territorial connection.

This dual representation enhances accessibility and may facilitate understanding by non-technical participants.³⁶ At the same time, it gives rise to interpretive challenges, particularly where discrepancies emerge between the code and the natural-language formulation.³⁷

Importantly, the use of natural language may itself constitute a connecting factor for private international law purposes, as it may indicate an implicit association with a particular legal system

35. See Bushansky, *supra* note 1, at 307 (“A participant wishing to accept the offer, does so by using their private key to transfer control over digital assets or currency, thereby satisfying the contract’s coded conditions.”).

36. See *id.* at 309; see also Amir Bushansky, *Consumer vs. Code: The Future of Consumer Smart Contracts*, 49 FORDHAM INT’L L.J. 49, 85 (2026) (“This dual representation enhances transparency and user comprehension but simultaneously introduces interpretive complexity.”).

37. See Bushansky, *supra* note 1, at 309 (“While this dual-representation enhances accessibility, it also creates interpretive challenges where discrepancies arise between the code and the natural language terms.”); see also Klass, *supra* note 28, at 107–08 (“This thought experiment suggests two general points. First, although some have suggested the possibility of ‘code-only’ smart contracts, it is difficult to imagine multiple parties interacting through a piece of software without some natural-language communications concerning its function and purpose. That is, smart contracts will almost always come ‘wrapped’ in natural language communications that describe the nature of the transaction and which will therefore serve as interpretive evidence of the parties’ agreement.”).

or linguistic context. Accordingly, this configuration may provide a limited but meaningful basis for identifying jurisdiction or determining the applicable law.

D. The Traditional-Virtual Configuration

The fourth configuration reflects a hybridization of traditional contracting practices and smart-contract technology.³⁸ In this scenario, the parties first negotiate and agree upon contractual terms in natural language, and subsequently encode those terms into a smart contract for automated execution.³⁹

This configuration presupposes a prior off-chain relationship between the parties, including negotiation, agreement, and often the involvement of third parties such as legal advisors or programmers.⁴⁰ As a result, it exhibits a stronger territorial connection than the preceding configurations. Although this configuration introduces the benefits of automated execution, it retains many features associated with traditional contracting frameworks. At the same time, its inherent complexity, the costs associated with its implementation, and the technical expertise required for its deployment have limited its widespread adoption.⁴¹

38. See Eliza Mik, *Smart Contracts: Terminology, Technical Limitations and Real World Complexity*, 9 L. INNOVATION & TECH. 269, 293 (2017) ("In comparison to their traditional counterparts, contracts written in code—or contracts written with subsequent encoding in mind—would increase in volume and complexity. As the number of errors increases in proportion to the number of lines of code, longer smart contracts would contain more errors and display a higher potential for erroneous self-enforcement."); see also Klass, *supra* note 28, at 73 ("The first is when both users take a hand in the coding, producing what I call a 'mutually programmed smart contract.' In these instances, the code can be analogized to course of performance evidence. Such mutually programmed smart contracts, while interesting to think about, are expensive to produce and will be rare.").

39. See Mik, *supra* note 38, at 291.

40. *Id.*

41. See Bushansky, *supra* note 1, at 310 ("Due to its inherent complexity, the high costs associated with its implementation, and the advanced technical expertise required of the contracting parties, this configuration has not achieved widespread adoption and remains limited to specialized contexts."); see also Mik, *supra* note 38, at 288 ("While there are no obstacles to the creation of one-off, customized smart contracts, economies of scale dictate that smart contracts take the form of generic programs that can be used on a mass-scale."); Klass, *supra* note 28, at 73 ("Such mutually programmed smart contracts, while interesting to think about, are expensive to produce and will be rare.").

From a private international law perspective, this configuration is comparatively less problematic. It is characterized by multiple territorial connections, which facilitate the identification of relevant connecting factors—ranging from the identity and place of residence of the parties, through their prior off-chain relationship and the involvement of third parties such as programmers, to the use of natural (national) language in formulating the contractual terms.⁴² Moreover, insofar as this configuration is typically employed by commercial actors, it may be reasonably assumed that they are aware of the legal implications relating to jurisdiction and choice of law, and are therefore likely to address these issues expressly within the contractual framework.⁴³

E. The Hybrid Configuration

The fifth configuration, commonly referred to as a hybrid contract, involves the simultaneous use of a smart contract and a complementary natural-language agreement.⁴⁴ In this model, the smart contract governs the automated execution of specific obligations—such as payments or asset transfers—while the natural language contract regulates the broader legal relationship between the parties.⁴⁵

This structure allows the parties to incorporate provisions that are difficult or impossible to encode,⁴⁶ including representations and warranties, dispute resolution mechanisms,

42. See Hartley, *supra* note 13, at 213 (“This is usually done by weighing up the connections or links between the forum and the defendant (sometimes also the claimant) ... and ... the events giving rise to the claim.”).

43. See LAW COMM’N (2021), *supra* note 7, app. 3, at 212, ¶ 10 (“Parties would be well advised to include choice of court and choice of law clauses in their smart legal contract, either in a separate natural language agreement, or by way of comments in the code.”).

44. *Id.* at vi. A hybrid contract is defined as: “A smart legal contract, some terms of which are defined in natural language and other terms of which are defined in the code of a computer program. Some or all of the contractual obligations are performed automatically by the code. In addition, the same contractual term(s) can be written in both natural language and in code.”

45. See Bushansky, *supra* note 36, at 86–87 (“Under this configuration, the smart contract automates only specific operational functions, including payment execution or the transfer of digital assets, while the parties’ substantive rights and obligations are articulated and governed by the accompanying textual agreement.”).

46. See Mik, *supra* note 38, at 294; see also *Contracts Ex Machina*, *supra* note 6, at 322.

and choice-of-law and jurisdiction clauses.⁴⁷ At the same time, it preserves the advantages of automation and certainty associated with smart contracts. This configuration is implemented in blockchain-based applications, such as parametric insurance, where natural-language agreements are coupled with automated execution through code.⁴⁸

From a private international law perspective, this configuration is characterized by multiple territorial connections, providing the strongest basis for identifying relevant connecting factors. These connections include the identity and place of residence of the parties, the place of conclusion of a natural-language contract, and the involvement of third parties such as lawyers and programmers. Taken together, these factors make the configuration more closely aligned with the assumptions underlying private international law.⁴⁹ Moreover, it enables the parties to express, in natural language, agreements regarding jurisdiction and choice of law, whereas the use of code alone may give rise to difficulties in articulating such arrangements.⁵⁰

The foregoing analysis yields a central insight: The determination of the configuration through which a smart contract

47. LAW COMM'N (2021), *supra* note 7, at 22, ¶ 2.51(2) ("At one end of the spectrum, the terms of a hybrid contract could be primarily written in code with a few natural language terms setting out, for example, the governing law and jurisdiction.").

48. A parametric insurance policy is a form of insurance in which the payout is determined by the occurrence of a specific event, measured by a predetermined parameter, rather than the actual loss suffered by the policyholder. See *Parametric Insurance: Closing the Protection Gap — Legal Considerations*, CLYDE & CO. (Apr. 20, 2018), <https://www.clydeco.com/en/reports/2018/04/parametric-insurance-closing-the-protectiongap> [<https://perma.cc/Z67D-MV2S>]; see also FIN. PROT. F., *DISASTER RISK FINANCE INSTRUMENTS: PARAMETRIC INSURANCE FOR DISASTER RESPONSE 2* (2023), <https://www.financialprotectionforum.org/publication/disaster-risk-finance-instruments-parametric-insurance-for-disaster-response> [<https://perma.cc/S88H-PPLB>]. See LAW COMM'N (2021), *supra* note 7, at 164, ¶ 6.29 ("We understand that the products developed by Etherisc take the form of natural language agreements which are performed automatically by smart contracts deployed on the Ethereum and xDai networks."). See generally ETHERISC, <https://etherisc.com> [<https://perma.cc/H3LL-F65F>] (last visited June 10, 2026).

49. See LAW COMM'N (2021), *supra* note 7, at 173, ¶ 7.25 ("For hybrid smart legal contracts, which are comprised of terms defined in natural language and terms defined in code, the place of contract formation will be highly fact-sensitive. If a hybrid smart legal contract is found to have been formed when a document containing the natural language terms is signed by the parties, the place of formation poses no novel difficulties.").

50. See *infra* Part VII.

is implemented must precede the identification of the relevant connecting factors for private international law purposes.

III. PSEUDONYMITY OF THE PARTIES AND ITS IMPLICATIONS

Parties engaging in transactions on blockchain networks typically operate under pseudonymous identities, using a public address and a private key, generally without disclosing their real-world identities.⁵¹ While the public address enables the transfer and receipt of digital assets, the private key functions as a cryptographic signature required to authorize transactions on the network.⁵²

This raises a fundamental question: How can legal proceedings be initiated and effective remedies obtained against a party whose identity is unknown? In this context, it is instructive to consider two recent judicial decisions—one by the English High Court and the other by the New York State Supreme Court—which approved the service of legal proceedings via blockchain, through a process commonly referred to as “airdropping” against anonymous defendants.⁵³ In such cases, the statement of claim was effectively delivered as a digital asset to the public addresses associated with the defendants on the blockchain.⁵⁴

These decisions directly address the difficulty of serving process on parties whose identities are unknown. In effect, courts endorsed the use of blockchain technology as a double-edged sword: the very infrastructure that facilitates anonymity may also be used to overcome it. To address the challenges posed by pseudonymity, courts have accepted that service via blockchain

51. See Alexander Savelyev, *Contract Law 2.0: ‘Smart’ Contracts as the Beginning of the End of Classic Contract Law*, 26 INFO. & COMM. L. 116, 117 (2017); see also *Contracts Ex Machina*, *supra* note 6, at 326–27.

52. Alan Cohn et al., *Smart After All: Blockchain, Smart Contracts, Parametric Insurance, and Smart Energy Grids*, 1 GEO. L. TECH. REV. 273, 278 (2017).

53. *D’Aloia v. Persons Unknown* [2022] EWHC (Ch) 1723 (Eng.); see *LCX AG v. 1.274M U.S. Dollar Coin*, 2022 N.Y. Slip Op. 32834(U), at 7–9 (Sup. Ct. N.Y. Cnty. Aug. 21, 2022).

54. *D’Aloia*, [2022] EWHC (Ch) 1723, [38] (“The application for service by alternative means on the first defendant is sought, both in relation to service by email, and, also, service by what is called the ‘non-fungible token’, which is a form of airdrop into the tda-finan wallets in respect of which the claimant first made his transfer to those behind the tda-finan website.”).

may satisfy applicable procedural requirements where it constitutes the most effective and appropriate method in the circumstances.

For example, in *D'Aloia v. Persons Unknown*, the English High Court held that proceedings may be brought against defendants who are not identified by name, provided that certain conditions are met. These include the existence of a serious issue to be tried (such as fraud or another tort), and that the defendants can be identified by their conduct, even if their personal identities remain unknown.⁵⁵ In that case, the claim concerned fraudulent conduct causing damage in England, and the anonymous defendants were identified through their control over specific blockchain wallet addresses.⁵⁶ The court therefore permitted service by means of NFTs sent to those public addresses, finding this method to be the most relevant, efficient, and expedient under the circumstances.⁵⁷

The 2024 decision in *Mooij v. Persons Unknown* further develops the principles established in *D'Aloia*, introducing additional distinctions—particularly with respect to the enforcement of judgments against blockchain users who are identifiable by their conduct through their public addresses, despite the fact that their personal identities remain unknown.⁵⁸ The court emphasized that the mere difficulty of enforcing a judgment against anonymous parties does not justify denying judicial relief, so long as a reasonable method of service is available.⁵⁹

It should also be noted that, despite the pseudonymous nature of blockchain transactions, there are methods for tracing users' real-world identities by analyzing their cryptocurrency transaction patterns, as transaction records on public blockchains such as Bitcoin are publicly accessible.⁶⁰ Specialized firms have

55. *Id.* at [8]–[9].

56. *Id.* at [20] (concluding that gateway 9 (claims in tort) applied because there was a good arguable case that the damage was sustained in England).

57. *Id.* at [40].

58. *Mooij v. Persons Unknown* [2024] EWHC (Comm) 814 (Eng.).

59. *Id.* at [54].

60. See Catchlove, *supra* note 4, at 3–4 (describing blockchain transaction records and the openness of public blockchains); *Contracts Ex Machina*, *supra* note 6, at 327 & n.74 (“Anyone can view a Bitcoin’s blockchain, and trace back transactions all the way to the original ‘genesis block’ created by Nakamoto.”); see also, e.g., *Chainalysis: The Blockchain*

developed the ability to de-anonymize users by tracking these transactional flows.⁶¹ Thus, although early perceptions of cryptocurrencies such as Bitcoin assumed complete anonymity—given that assets could be held without a bank account and without identity disclosure—most cryptocurrencies are not fully anonymous in practice.⁶²

Moreover, platforms subject to anti-money laundering (“AML”) regulations and know-your-customer (“KYC”) requirements are obligated to verify the identities of their users.⁶³ As a result, the identities of parties transacting on such platforms may be more readily ascertainable through regulatory or legal processes. In addition, permissioned blockchain networks, which

Data Platform, CHAINALYSIS, <https://www.chainalysis.com/> [<https://perma.cc/KM7L-47DT>] (last visited June 15, 2026) (leading U.S.-based blockchain analytics company providing software and tools to law enforcement agencies and financial institutions to trace cryptocurrency transactions and identify actors involved in illicit activity); *Investigations Case Scenarios When Analyzing Crypto*, CRYSTAL INTELLIGENCE (Nov. 29, 2021), <https://crystalintelligence.com/crypto-analytics-for-compliance/investigations/> [<https://perma.cc/FG86-8CZG>] (platform offering tools for analyzing cryptocurrency transactions, including capabilities to identify links between digital wallets and real-world entities); *How Blockchain Analytics Aids LEA’s in Tracing Crypto Assets to Off-Ramps*, MERKLE SCIENCE, <https://www.merklescience.com/how-blockchain-analytics-aids-leas-in-tracing-crypto-assets-to-off-ramps> [<https://perma.cc/Y45H-TATT>] (last visited June 21, 2026) (blockchain analytics company specializing in tools for law enforcement to monitor cryptocurrency flows and detect illicit activity).

61. See Bushansky, *supra* note 1, at 337.

62. *Id.* at 337–38; see Fergal Reid & Martin Harrigan, *An Analysis of Anonymity in the Bitcoin System* 26 (May 7, 2012) (unpublished manuscript), <https://arxiv.org/abs/1107.4524> [<https://perma.cc/V3RK-SB6E>] (“Using an appropriate network representation, it is possible to associate many public-keys with each other, and with external identifying information. With appropriate tools, the activity of known users can be observed in detail.”).

63. See FIN. ACTION TASK FORCE, GUIDANCE FOR A RISK-BASED APPROACH TO VIRTUAL ASSETS AND VIRTUAL ASSET SERVICE PROVIDERS 25–27, ¶¶ 90–92 (2019), <https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Updated-Guidance-VA-VASP.pdf.coredownload.inline.pdf> [<https://perma.cc/P2R8-ZFSX>] (requiring virtual asset service providers to implement customer due diligence measures); see also Directive (EU) 2015/849, of the European Parliament and of the Council of 20 May 2015 on the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing, art. 13(1)(a), 2015 O.J. (L 141) 73 (requiring obliged entities to identify their customers and verify their identities); Regulation (EU) 2023/1113, of the European Parliament and of the Council of 31 May 2023 on Information Accompanying Transfers of Funds and Certain Crypto-Assets and Amending Directive (EU) 2015/849, art. 38(2)(a), 2023 O.J. (L 150) 1 (amending Directive (EU) 2015/849 to bring crypto-asset service providers within the definition of “financial institution”).

require authorized access, may incorporate built-in verification mechanisms that further facilitate participant identification.⁶⁴ It is therefore plausible that, as smart contracts become more widely adopted, identity verification will become a central feature of commercial smart-contract platforms.⁶⁵

Accordingly, in cases where the claimant can identify both the identity and location of a defendant outside the forum, the initiation of proceedings typically requires judicial authorization for service of process abroad. In most jurisdictions, service outside the forum is subject to specific procedural rules designed to safeguard jurisdictional comity and procedural fairness.⁶⁶ Because service abroad may itself serve as a basis for the exercise of jurisdiction, courts approach such requests with particular caution.⁶⁷

In both common law and civil law systems, permission to effect service abroad generally depends on the existence of a recognized jurisdictional connection between the dispute and the forum.⁶⁸ These connecting factors are typically defined within a

64. See Bushansky, *supra* note 1, at 337–38 (“Furthermore, permissioned blockchain networks, which require explicit authorization for access, often incorporate identity verification protocols as a prerequisite for participation.”).

65. See LAW COMM’N (2021), *supra* note 7, at 44, ¶ 3.21 (“We expect that identity verification is likely to be a key feature of smart contract platforms which are developed for mainstream commercial use. In practice, we think it is unlikely that commercial parties will enter into smart legal contracts without being aware of the identity of their counterparty.”).

66. See Convention on the Service Abroad of Judicial and Extrajudicial Documents in Civil or Commercial Matters art. 1, Nov. 15, 1965, 20 U.S.T. 361, 658 U.N.T.S. 163 (“The present Convention shall apply in all cases, in civil or commercial matters, where there is occasion to transmit a judicial or extrajudicial document for service abroad.”); see also *Mullane v. Cent. Hanover Bank & Tr. Co.*, 339 U.S. 306, 314 (1950) (“An elementary and fundamental requirement of due process . . . is notice reasonably calculated, under all the circumstances, to apprise interested parties . . .”).

67. *Spiliada Mar. Corp. v. Cansulex Ltd.* [1987] AC 460 (HL) 476 (appeal taken from Eng.) (“The basic principle is that a stay will only be granted . . . where the court is satisfied that there is some other available forum . . . in which the case may be tried more suitably for the interests of all the parties and the ends of justice.”).

68. See Regulation (EU) 1215/2012, of the European Parliament and of the Council of 12 December 2012 on Jurisdiction and the Recognition and Enforcement of Judgments in Civil and Commercial Matters (Recast), 2012 O.J. (L 351) 1 [hereinafter *Brussels I Recast Regulation*]; see also *Int’l Shoe Co. v. Washington*, 326 U.S. 310, 316 (1945) (holding that “due process requires only that in order to subject a defendant to a judgment in personam, if he be not present within the territory of the forum, he have certain minimum contacts

structured framework—whether through statutory rules or jurisdictional doctrines—and are not indefinite in nature.⁶⁹ The claimant bears the burden of demonstrating not only the existence of a sufficient connection to the forum,⁷⁰ but also a *prima facie* case on the merits and, in many systems, that the forum constitutes an appropriate forum for adjudication.⁷¹

In the context of contractual disputes, the relevant connecting factors commonly include the place of contracting, the place of performance, and, in some systems, the place where the effects of non-performance occur.⁷² In addition, jurisdiction may, in certain circumstances, be established through a sufficiently close connection with the forum, such as where a branch, agency, or other establishment operates within its territory.⁷³ These factors serve to anchor the dispute within a particular legal system and justify the exercise of jurisdiction over defendants located outside the forum.⁷⁴

Once the identity and location of the relevant party have been established, those personal affiliations may themselves constitute independent jurisdictional connecting factors, and may also assume significance in the subsequent choice-of-law analysis.⁷⁵

with it such that the maintenance of the suit does not offend ‘traditional notions of fair play and substantial justice.’”).

69. See, e.g., Brussels I Recast Regulation, *supra* note 68, recital 15 (“The rules of jurisdiction should be highly predictable and founded on the principle that jurisdiction is generally based on the defendant’s domicile . . .”).

70. See *Spiliada*, [1987] AC at 476–78 (“The basic principle is that a stay will only be granted . . . where the court is satisfied that there is some other available forum . . . in which the case may be tried more suitably for the interests of all the parties and the ends of justice.”).

71. See *Brownlie v. Four Seasons Holdings Inc.* [2017] UKSC 80, [5]–[7] (appeal taken from Eng.); *Can. Tr. Co. v. Stolzenberg* (No. 2) [1998] 1 WLR 547 (CA) (Eng.) (holding that the applicable standard is a “good arguable case”).

72. See RESTATEMENT (SECOND) OF CONFLICT OF LAWS § 188(2)(a), (c) (A.L.I. 1971) (identifying “the place of contracting” and “the place of performance” as relevant contacts).

73. See Brussels I Recast Regulation, *supra* note 68, art. 7(5).

74. See *id.* arts. 7(1), 7(2), 7(5); see also *Int’l Shoe Co. v. Washington*, 326 U.S. 310, 316 (1945); *Calder v. Jones*, 465 U.S. 783, 789–90 (1984); *Burger King Corp. v. Rudzewicz*, 471 U.S. 462, 475 (1985).

75. See Brussels I Recast Regulation, *supra* note 68, arts. 4(1), 63(1) (providing that persons domiciled in a Member State shall, whatever their nationality, be sued in the courts of that Member State); see also RESTATEMENT (SECOND) OF CONFLICT OF LAWS § 188(2)(e) (identifying “the domicile, residence, nationality, place of incorporation and place of business of the parties” as relevant choice-of-law contacts); *Daimler AG v. Bauman*,

Notwithstanding the foregoing, even where a sufficient jurisdictional connection can be established and effective service of process achieved, a distinct and equally significant challenge arises in determining the territorial locus of smart-contract activity for the purposes of jurisdictional determination. Part V therefore examines the difficulties inherent in applying traditional connecting factors within a decentralized virtual blockchain environment.

IV. COMPARATIVE RESPONSES TO JURISDICTIONAL CHALLENGES IN DIGITAL TRANSACTIONS

Although smart contracts introduce novel technological features, the jurisdictional challenges they generate are not entirely unprecedented. Similar difficulties have long been recognized in the context of cross-border electronic commerce and internet-based transactions, where the dematerialized nature of digital interactions has complicated the application of territorially grounded rules governing jurisdiction, applicable law, and enforcement.⁷⁶ As observed in the private international law literature, where an activity has no clear geographical anchor, legal claims, regulatory assertions, and competing normative frameworks may extend across multiple jurisdictions.⁷⁷ These challenges have prompted both public and private regulatory responses at the international level.⁷⁸

571 U.S. 117, 137 (2014) (observing that “the place of incorporation and principal place of business are paradigm . . . bases for general jurisdiction.”).

76. See JONATHAN HILL, *CROSS-BORDER CONSUMER CONTRACTS* 133 (2008) (“E-commerce presents certain challenges to the traditional, territorial approach to questions of jurisdiction.”). See generally Zhen Chen, *Internet, Consumer Contracts and Private International Law: What Constitutes Targeting Activity Test?*, 32 *INFO. & COMM’NS TECH. L.* 23, 27 (2023).

77. See SVANTESSON, *supra* note 18, at vii (“[W]here there is no obvious ‘there’ there, laws easily get spread everywhere.”); see also *id.* at xii (“As far as private international law is concerned, I take such a broad view that I include not only the question of jurisdiction, as such, but also the related matters of applicable law, the possibilities of declining jurisdiction, and the matters of recognition and enforcement.”).

78. *Id.* at 91–112 (discussing “key court decisions, legislation as well as developments in the academic thinking on the topic.”).

A. Public Harmonization

The regulatory responses to these challenges have generally developed along two principal paths. The first seeks to promote greater uniformity and harmonization through international conventions, international organizations, and transnational legislative initiatives—with the aim of reducing fragmentation among national legal systems and enhancing cross-border legal certainty, regulatory coordination, and institutional cooperation.⁷⁹ In the context of globalization and cross-border electronic commerce, scholarly commentary has expressed cautious optimism regarding the capacity of such harmonization initiatives to produce meaningful convergence.⁸⁰ At the same time, other commentators have emphasized the structural limitations of this approach, pointing in particular to the practical and political difficulties inherent in achieving substantive consensus among states on questions of regulatory policy.⁸¹

While these initiatives may enhance predictability in cross-border transactions, their effectiveness remains constrained by the absence of universally accepted solutions to jurisdictional questions arising in decentralized digital networks.⁸²

79. See, e.g., U.N. COMM'N ON INT'L TRADE L., UNCITRAL MODEL LAW ON ELECTRONIC COMMERCE WITH GUIDE TO ENACTMENT 1996, WITH ADDITIONAL ARTICLE 5 BIS AS ADOPTED IN 1998, at 2, U.N. Sales No. E.99.V.4 (1999) (“[T]he establishment of a model law . . . acceptable to States with different legal, social and economic systems, could contribute significantly to the development of harmonious international economic relations.”); Convention on the Recognition and Enforcement of Foreign Judgments in Civil or Commercial Matters, pmbl., July 2, 2019, <https://www.hcch.net/en/instruments/conventions/full-text/?cid=137> [<https://perma.cc/M3M4-36UJ>] (“Convinced that such enhanced judicial co-operation requires, in particular, an international legal regime that provides greater predictability and certainty in relation to the global circulation of foreign judgments . . .”).

80. See, e.g., SVANTESSON, *supra* note 18, at vii (“The deleterious effects of the quagmire are increasingly felt as globalization, marching hand-in-hand with digitalization, continues to compress the world.”).

81. See GOLDSMITH & WU, *supra* note 16, at 171–72.

82. See Jack Goldsmith, *Unilateral Regulation of the Internet: A Modest Defence*, 11 EUR. J. INT'L L. 135, 135, 145–46 (2000) (observing that “the prospects for such harmonization are generally dim in many contexts.”).

B. Private Ordering and Technological Self-Regulation

A second regulatory response has emerged through mechanisms commonly described as private ordering or self-regulation. Under this model, market participants—rather than sovereign states—assume responsibility for structuring the normative framework governing their transactions.⁸³ This may include, *inter alia*, the establishment of substantive contractual rules, the design of dispute-resolution mechanisms, and the implementation of enforcement mechanisms capable of securing compliance with privately generated outcomes.⁸⁴

The private regulation of smart contracts in the context of dispute resolution has likewise received considerable scholarly attention. In particular, commentators have proposed integrating dispute-resolution mechanisms directly into smart-contract architecture. These mechanisms may include online dispute resolution systems, decentralized arbitration protocols, and oracle-based intervention mechanisms embedded within the contractual code itself, capable of suspending, modifying, or otherwise influencing contractual execution in response to external determinations.⁸⁵ Under such models, contractual code may incorporate a designated third party—whether human, institutional, or algorithmic—authorized to resolve disputes arising during performance and communicate the outcome of the dispute-resolution process to the smart contract through an oracle mechanism.⁸⁶ In this way, dispute resolution becomes integrated

83. See Jonathan Rohr & Aaron Wright, *Blockchains, Private Ordering, and the Future of Governance*, in *REGULATING BLOCKCHAIN: TECHNO-SOCIAL AND LEGAL CHALLENGES* 43, 43–44 (Philipp Hacker et al. eds., 2019) (arguing that, despite the possibility that it will allow parties to rely less on the governance arrangements currently provided by traditional business organizations, it is nonetheless consistent with American business law's "enabling" approach and the significant room it leaves for private ordering).

84. See Orna Rabinovich-Einy & Ethan Katsh, *Blockchain and the Inevitability of Disputes: The Role for Online Dispute Resolution*, 2019 J. DISP. RESOL. 47, 59–63.

85. See Pietro Ortolani, *The Impact of Blockchain Technologies and Smart Contracts on Dispute Resolution: Arbitration and Court Litigation at the Crossroads*, 24 UNIF. L. REV. 430, 438–40 (2019).

86. See, e.g., Stefan Thomas & Evan Schwartz, *Smart Oracles: A Simple, Powerful Approach to Smart Contracts*, BIIA (July 2, 2017), <https://www.biiia.com/smart-oracles-a-simple-powerful-approach-to-smart-contracts/> [https://perma.cc/9P27-DTWB] (describing smart oracles as mechanisms that relay external real-world data to blockchain-based contractual systems); Kristian Lauslahti, Juri Mattila & Timo Seppälä,

into the technological infrastructure of contractual performance itself.⁸⁷

Scholarly commentary has nevertheless recognized the potential drawbacks and normative concerns associated with the implementation of such mechanisms, which may erode some of the defining characteristics of smart contracts. To the extent that such mechanisms depend upon the intervention of an external actor—whether human, institutional, or algorithmic—they necessarily reintroduce an element of exogenous trust into a system designed to operate in a trust-minimized environment.⁸⁸ As a result, the parties' reliance on the functional integrity of the technological infrastructure becomes, at least in part, contingent upon their confidence in actors external to that infrastructure. This may undermine one of the core functional premises of blockchain-based contracting—namely, the creation of trust in a trustless environment through technological verification rather than human intermediation.⁸⁹ In this respect, the implementation of such mechanisms may diminish some of the distinctive characteristics and functional advantages traditionally associated with smart contracts.⁹⁰

Accordingly, while both public harmonization and private ordering provide partial responses to the jurisdictional challenges

Smart Contracts – How Will Blockchain Technology Affect Contractual Practices? 17 (ETLA Reports No. 68, Jan. 9, 2017), <https://www.etla.fi/wp-content/uploads/ETLA-Raportit-Reports-68.pdf> [<https://perma.cc/S7KV-2MR9>] (explaining that smart contracts may depend on trusted external data feeds for verification of off-chain events).

87. See Amy J. Schmitz & Colin Rule, *Online Dispute Resolution for Smart Contracts*, 2019 J. DISP. RESOL. 103, 117–23; see also Farshad Ghodoosi, *Contracting in the Age of Smart Contracts*, 96 WASH. L. REV. 51, 84–90 (2021).

88. See Nick Szabo, *Smart Contracts: Building Blocks for Digital Markets*, EXTROPY, no. 16, 1996, https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html [<https://perma.cc/8TXY-8ANJ>]; see also Bushansky, *supra* note 1, at 318–20.

89. See Bushansky, *supra* note 1, at 335–36 (“However, critics note that this approach undermines the trustless nature of smart contracts by introducing reliance on an external adjudicator, thereby compromising the conceptual integrity of the system.”).

90. See, e.g., Eliza Mik, *Smart Contracts: A Requiem*, 36 J. CONT. L. 70, 76 (2020) (“The contracting parties must rely on third parties (so-called ‘oracles’) that confirm delivery and, if possible, conformance. As ‘oracles’ exist outside of the blockchain, they are not ‘trustless’ and there is no technical mechanism preventing them from misrepresenting outside events or providing incorrect information. Consequently, the ‘trustless’ character of the blockchain is of little value if ‘smart contracts’ must rely on sources of information, which are not ‘trustless.’”); see also Mik, *supra* note 38, at 298.

of digital commerce, neither eliminates the need for territorially grounded connecting factors capable of allocating judicial authority in disputes arising from blockchain-based transactions. The analysis developed in this Article therefore proceeds on the premise that, notwithstanding technological innovation, the identification of legally significant territorial connections remains indispensable to the operation of private international law.

V. IDENTIFYING THE APPROPRIATE FORUM IN SMART CONTRACTS

The interaction between smart contracts and the connecting factors of private international law gives rise to several conceptual and practical challenges. These difficulties concern both the determination of the place of contracting and performance or non-performance, as well as the identification of the place of business or residence of an agent or representative acting on behalf of a party.⁹¹ This Part therefore analyzes these connecting factors across the different configurations of smart contracts, each of which exhibits a distinct degree of connection to the physical world for the purposes of forum determination.

Before turning to each connecting factor separately, it is necessary to address a broader difficulty common to all of them: the localization of legally relevant conduct in digital environments. This difficulty reflects a well-established challenge in private international law: the characterization of cyberspace as a non-territorial or a-territorial domain.⁹² Cyberspace does not exist in any single geographical location; rather, it operates simultaneously across multiple jurisdictions. As a result, attempts to anchor legally relevant conduct to a particular territorial framework become inherently problematic.

However, these challenges are not entirely novel. Similar issues have long arisen in the context of the internet and cross-

91. See Bushansky, *supra* note 1, at 333 (“Smart contract engagements thus pose a significant challenge to the traditional doctrines of jurisdiction and choice of law, demanding doctrinal re-evaluation and adaptation.”); see also LAW COMM’N (2021), *supra* note 7, at 200, ¶ 7.145; Jeanette Hofmann, *Internet Governance: A Regulative Idea in Flux*, in INTERNET GOVERNANCE: AN INTRODUCTION 96–97 (Ravi Kumar Jain Bandamutha ed., 2007).

92. See HILL, *supra* note 76, at 133.

border digital activity. While the digital environment itself may lack physical boundaries, the actors operating within it remain individuals or legal entities situated in identifiable locations.⁹³ Their activities are conducted from tangible and geographically defined places, even when conducted through digital or online environments, and are ultimately initiated, directed, and economically realized from such locations.⁹⁴ Accordingly, legal systems have progressively adapted jurisdictional principles to the realities of internet-based activity, recognizing that online conduct may give rise to legally relevant connections with multiple jurisdictions simultaneously.⁹⁵ This insight is directly relevant to smart contracts, which both replicate and intensify these challenges through their decentralized and automated nature.

A. *The Place of Contracting*

The determination of the place of contracting in the context of smart contracts depends fundamentally on the specific configuration through which the contract is formed.⁹⁶ In the default configuration, the default bilingual configuration, and configurations involving the autonomous interaction of computer programs, this determination becomes particularly complex.⁹⁷ At first glance, the place of contracting in such configurations appears to be the blockchain network itself—a virtual environment lacking a fixed territorial location and therefore devoid of a clearly identifiable territorial nexus.⁹⁸

93. See Jack L. Goldsmith, *Against Cyberanarchy*, 65 U. CHI. L. REV. 1199, 1250 (1998) (“Cyberspace transactions are no different from ‘real-space’ transnational transactions. They involve people in real space in one jurisdiction communicating with people in real space in other jurisdictions in a way that often does good but sometimes causes harm.”).

94. See *id.*

95. See Joined Cases C-509/09 & C-161/10, *eDate Advert. GmbH v. X*, 2011 E.C.R. I-10269; see also *Zippo Mfg. Co. v. Zippo Dot Com, Inc.*, 952 F. Supp. 1119, 1124 (W.D. Pa. 1997).

96. See *supra* Part II; see also LAW COMM’N (2021), *supra* note 7, at 171–73, ¶¶ 7.18–7.25.

97. See *supra* notes 22–37 and accompanying text.

98. See LAW COMM’N (2021), *supra* note 7, at 173, ¶ 7.24 (“For solely code smart legal contracts that are formed by the autonomous interaction of computer programs, there is an even greater degree of uncertainty, and a greater variety of possibilities. For example, the contract could be said to be formed either at the place where Bob is located at the moment when his computer program accepts the offer, or at the place where Bob is located

In the default and default bilingual configurations, the parties operating the smart contract on a blockchain network are natural persons acting from identifiable, physical locations. At first glance, one may argue that the place of contracting is the place where the offeror receives the offeree's acceptance.⁹⁹ However, in the context of these smart-contract configurations, no express communication of acceptance is transmitted. Rather, acceptance is manifested through conduct.¹⁰⁰ Where the offer invites acceptance by performance, the contract is concluded upon the performance of the requested act.¹⁰¹ In such cases, the act simultaneously fulfills both elements of acceptance: it evidences the offeree's intent to be bound, and constitutes the performance of the contractual obligation itself.¹⁰² In these circumstances, the localization of acceptance for jurisdictional purposes becomes inherently uncertain.

One may therefore argue that the contract is formed in the place where the offeree was located at the time of acceptance by conduct—namely, upon the transfer of a digital asset or cryptocurrency to the offeror. On the other hand, it may be argued that the contract is formed in the place where the offeror was located at the moment such acceptance by conduct occurred.¹⁰³ In

at the moment when his acceptance is communicated to Alice (if that occurs). Or, the smart legal contract could be said to be formed at the place where Alice is located at the moment that acceptance takes place, or at the place where Alice is located at the moment when that acceptance is communicated. As a further alternative, if the computer programs are running on distributed ledgers, it may be that the place of contract formation is determined by the location of some quantity of participating nodes.”).

99. *Entores Ltd. v. Miles Far East Corp.* [1955] 2 QB 327 (CA) (Eng.); RESTATEMENT (SECOND) OF CONTRACTS § 64 (A.L.I. 1981).

100. Bushansky, *supra* note 1, at 307–08 (“[O]nce the actions of the offeree, through their conduct, constitute full acceptance in accordance with the terms encoded in the smart contract.”).

101. *See id.*

102. *See* RESTATEMENT (SECOND) OF CONTRACTS § 50(2) (“Acceptance by performance requires that at least part of what the offer requests be performed . . .”); *see also id.* § 54(1) (providing that no notification of acceptance is necessary where acceptance is rendered by performance).

103. *See* LAW COMM’N (2021), *supra* note 7, at 173, ¶ 7.23 (“For unilateral solely code smart legal contracts, there is a degree of uncertainty about the place of contract formation. The smart legal contract could be said to be formed at the place where Bob performs the act specified in the deployed code, albeit this location might be something over which Alice has little control. Alternatively, it could be said to be formed at the place where Alice has the acceptance communicated to her (if that occurs), despite the fact that

what follows, this Article argues that it is appropriate, on policy grounds, to prefer one of these alternatives over the other.

The configuration involving the autonomous interaction of computer programs further intensifies this uncertainty, as the processes of offer and acceptance are carried out entirely by software, without any human involvement.¹⁰⁴ This stands in contrast to the default configurations, in which acceptance is manifested through the offeree's conduct—namely, the use of a private key to transfer control over a digital asset or cryptocurrency in accordance with the terms embedded in the code.¹⁰⁵

By contrast, in the hybrid configuration, where the smart contract is accompanied by a natural-language agreement, the place of contracting may be easier to identify if the contract is deemed to be formed upon execution of that natural-language document. If, however, the contract is considered to be formed only when the code is deployed to the blockchain, the analysis may again produce either no clear territorial connection or several plausible connecting factors.¹⁰⁶ Accordingly, the determination of the place of contracting in hybrid configurations remains fact-sensitive and depends upon the relationship between the natural-language agreement, the coded terms, and the act of deployment.¹⁰⁷

However, given that this configuration typically involves prior real-world negotiations, it may be appropriate to take into account the location of those negotiations as part of the relevant connecting factors linking the dispute to the forum.¹⁰⁸ The rationale for this approach lies in the virtual nature of blockchain networks. Rather than relying exclusively on a purely technical analysis of contract formation, it may be appropriate to take into account tangible and

actual communication of acceptance is not typically required for the formation of unilateral contracts. Finally, it could be formed at some other place(s).”).

104. See *supra* notes 22–24 and accompanying text.

105. See *supra* notes 25–27 and accompanying text.

106. See *supra* notes 45–50 and accompanying text.

107. See LAW COMM'N (2021), *supra* note 7, at 173, ¶ 7.25.

108. See *Burger King Corp. v. Rudzewicz*, 471 U.S. 462, 479 (1985) (“prior negotiations . . . must be evaluated”); see also *Joined Cases C-585/08 & C-144/09, Pammer v. Reederei Karl Schlüter GmbH & Co. KG*, 2010 E.C.R. I-12527 (assessing whether activities were directed to a Member State in light of pre-contractual conduct).

identifiable real-world connections, including the location where negotiations occurred.¹⁰⁹

A similar analysis applies to the traditional-virtual configuration, which likewise involves a pre-existing relationship between the parties in the physical world.¹¹⁰ In such cases, the parties reach agreement through real-world interactions, which are subsequently expressed in the code of the smart contract.¹¹¹ Although the smart contract is ultimately deployed and executed on the blockchain, the same considerations arise as in the hybrid configuration. Accordingly, the determination of the place of contracting remains fact-dependent. Where the contract is deemed to be formed upon its deployment to the blockchain, it may be preferable to avoid a purely technical approach and instead take into account the location where the negotiations took place as part of the overall assessment of the dispute's connection to the forum.

B. The Place of Performance and Non-Performance

As a matter of private international law, the place of performance of a contractual obligation constitutes a well-recognized connecting factor for the purpose of determining the appropriate forum. In the European Union, a defendant may be sued, in matters relating to a contract, in the courts of the place of performance of the obligation in question.¹¹² Under US law, while no formal rule designates the place of performance as an independent jurisdictional ground, the failure to perform contractual obligations required to be carried out in the forum—namely, the place where the obligation ought to have been performed but was not—may nevertheless establish a sufficient connection for the exercise of jurisdiction.¹¹³

109. See SVANTESSON, *supra* note 18, at 106; see also *Spiliada Mar. Corp. v. Cansulex Ltd.* [1987] AC 460 (HL) 476 (appeal taken from Eng.).

110. See *supra* notes 38–43 and accompanying text.

111. See *supra* notes 39–40 and accompanying text.

112. See Brussels I Recast Regulation, *supra* note 68, art. 7(1) (conferring jurisdiction at the place of performance of the obligation in question).

113. See *Burger King*, 471 U.S. at 463–64 (describing Florida's long-arm statute, which reaches a person who breaches a contract in the state by failing to perform acts required by the contract to be performed there); see also Brussels I Recast Regulation, *supra* note 68, art. 7(1)(a)–(b) (providing jurisdiction "in the courts for the place of performance of the obligation in question," including the place where goods "were

From a general perspective, performance, in the context of smart contracts, has been argued to be characterized by a high degree of certainty, in light of their autonomous, deterministic, and irreversible execution mechanisms—thereby reducing the likelihood of disputes.¹¹⁴ However, while smart contracts may significantly reduce the risk of non-performance, they do not preclude situations in which performance is defective or does not correspond to the parties' intentions.¹¹⁵ Accordingly, this characterization does not displace the relevance of performance as a connecting factor. Rather, it tends to obscure the fact that, even in such systems, the relevance of the place of performance remains a vital connecting factor for jurisdictional purposes.

The place of non-performance should be determined by reference to the place of performance of the obligation in question, rather than by reference to the incidental or fortuitous location of a party at the time of non-performance. This approach reflects the need for commercial certainty, legal clarity, and the protection of the legitimate expectations of the counterparty.¹¹⁶ The place of performance is determined by the nature of the obligation in question.¹¹⁷ In the case of an obligation to deliver goods, the place of performance—and thus the place of non-performance—is generally identified as the agreed place of delivery, or, in the absence of such agreement, the place where the goods were delivered or should have been delivered.¹¹⁸ In the case of an obligation to provide services, the place of performance is generally the place where the services are provided or should have been provided.¹¹⁹ By contrast, in the case of an obligation to make payment, the place of performance is generally the place where the

delivered or should have been delivered" or services "were provided or should have been provided.").

114. See LAW COMM'N (2021), *supra* note 7, at 134–35, ¶ 5.109.

115. *Id.* at 142, ¶ 5.136 ("This feature of automaticity entails that, in practice, breach of contract is more likely to be in the form of defective performance, rather than non-performance of the smart legal contract.").

116. See Case C-386/05, *Color Drack GmbH v. Lexx Int'l Vertriebs GmbH*, 2007 E.C.R. I-3699, ¶ 20; see also Case C-204/08, *Rehder v. Air Baltic Corp.*, 2009 E.C.R. I-6073, ¶¶ 6, 45.

117. See Brussels I Recast Regulation, *supra* note 68, art. 7(1)(b).

118. See *id.*; see also Case C-381/08, *Car Trim GmbH v. KeySafety Sys. Srl*, 2010 E.C.R. I-1255, ¶ 60.

119. See Brussels I Recast Regulation, *supra* note 68, art. 7(1)(b).

payment is to be received, usually the creditor's place of business, unless otherwise agreed.¹²⁰

The central question, however, is how the place of performance is to be identified in the context of blockchain-based transactions. Framed in doctrinal terms, this requires determining where the place of performance should be located, having regard to the nature of the obligation in question. This inquiry must be approached in light of the functional characteristics of smart contracts. As has been observed, execution certainty presupposes that performance is carried out entirely within the blockchain environment, without reliance on external intervention and with complete immunity from human interference.¹²¹ Accordingly, such transactions must involve digital assets or tokenized representations of assets capable of autonomous on-chain transfer.¹²² By contrast, obligations involving the provision of services, the performance of work, physical delivery, or payment in fiat currency necessarily depend on off-chain processes and human facilitation, and are therefore incompatible with purely autonomous execution.¹²³ Smart-contract transactions are thus, by their nature, more closely aligned with obligations concerning the transfer of digital assets or digital payments, rather than with contracts for the provision of services.

In blockchain-based transactions, delivery and payment obligations converge functionally: Both are performed through the transfer of control over a digital asset or cryptocurrency to the receiving party, that is, to the recipient's public address.¹²⁴ Control is exercised through a digital wallet, in which a private key is linked to that public address—the mechanism by which transactions are executed on the blockchain.¹²⁵ Given that such a public address lacks an inherent geographical location, identifying an appropriate territorial anchor raises a fundamental difficulty, as it is unclear

120. See Case 14/76, *De Bloos v. Bouyer*, 1976 E.C.R. 1497; see also *Burger King Corp. v. Rudzewicz*, 471 U.S. 462, 480 (1985); RESTATEMENT (SECOND) OF CONFLICT OF LAWS § 195.

121. See Bushansky, *supra* note 1, at 317–18.

122. *Id.* at 314.

123. *Id.*

124. *Id.* at 322–23.

125. *Id.*

whether reference should be made to the location of the holder's economic activity, or some other connecting factor.¹²⁶

C. *The Place of Intermediaries*

In determining jurisdiction, the activities carried out through an intermediary may, in limited circumstances, be taken into account where that intermediary forms part of a place of business having an appearance of permanency and acts as an extension of the defendant in its dealings with third parties.¹²⁷ This reflects a functional approach to jurisdiction, under which the identification of the appropriate forum is informed not only by the formal parties to the dispute, but also by the operational reality through which the relevant transaction is conducted. However, jurisdiction on that basis may be exercised only where the dispute arises out of the operations carried out through that intermediary.¹²⁸

Against this doctrinal background, a comparable question arises in the context of smart contracts, where a programmer may participate in the formation or deployment of the agreement. Where such a programmer acts on behalf of one or both parties and plays a substantial role in structuring and implementing the transaction, it may be argued that the programmer performs a function analogous to that of an intermediary whose activities may, in appropriate circumstances, be taken into account for jurisdictional purposes. In such circumstances, and subject to a sufficiently close connection between the dispute and the programmer's activities, the place of the programmer's professional activity may serve as a relevant jurisdictional connecting factor. The relevance of this connecting factor in the context of smart contracts is not uniform and should therefore be assessed on a configuration-by-configuration basis, having regard

126. See *Contracts Ex Machina*, *supra* note 6, at 371 ("The parties to a smart contract, at a technical level, are not people. They are cryptographic private keys. The secret private key represents the individual, based on a mathematical relationship with the associated public key.").

127. See Brussels I Recast Regulation, *supra* note 68, art. 7(5); see also Case 33/78, *Somafer SA v. Saar-Ferngas AG*, 1978 E.C.R. 2183, ¶ 12 (interpreting the predecessor provision, art. 5(5) of the Brussels Convention).

128. See Brussels I Recast Regulation, *supra* note 68, art. 7(5).

to the nature, extent, and legal significance of the programmer's involvement in the process of contract formation.

In the default and default bilingual configurations, this connecting factor is devoid of practical significance, as no third party participates in the formation of the agreement beyond the contracting parties themselves.¹²⁹ In such configurations, the offeror may independently encode its offer in the form of a smart contract, or may rely on a standardized contractual template supplied by the platform on which the parties operate¹³⁰—an option available in contemporary blockchain-based transactions. Even where the offeror engages a programmer acting exclusively on its own behalf in preparing the smart contract, such programmer remains uninvolved in the contractual relationship *vis-à-vis* the counterparty and therefore lacks independent jurisdictional significance. More fundamentally, the likelihood that the counterparty will know, let alone be in a position to verify, the programmer's identity or place of business will generally be remote.

The position differs, however, in the hybrid and traditional-virtual configurations, in which the involvement of a programmer may become legally significant. In the hybrid and traditional-virtual configurations, where a programmer known to and accepted by both parties encodes and deploys the smart contract on their behalf, such programmer may plausibly be regarded as their functional intermediary, and the programmer's place of business or habitual residence may serve as a relevant jurisdictional connecting factor.

A distinct question arises in the autonomous-interaction configuration, in which each party acts through separate software agents independently programmed and deployed onto the blockchain. This gives rise to two related questions: first, whether

129. See *supra* notes 25, 36 and accompanying text.

130. See *Contracts Ex Machina*, *supra* note 6, at 375 (footnote omitted) ("Already, organizations involved in the development of smart contract platforms are starting to create templates that embody best practices for smart contract drafting. Using these templates, parties could avoid repeating mistakes in prior smart contracts, and they could draw on the expertise of industry groups carefully thinking about potential pitfalls."); see also Raskin, *supra* note 5, at 310; Klass, *supra* note 28, at 101 ("Or users might obtain the software from a third-party vendor that gives them access to the code.").

software may itself be regarded as the functional equivalent of an agent acting on behalf of the party that deployed it; and second, whether the activities of the programmers who designed and deployed such software may, in appropriate circumstances, be taken into account by analogy to the intermediary-based jurisdictional principles discussed above. While the former question raises an important theoretical issue concerning the legal status of autonomous software, it is of limited practical significance for present purposes, as software operating within a virtual environment lacks any independent territorial connection and therefore contributes little to the identification of a relevant forum.¹³¹ By contrast, the programmers who designed and deployed those systems on behalf of each contracting party remain natural persons possessing an identifiable place of business or habitual residence and may therefore provide a meaningful territorial anchor. To the extent that their identity and location are known, this connecting factor may be applied without difficulty. Practical difficulties may nevertheless arise where each party relies on a different programmer whose identity or location has not been disclosed to the counterparty, thereby limiting the practical utility of this connecting factor.

VI. APPLICABLE LAW IN SMART-CONTRACT DISPUTES

The difficulties identified in the preceding discussion of jurisdictional connecting factors re-emerge, albeit in a distinct doctrinal context, in determining the law applicable to smart-contract disputes. Whereas jurisdictional analysis seeks to identify the appropriate forum for adjudication, choice-of-law analysis seeks to identify the legal system bearing the closest substantive connection to the contractual relationship.¹³² To that end, private

131. See LAW COMM'N (2021), *supra* note 7, at 177, ¶ 7.44 ("We have considered whether a computer program, which has autonomously reached an agreement that binds the relevant party to the smart legal contract, could be regarded as that party's agent. We have concluded that it could not."); see also *id.* at 178, ¶ 7.46 ("[A] computer program cannot be an 'agent' because only a person with a 'mind' can be an agent at law." (citing *R (Software Sols. Partners Ltd.) v. HM Customs & Excise* [2007] EWHC (Admin) 971, [67] (Eng.))).

132. See LAW COMM'N, DIGITAL ASSETS AND (ELECTRONIC) TRADE DOCUMENTS IN PRIVATE INTERNATIONAL LAW 14, ¶ 2.26 (Consultation Paper No. 273, 2025) (UK) [hereinafter LAW COMM'N (2025)].

international law traditionally relies on a series of established connecting factors, including the place of contracting, the place of negotiation, the place of performance, the location of the contractual subject matter, and the territorial affiliations of the contracting parties.¹³³ At the same time, neither European nor American choice-of-law doctrine treats these connecting factors as exhaustive. Rather, both preserve sufficient methodological flexibility to take account of other circumstances materially relevant to determining the legal system most closely connected to the dispute.¹³⁴

The factual and technological complexities affecting several of these connecting factors in the context of smart contracts have already been examined in the preceding jurisdictional analysis.¹³⁵ Those difficulties need not be rehearsed here. As a preliminary matter, however, the application of each connecting factor remains contingent upon the identification of the relevant smart-contract configuration, since the territorial significance of any particular contact depends upon the degree to which the transaction remains connected to off-chain commercial activity.¹³⁶ The present discussion instead focuses on the choice-of-law implications of those same connecting factors, and whether blockchain-based transactions generate additional territorially relevant connecting factors bearing on the determination of the applicable law. In what follows, this Article develops a policy-based framework for resolving conflicts between competing territorial connections in determining the applicable law.

A. The Place of Contracting

For the reasons discussed in the preceding jurisdictional analysis, the place of contracting gives rise to competing territorial connections in the default, default bilingual, and autonomous

133. See Regulation (EC) 593/2008, of the European Parliament and of the Council of 17 June 2008 on the Law Applicable to Contractual Obligations (Rome I), arts. 4(1)–(4), 2008 O.J. (L 177) 6, 10–11 [hereinafter Rome I Regulation]; see also RESTATEMENT (SECOND) OF CONFLICT OF LAWS § 188(2).

134. See Rome I Regulation, *supra* note 133, art. 4(3); RESTATEMENT (SECOND) OF CONFLICT OF LAWS §§ 6, 188.

135. See *supra* Part V.

136. See *supra* Part II.

interaction of computer programs configurations.¹³⁷ By contrast, in hybrid and traditional-virtual configurations, the parties maintain a prior off-chain relationship and reach substantive agreement before the deployment of the code. In such cases, the place where the parties reached their substantive agreement may constitute a particularly significant territorial connection, reducing the uncertainty associated with identifying the place of contracting by reference to the subsequent deployment of the smart contract onto the blockchain.

B. The Place of Negotiation

The place of negotiation constitutes an additional connecting factor capable of identifying the legal system most closely connected to the contractual relationship.¹³⁸ As demonstrated in the preceding analysis, this connecting factor is of little practical significance in the default, default bilingual, and autonomous interaction of computer programs configurations, where no negotiation takes place between the parties prior to the execution of the smart contract.¹³⁹

By contrast, in hybrid and traditional-virtual configurations, where the parties negotiate the substantive terms of their transaction before deploying the smart contract, the place of negotiation may, in appropriate circumstances, provide a particularly significant territorial connection for purposes of determining the applicable law.¹⁴⁰

C. The Place of Performance and Non-Performance

For the reasons developed in the preceding jurisdictional analysis, the determination of the place of performance—and, correspondingly, the place of non-performance—in blockchain-based transactions gives rise to competing territorial connections.¹⁴¹ As demonstrated above, where performance

137. See *supra* notes 24, 32, 36 and accompanying text.

138. See Rome I Regulation, *supra* note 133, art. 4(3); RESTATEMENT (SECOND) OF CONFLICT OF LAWS § 188.

139. See *supra* Part II.

140. See *supra* Part II.

141. See *supra* Part V.B.

consists of the on-chain transfer of control over digital assets or cryptocurrency, the absence of any inherent geographical location associated with the receiving address renders the territorial localization of performance inherently uncertain. The same uncertainty necessarily carries over into the choice-of-law context.

As discussed in the preceding jurisdictional analysis, payment obligations in blockchain-based transactions raise distinct territorial questions, notwithstanding their doctrinal characterization as a form of contractual performance. Accordingly, where payment constitutes the economically significant obligation in dispute, the applicable law may ultimately be influenced by the situs attributed to the relevant crypto-asset, a question addressed further below in connection with the location of the contractual subject matter.

D. The Location of the Contractual Subject Matter

The location of the contractual subject matter may provide an independent territorial connection where the transaction concerns identifiable assets. In the context of smart contracts, this connecting factor assumes particular importance where the transaction involves crypto-assets, tokenized assets, or other forms of digitally represented property.¹⁴²

This issue has received particular attention in both academic commentary and recent judicial practice. In *Ion Science Ltd. v. Persons Unknown* and *Fetch.ai Ltd. v. Persons Unknown*, both involving applications for urgent injunctive relief aimed at preventing the dissipation of crypto-assets allegedly obtained by fraud, the English Commercial Court adopted the view advanced by Andrew Dickinson that, for conflict-of-laws purposes, a crypto-asset is located in the place where its owner is domiciled or habitually resident.¹⁴³

142. See Rome I Regulation, *supra* note 133, arts. 4(2), 19(1)–(2); RESTATEMENT (SECOND) OF CONFLICT OF LAWS § 188(2)(d); see also LAW COMM’N (2025), *supra* note 132, at 12–13, ¶¶ 2.15–2.21, 23, ¶¶ 2.72–2.76 (explaining that the location of an object of property rights is a territorial connecting factor and discussing the difficulty of applying location-based rules to modern digital assets); *id.* at 3, ¶ 1.17 (recognizing crypto-tokens and certain other digital assets as objects of property rights).

143. *Ion Science Ltd. v. Persons Unknown* (unreported, Dec. 21, 2020) (Comm. Ct. (Eng.)); *Fetch.ai Ltd. v. Persons Unknown* [2021] EWHC (Comm) 2254 (Eng.); Andrew

To the extent that this approach gains broader acceptance, it may provide a meaningful territorial anchor for blockchain-based transactions. Difficulties nevertheless remain. Smart-contract transactions frequently involve two distinct assets: first, the digital or tokenized asset constituting the substantive object of the transaction; and second, the cryptocurrency transferred as consideration, which is itself capable of proprietary characterization as an asset under both English and American law.¹⁴⁴ Accordingly, multiple equally plausible asset-based connections may arise. The question therefore becomes whether, and on what policy grounds, one of these competing territorial connections should be preferred in determining the applicable law.

E. The Territorial Affiliations of the Parties

The domicile, habitual residence, incorporation, and principal place of business of the contracting parties remain among the most stable personal connecting factors in contractual choice-of-law analysis.¹⁴⁵ As discussed above, parties operating through smart contracts frequently transact pseudonymously, initially obscuring these territorial affiliations. However, once judicial proceedings have been initiated, this difficulty is substantially reduced, since the identity and territorial affiliation of the relevant party will ordinarily have been ascertained. Accordingly, this connecting

Dickinson, *Cryptocurrencies and the Conflict of Laws*, in CRYPTOCURRENCIES IN PUBLIC AND PRIVATE LAW 93 (David Fox & Sarah Green eds., 2019); see LAW COMM'N (2021), *supra* note 7, at 200, ¶ 7.146 ("These cases involved applications for urgent injunctive relief to prevent the dissipation of quantities of cryptocurrencies of which the claimants alleged that they had been fraudulently deprived. In both cases, the courts adopted Professor Andrew Dickinson's view that a crypto asset is located in the place where its owner is domiciled.").

144. See *AA v. Persons Unknown* [2019] EWHC (Comm) 3556, [59] (Eng.) (holding that Bitcoin was property for purposes of a proprietary injunction); see also UK JURISDICTION TASKFORCE, LEGAL STATEMENT ON CRYPTOASSETS AND SMART CONTRACTS 18–27, ¶¶ 86–112 (2019), https://technation.io/wp-content/uploads/2019/11/6.6056_JO_Cryptocurrencies_Statement_FINAL_WEB_111119-1.pdf [<https://perma.cc/YKW7-ARRR>] (concluding that crypto-assets are capable of constituting property under English law); I.R.S. Notice 2014-21, 2014-16 I.R.B. 938, Q&A-1 ("For federal tax purposes, virtual currency is treated as property."); *Commodity Futures Trading Comm'n v. McDonnell*, 287 F. Supp. 3d 213, 228 (E.D.N.Y. 2018) (holding that virtual currencies may be regulated as commodities under the Commodity Exchange Act).

145. See RESTATEMENT (SECOND) OF CONFLICT OF LAWS § 188(2)(e); see also Rome I Regulation, *supra* note 133, arts. 4(2), 19(1)–(2).

factor retains substantial practical significance across all configurations of smart contracts and may, in many cases, provide the most stable and readily ascertainable territorial connection for purposes of determining the applicable law.

F. Additional Smart-Contract-Specific Connecting Factors

The open-ended structure of modern choice-of-law analysis further permits consideration of additional territorially relevant connecting factors generated by blockchain-based transactions.¹⁴⁶

1. Tax Liabilities

A further territorially relevant contact may arise from the tax and regulatory consequences associated with the use of cryptocurrency as contractual consideration. In both the United States and the European Union, crypto-assets are generally treated, for tax purposes, not as sovereign currency, but as forms of property, digital assets, or other taxable assets.¹⁴⁷ As a result, the use of cryptocurrency to discharge a payment obligation under a smart contract may itself constitute a taxable realization event, potentially giving rise to independent reporting and tax-payment obligations in one or more jurisdictions connected to the parties.¹⁴⁸ These fiscal obligations may, in turn, reflect pre-existing personal connecting factors—most notably domicile or habitual residence—which private international law traditionally recognizes as giving rise to significant mutual rights and obligations between individuals and the state, including liability for taxation.¹⁴⁹

The question therefore arises whether such fiscally generated territorial connections should bear upon the identification of the

146. See Rome I Regulation, *supra* note 133, art. 4(3); see also RESTATEMENT (SECOND) OF CONFLICT OF LAWS § 188.

147. See I.R.S. Notice 2014-21, 2014-16 I.R.B. 938, Q&A-1 (“For federal tax purposes, virtual currency is treated as property.”); see also Council Directive (EU) 2023/2226, of 17 October 2023 Amending Directive 2011/16/EU on Administrative Cooperation in the Field of Taxation, 2023 O.J. (L 2226) 1.

148. See LAW COMM’N (2025), *supra* note 132, at 23, ¶ 2.77.

149. *Id.* at 118, ¶ 4.216 (observing that habitual residence and domicile give rise to “more significant mutual rights and obligations as between a person and a state,” including “the liability to pay taxes”).

applicable law. Given the open-ended structure of modern choice-of-law analysis, there is a principled basis for considering such connections, at least where they disclose a manifestly closer connection to the transaction, or where, in light of the particular issue in dispute, they assume particular significance.¹⁵⁰

2. Technologically Generated Connecting Factors

A final category of potentially relevant connecting factors arises from the technological architecture and governance structure of blockchain-based systems. Recent institutional analysis has suggested that, depending upon the design of the relevant protocol, such connecting factors may include the geographical concentration of validating or mining nodes, the place where the protocol's white paper or associated website is maintained, administered, or registered, or the location of the core development team responsible for maintaining the protocol. Additional factors may include the domicile, habitual residence, or principal place of business of the protocol's creator or principal developer, the location of external auditors responsible for reviewing the relevant smart contract infrastructure, or the location of the legal entity responsible for operating, administering, or maintaining the blockchain platform, where such an entity exists. These factors may, in appropriate circumstances, provide further evidence of the geographical origin, operational center, or governance structure of the relevant blockchain-based system.¹⁵¹

The practical significance of these factors necessarily depends upon the architecture of the relevant blockchain network.¹⁵² In public and highly decentralized systems, the absence of any centralized operator, together with the geographically dispersed, constantly changing, and, in some cases, difficult-to-verify

150. See Rome I Regulation, *supra* note 133, art. 4(3); RESTATEMENT (SECOND) OF CONFLICT OF LAWS §§ 6, 188.

151. See LAW COMM'N (2025), *supra* note 132, at 184, ¶ 6.112 (identifying, among possible connecting factors, the place where the majority of mining nodes are located, the place where the website with the white paper is registered, the location of the platform's contributor team, the domicile of the protocol's creator, and the location of the last auditor); see also Dickinson, *supra* note 143, ¶¶ 5.61–5.67.

152. See, e.g., Catchlove, *supra* note 4, at 3–5.

distribution of validating nodes, may significantly reduce the practical utility of such factors as stable territorial anchors.¹⁵³ By contrast, in private, permissioned, semi-centralized, or otherwise governance-based systems—where platform administration, validation, or protocol maintenance is performed by an identifiable legal entity or a limited and identifiable group of participants possessing an ascertainable place of business—the location of such technological infrastructure may provide a more stable and meaningful territorial connection.¹⁵⁴

The question therefore becomes whether, and to what extent, such technologically contingent connections should be taken into account in identifying the applicable law. Blockchain-based transactions may generate multiple plausible territorial connections, raising the question of which should determine the applicable law.

VII. CHOICE-OF-LAW AND FORUM-SELECTION CLAUSES IN SMART CONTRACTS

Party autonomy occupies a central position in contemporary private international law. Under the Rome I Regulation, parties are generally free to choose the law governing their contractual relationship, while jurisdiction agreements are similarly recognized under the Brussels I Recast Regulation, subject to specified limitations.¹⁵⁵ English law likewise gives substantial effect to contractual choice-of-law and jurisdiction clauses, reflecting the broader principle that commercial parties should ordinarily be permitted to structure their legal relationships as

153. See *Contracts Ex Machina*, *supra* note 6, at 332 (“And, because blockchains run on a distributed network of independent nodes, with no central control point, a litigant seeking to enjoin performance of a smart contract has no one to sue.”); LAW COMM’N (2021), *supra* note 7, at 189, ¶ 7.93 (“Other factors suggested, such as the identities, habitual residences, and domiciles of the parties, or the location of the nodes running the smart legal contract, may be trickier to apply (or less relevant) in the smart legal contract context, as we discuss above.”).

154. See Bushansky, *supra* note 1, at 305; LAW COMM’N (2021), *supra* note 7, at 188, ¶ 7.92(5)–(6).

155. See Rome I Regulation, *supra* note 133, art. 3; see also Brussels I Recast Regulation, *supra* note 68, art. 25.

they see fit.¹⁵⁶ American conflict-of-laws doctrine adopts a broadly similar approach, although subject to public-policy limitations and specific statutory protections in particular contexts.¹⁵⁷

The challenges raised by choice-of-law and forum-selection clauses in smart contracts are therefore twofold. The first is whether such clauses can be meaningfully incorporated into agreements expressed wholly or partly through computer code. The second and more difficult question is how such clauses can operate within a contractual framework optimized for the autonomous execution of conditional obligations. These questions arise from the distinctive characteristics of the programming languages and technological architectures through which smart contracts are created and operate, and are closely connected to the particular smart-contract configurations adopted by the parties.

The prevailing view is that parties remain free, as a matter of contractual autonomy, to express their agreement through computer code.¹⁵⁸ However, programming languages possess characteristics fundamentally different from those of the natural language traditionally used in contractual drafting. Smart contracts are typically written in computer code based upon Boolean logic and are designed to facilitate the autonomous execution of predefined obligations upon the occurrence of predetermined conditions.¹⁵⁹ Their operation is therefore conditional, deterministic, and execution-oriented.¹⁶⁰

156. *See* Enka Insaat Ve Sanayi AS v. OOO Ins. Co. Chubb [2020] UKSC 38, [29] (appeal taken from Eng.) (“The starting point at common law . . . is that contracting parties are free to choose the system of law which is to govern their contract . . .”).

157. RESTATEMENT (SECOND) OF CONFLICT OF LAWS § 187.

158. *See* Bushansky, *supra* note 1, at 312 (“The prevailing view is that, under the principle of freedom of contract, no legal barrier prevents parties from expressing their contractual obligations through computer code.”).

159. *See* Savelyev, *supra* note 51, at 125 (“A computer language does not allow discretion in its interpretation by the machine. Smart contract terms are interpreted by machine on the basis of Boolean logic, in contrast to classic contracts, where interpretation of terms is performed by the human brain on the basis of subjective criteria and analogous ways of thinking.”).

160. *See id.* at 126 (“Smart contract is drafted on one of the computer languages. Conditional statements are foundational to computing: computer code is based on statements like ‘if “x” then “y”’. Such an approach is in harmony with contractual terms and conditions.”).

This functional characteristic distinguishes smart contracts from conventional contracts, which routinely contain provisions that are not themselves executable obligations. Commercial agreements commonly include representations, warranties, indemnities, confidentiality undertakings, governing-law clauses, and forum-selection clauses, all of which perform important legal functions without themselves constituting executable obligations. Accordingly, while such provisions may be incorporated into a smart-contract environment, they are not themselves capable of autonomous execution through code. The fundamental difficulty is therefore not whether parties may agree upon a governing law or forum, but how such clauses can be effectively incorporated into, and operate within, a contractual framework optimized for the automated execution of conditional obligations.

Two related challenges arise from this distinction. As Harry Surden has observed, computer code is not designed to express the full range of contractual provisions commonly found in commercial agreements, nor is it capable of autonomously performing all such provisions.¹⁶¹ In his view, the first step is to determine whether a contractual provision can be translated into what he terms a “data-oriented expression.”¹⁶² Only once contractual terms have been represented in a form capable of machine processing can the parties create what he describes as a “computable contract”—namely, a contractual arrangement composed of instructions capable of automated execution while accurately reflecting the parties’ underlying agreement.¹⁶³ The consequence is that many contractual provisions perform legal, interpretive, or risk-allocation functions that cannot readily be reduced to executable code.¹⁶⁴ This distinction is particularly

161. See Harry Surden, *Computable Contracts*, 46 U.C. DAVIS L. REV. 629, 647–53 (2012).

162. *Id.* at 658 (“However, once contract information has been deliberately formulated to be processable by computers, parties can take apply [sic] the analytical abilities of computers to the substance of their contractual obligations.”).

163. *Id.* (“The basic idea behind a computable contract term is to create a series of actionable, computer-processable instructions that approximate what it is that the parties are intending to do in their contractual arrangement.”).

164. See Bushansky, *supra* note 1, at 312 (“This rigidity contrasts with the flexibility of traditional contracts, which often account for future contingencies. Traditional contracts frequently include provisions that are not strictly conditional or interdependent but address future obligations or contain non-operational clauses not defined by

significant in the context of governing-law and forum-selection clauses, which perform important legal functions but are not themselves naturally suited to computational execution.

The practical significance of these challenges varies according to the configuration of the smart contract. In hybrid and default bilingual smart-contract configurations, parties may, much as they would in conventional contracting, include governing-law and forum-selection clauses within an accompanying natural-language document. Greater difficulties arise in the default configuration, the traditional-virtual configuration, and the autonomous interaction of computer programs configuration, where no separate natural-language agreement exists. In such circumstances, the question becomes how governing-law and forum-selection clauses can be effectively incorporated into a contractual framework expressed primarily through executable code.

This issue has been considered by the UK Law Commission.¹⁶⁵ In response to its call for evidence, consultees proposed several possible solutions. The first is to incorporate a governing-law or forum-selection clause in natural language within smart-contract code itself.¹⁶⁶ Because uncertainty may arise concerning the legal status of such a provision, the Commission further suggested that parties expressly state that the clause forms part of the contractual agreement and is intended to have binding legal effect.¹⁶⁷ Modern programming languages generally permit natural-language comments and annotations to be embedded within smart-contract code, making such a technique technically feasible.¹⁶⁸ Nevertheless, while this approach may successfully incorporate

conditional outcomes (e.g., declarations, indemnity obligations, or confidentiality clauses).”).

165. See LAW COMM’N (2021), *supra* note 7, at 183–85, ¶¶ 7.71–7.77.

166. See *id.* at 184, ¶ 7.76 (“Our view remains that it would be difficult for parties to include a coded choice of law clause in their smart legal contract. However, it would not be difficult for parties to include a comment or other natural language provision to this effect, and we think parties would be well advised to do so.”).

167. See *id.* at 93, ¶ 4.75 (“Whether such comments do constitute contractual terms will be a matter of contractual interpretation and construction. To avoid any uncertainty or ambiguity, parties would be well advised to make clear the status of any comments in code, and whether such comments form part of the parties’ contract.”).

168. See *id.* at 9–11, ¶¶ 2.7–2.10 (discussing the ability to include comments in source code).

the clause into the contract, it does not render the clause capable of autonomous execution or enforcement by the code itself.¹⁶⁹

A second possibility is the implementation of an algorithmic choice-of-law mechanism.¹⁷⁰ Under this approach, the smart contract would contain operational conditions that determine the applicable law governing the parties' relationship. Consultees suggested, for example, a smart-loan agreement providing that timely repayment triggers the application of one legal system, whereas default triggers the application of another.¹⁷¹ In this sense, it may be possible to construct a conditional and operational choice-of-law mechanism. Nevertheless, such arrangements remain fundamentally different from conventional governing-law clauses, since the applicable law varies according to predefined contractual events, rather than providing a stable legal framework governing the parties' relationship from its inception.

Recent empirical research cited by the Law Commission suggests that many DeFi applications already include express governing-law clauses.¹⁷² However, the same research demonstrates that a significant number do not include these clauses, thereby leaving applicable law to be determined through traditional private international law connecting factors, thus illustrating the continuing practical importance of express choice-of-law provisions in blockchain-based transactions.¹⁷³ Similar recommendations appear throughout the academic literature and are difficult to dispute.¹⁷⁴ Nevertheless, although governing-law and forum-selection clauses may be desirable in commercial

169. *See id.* at 184, ¶ 7.74.

170. *See id.* ("Nonetheless, we think it may be possible for parties to set up an algorithmic determination of governing law to alter the risk profile between the parties, or to avoid potential conflict of laws issues. For example, the parties could program the code such that, if the current operational state of the smart legal contract is X, the law of jurisdiction Y applies; if not, the law of jurisdiction Z applies. In this case, the coded provision could be said to have operational effect.").

171. *See id.*

172. *See* LAW COMM'N (2025), *supra* note 132, at 139, ¶ 5.69.

173. *See* Pascal Favrod-Coune, Presentation at the Digital Assets and Private International Law Conference, Interdisciplinary Association of Comparative and Private International Law, University of Vienna & European Banking Institute: Decentralised Finance (DeFi)—Which Law Is Governing the Entities, Which Transactions? (Apr. 11–12, 2024), *cited in* LAW COMM'N (2025), *supra* note 132, at 139–40, ¶¶ 5.69–5.71 & n.370.

174. *See* LAW COMM'N (2025), *supra* note 132, at 139–40, ¶¶ 5.69–5.71.

smart-contract transactions, their effectiveness cannot be assumed in every context. Most notably, in consumer and standard-form contracting, such clauses remain subject to domestic and supranational limitations, as well as other mandatory protections designed to safeguard weaker parties.¹⁷⁵

VIII. THE CLAIMANT AS THE PRIMARY CONNECTING FACTOR

The preceding analysis demonstrates that blockchain-based transactions may simultaneously generate a multiplicity of territorially plausible connecting factors. Depending upon the architecture of the relevant system and the configuration of the smart contract itself, the same dispute may exhibit meaningful connections to the domicile or place of business of the contracting parties, the place of negotiation or performance, the situs attributed to the relevant digital asset, the jurisdictions in which tax-reporting or regulatory obligations arise, or the location of custodians or intermediaries. Additional connections may arise from the place of protocol creation or deployment, the geographical distribution of validating nodes, the domicile of protocol creators or developers, or the place of operation of governance entities or platform operators. In genuinely decentralized environments, these connections may be dispersed across numerous jurisdictions, each possessing an equally plausible claim to territorial relevance. The central normative question therefore becomes how private international law should respond where no single connecting factor emerges as naturally, doctrinally, or normatively superior.¹⁷⁶

The novelty of this problem does not lie in the mere existence of multiple territorially relevant connections. Modern private international law has long accommodated competing connecting

175. See Rome I Regulation, *supra* note 133, art. 6; see also Brussels I Recast Regulation, *supra* note 68, arts. 17–19; *M/S Bremen v. Zapata Off-Shore Co.*, 407 U.S. 1, 10–15 (1972); *Carnival Cruise Lines, Inc. v. Shute*, 499 U.S. 585, 593–95 (1991).

176. See LAW COMM'N (2025), *supra* note 132, at 12, ¶ 2.13 (“The basic problem is, therefore, that application of the traditional rules of private international law in an increasingly globalised socio-economic environment usually points to a multiplicity of places rather than a single place. It therefore becomes harder to resolve conflicts of jurisdictions and of applicable laws because no single national court or single system of private law emerges as the clear ‘winner’ over each of the others.”); see also *id.* at 18, ¶ 2.48.

factors through flexible doctrines designed to identify the legal system most closely connected to the dispute. The difficulty presented by genuinely decentralized smart-contract transactions is more fundamental. As recent institutional analysis has observed, in circumstances of true decentralization, “the techniques used by private international law to connect the facts and issues arising in a case to a single legal system are no longer as effective,” because “there is no single feature in a wholly decentralised DLT network that emerges as particularly prominent, such that it may be effectively used as a connecting factor.”¹⁷⁷

Recent institutional analysis suggests that, where no naturally dominant connecting factor emerges, courts should adopt a highly analytical and issue-specific approach, identifying the connecting factor that best advances the policy underlying the particular private international law rule at issue.¹⁷⁸ While such an approach offers considerable flexibility, its application to decentralized smart-contract disputes risks undermining legal certainty by requiring courts to undertake repeated issue-specific assessments of competing territorial connections.

This Article advances a different normative response. Rather than abandoning the search for a single primary connecting factor, it argues that the distinctive characteristics of smart contracts justify the development of a novel connecting-factor framework specifically adapted to decentralized digital transactions. Unlike the digital environments that have traditionally informed the development of contemporary private international law—including electronic commerce, online platforms, and internet-mediated contractual relationships—smart contracts combine autonomous execution, pseudonymous participation, and decentralized technological infrastructure in a manner capable of simultaneously disrupting traditional assumptions concerning performance, dispute resolution, and territorial localization.¹⁷⁹

177. *Id.* at 18, ¶ 2.48.

178. *See id.* at 14, 23, ¶¶ 2.26, 2.72.

179. *See id.* at 24, ¶ 2.58 (“Throughout this paper, we identify particular issues which we think parties could usefully consider and address in the terms of their smart legal contract. We include a short, non-exhaustive list of these issues in Appendix 3. Dealing directly with these issues in contractual terms should reduce uncertainties regarding the legal treatment of the parties’ smart legal contract, and reduce the scope for potential disputes.”); *see also supra* notes 6–7, 9, 11, 19 and accompanying text.

Their performance is frequently autonomous and technologically irreversible; judicial intervention commonly occurs only after execution has been completed;¹⁸⁰ disputes tend to focus on restitutionary and corrective relief rather than enforcement of executory obligations;¹⁸¹ and the burden of initiating litigation is often shifted to the party adversely affected by autonomous execution.¹⁸² At the same time, decentralized blockchain environments may generate a multiplicity of territorially plausible connecting factors, none of which emerges as naturally, doctrinally, or normatively dominant.¹⁸³

In these circumstances, the continued multiplication of issue-specific connecting factors risks compounding the very uncertainty that private international law seeks to reduce.¹⁸⁴ Accordingly, this Article proposes a single primary connecting factor capable of promoting certainty, predictability, and effective access to justice while remaining responsive to the distinctive procedural realities of smart-contract disputes. Under this framework, the domicile, habitual residence, incorporation, or principal place of business of the claimant constitutes the most appropriate candidate for that role.

This conclusion does not rest upon any abstract preference for the claimant as such. Rather, it follows from the manner in which smart-contract architecture fundamentally transforms the

180. See *Contracts Ex Machina*, *supra* note 6, at 376 (explaining that complaining parties will seek to undo or reverse completed transactions rather than obtain fulfillment of alleged promissory obligations).

181. *Id.* (“Rather than complaining parties seeking fulfillment of alleged promissory obligations, complaining parties will seek to undo or reverse completed transactions.”); see LAW COMM’N (2021), *supra* note 7, at 128, ¶ 5.90 (noting that, where smart contracts perform automatically, disputes may arise only after execution has occurred and remedial questions may therefore focus on reversal, restitution, or other corrective relief); Sarah Green & Adam Sanitt, *Smart Contracts*, in CONTENTS OF COMMERCIAL CONTRACTS: TERMS AFFECTING FREEDOMS 191, 191 (Paul S. Davies & Magda Raczynska eds., 2020) (“The way in which smart contracts operate, therefore, means that any adjudication of them is likely to need to emphasize restorative rather than enforcement remedies.”).

182. See *Contracts Ex Machina*, *supra* note 6, at 376 (“Reversing who stands as plaintiff shifts the burdens of proof and litigation.”).

183. See LAW COMM’N (2025), *supra* note 132, at 12, ¶ 2.13.

184. See *id.* at 14, ¶ 2.26 (describing private international law’s “highly analytical and granular approach”); see also *id.* at 11, ¶ 2.11 (observing that the historical effectiveness of private international law derived from connecting rules that ordinarily pointed to a single place and, therefore, a single legal system).

procedural structure of contractual disputes and systematically reallocates the burdens of corrective judicial intervention.¹⁸⁵ The normative justification for this approach rests upon several interrelated features of smart-contract architecture that bear directly upon the policy objectives of certainty, predictability, efficiency, and access to justice that private international law has traditionally sought to promote.¹⁸⁶

First, the autonomous execution of smart contracts fundamentally alters the remedial posture of contractual disputes. In conventional contractual relationships, judicial proceedings typically arise prior to, or contemporaneously with, non-performance and commonly seek enforcement, injunctive relief, or expectation-based remedies. By contrast, where contractual obligations are performed autonomously and, in many cases, irreversibly through blockchain-based execution, judicial intervention frequently becomes practically available only after performance has already occurred. As a result, contractual litigation is increasingly transformed from a mechanism for compelling performance into one concerned with reversal, restitution, corrective transfers, or other functionally equivalent restorative remedies.¹⁸⁷

Second, autonomous execution fundamentally alters the procedural posture of litigation itself. A party whose obligations have already been autonomously executed—despite the existence of vitiating factors or other grounds affecting the validity, enforceability, or legitimacy of the transaction—may obtain meaningful judicial relief only after the disputed transaction has been completed.¹⁸⁸

185. See *Contracts Ex Machina*, *supra* note 6, at 376; see also LAW COMM'N (2021), *supra* note 7, ch. 5 (discussing remedies and the consequences of automated contractual performance).

186. See Bushansky, *supra* note 1, at 303, 313–14, 319; see also LAW COMM'N (2025), *supra* note 132, at 12, ¶ 2.13 (explaining that the multiplication of potentially relevant locations creates uncertainty concerning jurisdiction and applicable law); RESTATEMENT (SECOND) OF CONFLICT OF LAWS § 6(2)(f)–(g) (identifying “certainty, predictability and uniformity of result” and “ease in the determination and application of the law to be applied” as relevant choice-of-law considerations); Brussels I Recast Regulation, *supra* note 68, recitals 15–17.

187. See sources cited *supra* note 186.

188. See *Contracts Ex Machina*, *supra* note 6, at 376.

Third, the distinctive characteristics of blockchain-based transactions substantially amplify these burdens. Smart-contract disputes frequently involve pseudonymous counterparties, decentralized infrastructure, digital assets capable of rapid transfer across jurisdictions, and uncertainty concerning the location of relevant persons, assets, evidence, and technological actors.¹⁸⁹ The party seeking relief may therefore be required not only to establish the substantive merits of the claim, but also to identify the relevant defendant and overcome significant jurisdictional, choice-of-law, evidentiary, and enforcement-related obstacles to initiate and effectively pursue corrective proceedings.¹⁹⁰

In such circumstances, selecting the domicile or equivalent personal affiliation of the claimant does more than merely promote procedural efficiency. Rather, it aligns the principal territorial connecting factor with the procedural realities of smart-contract disputes by linking it to the party upon whom smart-contract architecture systematically imposes the burden of corrective litigation. Such an approach promotes access to justice, reduces the costs associated with corrective proceedings, enhances legal certainty, and preserves the traditional private international law objective of identifying a single predictable territorial anchor.¹⁹¹

This proposal is not without precedent in the broader structure of private international law. Although connecting-factor analysis is frequently presented as territorially neutral, private international law has long accommodated policy-driven departures from purely geographical localization where important systemic objectives are at stake. The traditional distinction between substance and procedure provides a prominent example. While courts routinely apply the substantive law of other legal systems, procedural matters remain governed by the *lex fori*, reflecting the view that the legal system responsible for administering the proceedings possesses the strongest claim to regulate their conduct.¹⁹² Similar policy choices are reflected in the

189. See Bushansky, *supra* note 1, at 321–22.

190. See LAW COMM'N (2025), *supra* note 132, at 12, 18, 184, ¶¶ 2.13, 2.48, 6.112.

191. See *id.* at 14, ¶ 2.26.

192. See RESTATEMENT (SECOND) OF CONFLICT OF LAWS § 122 (“A court usually applies its own local law rules prescribing how litigation shall be conducted even when it applies

special protections afforded to consumers and employees under modern European private international law, in the recognition of overriding mandatory provisions and the public-policy exception, and in the policy-sensitive methodologies employed in modern American conflicts law.¹⁹³ In each instance, private international law recognizes that certain normative objectives—including access to justice, procedural fairness, protection of weaker parties, efficient judicial administration, and legal certainty—may justify departures from an otherwise territorially neutral connecting-factor analysis.¹⁹⁴

The claimant-centered approach proposed here may be understood as a comparable adaptation. Smart contracts generate a distinctive procedural reality in which autonomous and frequently irreversible execution reallocates the burdens of corrective litigation to the party adversely affected by that execution. Where decentralized architecture simultaneously produces multiple equally plausible territorial connections, selecting the domicile, habitual residence, incorporation, or principal place of business of the claimant as the primary connecting factor serves the same objectives that have historically justified other policy-based adaptations within private international law. Rather than abandoning the discipline's underlying commitment to territorial ordering, the proposed approach seeks to preserve legal certainty, predictability, and effective access to justice by providing a single, readily ascertainable territorial anchor for both jurisdiction and applicable law.

the local law rules of another state to resolve other issues in the case.”); *see also* Regulation (EC) 864/2007, of the European Parliament and of the Council of 11 July 2007 on the Law Applicable to Non-Contractual Obligations (Rome II), art. 1(3), 2007 O.J. (L 199) 40, 43 (excluding evidence and procedure from the scope of the Regulation).

193. *See* Rome I Regulation, *supra* note 133, arts. 6–9, 21; *see also* Brussels I Recast Regulation, *supra* note 68, recitals 15–18; RESTATEMENT (SECOND) OF CONFLICT OF LAWS § 6(2)(b), (d), (f)–(g) (identifying the policies of interested states, the protection of justified expectations, and the values of certainty, predictability, and uniformity of result as relevant choice-of-law considerations).

194. *See* sources cited *supra* note 193.

IX. CONCLUSION

Smart contracts challenge some of the foundational assumptions upon which private international law has traditionally been constructed. Although private international law has previously adapted to the challenges posed by electronic commerce, online platforms, and other internet-mediated transactions, smart contracts present a distinct problem. The decentralized, automated, and frequently pseudonymous nature of blockchain-based transactions complicates the identification of the territorial connecting factors that have historically enabled courts to determine both the appropriate forum and the applicable law.

Unlike both conventional contractual relationships and the digital technologies that have traditionally confronted private international law, smart contracts may be formed, performed, and executed through decentralized technological infrastructures that lack a clear territorial center while simultaneously generating multiple competing connections to different legal systems.

Although traditional connecting factors remain capable of operating in certain smart-contract configurations—particularly where the transaction retains meaningful links to the physical world—genuinely decentralized blockchain environments may both complicate the identification of territorially relevant connections and generate a multiplicity of competing territorial connecting factors, none of which emerges as naturally or doctrinally superior. The resulting difficulty lies not only in identifying the territorial connections associated with a transaction, but also in determining which of those connections should govern the allocation of jurisdiction and the selection of the applicable law.

Recent institutional analysis has suggested that this difficulty should be addressed through increasingly issue-specific connecting-factor analysis, under which different aspects of the same dispute may be connected to different legal systems according to the policy underlying the particular private international law rule in question.

This Article has argued, however, that where decentralized blockchain environments generate multiple equally plausible territorial connections, the continued multiplication of connecting

factors risks reintroducing the very uncertainty that both private international law and smart-contract architecture seek to minimize. Smart contracts are often valued for their capacity to promote certainty through automated and predictable execution, as well as their immunity to human intervention during the performance phase.¹⁹⁵ Private international law pursues a similar objective, seeking to reduce uncertainty through the identification of predictable jurisdictional and choice-of-law rules that enable parties to anticipate the legal consequences of their transactions. Yet, increasingly issue-specific connecting-factor analysis risks generating fragmentation and unpredictability at precisely the stage where both systems aspire to provide clarity. Indeed, because both smart-contract architecture and private international law are fundamentally certainty-enhancing systems, a methodology that multiplies uncertainty at the jurisdictional and choice-of-law stage is difficult to reconcile with the objectives of either.

The central claim advanced in this Article is that the distinctive characteristics of smart contracts justify a different normative response. Smart contracts are not merely another form of electronic commerce. Their autonomous and frequently irreversible execution, limited susceptibility to human intervention during the performance phase, and tendency to shift the practical burden of corrective litigation onto the party seeking relief fundamentally alter the procedural structure of contractual disputes. These features justify the development of a connecting-factor methodology specifically adapted to smart-contract disputes, where decentralized architecture may both complicate the identification of meaningful territorial connections and generate multiple competing territorial connections without revealing a naturally dominant territorial anchor.

The analysis reveals two related difficulties: identifying meaningful territorial connections where none is readily apparent, and selecting among competing connections where several are plausible. Both difficulties limit the guidance that conventional connecting factors can provide in decentralized smart-contract disputes. A claimant-centered model responds by anchoring

195. See Bushansky, *supra* note 1, at 315–18.

jurisdiction and applicable law in the claimant's territorial affiliation, promoting certainty, predictability, and coherence while recognizing the burden of seeking corrective relief after automated execution.

This common anchor reduces reliance on broad judicial discretion and places corrective proceedings within a more predictable legal setting. The resulting adaptation retains the core structure of territorial connecting-factor analysis while responding to the procedural consequences of automated execution. In this way, the framework facilitates the integration of smart-contract transactions into private international law while promoting certainty, predictability, and access to justice.