ISSLP
Interdisciplinary Studies in Society, Law and Politics

Original Research

International Privacy Protection Laws in Smart Contracts

Amin. Karimpour Aliabad[1]

[1] Department of Law, Yas.C., Islamic Azad University, Yasuj, Iran

*** Corresponding author email address**: 4231891915@iau.ac.ir

Received: 2026-01-08 **Revised:** 2026-05-04 **Accepted:** 2026-05-13 **Published:** 2026-05-01

This article examines the relationship between international privacy protection laws and smart contracts as automated instruments of blockchain-based transactions. Smart contracts offer efficiency, transparency, immutability, and decentralized execution, yet these same features create significant legal challenges for privacy protection. The article argues that the architecture of distributed ledgers may conflict with core data protection principles, including data minimization, purpose limitation, consent, transparency, accountability, rectification, and erasure. While blockchain systems often rely on pseudonymity, pseudonymous identifiers may still become personal data when linked to identifiable individuals through transaction analysis, wallet activity, or off-chain datasets. The study analyzes the conceptual foundations of privacy, the legal nature of smart contracts, and the main privacy risks associated with public ledgers, immutable storage, cross-border data flows, oracle systems, and unclear allocation of responsibility. It also evaluates comparative legal responses, particularly in rights-based and data-protection-oriented frameworks, and highlights the need for privacy-by-design approaches in smart contract development. The article concludes that privacy protection in smart contracts cannot depend solely on user consent, technical security, or decentralization claims. Instead, effective governance requires a combined legal and technological framework that minimizes on-chain personal data, uses cryptographic verification tools, clarifies accountability, and enables meaningful user control. Smart contracts can support privacy-preserving digital transactions only when legal compliance is embedded into their architecture from the beginning.

Keywords: *Smart contracts; privacy protection; blockchain; data protection law; international privacy law; privacy by design; personal data; decentralized governance.*

How to cite this article:
Karimpour Aliabad, A. (2026). International Privacy Protection Laws in Smart Contracts. *Interdisciplinary Studies in Society, Law, and Politics, 5*(3), 1-14. https://doi.org/10.61838/kman.isslp.495

1. Introduction

The rapid emergence of blockchain-based contracting has transformed the legal and technological imagination of contemporary commerce. Smart contracts are no longer merely a speculative innovation associated with cryptocurrencies; they are increasingly treated as instruments for automating transactions, reducing reliance on intermediaries, and embedding contractual performance into computational environments. Their appeal lies in the promise that contractual obligations can be translated into code and executed automatically when predefined conditions are satisfied. This transformation, however, does not eliminate legal complexity. Rather, it relocates many traditional legal concerns into a new technological architecture. One of the most significant concerns is the protection of privacy. The architecture of distributed ledgers, especially public blockchains, often depends on transparency, replication, and immutability, while privacy law depends on principles such as purpose limitation, data minimization, consent, accountability, and individual control over personal information. The tension between these logics has become one of the

central issues in the legal governance of smart contracts. The classic understanding of privacy as a right against unwanted intrusion has long been foundational in legal thought, beginning with the early formulation of privacy as the "right to be let alone" (Warren & Brandeis, 1890). Yet in the digital environment, privacy is no longer limited to secrecy or solitude; it increasingly concerns the collection, processing, circulation, inference, and governance of data across complex information systems (Solove, 2008). Smart contracts intensify this shift because they make legal and economic relationships dependent on automated data flows, computational execution, and distributed verification.

The legal significance of smart contracts cannot be understood without first recognizing their hybrid character. They are technological tools, but they also carry contractual, evidentiary, governance, and regulatory implications. Raskin explains that smart contracts raise questions about formation, enforcement, interpretation, and remedies because coded performance may not map neatly onto traditional doctrines of contractual intention and legal obligation (Raskin, 2017). De Filippi similarly emphasizes that blockchain systems challenge conventional legal categories because code can regulate behavior directly, sometimes before courts or regulators have the opportunity to intervene (De Filippi & Wright, 2018). In this sense, smart contracts do not merely digitize traditional contracts; they alter the temporal and institutional structure of contractual governance. In conventional contracting, legal rights and obligations may be interpreted after a dispute arises, but smart contracts may execute immediately and irreversibly once programmed conditions are met. This creates advantages of speed, reliability, and reduced transaction costs, yet it also produces risks when personal data is embedded into contractual logic. If a smart contract requires identity verification, credit scoring, health information, location data, biometric authentication, or transactional metadata, the execution of the contract may involve processing data that international privacy norms treat as legally protected. The problem is therefore not whether smart contracts can function technically, but whether they can function consistently with privacy protection obligations.

The central research problem of this article is the legal incompatibility that may arise between international privacy protection principles and the operational structure of smart contracts. Public blockchain systems often require that transactions be visible to network participants, stored across multiple nodes, and preserved permanently. Narayanan and colleagues show that blockchain transparency does not necessarily mean complete identification of users, because many systems use pseudonymous addresses rather than direct personal names (Narayanan et al., 2016). However, pseudonymity is not the same as anonymity. Transactional patterns, address clustering, off-chain identifiers, and external datasets may allow individuals to be reidentified. Zyskind, Nathan, and Pentland argue that blockchain may be used to improve personal data control, but they also acknowledge that the design of data storage and permission structures is crucial to determining whether privacy is protected or undermined (Zyskind et al., 2015). This distinction is essential for smart contracts because the privacy consequences of a smart contract depend not only on the code itself, but also on the blockchain infrastructure, the nature of the data processed, the identity mechanisms used, the role of oracles, and the governance arrangements surrounding the system. A smart contract that stores only cryptographic hashes may raise different privacy issues from one that records personal attributes directly on-chain. Likewise, a permissioned blockchain used among regulated institutions differs from a public blockchain accessible to anyone.

International privacy protection law has developed through multiple doctrinal traditions. Human rights law frames privacy as a fundamental interest linked to dignity, autonomy, and freedom from arbitrary interference. Data protection law, particularly in its European form, treats privacy as a regulatory framework for lawful, fair, transparent, and accountable data processing. Information privacy scholarship expands the analysis further by showing that privacy harms may include surveillance, aggregation, secondary use, exclusion, insecurity, disclosure, distortion, and decisional interference (Solove, 2008). Solove and Schwartz emphasize that modern privacy law must address institutional practices of data processing rather than focusing only on isolated acts of disclosure (Solove & Schwartz, 2021). This insight is especially relevant to smart contracts because privacy risks often arise from the entire ecosystem rather than from a single

transaction. A user may consent to one blockchain interaction without fully understanding that the transaction data will remain permanently visible, may be linked to other data, may be processed by analytics firms, or may be used across borders. Consequently, smart contracts must be assessed within the broader legal and infrastructural environment in which they operate.

The international dimension of this issue is particularly important. Blockchain networks are rarely confined to one jurisdiction. Nodes may be located in multiple states, users may transact across borders, developers may be dispersed globally, and data may be replicated without regard to territorial boundaries. Kuner's work on transborder data flows demonstrates that privacy law has long struggled with the movement of personal data across jurisdictions that apply different standards of protection (Kuner, 2013). Smart contracts intensify this challenge because they can automate cross-border transactions without identifying a clear territorial center of processing. Kahn and Kellaris similarly describe cross-border blockchain systems as legally difficult because responsibility, jurisdiction, and applicable law become fragmented when data is processed through decentralized infrastructures (Kahn & Kellaris, 2021). This raises practical questions about who qualifies as a data controller, whether blockchain participants are processors or joint controllers, how data subject rights can be exercised, and which national or regional authority has enforcement competence. These questions do not have simple answers because smart contract systems often distribute agency across developers, users, validators, protocol designers, wallet providers, exchanges, oracle services, and decentralized autonomous organizations.

The rise of smart contracts also coincides with broader transformations in digital capitalism. Blockchain advocates often describe distributed ledger technology as a mechanism for trust, disintermediation, and transparency. Tapscott and Tapscott present blockchain as a foundational technology capable of transforming financial systems, business models, and institutional trust (Tapscott & Tapscott, 2016). Casey and Vigna similarly describe blockchain as a trust machine that may reshape economic coordination by reducing reliance on centralized recordkeepers (Casey & Vigna, 2018). Yet privacy protection requires more than trust in technical architecture. A system may be transparent, tamper-resistant, and decentralized while still exposing individuals to surveillance, profiling, or loss of informational control. In fact, the very features that make blockchain attractive for verification may conflict with the legal need to limit data exposure. Swire and Litan's metaphor of fitting "square pegs into round holes" captures this difficulty, as blockchain's permanence and decentralization do not easily align with conventional privacy law mechanisms such as deletion, rectification, and centralized accountability (Swire & Litan, 2018). The legal challenge is therefore not simply to decide whether smart contracts are good or bad for privacy, but to determine under what conditions they can be designed and governed in ways compatible with international privacy norms.

The research objective of this article is to analyze how international privacy protection laws apply to smart contracts and to identify the legal and technical tensions that must be addressed in order to make smart-contract systems compatible with privacy rights and data protection obligations. The article examines the conceptual foundations of privacy protection, the technological characteristics of smart contracts, the major privacy risks created by blockchain-based contracting, and the comparative regulatory responses that may guide future legal development. The significance of the study lies in its attempt to connect legal doctrine with system design. Privacy protection in smart contracts cannot be achieved only through after-the-fact legal remedies, because many privacy harms become difficult or impossible to reverse once data is recorded on-chain. Cavoukian's concept of privacy by design is therefore central: privacy must be embedded into the architecture of information systems from the outset rather than added as an external compliance layer after deployment (Cavoukian, 2012). This article proceeds from the premise that privacy-compliant smart contracts require a combined legal and technical framework in which data minimization, cryptographic protection, governance accountability, and cross-border legal coordination operate together.

2. Conceptual and Legal Foundations

The conceptual foundation of privacy protection in smart contracts begins with the meaning of privacy itself. Privacy is not a single, fixed, or purely negative right. It includes personal autonomy, secrecy, dignity,

confidentiality, control over information, protection from surveillance, and the ability to participate in social and economic life without continuous exposure. Warren and Brandeis framed privacy as a legal response to technological change, especially the capacity of new media to intrude into personal life (Warren & Brandeis, 1890). Their insight remains important because each major communication technology has forced law to reconsider the boundaries of personal protection. In the blockchain environment, the intrusion is not necessarily physical or journalistic; it may occur through permanent transactional visibility, automated profiling, and the aggregation of pseudonymous records. Solove argues that privacy should be understood through a taxonomy of problems rather than reduced to secrecy or consent (Solove, 2008). This approach is useful for smart contracts because the privacy risks are diverse: information may be collected unnecessarily, stored permanently, linked across contexts, accessed by unknown actors, or used for purposes beyond the user's expectations. Therefore, the legal analysis must move beyond the narrow question of whether personal data is disclosed and instead ask how blockchain-based contracting restructures the entire life cycle of data.

Data protection law adds a more operational dimension to privacy. It focuses on identifiable information, lawful processing, rights of the data subject, obligations of controllers and processors, and institutional accountability. Solove and Schwartz explain that modern information privacy law developed because personal data processing became a structural feature of governance, commerce, and digital life (Solove & Schwartz, 2021). In smart contracts, data processing is not incidental; it may be embedded into the contract's execution logic. For example, a smart insurance contract may process weather data, location data, identity attributes, and payment information. A decentralized finance contract may process wallet addresses, asset balances, transaction histories, and risk profiles. A supply-chain smart contract may process business identities, shipment data, and compliance certifications. The legal difficulty is that these data points may become personal data when they relate to identifiable individuals or can be linked to them indirectly. Finck's analysis of blockchain and data protection in the European Union demonstrates that blockchain systems can fall within data protection law even where they use pseudonymous identifiers, because identifiability depends on the possibility of linkage rather than direct naming alone (Finck, 2018). This means that smart contract designers cannot avoid privacy obligations merely by replacing names with wallet addresses.

A central principle of privacy protection is consent, but consent becomes complicated in automated and decentralized systems. In traditional legal settings, consent is often treated as a manifestation of individual autonomy. In data protection law, however, consent must usually be informed, specific, freely given, and revocable. Smart contracts create several obstacles to meaningful consent. Users may interact with code they cannot read, with protocols whose future behavior may change, or with blockchain networks whose data retention practices are not easily reversible. Raskin explains that smart contracts may execute according to code even when human expectations are more nuanced than the program's formal conditions (Raskin, 2017). This matters for privacy because a user may click to approve a transaction without understanding that the smart contract interaction will generate permanent metadata accessible to third parties. Moerel and Prins argue that digital privacy frameworks must respond to the realities of pervasive datafication, where individuals often lack meaningful bargaining power or practical understanding of data flows (Moerel & Prins, 2016). In smart contracts, this problem is intensified by technical opacity. Even sophisticated users may not fully understand how on-chain and off-chain components interact, how oracle services provide external data, or how blockchain analytics may reconstruct identity from transaction patterns.

The principle of data minimization is another essential foundation. Data minimization requires that only necessary data be collected and processed for a legitimate purpose. This principle is difficult to reconcile with systems that replicate data across many nodes and preserve records indefinitely. Finck emphasizes that blockchain's append-only structure creates tension with data protection requirements because information stored on-chain is resistant to alteration or erasure (Finck, 2020). The issue is not simply that blockchain stores data; databases also store data. The distinctive problem is that blockchain may distribute copies across independent participants who are not easily controlled by a single legal actor. This complicates compliance with

rights such as erasure, rectification, objection, and restriction of processing. Swire and Litan note that blockchain's immutability challenges legal frameworks built around centralized data controllers who can modify or delete records when legally required (Swire & Litan, 2018). Smart contracts add another layer because the contract code itself may require or generate data as part of performance. If personal data is written directly into smart contract states, event logs, or transaction payloads, later compliance may become practically impossible. A privacy-conscious design must therefore avoid unnecessary on-chain personal data and rely where possible on off-chain storage, cryptographic commitments, selective disclosure, and permissioned access models.

Transparency has a dual meaning in this field. Blockchain transparency refers to the ability of network participants to verify transactions and inspect ledger states. Legal transparency refers to the ability of individuals to understand how their data is processed, by whom, for what purposes, and with what consequences. These two meanings may conflict. A public blockchain may be technically transparent because all transactions are visible, yet legally opaque because users do not understand the privacy implications of the system. De Filippi and Wright argue that blockchain creates new forms of governance in which code, protocol design, and network consensus shape behavior alongside formal law (De Filippi & Wright, 2018). This insight shows that legal transparency must extend to technical governance. Users need not only contractual terms but also intelligible information about data flows, smart contract functions, upgrade mechanisms, oracle dependencies, and risks of public traceability. Cavoukian's privacy-by-design framework supports this orientation because it treats privacy as proactive, preventive, embedded, and user-centric (Cavoukian, 2012). In the smart contract context, this means that transparency should not be limited to publishing source code. Legal transparency requires explainable interfaces, clear allocation of responsibilities, accessible privacy notices, auditability, and mechanisms for meaningful user control.

Accountability is equally important. International privacy protection depends on the ability to identify responsible actors and impose obligations upon them. In centralized systems, responsibility can usually be assigned to organizations that determine the purposes and means of processing. In decentralized systems, this allocation becomes uncertain. Kahn and Kellaris argue that cross-border blockchain systems create accountability problems because participants may be distributed across jurisdictions and may perform different technical and legal roles (Kahn & Kellaris, 2021). A developer may write the code, a deployer may launch the contract, validators may maintain the ledger, users may trigger functions, and front-end providers may facilitate access. Whether any of these actors should be treated as a controller or processor depends on their degree of influence over data processing. Kuner's analysis of transborder data flows shows that international privacy law must address not only data movement but also institutional responsibility across borders (Kuner, 2013). Smart contracts complicate this because some systems are intentionally designed to minimize centralized control. However, absence of centralized control does not necessarily mean absence of responsibility. Legal systems may look to functional control, economic benefit, governance authority, or capacity to influence processing when assigning obligations.

The cryptographic foundations of smart contracts are also legally relevant. Cryptography may protect confidentiality, authenticate transactions, and support selective disclosure. Katz and Lindell's work on modern cryptography clarifies that cryptographic systems can provide confidentiality, integrity, authentication, and secure computation, but their effectiveness depends on design assumptions, key management, and implementation quality (Katz & Lindell, 2014). Blockchain privacy is therefore not automatically guaranteed by cryptography. Public-key addresses may obscure civil identity, yet they also create persistent identifiers that can be analyzed over time. Zero-knowledge proofs, encryption, secure multiparty computation, and commitment schemes may reduce data exposure, but they must be integrated into legal compliance strategies. Kshetri argues that blockchain can strengthen cybersecurity and privacy when properly designed, particularly by reducing reliance on vulnerable centralized databases and enabling more secure data verification (Kshetri, 2021). However, cybersecurity and privacy are related but not identical. A system may be secure against tampering while still privacy-invasive. For smart contracts, legal compliance requires both

technical security and principled limitation of data processing.

The conceptual framework for this article therefore rests on four interconnected elements: privacy as a human and informational interest, data protection as a legal governance regime, smart contracts as automated and distributed contractual infrastructures, and international law as a fragmented but evolving field of cross-border regulation. The article treats smart contracts not as isolated pieces of code but as socio-technical systems involving legal relationships, data flows, institutional actors, and technical protocols. This approach aligns with Wirtz and Lihotzky's view of smart contracts as governance mechanisms rather than merely technological scripts (Wirtz & Lihotzky, 2020). It also reflects Zwitter's broader argument that big data and international privacy regulation require legal systems to address scale, complexity, and transnationality (Zwitter, 2014). In the context of smart contracts, privacy protection cannot be reduced to user consent, cryptographic pseudonymity, or national regulation alone. It must be understood as a layered framework in which design choices, legal obligations, institutional accountability, and cross-border cooperation determine whether automation enhances or undermines privacy.

3. Privacy Risks and Compliance Challenges in Smart Contracts

The most visible privacy risk in smart contracts arises from public ledger exposure. In many blockchain systems, transaction histories are publicly accessible, replicated across nodes, and analyzable by anyone with sufficient technical capacity. Although users may appear through alphanumeric addresses rather than legal names, these addresses can become persistent identifiers. Narayanan and colleagues demonstrate that cryptocurrency systems involve complex relationships between pseudonymity, transaction transparency, and network analysis (Narayanan et al., 2016). This is directly relevant to smart contracts because smart contract interactions may reveal more than simple payments. They may disclose the types of services used, the timing of interactions, asset ownership, governance votes, lending behavior, insurance claims, or participation in decentralized applications. When such patterns are linked to real-world identities through exchanges, wallet providers, social media, IP data, or commercial analytics, the privacy risk becomes significant. The problem is not only that personal data may be placed on-chain, but also that behavioral profiles may be inferred from on-chain activity. Solove's taxonomy of privacy harms is useful here because aggregation and secondary use can be as harmful as direct disclosure (Solove, 2008). A smart contract may not reveal a user's name, yet it may expose enough contextual information to make the user vulnerable to profiling, discrimination, financial targeting, or surveillance.

Immutability creates another major compliance challenge. Blockchain immutability is often praised because it strengthens evidentiary integrity and reduces the risk of unauthorized alteration. Casey and Vigna describe blockchain's value as partly dependent on its ability to create reliable records without centralized trust (Casey & Vigna, 2018). However, privacy law often requires flexibility after data has been collected. Individuals may have rights to correct inaccurate data, withdraw consent, object to processing, restrict use, or request erasure. Finck explains that blockchain's immutability creates a direct tension with such rights because data stored on-chain may not be practically removable (Finck, 2020). Even where data is encrypted, the permanence of encrypted personal data may still be legally problematic if future decryption becomes possible or if the encrypted record remains linkable to an individual. Swire and Litan similarly argue that blockchain systems challenge the assumption that a legally responsible entity can simply delete or modify data upon request (Swire & Litan, 2018). Smart contracts worsen this difficulty because data may be embedded into contract states or execution histories. Once a function is called and recorded, the transaction may become part of a permanent public record. This requires developers to think carefully before placing any personal data on-chain, because later legal compliance may be technically constrained.

A third risk concerns the role of oracles and off-chain data sources. Smart contracts are often described as self-executing, but many require external information to determine whether conditions have been satisfied. Christidis and Devetsikiotis explain that smart contracts in Internet of Things environments may depend on data from sensors, devices, and external systems (Christidis & Devetsikiotis, 2016). These data sources may include

personal information such as location, biometric indicators, consumption habits, health data, or behavioral patterns. The oracle does not merely transmit neutral facts; it becomes a critical point where privacy risks, security vulnerabilities, and legal responsibilities converge. If an oracle collects excessive data, transmits data insecurely, or provides inaccurate information, the smart contract may execute in a way that harms the data subject. Moreover, the user may not know which oracle is being used, what data it collects, how long it retains the data, or whether it shares the data with third parties. Huckle and White's analysis of FinTech and blockchain privacy highlights the importance of understanding data processing across the entire financial technology ecosystem rather than focusing only on the ledger itself (Huckle & White, 2019). In smart contracts, privacy compliance must therefore include oracle governance, off-chain storage arrangements, API providers, identity verification systems, and user interfaces.

Cross-border data flows represent a further compliance challenge. Smart contracts often function across borders by design. A user in one country may interact with a decentralized protocol developed in another country, hosted through front-end infrastructure in a third country, and validated by nodes distributed globally. Kuner's work shows that transborder data flows create enduring legal difficulties because privacy protections vary across jurisdictions and because data may move to places with different levels of protection (Kuner, 2013). In blockchain systems, this challenge becomes more complex because data may not simply "move" from one controller to one recipient; it may be replicated across an indeterminate network. Kahn and Kellaris describe this as a major challenge for blockchain-based data protection because jurisdiction, enforcement, and responsibility may become difficult to locate (Kahn & Kellaris, 2021). Smart contracts used in international trade, decentralized finance, digital identity, or supply-chain management may process data in ways that trigger multiple privacy regimes simultaneously. The result is a risk of regulatory conflict, where compliance with one jurisdiction's rules may not satisfy another's, and where decentralized actors may find it unclear which rules apply at all.

Another serious risk is the insufficiency of anonymization. Many blockchain projects rely on the claim that data is not personal because it is pseudonymous. However, privacy law often treats pseudonymous data as protected when reidentification is reasonably possible. Finck's analysis of European data protection and blockchain emphasizes that blockchain addresses may qualify as personal data if they can be linked to identifiable persons (Finck, 2018). This is especially important for smart contracts because users frequently interact with the same wallet across multiple services. Even if each individual transaction appears harmless, a long-term pattern may reveal sensitive information. Zyskind, Nathan, and Pentland propose decentralized privacy architectures that allow users to control access to personal data rather than surrendering it to centralized platforms (Zyskind et al., 2015). Their approach suggests that blockchain can support privacy-enhancing models, but only if personal data is not carelessly exposed. The compliance challenge is therefore to distinguish between privacy-preserving decentralization and transparency-based exposure. A smart contract that verifies eligibility through a zero-knowledge proof may protect privacy, while a smart contract that records eligibility attributes directly on-chain may violate data minimization principles.

Consent and user comprehension also present significant risks. Smart contract systems often require users to approve transactions through wallets, but a transaction approval is not the same as informed consent to data processing. Solove and Schwartz emphasize that privacy notices and consent mechanisms often fail when they are too complex, frequent, or disconnected from real user understanding (Solove & Schwartz, 2021). In decentralized applications, users may approve permissions without understanding the legal and technical consequences. They may not know whether their transaction will be permanently recorded, whether the smart contract can be upgraded, whether a governance body can change rules, whether data will be analyzed by third parties, or whether the protocol has been audited. Raskin's discussion of smart contract legality shows that code may execute rigidly even when human expectations are incomplete or mistaken (Raskin, 2017). In privacy terms, this means that formal user approval cannot substitute for meaningful transparency and fair processing. The challenge is especially acute where users are consumers rather than technical experts. If smart contracts become common in insurance, employment, finance, healthcare, or public services, the

imbalance between technical complexity and user understanding may become a major privacy justice issue. Security vulnerabilities create another pathway to privacy harm. Smart contracts may contain coding errors, flawed access controls, insecure dependencies, or vulnerabilities in linked applications. Katz and Lindell's cryptographic analysis reminds us that secure systems require rigorous design and correct implementation, not merely the use of cryptographic terminology (Katz & Lindell, 2014). A smart contract may use cryptographic signatures and still leak data through event logs, metadata, poor key management, or insecure oracles. Kshetri argues that blockchain can strengthen cybersecurity by reducing single points of failure, improving integrity, and supporting more secure verification mechanisms (Kshetri, 2021). Yet decentralized systems also introduce new risks, including irreversible transactions, exposed smart contract bugs, and distributed attack surfaces. Privacy law increasingly treats security as part of data protection because unauthorized access, loss, or misuse of personal data can cause serious harm. In smart contract systems, a vulnerability may not only expose data but also trigger automated execution based on compromised information. Therefore, privacy compliance must include security audits, formal verification where appropriate, careful access control, secure key management, and incident response mechanisms.

A further compliance challenge concerns governance. Many smart contracts are deployed in decentralized ecosystems where no single actor appears to be in charge. De Filippi and Wright argue that blockchain governance operates through a combination of code, community norms, economic incentives, and legal institutions (De Filippi & Wright, 2018). This hybrid governance creates uncertainty for privacy enforcement. If a smart contract violates privacy obligations, who must respond? The developer, the deployer, the decentralized autonomous organization, the validators, the front-end operator, or the users? Wirtz and Lihotzky characterize smart contracts as governance mechanisms because they structure behavior and decision-making through automated rules (Wirtz & Lihotzky, 2020). This means that governance design is not external to privacy protection; it is part of it. A privacy-compliant smart contract system should include mechanisms for accountability, auditing, user rights requests, dispute resolution, emergency intervention, and legal representation. Fully immutable and ungoverned systems may be attractive from a decentralization perspective, but they can create serious difficulties when privacy harms occur or when legal obligations require a response.

Finally, smart contracts raise questions about fairness and power. Privacy risks are not distributed equally. Sophisticated actors may use blockchain analytics, legal structuring, and technical expertise to extract value from data, while ordinary users may bear the risks of exposure. Zwitter's work on big data and international privacy regulation highlights the need to address power asymmetries created by large-scale data processing (Zwitter, 2014). In smart contracts, these asymmetries may arise when platforms present decentralized systems as user-controlled while retaining influence through interfaces, governance tokens, upgrade keys, or proprietary analytics. Moerel and Prins argue that privacy law must adapt to a world where data-driven systems shape human autonomy and social participation (Moerel & Prins, 2016). This is directly relevant to smart contracts because automated execution may make data-based decisions immediate and difficult to contest. The compliance challenge is therefore not merely technical. It is also institutional and ethical. Smart contracts must be designed so that privacy protection is not dependent solely on the user's technical literacy, bargaining power, or ability to avoid harmful systems. The future of privacy-compliant smart contracts depends on embedding legal safeguards into architecture, governance, and market practice.

4. International Legal Responses and Comparative Analysis

International privacy protection in smart contracts is shaped by fragmented but increasingly convergent legal principles. Although no single global treaty comprehensively governs smart contracts and blockchain privacy, many legal systems recognize privacy, data protection, cybersecurity, and cross-border data governance as essential regulatory domains. The European approach is especially influential because it treats data protection as a rights-based and compliance-oriented framework. Finck's work on blockchain and data protection in the European Union shows that blockchain systems must be evaluated in light of

principles such as lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, confidentiality, and accountability (Finck, 2018). These principles are highly relevant to smart contracts because the execution of coded obligations may involve personal data at multiple stages. Huckle and White further show that financial technology applications using blockchain face significant privacy obligations when they process user data in regulated financial environments (Huckle & White, 2019). The European model is not merely regional in practical effect because many blockchain projects operate globally and may need to comply with European standards if they involve European users or data subjects. Therefore, European data protection law has become a major reference point for international analysis.

One of the most difficult questions under the European-style approach is identifying the controller. A controller determines the purposes and means of data processing, but smart contract systems often distribute control. Finck argues that blockchain networks challenge the controller-processor distinction because different actors may influence different parts of the system (Finck, 2020). For example, developers may design a smart contract, but users may decide whether to interact with it. Validators may maintain the ledger, but they may not determine the purpose of a particular transaction. A decentralized organization may vote on protocol changes, while a front-end provider may determine how users access the service. Kahn and Kellaris identify similar difficulties in cross-border blockchain systems, where legal responsibility may be difficult to allocate among dispersed technical actors (Kahn & Kellaris, 2021). Comparative analysis suggests that privacy protection cannot rely only on formal decentralization claims. Regulators may increasingly examine functional control, economic benefit, and governance power. If a platform markets a smart contract service, designs the interface, controls updates, and benefits from user data, it may be difficult to deny responsibility simply because the underlying ledger is decentralized.

The right to erasure or deletion is another point of legal tension. Traditional data protection systems assume that data can be modified, deleted, or restricted by the responsible organization. Blockchain systems often resist this assumption. Swire and Litan's analysis captures the structural mismatch between blockchain immutability and legal rights that require post-collection intervention (Swire & Litan, 2018). Finck likewise emphasizes that storing personal data directly on-chain may be incompatible with rights that require correction or erasure (Finck, 2020). Comparative legal responses increasingly point toward architectural solutions rather than purely doctrinal ones. One approach is to avoid storing personal data on-chain and instead store data off-chain under the control of a legally responsible entity. Another approach is to store only hashes, commitments, or proofs on-chain, though even hashes may raise legal issues if they are linkable or derived from personal data. Zyskind, Nathan, and Pentland's proposal for decentralized personal data control illustrates how blockchain can be used as an access-control layer rather than as a repository of personal information (Zyskind et al., 2015). This approach aligns more closely with privacy law because it separates verification from exposure.

The United States presents a different comparative model because its privacy law has traditionally been sectoral, fragmented, and more closely connected to consumer protection, tort, constitutional doctrine, and specific regulatory domains. Solove and Schwartz describe information privacy law as a broad field that includes statutory, regulatory, constitutional, and common-law dimensions (Solove & Schwartz, 2021). This fragmentation matters for smart contracts because privacy obligations may vary depending on whether the smart contract is used in finance, healthcare, education, employment, consumer commerce, or government services. A decentralized finance protocol may raise financial privacy and cybersecurity questions, while a healthcare smart contract may involve sensitive medical information. The U.S. model may allow innovation through flexible sectoral development, but it may also leave gaps where smart contract applications do not fit neatly into existing categories. The foundational privacy tradition of Warren and Brandeis still informs American privacy thought by emphasizing protection against intrusive uses of personal information (Warren & Brandeis, 1890). However, smart contracts require more than tort-based remedies after intrusion occurs. Because blockchain privacy harms may be permanent and difficult to reverse, preventive regulation and privacy-by-design principles become especially important.

International and comparative analysis must also consider the role of private governance. Blockchain ecosystems often develop standards, audits, code repositories, governance forums, and technical norms before formal law fully responds. De Filippi and Wright argue that blockchain governance involves both legal regulation and regulation by code (De Filippi & Wright, 2018). This means that international privacy protection may emerge not only from statutes and treaties but also from design practices, developer norms, certification systems, and contractual governance. Cavoukian's privacy-by-design framework is especially influential here because it provides a normative bridge between legal principles and technical implementation (Cavoukian, 2012). Privacy by design requires proactive prevention, default protection, embedded safeguards, full functionality, end-to-end security, visibility, transparency, and respect for users. In smart contracts, these principles may translate into off-chain storage of personal data, zero-knowledge verification, minimal event logging, role-based access control, privacy-preserving identity systems, clear governance structures, and meaningful user interfaces. Comparative legal systems may differ in enforcement, but privacy by design offers a common operational vocabulary.

Cross-border data transfer rules are particularly important for international smart contracts. Kuner explains that transborder data flow regulation seeks to prevent personal data from losing protection when transferred across jurisdictions (Kuner, 2013). Smart contracts complicate this because data may be replicated, validated, or accessed globally without a conventional transfer from one identifiable exporter to one identifiable importer. Kahn and Kellaris show that blockchain systems create difficulties for territorial privacy regulation because distributed infrastructures do not map cleanly onto national borders (Kahn & Kellaris, 2021). A comparative legal response must therefore address whether blockchain replication counts as international transfer, whether node operators in other jurisdictions are recipients, and whether users can be informed meaningfully about the countries in which their data may be processed. In permissioned blockchain systems, these questions may be manageable because participants are known and governed by contractual arrangements. In public permissionless systems, they are much harder. This suggests that smart contracts involving personal or sensitive data may be more compatible with permissioned or hybrid architectures than with fully public blockchains.

The relationship between privacy and cybersecurity also differs across legal systems but is increasingly central everywhere. Kshetri emphasizes that blockchain can improve cybersecurity by enhancing integrity, decentralizing records, and reducing dependence on vulnerable centralized databases (Kshetri, 2021). However, international privacy laws generally require not only secure storage but also lawful and limited processing. Katz and Lindell's work on cryptography indicates that technical security depends on robust assumptions and proper implementation (Katz & Lindell, 2014). In smart contracts, legal compliance may require independent code audits, vulnerability disclosure processes, encryption standards, secure oracle design, and governance arrangements for responding to breaches. The international trend is toward treating security as part of accountability. A smart contract provider or governance body cannot simply claim that blockchain is secure by nature. It must demonstrate that the specific system has been designed, tested, monitored, and governed in a way that protects data subjects. This is especially important where smart contracts process financial or sensitive personal information.

A comparative analysis of blockchain privacy also reveals different attitudes toward transparency. Blockchain communities often valorize transparency because it supports verification and trust. Tapscott and Tapscott describe blockchain as a technology that may transform trust by making records more transparent and tamper-resistant (Tapscott & Tapscott, 2016). Casey and Vigna likewise emphasize the institutional significance of distributed verification (Casey & Vigna, 2018). Yet legal systems distinguish between accountability transparency and exposure transparency. Privacy law does not reject transparency; it requires transparency toward the data subject and accountability to regulators. But it does not require public exposure of personal transactional histories. The challenge is to design smart contracts that preserve verifiability without unnecessary disclosure. Zero-knowledge proofs, selective disclosure credentials, and cryptographic commitments may allow parties to prove compliance or eligibility without revealing underlying personal data. This reflects a deeper shift from data publication to data verification.

International privacy protection will likely favor systems that can demonstrate facts without exposing identities or raw personal information.

Smart contracts also raise questions about contractual autonomy and mandatory privacy protections. Parties may choose to use smart contracts, but they cannot necessarily waive fundamental privacy rights or data protection obligations. Raskin's legal analysis shows that smart contracts must still be situated within broader legal doctrines and cannot be treated as outside law merely because they execute through code (Raskin, 2017). De Filippi and Wright similarly argue that blockchain systems exist in a relationship of interaction with legal systems, not in complete independence from them (De Filippi & Wright, 2018). This is important because some blockchain discourse suggests that code can replace law. From the perspective of international privacy protection, this claim is untenable. Code may automate performance, but it cannot determine by itself whether data processing is lawful, fair, proportionate, or respectful of human dignity. Legal systems will continue to impose mandatory obligations, especially where personal data, consumers, vulnerable individuals, or cross-border services are involved. Smart contract design must therefore incorporate legal compliance rather than assuming that technical execution displaces legal review.

The comparative future of smart contract privacy will likely involve hybrid governance. Purely national regulation is insufficient because blockchain systems are transnational. Purely technical self-regulation is insufficient because privacy is a legal and human interest, not merely an engineering preference. Purely contractual consent is insufficient because users often lack technical knowledge and bargaining power. Moerel and Prins argue that privacy frameworks must be revised for the digital individual whose life is increasingly mediated by data systems (Moerel & Prins, 2016). Zwitter similarly emphasizes that international privacy regulation must address large-scale data processing and global data power (Zwitter, 2014). In smart contracts, this means that legal responses should combine international principles, domestic enforcement, technical standards, industry certification, and user rights mechanisms. Regulators should encourage architectures that avoid on-chain personal data, support privacy-preserving verification, clarify accountability, and provide remedies when automated execution causes harm. Developers should treat privacy as a design requirement rather than a compliance afterthought. Users should be given intelligible explanations, not merely code repositories or transaction prompts.

5. Conclusion

Smart contracts have introduced a new stage in the evolution of digital contracting by converting certain forms of contractual performance into automated computational processes. Their legal significance lies not only in their ability to execute transactions without traditional intermediaries, but also in their capacity to restructure the relationship between law, code, data, and institutional trust. Privacy protection stands at the center of this transformation because smart contracts often depend on the collection, verification, and transmission of information. In many cases, that information may be personal, linkable, sensitive, or commercially revealing. Even where smart contracts do not directly store names or obvious identifiers, they may generate transaction patterns, behavioral records, and metadata capable of exposing individuals to profiling and surveillance. The central finding of this article is that smart contracts create a structural tension between blockchain transparency and privacy protection. Transparency may support verification, but it may also produce unwanted exposure. Immutability may support evidentiary reliability, but it may also frustrate correction, erasure, and withdrawal of consent. Decentralization may reduce dependence on central intermediaries, but it may also obscure responsibility and complicate enforcement.

International privacy protection laws provide important principles for addressing these tensions, but they were not originally designed for decentralized and immutable infrastructures. Principles such as lawfulness, fairness, transparency, purpose limitation, data minimization, security, accountability, and user control remain highly relevant. Yet their application to smart contracts requires reinterpretation and technical adaptation. The problem is not that privacy law is obsolete. Rather, the problem is that privacy law must be operationalized within new architectures. A smart contract cannot be considered privacy-compliant merely because it is technically secure or because it uses pseudonymous blockchain addresses. Compliance requires a broader

inquiry into whether personal data is processed, whether users understand the processing, whether data is necessary for the contractual purpose, whether data can be corrected or deleted where legally required, whether responsible actors can be identified, and whether the system provides effective remedies for privacy harm. These questions must be answered before deployment, not only after disputes arise.

The analysis also shows that privacy risks in smart contracts are not limited to on-chain storage. They may arise from oracles, wallet providers, front-end interfaces, analytics firms, identity systems, governance mechanisms, and off-chain databases. A smart contract is therefore not merely a piece of code. It is part of a broader socio-technical system. Privacy protection must address the whole system rather than focusing narrowly on the blockchain ledger. If personal data is kept off-chain but oracle providers collect excessive information, privacy risks remain. If a protocol avoids direct identifiers but creates persistent behavioral traces, privacy risks remain. If users approve transactions without meaningful understanding, privacy risks remain. If governance is decentralized in form but controlled in practice by a small group of actors, accountability risks remain. Effective legal analysis must therefore look beyond formal labels and examine functional control, technical architecture, economic benefit, and practical user impact.

The international character of smart contracts makes the problem more complex. Blockchain systems frequently operate across borders, and their participants may be located in different legal systems. This creates uncertainty about applicable law, jurisdiction, enforcement, and cross-border data transfers. Public permissionless networks are especially difficult because personal data may be replicated across unknown nodes in multiple jurisdictions. Permissioned and hybrid systems may offer greater compliance capacity because participants can be identified, responsibilities can be allocated contractually, and technical controls can be implemented more effectively. However, even permissioned systems must avoid excessive data collection and must provide meaningful safeguards. The comparative lesson is that no single legal model can fully resolve the privacy challenges of smart contracts. Rights-based privacy regimes provide strong principles, sectoral regimes provide contextual flexibility, and technical governance provides operational tools. The most viable path is an integrated approach that combines legal obligations with privacy-preserving design.

One of the most important recommendations is that personal data should not be stored directly on public blockchains unless there is a compelling and legally justified reason. In most cases, smart contract systems should use off-chain data storage, cryptographic proofs, hashed references, selective disclosure mechanisms, and privacy-preserving identity tools. However, even these tools must be used carefully. A hash may still be problematic if it is linkable to personal data or if the underlying data can be reconstructed. Encryption may not solve privacy problems if encrypted data remains permanently available and future decryption is possible. Pseudonymity may not be sufficient if transaction analysis can identify users. The guiding principle should be minimization by architecture: the system should be designed so that the smart contract verifies only what it needs to verify and exposes as little personal information as possible. Verification should replace disclosure wherever feasible.

Another key recommendation is that privacy by design should become a mandatory expectation for smart contract development. Developers, legal advisers, businesses, and regulators should treat privacy as a core design requirement at the earliest stage of system architecture. Privacy impact assessments should be conducted before deployment, especially where smart contracts involve financial information, identity data, health data, employment data, consumer data, or cross-border transactions. Code audits should include privacy analysis, not only security analysis. User interfaces should explain data consequences in clear language. Governance arrangements should specify who is responsible for responding to data subject requests, security incidents, disputes, and regulatory inquiries. Smart contracts that cannot support any meaningful accountability mechanism should not be used for processing personal or sensitive data in high-risk contexts.

Regulators should also develop clearer guidance for blockchain-based contracting. Existing privacy principles are valuable, but many actors need more specific direction on issues such as controller identification, on-chain personal data, smart contract

auditability, oracle responsibility, decentralized governance, cross-border node participation, and privacy-preserving verification. International coordination is especially important because fragmented regulation may either discourage responsible innovation or allow privacy-invasive systems to exploit jurisdictional gaps. International standards, model clauses, technical certification mechanisms, and regulatory sandboxes could help align innovation with privacy protection. However, such mechanisms should not weaken fundamental rights or allow privacy to become a purely voluntary market feature. The purpose of legal development should be to make privacy compliance practical without reducing the level of protection owed to individuals.

The article also emphasizes that users should not carry the full burden of privacy protection. In many smart contract systems, users are expected to read technical documentation, understand wallet permissions, evaluate code risks, and accept permanent data consequences. This expectation is unrealistic for ordinary participants. Legal systems should therefore require developers and service providers to provide accessible explanations, default privacy protection, and meaningful choices. Consent should not be treated as valid when users cannot reasonably understand the data consequences of their actions. The future legitimacy of smart contracts depends on whether users can participate in automated digital transactions without being forced to surrender privacy through complexity, opacity, or lack of alternatives.

Ultimately, smart contracts can either undermine or strengthen privacy depending on how they are designed and governed. They may undermine privacy when they expose personal data, create permanent behavioral records, obscure responsibility, and deny users effective control. They may strengthen privacy when they use cryptographic verification, decentralized identity, data minimization, secure architecture, and accountable governance. The legal challenge is to direct technological development toward the second path. International privacy protection laws should not be viewed as barriers to smart contract innovation. They should be understood as conditions for trustworthy innovation. A smart contract ecosystem that disregards privacy may achieve technical automation but fail to achieve legal legitimacy. A privacy-respecting smart contract ecosystem, by contrast, can combine automation with dignity, efficiency with accountability, and decentralization with rights protection.

Authors' Contributions

Authors contributed equally to this article.

Declaration

In order to correct and improve the academic writing of our paper, we have used the language model ChatGPT.

Transparency Statement

Data are available for research purposes upon reasonable request to the corresponding author.

Acknowledgments

We would like to express our gratitude to all individuals helped us to do the project.

Declaration of Interest

The authors report no conflict of interest.

Funding

According to the authors, this article has no financial support.

Ethical Considerations

In this research, ethical standards including obtaining informed consent, ensuring privacy and confidentiality were observed.

References

Casey, M., & Vigna, P. (2018). *The Truth Machine: The Blockchain and the Future of Everything*. St. Martin's Press.

Cavoukian, A. (2012). *Privacy by Design: The Definitive Workshop*. Information & Privacy Commissioner of Ontario.

Christidis, K., & Devetsikiotis, M. (2016). Blockchains and Smart Contracts for the Internet of Things. *IEEE Access*, *4*, 2292-2303.

De Filippi, P., & Wright, A. (2018). Blockchain and the Law: The Role of Smart Contracts in Privacy Compliance. *Harvard Journal of Law & Technology*, *31*(2), 487-524.

Finck, M. (2018). Blockchains and Data Protection in the European Union. *Eur. Law J.*, *24*(6), 923-947.

Finck, M. (2020). *Blockchain and Data Protection: Challenges and Legal Implications*. Oxford University Press.

Huckle, S., & White, M. (2019). FinTech and the GDPR: Implications for Blockchain Privacy. *Journal of Financial Regulation and Compliance*, *27*(2), 190-205.
Kahn, R., & Kellaris, G. (2021). Data Protection Challenges in Cross-Border Blockchain Systems. *Computer Law & Security Review*, *41*(3), 105-124.
Katz, J., & Lindell, Y. (2014). Introduction to Modern Cryptography. *Journal of Cryptology*, *27*(1), 1-30.
Kshetri, N. (2021). *Blockchain's Roles in Strengthening Cybersecurity and Protecting Privacy*. MIT Press.
Kuner, C. (2013). *Transborder Data Flows and Data Privacy Law*. Oxford University Press.
Moerel, L., & Prins, C. (2016). Privacy for the Homo Digitalis: Proposal for a Revised Privacy Framework. *International Data Privacy Law*, *6*(2), 82-104.
Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton University Press.
Raskin, M. (2017). The Law and Legality of Smart Contracts. *Georgetown Law Technology Review*, *1*(2), 305-341.
Solove, D. J. (2008). *Understanding Privacy*. Harvard University Press.
Solove, D. J., & Schwartz, P. M. (2021). *Information Privacy Law*. Aspen Publishers.
Swire, P., & Litan, A. (2018). Privacy and Blockchain: Fitting Square Pegs into Round Holes. *Journal of Law, Technology & Policy*, *2018*, 1-36.
Tapscott, D., & Tapscott, A. (2016). *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World*. Portfolio.
Warren, S. D., & Brandeis, L. D. (1890). *The Right to Privacy*. Harvard Law Review.
Wirtz, B. W., & Lihotzky, N. (2020). Smart Contracts as a Governance Mechanism. *Electronic Markets*, *30*(2), 277-294.
Zwitter, A. (2014). Big Data and International Privacy Regulation. *Journal of International Affairs*, *67*(1) 1-14.
Zyskind, G., Nathan, O., & Pentland, A. (2015). Decentralizing Privacy: Using Blockchain to Protect Personal Data. *IEEE Security & Privacy*, *13*(5), 23-33.