



Smart Contracts and Legal Enforceability: Bridging the Gap Between Code and Law

Ting Ting Mimi Jiang*

College of Business, City University of Hong Kong, Hong Kong, China

*tingjiang497@gmail.com

Abstract. As smart contracts becomes increasingly popular, people start to be aware of how it can integrate with the traditional law systems. This paper examines the enforceability of smart contracts and the consistent gap between law and coding. Firstly, it identifies four core conflicts that codes and legitimacy have, including their mutability and flexibility natures, transparency compare to privacy, and usefulness in courts. Methodologically, it synthesises from three aspects: technical, economic and legal analysis to propose a layered framework for attempts to reduce the "gap". Technically, it suggests zero-knowledge proofs (ZKPs), redactable blockchain innovation, formal verifications and fuzzing when accessing the smart contracts, and on-chain dispute resolution. These may mitigate privacy, immutability and security issues. From the legal perspective, it advocates hybrid-tech frameworks like hybrid smart legal contracts, binding Terms of Use (TOU) as procedural layers, Oracle utilisation, and digital signatures and statutory recognition of smart contracts explicitly. Finally, this essay proposes identity and reputation systems using self-sovereign identity (SSI) frameworks to align privacy with accountability. All the solutions are explained and provided with examples in the essay. The findings support a co-evolutionary model where code and law are paralleled and used co-dependently, enabling an efficient development of the society.

Keywords: Smart contract, Blockchain, Legal enforceability

1 Introduction

Smart contracts are coded agreements with decentralized quality and are stored on blockchains. They are not simply just contracts on chain [1], but a holistic negotiation and execution process that occurs on the blockchain, resembling processes from real-life scenarios. In this paper, it would also be referred to as self-executing agreements since smart contracts are served for transaction purposes, and executed with autonomy. It mainly consists of three parts, including a natural language contract, a user interface to make the contract user-accessible, and several components used to handle the self-executing parts. It is often used in Ethereum, blockchain and other new technical worlds for transactions between users, with core qualities like transparency, anonymity, and

immutability. This directly clashes with the legal system's need for privacy, identifiable parties, and judicial discretion to ensure fairness.

Contemporarily, many people get interested in the blockchain industry and smart contracts, not only because it's new, but because it provides benefits like elimination of intermediaries and automated processes. They use it for transactions in many areas such as real estate, finance, or identity management. However, it neglected its inflexibility towards accidental events and stubborn integration between codes and laws. That means, there is a gap between code and law. Intrinsically, the gap is pointed towards the barrier of implementation of codes and smart contracts influence in real-life scenarios. In the current legal system, it is often more complex, having numerous scenarios to be flexibly treated, with the need of clear and certain identities from the courts, "law is law", and respect of privacy. Both sides experienced many conflicts, mainly focused on three parts: technical, economical and lawful perspectives. For instance, if there are bugs in codes, it can be manipulated by malicious hackers that legislation can't assist or find them. Responsible parties for accidents like whether it's faults from communities, developers or miners in coding can also be hardly found. Thus, self-executing contracts are hardly being recognised by many countries from a lawful perspective. There are some existing legal problems in smart contracts, which often leads to legitimate threat and association of bad governance. In 2016, the DAO hack was a devastating yet good lesson to be learnt as it covered concepts of unclear lawful status, uncertain liability, leading to a leakage of 3.6 million ETH.

In the recent studies, Vatiere wrote a paper that aims to analyse transaction cost [2], mentioned that enforcement of blockchain protocol can increase transaction cost due to "bad adaptation" via consensus systems. Also, one of the crucial advantages that self-executing agreements have is that it is more deterministic and able to prevent over-intervention from the legal system, increasing efficiency of transactions. The essay had inspired a new concept of bridging the gap from an economic perspective, and how to solve some fundamental technical problems that smart contracts have. Moreover, Bassan, F., & Rabitti, M. emphasized that self-executing contracts and implementation of blockchain principles are not aiming to replace the entire law system [2], but to enhance it and complement it. It is important to have a new and hybrid legal-tech infrastructure where natural language has its own legitimate meaning, and smart codes can serve as a tool for execution. However, the implementation of the new infrastructure still remains in theory and could be challenging to impose as legal systems have enormous complicated questions that pure codes can't be effective enough. Effective execution processes were yet to be found. Stipic et al even stated that in Croatia, smart contracts are illegal because it's outside of the legislations [3]. That means, self-executing agreements are still sitting in the legal grey area, and people still have technological intimidation and a lack of trust over new technologies and use of online smart contracts specifically. The researchers identified that legal advisors will remain essential, at least in the drafting phase to ensure that codes remain the intended legal relationships. Though they've only outlined some critical "gaps" that code and legislation have, but didn't manage to resolve this situation. Laarabi suggested in a paper that the TOU agreement, which is the procedural layer of blockchain [4], sets the "rules of the road" for the blockchain platforms. Particularly, it could be used to serve for governing purposes as it disputes

resolution and other key terms, in which courts can utilize TOU agreement as a tool to interpret self-executing agreements. This could be effective information in the solution part of the essay. In addition, Perez, A. J., & Zeadally, S. claimed a new concept of “right to privacy” [5], again emphasizing the opposition of the principles of law and codes. They’ve proposed some solutions towards the privacy issue, like ZKPs and redactable blockchains that could be favourable in developing new solutions for “bridging the gap”.

Building on the findings and spot of many existing problems in smart contracts, this paper is written fundamentally to first, outline the conflicts between smart contract and traditional law structure, and suggest some solutions towards reducing the gap between the two. More importantly, for the "bridge" solutions, it is not just all-or-nothing, but can be adjusted to minimum or maximise use of smart contracts based on involved parties, making it more applicable and possible to impose in reality. It will also evaluate a spectrum of pragmatic solutions to propose a future where code and law are not in opposition, but in synergy.

2 The Conflicts Between Smart Contracts and Law

2.1 Code Immutability VS. Legal Mutability

Immutability is one of the natures that blockchain have, in which data becomes unerasureable online or with any use of methods [5]. Paradoxically, benefits of smart contracts and blockchain codes can also be drawbacks. As it can’t be altered anymore, it does not serve the same as the current world’s legislation rules where people can choose what to remain and what to remove. One of the critical examples would be the EU’s Art.7 [6], which promotes the right to erasure. That means, depending on the union in which the controller is headquartered, the personal data must be erased by law. The courts hold the rights to erase certain data, while smart contracts in opposition cannot alter the data after it is executed.

It is also noted that immutability clashed with doctrines of contractual adaptability and judicial oversight. When self-executing agreements bind with legislations that later become illegal, possibly due to regulatory changes, courts could reform and revise the agreement. However, there is a disconnect risk for smart contracts since the underlying code will continue to execute regardless. Unless it was pre-programmed or equipped with upgrade mechanisms, the produced outcomes would only be technically enforced and legally void in which undermines both legitimate certainty and user trust.

2.2 Transparency VS. Privacy

Public blockchains held the natures of transparency and auditability. This is conflicted to the lawful expectations of commercial confidentiality and privacy. Some of the potential cyberattack such as re-identification attack - where anonymized wallet addresses can be linked to real-world identities with off-chain data, may place users in privacy risks that would be illegally consented [7]. In the commercial context, transparency is also a paramount for them since businesses need to protect sensitive contractual terms,

pricing strategies, or their private supply chain data [8]. If public blockchain ledgers were used by the commercials, competitors could intentionally mine these data from the ledgers for strategic insights, leading to unfair competition.

2.3 “Code is Law” VS. “Law is Law”

Smart contracts are executed based on codes, whereas regulations are designed by humans and recorded in books and guidelines. Consequently, codes unintentionally ignored the human intentions towards the transactions and behaviours, which means people can't justify purely with the codes to explain whether the event is made in which intents - positive, neutral or negative. In addition, surrounding circumstances, reasonableness and fairness etc will all be hard to judge in dependence with sole display of code snippets. For instance, an unforeseen edge case in the code that leads to significant loss of assets, may seem to be technically correct, but could be considered unintended in courts.

2.4 Code Inflexibility VS. Law Flexibility

Some studies show self-executing agreements are not functionally flexible. When using legal mechanisms to execute a contract, its terms and conditions will frequently be supplemented, revised or changed based on scenarios [9]. However, the nature of the smart contracts made the process difficult to change. As they are deterministic pieces of code, their rules of execution are done automatically and immutably without room for discretion. This rigidity leads to several issues, including amendment barriers, technical opacity, and a lack of interpretive mechanisms. Firstly, an update of an already-deployed self-executing agreement often needs a deployment of a new contract to migrate state data, which would be technically complex and costly. Due to technical limitations, accessing self-executing agreements can be tough as it often requires access to platforms like Etherscan or solidity compiler platforms to monitor transactions. Smart contracts also cannot flexibly adapt to accidental circumstances. Thus, the absence of interpretive flexibility in digital agreements may cause the outcome in law to be inequitable or unenforceable.

3 Solutions for Bridging the Gap between Smart Contracts and Conventional Law System

3.1 Technical Solutions for Legal Compliance

As previously mentioned, the privacy issue could potentially be addressed by use of privacy-enhancing technologies to ensure users enjoy their right of anonymity online. A prime example is privacy-preserving crowdsensing [5], whose architecture is depicted in Figure 1.

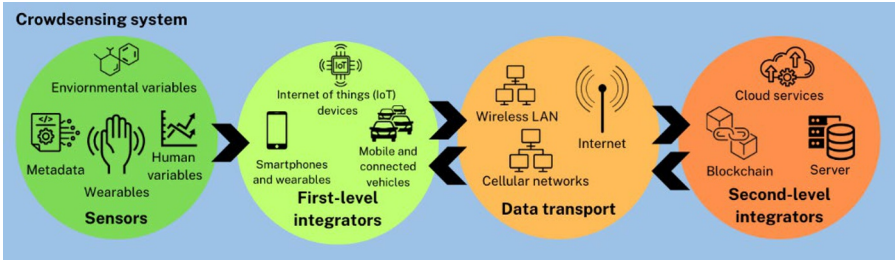


Fig. 1. Crowdsensing system hierarchical layer structure [10]

The crowdsensing system has a typical flow from sensors to second-level integrators, also known as central integrators, that handles users' sensitive personal data like locations and health metrics. As the blockchain icon is inserted into the second-level integrator level, smart contracts can be used to assist in removing the intermediary and resolve the privacy and trust issues. Nevertheless, to intrinsically bridge the gap does not mean to fully replace the current legislation system, but to enable two systems to work codependently and efficiently.

In terms of immutability on-chain, industries may innovate new blockchain platforms that encourage edibility and redact ability. That means people could advance and adopt consensus mechanisms that contain functions like "amending" or "redacting" under strictly defined and auditable environments for compliance with the right of erasure [11]. It is noted that the innovation of "erasable" blockchain platforms does not mean an entire substitution or elimination of the immutable blockchains, it simply enables users to have multiple options to choose from, and serve to increase convenience for the law regulators.

Developers could make use of On-Chain Dispute Resolution (ODR) to build dispute resolution mechanisms directly into the contractual architecture [12]. Like Kleros or Aragon Court, the decentralized "courts" are used to crowdsource jurors to solve all the arguments. One of the principal advantages that ODR has is that it gives a scalable and transparent method for resolving conflicts without reliance on third parties, while still producing outcomes that would be recognized by the traditional legal systems. Further, to ameliorate the security issues and increase the flexibility of codes so as to make it useful in legitimate status, static analysis could be used to mathematically verify that a smart contract's code is correctly implemented in its intended logic. More formal methods like dynamic analysis (E.g. Fuzz testing) can be utilized to simulate real world interactions with the contract. This helps minimize bugs and errors, and enhances the contract's legal validity.

Moreover, ZKPs, also known as Zero-Knowledge Proofs, could be used to allow verification of contract execution without exposure of users' private data on-chain, reconciling transparency with privacy. This can also be used as a method to prove knowledge about a piece of data. ZKPs and redactable blockchains were described as technical measures to resolve the conflict between privacy and transparency [13]. Fundamentally, users are not required to learn any new knowledge, and verifications of data can be carried out without requiring uninvolved parties to notice what the data is. This increases privacy and flexibility for the relevant parties.

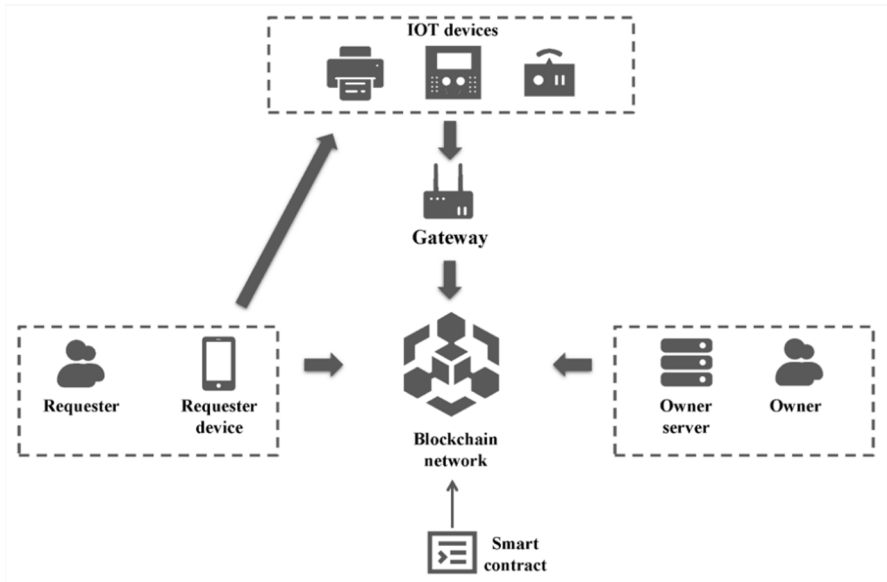


Fig. 2. Overview of the ZKP system workflow [14]

In Figure 2, it demonstrates the abstract process flow of smart contracts and most importantly, the Zero Knowledge Proof (ZKP) technology. This ensured a secure and verifiable access control for any IoT devices. Firstly, the requester will initiate the access control through their Requester device while preserving privacy. On the other hand, the owner will define access policies through their Owner server in which it will evaluate authorization requests and generate a ZKP off-chain, encapsulating whether requester attributes satisfy the required policies—without exposing sensitive data. This proof is submitted on-chain, where the smart contract performs verification using pre-registered keys. In the prerequisite of successful verification, an access token will be issued to the requester by the smart contract. The requester will then use this token to access the IoT device through the gateway, which will interact with the smart contract to verify the token. The gateway will ensure efficient and secure communication between resource-constrained IoT devices and the blockchain. Throughout this process, smart contracts orchestrate several key phases including user and device registration, ZKP verification for access control authorization, and final token authentication. Blockchain serves as both the secure communication medium and the trusted verifier, enabling decentralized, privacy-preserving, and scalable IoT access management through assurance of cryptography and automated enforcement.

3.2 Legal and Procedural Frameworks for Legitimacy

Hybrid Tech-legal framework. This framework is frequently discussed recently by developers as it could post tremendous efforts in bridging the gap. Hybrid contracts are smart contracts that can be executed and enforced by computer executable code with

automation, aligned with humans Law Commission in 2020, and Law Commission in 2021. It smoothly merged human consensus and node consensus via human intervention with hybrid contracts, elevating the code's flexibility.

Besides, from the observation of previous new developments that smart contracts have, traditional legal enforcements are seemingly necessary for the society and should be kept available for now. To emphasize, every smart contract clause that is referenced to the external inputs should be mirrored in natural language that aligns with the oracle governance. In the UK's Smart Legal Contract model, it provided a licit framework for integrating code with the current law language that aims to address the "gap" [15]. Instead of using a pure-code contract, a hybrid contract is applied where two languages - code and "regulations", are combined together and used mutually. This ensures that the code remains its own nature while law can still interpret the smart contracts with its unique ways. Agrello, for example, is a platform that creates parallel and legally-binded natural language documents that can be presented to the courts if legitimate actions were requested, particularly in some corner cases [16]. In the natural language contracts, it should include warranties and service level agreements (SLAs) with oracle providers, define fallback mechanisms for oracle failure, and specify the legal consequences (e.g., restitution, contract voidability) for the four failure scenarios [16], including incorrect data, unavailable data, delayed data and manipulated data.

Binding TOU and Procedure layers. To increase the flexibility of codes and integrate with traditional legal systems, a human-readable TOU could be paired with each of the self-executing contracts so as to govern the relationship. That means, the terms of the TOU will not have negotiations between parties. Consequently, before interaction with the digital contract begins, users must agree to the TOU agreement affirmatively for the contract to produce legitimate effects (E.g. Using digital signature). This enabled enforceability under existing doctrines for online smart contracts. Further, the TOU specifies jurisdiction, governing law, dispute resolution forums, and fallback rules if the code could not function properly. The TOU acts as a procedural layer which resembles a roadmap for judges and arbitrators [17]. Take Oracle as an instance, if its data is unavailable, a substitute input will be determined by arbitration within 5 business days. Courts can then use the standardized TOU templates to interpret what intentions parties have in a specific scenario, such as an unexpected output produced by codes. This accelerates legalized certainty and reduces the conflict between code and law. These days, online TOU agreement validity has been given effect by the courts and maintained court proceedings, hence ensuring disputes were proceeded through arbitration [4]. Additionally, it has a higher likelihood to happen when commercial entities utilize the TOU agreements in courts, and it is certain, recognized and noticed by all the parties [18].

Giving Smart Contract a Legal status. Smart contracts, nowadays, still do not have a fixed definition recorded in the legislations and rules. Thus, legislatures could explicitly define the valid status of digital contracts, digital signatures on blockchain, and tokens to increase legitimate certainty. The "Lex Cryptographia" Model is developed to describe a new subset of justifiable principles and standards specifically designed for blockchain-based contracts and organizations [19]. That the lawful organisations could

consider creating new rules for self-executing contracts which directly addresses the existing merging problems.

Legal documents that are governed by a chosen jurisdiction would define the terms of use, intent and dispute resolution process, while the code simply gift the performances with automation. In particular, Oracles, where an off-chain legit event can trigger an on-chain action, are commonly used to connect self-executing contracts with the transaction scenarios. Hence regulatory guidance for oracles is a major step towards minimising the gap [18]. People may potentially treat critical AI oracles like official financial data providers or requiring audits for their decision-making models [16]. In addition, Oracle also has a service agreement that defines the relationship and allocation of risks. Smart contracts could then be, not just limited to the code and Blockchain TOU [4], but also gave an extension to the service contracts with oracle providers, enabling a multi-layered authorized architecture. Possibly, smart contracts can be aligned with data protection law for integration of code and legislations, for example.

3.3 Identity and Reputation Systems

One of the common methods developers use to identify accountable parties is to implement self-sovereign identity (SSI) frameworks – Enabling users' digital identity is within their control completely and needless of reliance on the intermediaries, similar to the blockchain technology concept [20]. For example, a user can prove they are of licit age without disclosing extraneous private data, enabling the participant to be more accountable and well-identified within a lawful framework.

Use of credits can also be an effective way of proving identities. By incorporating reputation scoring to SSI credentials, reputation can be built through verified history of transactions, arbitration outcomes, and peer endorsements. This will incentivise users to behave positively and provide a track record of trustworthiness to the legal authorities. Additionally, smart contracts may request counterparties to provide their credentials via SSI before execution for bridging the gap.

4 Conclusion

In conclusion, this paper examined multifaceted perspectives between smart contracts and traditional legal frameworks, analysing the mismatches from technical, justifiable, and philosophical sides that made the integration unavailable currently. While digital contracts promise automatic and trust-less execution, these features often contradict lawful principles including mutability, whether code is law or not, the extent of flexibility, and privacy. These reveal that trust-less online contracts, in their current formation, cannot fully integrate with the human-centric legit mechanisms. On the other hand, this paper argues that code and law were not mutually exclusive, but could potentially find ways to bridge the gap between the two. From a hybrid approach, it will leverage the strength of both. As previously mentioned, Zero-Knowledge Proofs (ZKPs), redactable blockchains, and on-chain dispute resolution (ODR) were offered as promising tools to reconcile the regulated requirements with blockchain architecture.

The concept of hybrid smart contract where natural language integration clauses with automated execution demonstrates a practical pathway for aligning intents with outcomes. Further, a legal mechanism consisting of TOU agreements, identity and reputation systems, and the formal recognition of trust-less online contracts, could be implemented to increase enforceability and legitimacy.

To emphasize, the gap is bridged by adapting existing law, not discarding it. That means, the ideal future lies in a co-evolution where law and code exist and inform each other. This paper embraces the notion that the distance between code and law can be reduced with a well-organised and layered approach – One that incorporates human-readable agreements, enforceable TOUs, service-level contracts with oracles, and privacy-protected technologies. Additionally, traditional constitutional systems must develop to accommodate novel digital interactions, while developers must embed legitimate logic and accountability into smart contract frameworks.

Ultimately, the enforceability of smart contracts depends not only on technological innovation but also on its adaptability to legislations, interdisciplinary cooperation, and commitments to privacy, and transparency from all of the involved parties. By constructing a legal-tech infrastructure that respects both the precision of machines and the unpredictability of real-life circumstances, society can unlock the full potential of trust-less online contracts without sacrificing legal integrity. In this way, the gap between code and law is not an unbridgeable divide but a space for innovation, requiring navigation with carefulness, and collaborative effort.

References

1. Bassan, F., Rabitti, M.: From smart legal contracts to contracts on blockchain: An empirical investigation. *Computer Law & Security Review* 55, 106035 (2024). <https://doi.org/10.1016/j.clsr.2024.106035>.
2. Vatiero, M.: Smart contracts vs incomplete contracts: A transaction cost economics viewpoint. *Computer Law & Security Review* 46, 105710 (2022). <https://doi.org/10.1016/j.clsr.2022.105710>.
3. Vinšalek Stipičić, V., Česić, Z., Vičić, M.: Analysis of the Perception of Managers of Small and Medium-Sized Enterprises on the Advantages and Disadvantages of Electronic Business Contracts and Smart Contracts. In: *MIPRO 2024*, pp. 1–6. IEEE, Croatia (2024). <https://doi.org/10.1109/mipro60963.2024.10569775>.
4. Cadogan, M.S.: Enforcing Smart Legal Contracts: Challenges. In: *Enforcing Smart Legal Contracts*, pp. 10–15. Centre for International Governance Innovation, Ontario (2023). <https://doi.org/10.2307/resrep47331.12>.
5. Susnjara, S., Smalley, I.: What is Blockchain? IBM (2025). <https://www.ibm.com/think/topics/blockchain>.
6. GDPR: Art. 7 GDPR – Conditions for consent. *General Data Protection Regulation (GDPR)*. <https://gdpr-info.eu/art-7-gdpr/> (last accessed 2025/09/11).
7. Vamosi, S., Platzer, M., Reutterer, T.: AI-based Re-identification of Behavioral Clickstream Data. *arXiv preprint arXiv:2201.10351* (2022). <https://arxiv.org/abs/2201.10351>.
8. Gs, D.R., Lingam, D.M.S.: Blockchain Technology in Digital Advertising: Transparency, Fraud Prevention and Trust. *Educational Administration: Theory and Practice* 30(4), 3041–3049 (2024). <https://doi.org/10.53555/kuey.v30i4.1477>.

9. Mayorov, A.A.: Smart Contract as a New Way to Conclude a Contract. *Courier of Kutafin Moscow State Law University (MSAL)* 4, 143–150 (2022). <https://doi.org/10.17803/2311-5998.2022.92.4.143-150>.
10. Perez, A.J., Zeadally, S.: Secure and privacy-preserving crowdsensing using smart contracts: Issues and solutions. *Computer Science Review* 43, 100450 (2022). <https://doi.org/10.1016/j.cosrev.2021.100450>.
11. Intersoft Consulting: Art. 17 GDPR – Right to erasure (“right to be forgotten”). *General Data Protection Regulation (GDPR)*. <https://gdpr-info.eu/art-17-gdpr/> (last accessed 2025/09/11).
12. Circiumaru, A., Casolari, F., Taddeo, M., Turillazzi, A., Floridi, L.: How to Improve Smart Contracts in the European Union Data Act. *Digital Society* 2(1) (2023). <https://doi.org/10.1007/s44206-023-00038-2>.
13. Perez, A.J., Zeadally, S.: Secure and privacy-preserving crowdsensing using smart contracts: Issues and solutions. *Computer Science Review* 43, 100450 (2022). <https://doi.org/10.1016/j.cosrev.2021.100450>.
14. Lin, X., Zhang, Y., Huang, C., Xing, B., Chen, L., Hu, D., Chen, Y.: An Access Control System Based on Blockchain with Zero-Knowledge Rollups in High-Traffic IoT Environments. *Sensors* 23(7), 3443 (2023). <https://doi.org/10.3390/s23073443>.
15. ALqodsi, E.M., Arenova, L.: Smart Contracts in Contract Law as an Auxiliary Tool or a Promising Substitute for Traditional Contracts. *Journal of Legal Affairs and Dispute Resolution in Engineering and Construction* 16(3) (2024). <https://doi.org/10.1061/jladah.ladr-1132>.
16. Papadouli, V., Papakonstantinou, V.: A Preliminary Study on Artificial Intelligence Oracles and Smart Contracts: A Legal Approach to the Interaction of Two Novel Technological Breakthroughs. *Computer Law & Security Review* 51, 105869 (2023). <https://doi.org/10.1016/j.clsr.2023.105869>.
17. Knierim, E.R.: The Big FAQs About TOU. Founderslaw.com (2024). <https://www.founderslaw.com/insights/the-big-faqs-about-terms-of-use>.
18. Scientifico, S.: Ciclo XXXIII Settore Concorsuale: 12/A1 Implications of Blockchain-Based Smart Contracts on Contract Law. University of Bologna (2021).
19. Lex Cryptographia: Guidelines for Ensuring Due Process in Transnational Blockchain-Based Arbitration. *IBA.net* (2022). <https://www.ibanet.org/lex-cryptographia-due-process-blockchain-based-arbitration>.
20. Seo, J., Lee, J., Joo, Y., Lee, K., Sugumaran, V., Park, S.: A Blockchain-Based E-Participation Framework Utilizing Zero-Knowledge Proofs With Guaranteed Sampling and Differential Reward Mechanisms. *IEEE Access* 13, 25752–25764 (2025). <https://doi.org/10.1109/access.2025.3538006>.

Open Access This chapter is licensed under the terms of the Creative Commons Attribution-NonCommercial 4.0 International License (<http://creativecommons.org/licenses/by-nc/4.0/>), which permits any noncommercial use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.

