Fall 11-2023

Ensuring Data Privacy in a Decentralized World: An Analysis of the Legal Challenges and Implications of Smart Contracts

Khusbeen Dhillon
University of San Francisco, dhillonkhusbeen@gmail.com

Ensuring Data Privacy in a Decentralized World: An Analysis of the Legal Challenges and Implications of Smart Contracts

Khusbeen Dhillon

USF School of Law

November 2023

INTRODUCTION

In a world where contracts were once stacks of paper that would get locked into filing cabinets once they were signed, the digital drive has been revolutionary in improving efficiency for contracting. Advances in technology have further revolutionized what a contract can be: lines of code that are stored on a decentralized network, otherwise known as smart contracts. Smart contracts use blockchain technology to create "self-executing" agreements, which are simply a series of "if then" conditions that remove some of the human discretion involved in contracting.[1] As the use of blockchain technology is increasingly adopted across industries, smart contracts are projected to give a better solution to conventional contracts in terms of reducing risk, reducing costs, and enhancing the efficiency of corporate processes in a variety of businesses.[2] However, this new era of technology comes with a set of complex legal challenges that must be addressed before smart contracts can fully transform the way that business is conducted.

This paper examines the legal challenges and implications that arise in the context of data privacy laws within the United States in the implementation and enforcement of smart contracts and addresses how these challenges can potentially be resolved. Section I provides an overview of blockchain technology. Section II explains what smart contracts are and how they operate on the blockchain. Section III provides an in-depth examination of data privacy laws in the United States, focusing on relevant legislation within the country and drawing a comparison to the comprehensive scheme that the European Union has adopted. Section IV delves into specific privacy challenges that smart contracts may pose. Section V discusses the legal challenges that arise from the intersection of smart contracts and data privacy laws. Finally, Section VI discusses

[1] Adam Sulkowski, *Blockchain, Business Supply Chains, Sustainability, and Law: The Future of Governance, Legal Frameworks, and Lawyers?*, 43 DEL. J. CORP. L. 303, 309 (2019).
[2] Hamed Taherdoost, *Smart Contracts in Blockchain Technology: A Critical Review*, 14(2) INFORMATION 117 (2023).

a proposal for a federal data privacy regulation scheme that addresses the legal challenges associated with smart contracts.

I. BLOCKCHAIN OVERVIEW

Blockchain technology is the use of a distributed and decentralized ledger to verify and record transactions through a peer-to-peer network of computers.[3] Technically speaking, blockchain is a database that consists of chronically arranged bundles of transactions, also known as blocks, on which any proposed transaction can be checked with confidence in the validity of any particular block.[4] Once information is entered on the blockchain, it is immutable, meaning that it cannot be altered or erased.[5] Additionally, this information is transparent and public, meaning that it can be viewed by anyone at any time.

One of the most prominent use cases of blockchain technology is cryptocurrencies. Since this is the most widely known and accepted use of blockchain, many people mistakenly equate the two terms whereas blockchain is, in fact, the underlying technology that enables cryptocurrency transactions. However, its potential extends far beyond cryptocurrencies, and many industries ranging from finance to healthcare have made use of this transformative technology. Real-world applications of blockchain in decentralized finance, supply chain management, healthcare, voting systems, intellectual property management, energy trading, gaming and digital assets, and governance and identity management have revolutionized each of these industries.[6]

---

[3] Hossein Kakavand, Nicolette Kost De Sevres, & Bart Chilton, *The Blockchain Revolution: An Analysis of Regulation and Technology Related to Distributed Ledger Technologies*, SSRN ELECTRONIC JOURNAL (2017), https://doi.org/10.2139/ssrn.2849251.
[4] *Id.*
[5] *Id.*
[6] James Ford, *Blockchain Beyond Cryptocurrency: Real-World Applications*, MEDIUM (Sept. 9, 2023), https://medium.com/@JAMESFORDUSA/blockchain-beyond-cryptocurrency-real-world-applications-a4604a79f98b.

II. UNDERSTANDING SMART CONTRACTS

Blockchain technology, with its robust capabilities, serves as the foundation for the development and implementation of smart contracts.[7] First conceptualized by Nick Szabo in the 1990s, smart contracts serve as a significant development in blockchain. In simple terms, smart contracts are mechanisms that capture the terms of an agreement in computer code and automatically enforce them.[8] Conceptually, this means that smart contracts are basically containers of code that embody the terms of real-world contracts in the digital realm.[9] However, there is no universally accepted definition of smart contracts, and therefore, understanding what smart contracts are requires understanding how they work.

Smart contracts, as they function today, are self-executing agreements that leverage the capabilities of blockchain technology to automatically enforce the terms of the agreement.[10] Combining code-driven smart contracts with blockchain systems that facilitate transfers of digital assets without relying on centralized authorities, smart contracts can automatically transmit value, assets, and data based on the operation of "if then" logic without needing the software to interface with external systems, physical assets, or in some cases, external inputs.[11] For the code to execute, the smart contract needs to be funded with a transaction of a digital asset to its wallet address, and the smart contract code needs to execute, which will cause the wallet to transact assets.[12]

---

[7] Syamsu Rijal & Fajar Saranani, *The Role of Blockchain Technology in Increasing Economic Transparency and Public Trust*, 1 TECHNOLOGY AND SOCIETY PERSPECTIVES (TACIT) 56-67 (2023).
[8] James Grimmelman, *All Smart Contracts Are Ambiguous,* 2 JOURNAL OF LAW AND INNOVATION 1, 2 (2019).
[9] Taherdoost, *supra* note 2.
[10] DANIEL T. STABILE, KIMBERLY A. PRIOR, & ANDREW M. HINKES, DIGITAL ASSETS AND BLOCKCHAIN TECHNOLOGY 216 (Edward Elgar Publishing 2020).
[11] *Id.*
[12] *See id.* at 218.

The use of smart contracts eliminates the need for intermediaries, which increases efficiency, lowers costs, and increases transparency in the contract process. Additionally, smart contracts annex the immutability of blockchain technology, and data encryption adds a layer of security to the transaction. However, as the use of smart contracts expands across industries, it is important to understand that for a smart contract to be legally enforceable, the basic rules of contract law still apply; as with any agreement, there must be an offer, acceptance, and consideration.[13] Additionally, the factors that differentiate smart contracts from traditional contracts impose a new set of legal challenges, such as difficulty in remedying automatic enforcement, modifying the contract, and handling disputes.[14] That is just the beginning, as the transparent and immutable nature of blockchain technology imposes significant challenges regarding an individual's right to control their personal information in the context of smart contracts.

III. DATA PRIVACY LAWS IN THE UNITED STATES

A. Federal Laws

Despite numerous proposals, there is not a comprehensive data privacy law in effect in the United States. Discussions about potential legislation that aims to establish a federal standard for data privacy have been ongoing, but as of today, data privacy law remains an evolving landscape with several regulations that govern different aspects of it federally. For example, the Privacy Act of 1974 prohibits federal agencies from disclosing personal information about individuals from its system of records without written consent, subject to a few exceptions.[15] The

[13] Jonathan Herpy, *Smart Contracts And The Law: What You Need To Know*, FORBES (Mar. 17, 2022), https://www.forbes.com/sites/forbesbusinesscouncil/2022/03/17/smart-contracts-and-the-law-what-you-need-to-know/?sh=1409ff5c3d03.
[14] *Id.*
[15] Conor Murray, *U.S. Data Privacy Protection Laws: A Comprehensive Guide*, FORBES (Apr. 21, 2023), https://www.forbes.com/sites/conormurray/2023/04/21/us-data-privacy-protection-laws-a-comprehensive-guide/?sh=4dcddbbe5f92.

Health Insurance Portability and Accountability Act creates standards for how healthcare providers can use a patient's personal data.[16] Additionally, the Federal Trade Commission enforces data privacy with a selection of narrow federal statutes that were enacted without the advancements in technology that we have today, such as the Gramm-Leach-Bliley Act (GLBA) and the Children's Online Privacy Protection Act (COPPA).[17] However, the GLBA is limited to financial institutions, and COPPA only protects data collected from children under the age of thirteen.[18] What this essentially means is that a vast majority of data that is collected is not regulated, so companies that function outside of the specific regulations are free to use, share, or sell the data that they collect without having to notify the individuals whose data they collected (except in states that have their own data privacy law).[19]

The American Data Privacy Protection Act (ADPPA) introduced in May 2022, is the latest attempt to establish an all-encompassing federal data privacy law.[20] The bill, which distinguishes covered data from sensitive covered data which would be subject to heightened requirements, defines covered data as "information identifying, linked, or reasonably linkable to an individual or device linkable to an individual."[21] While the ADPPA received enough bipartisan support to make it out of committee, chances for passage remain unclear, as it failed to advance to the House or Senate floors in the last Congress.[22] However, as the trend of increased attention on data privacy continues, there is hope for the ADPPA to receive enough support to

---

[16] *Id.*
[17] Jason Heitz, *Federal Legislation Does Not Sufficiently Protect American Data Privacy*, 49 N. KY. L. REV. 287, 291 (2022).
[18] *Id.*
[19] Murray, *supra* note 15.
[20] Gregory T. Parks & Ronald W. Del Sesto, *U.S. Data Privacy Legislation: Could A Federal Law Be On The Horizon?*, MORGAN LEWIS PUBLICATIONS (Jul. 21, 2023), https://www.morganlewis.com/pubs/2023/07/us-data-privacy-legislation-could-a-federal-law-be-on-the-horizon.
[21] American Data Privacy Protection Act, H.R. 8152, 118th Cong. (2022).
[22] Parks & Del Sesto, *supra* note 20.

get it signed into law. In the meantime, while the ADPPA makes its way through Congress, many states are continuing to establish their own data privacy laws.

B. State Laws

It comes as no surprise that California, considered by many to be the technology capital of the United States, was the first state to enact enhanced data privacy rights and protections statutes for its residents. The California Consumer Protection Act of 2018 (CCPA) gives consumers more control over the data that is collected about them, including the right to know about the personal information that a business collects and how it is used and shared, the right to delete personal information collected from them—subject to a few exceptions, the right to opt-out of the sale or sharing of their personal information, and the right to not be discriminated against for exercising their CCPA rights.[23] In addition to that, the California Privacy Rights Act of 2020 (CPRA) extended these protections by giving consumers the right to correct inaccurate data that is collected about them and the right to limit the use and disclosure of sensitive personal data.[24] California's data privacy protections are regarded as the strongest in the United States, and many states have implemented their own comprehensive data privacy schemes in an attempt to follow.[25]

Modeled after the CCPA, the Virginia Consumer Data Protection Act (VCDPA) gives consumer many of the same rights, such as the right to confirm and access their personal data, request that the data be deleted, and the right to opt-out of the processing of personal data for targeted advertising, sale of personal data, or profiling.[26] However, there are key differences

[23] Cal. Civ. Code §1798.100 (2018).
[24] Murray, *supra* note 15.
[25] Jazmine Ulloa, *California Has Become a Battleground for the Protection of Consumer Privacy Laws*, L.A. TIMES (Mar. 11, 2019), https://www.latimes.com/politics/la-pol-ca-california-privacy-law-battles-20190311-story.html.
[26] Va. Code §§ 59.1-575—59.1-585 (2023).

between each state's statutes in the areas of enforcement, exemptions, and how consumer rights are defined, and California's protections are simply broader. Similarly, Colorado and Connecticut have respectively adopted the Colorado Privacy Act (CPA) and the Connecticut Data Privacy Act (CDPA) that came into effect this year and contain many of the same provisions as the VCDPA. Additionally, Utah, which was actually the fourth state to pass a comprehensive data privacy law before Connecticut, has its Utah Consumer Privacy Act (UCPA) set to take effect in December of this year.[27] Currently, there are thirteen states that have passed comprehensive data privacy laws in the United States: California, Virginia, Colorado, Connecticut, Utah, Iowa, Indiana, Tennessee, Texas, Florida, Montana, Oregon, and Delaware.[28] It is important to note, however, that irrespective of which state a company is located in, the rights that these laws provide only apply to residents of that state.

C. Comparison to the GDPR

As states shift from the "harms-prevention-based" data privacy standard that the United States has historically implemented and as the profound shift in the philosophy underlying data privacy laws transcends, credit must be given to the European Union for exemplifying a "rights-based" approach after which the CCPA and other states' data privacy laws have been modeled.[29] The European Union's General Data Protection Regulation (GDPR) offers robust protections for the privacy rights of an individual because it effectively gives individuals ownership of their personal data, which gives them the presumptive legal right to control who can use it.[30] As such, the GDPR employs a broad concept of personal data, defining it as "[a]ny information relating to

[27] F. Paul Pittman, *U.S. Date Privacy Guide*, WHITE & CASE LLP (Sept. 20, 2023), https://www.whitecase.com/insight-our-thinking/us-data-privacy-guide.
[28] *Id.*
[29] Fredric D. Bellamy, *U.S. Data Privacy Laws To Enter New Era in 2023*, REUTERS (Jan. 12, 2023), https://www.reuters.com/legal/legalindustry/us-data-privacy-laws-enter-new-era-2023-2023-01-12/.
[30] *Id.*

an identified or identifiable natural person ('data subject') . . . ."[31] This definition is incredibly expansive, as the data subject does not need to be specifically identified by the data; being identifiable is sufficient for personal data protection to apply.[32] In the blockchain context, transactional data stored on the blocks can potentially be classified as personal data, which would trigger the application of the GDPR in smart contracts.[33]

IV. PRIVACY CONSIDERATIONS IN SMART CONTRACTS

Privacy involves the protection of personal information, which is data that can be traced, directly or indirectly, to a living person.[34] Provided that smart contracts involve processing and storing data on the blockchain and the transparent and immutable nature of blockchain technology, there are bound to be data privacy considerations that must be addressed at the outset of implementation. By design, smart contract transactions are not private; information on the blockchain is itself public by the very nature of the technology. Therefore, it goes without saying that one of the primary challenges in smart contract data security is data exposure.[35] What this essentially means is that if sensitive information is not handled properly, it can become accessible by unauthorized parties, which can lead to complex issues in the digital era.

Another major concern of smart contract data security is that blockchain's immutable nature can lead to problems when dealing with personal data, especially sensitive personal data, because that information cannot be altered or destroyed once it is on the blockchain. Without

---

[31] General Data Protection Regulation, art. 4(1), 2016/C 213/05, EUR.
[32] W Gregory Voss, *Data Protection Issues for Smart Contracts*, SMART CONTRACTS: TECHNOLOGICAL, BUSINESS AND LEGAL PERSPECTIVES 79, 83 (2021) https://ssrn.com/abstract=3977477.
[33] *Id.* at 84–85.
[34] Jelena Madir, *Smart Contracts: (How) Do They Fit Under Existing Legal Frameworks?*, SSRN ELECTRONIC JOURNAL (2018), http://dx.doi.org/10.2139/ssrn.3301463.
[35] Aiswarya PM, *Smart Contracts and Data Security: Challenges and Solutions*, ANALYTICS INSIGHT (Oct. 9, 2023), https://www.analyticsinsight.net/smart-contracts-and-data-security-challenges-and-solutions/#:~:text=Vulnerabilities%20within%20the%20smart%20contract,exploited%20to%20compromise%20data%20security.in

strong privacy protections, smart contracts may be unsuitable for agreements where confidentiality is crucial, which could ultimately limit the technology's adoption.[36]

Since smart contracts operate on the blockchain, they are typically accessible by the public due to the open and transparent nature of the technology.[37] This means that the data is visible to all participants, which may be unappealing to contracting parties who want to keep the terms of their agreement private.[38] However, it should be noted that though it is possible to store data in plain text, most data is encrypted or hashed before it is added to the blockchain.[39] Nonetheless, even if it is strongly encrypted, there is always potential of data being leaked, and data on the blockchain is in danger of exposure if the data is accessed through the relevant encryption keys and unlocked by hackers.[40] Strong encryption simply makes it more challenging, not impossible, to access the data unauthorized. Additionally, identification techniques can be used to discern the identities of transacting parties within a smart contract, and all operations performed with that account can be traced back to that identity, which limits the potential of smart contracts to replace traditional contracts in many commercial settings.[41]

Errors in coding could further escalate the possibility of data exposure vulnerability. Since there is no method to address a security issue in a smart contract besides redeployment, there is a significant possibility of loss.[42] This means that if the necessary safeguards are not implemented, blockchains can reveal all data that is stored on them.[43] A potential solution that

[36] PRIMAVERA DE FILIPPI & AARON WRIGHT, BLOCKCHAIN AND THE LAW: THE RULE OF CODE 83 (Harvard University Press 2018).
[37] *Id.*
[38] DE FILIPPI & WRIGHT, *supra* note 36.
[39] Michèle Finck, *Blockchains and Data Protection in the European Union*, 4(1) EUROPEAN DATA PROTECTION L. REV. 17, 19 (2018), https://doi.org/10.21552/edpl/2018/1/6.
[40] *Id.*
[41] DE FILIPPI & WRIGHT, *supra* note 36.
[42] Taherdoost, *supra* note 2.
[43] Finck, *supra* note 39, at 21.

has been discussed to data exposure is to store all sensitive data off the blockchain, which saves space and resources on the blockchain, but if the point of smart contracts is efficiency, this seems to be a barrier in the ability of smart contracts to take over traditional contracting.[44]

Another privacy consideration is the inability of personal data that is in smart contracts to be altered or destroyed once it is on the blockchain. The immutable nature of blockchain technology is one of its key features, considering that it enhances security, promotes trust and transparency, and supports decentralization. However, that same feature makes it more difficult to manage personal data on the blockchain because if circumstances change, there is no simple way to amend a smart contract that could contain sensitive or erroneous information.[45] As data is implicated in all smart contracts, it is essential to consider what information is being processed, how it is used, who is accessing it, and where it is being stored and transmitted because privacy is a concern in all jurisdictions.[46] Thus, the presence of personal data in smart contracts could trigger the need for regulatory compliance.

V. LEGAL CHALLENGES

Taking the aforementioned privacy considerations into mind, it is evident that smart contracts present a plethora of legal challenges relating to data privacy, especially in a world where compliance with data privacy laws involves a patchwork of regulations that vary from jurisdiction to jurisdiction. Not only does the lack of regulatory clarity complicate cross-border data transfers and enforcement across jurisdictions, it also creates challenges in the legality and enforcement of smart contracts as a whole. Privacy presents the most difficult of issues

---

[44] Niclas Kannengieber, et al., *Challenges and Common Solutions in Smart Contract Development*, 48 IEEE TRANSACTIONS ON SOFTWARE ENGINEERING 4291, 4301 (2022).
[45] Shafaq Naheed Khan, et al., *Blockchain Smart Contracts: Applications, Challenges, and Future Trends*, 14 PEER-TO-PEER NETWORKING AND APPLICATIONS 2901-2925 (2021), https://doi.org/10.1007/s12083-021-01127-0.
[46] Wendy Callaghan & Rajika Bhasin, *Legal Considerations in the Use of Blockchain Technology and Smart Contracts for Multinational Business*, ACC DOCKET (June 1, 2018), https://docket.acc.com/legal-considerations-use-blockchain-technology-and-smart-contracts-multinational-business.

surrounding smart contracts because there are conflicting interests, obligations, and legal duties at play when dealing with blockchain technology.[47] Issues relating to transparency and immutability must be addressed at the outset, as they pose anticipated challenges in contracting where confidentiality and amenability are sought after, if not typically required. Additionally, in the ever-evolving landscape of data privacy, the transparent and immutable nature of blockchain technology may also conflict with the rights of an individual to control how their personal data is handled.

A. Transparency and Data Handling

While the European Union is often cited as the jurisdiction where privacy is most protected, data privacy is required by the federal statutes and state regulatory schemes discussed earlier in this paper. In addition to that, the ADPPA increases the urgent need for corporate data protection practices if it is passed by Congress.[48] Many businesses have already begun implementing strict data collection practices to comply with California, Virginia, Colorado, Connecticut, and Utah state regulations, while others have made more rigorous changes to comply with the GDPR.[49] Fundamentally, the ADPPA, similar to the state regulatory schemes modeled after the GDPR, calls for adoption of a "privacy by design" mindset.[50] In addition to that, it calls for transparency in data collection practices.[51] However, while transparency is a key feature of blockchain technology, the transparency of smart contracts significantly differs from transparency in data collection. Transparency as it pertains to smart contracts makes the data that is collected transparent, which poses a complex set of legal challenges.

---

[47] Ravi Antanid, *The Resistance of Memory: Could the European Union's Right to Be Forgotten Exist in the United States?* 30 BERKELEY TECH. L. J. 1173 (2015).
[48] Ben Robinson, *Preparing for New U.S. Data Privacy Laws*, 69 RISK MANAGEMENT, Sept.-Oct. 2022, at 24–26.
[49] *Id.*
[50] *Id.*
[51] *Id.*

Initials calls for research into privacy implications associated with blockchain technology have pointed out that exposure of sensitive information should explicitly be researched because processing of data in blockchains often conflicts with business' policies and regulations associated with sensitive organization and customer information.[52] In public blockchains, every block is generally disseminated to every node, which leads to challenges associated with the exposure of sensitive information such as critical business data or personally identifiable user data.[53] While many blockchain projects have attempted to mitigate privacy issues by putting the data in encrypted or hashed form, encryption and hashing render data practically useless as inputs for smart contracts since conducting tasks typically performed by smart contracts is generally not possible on obfuscated data.[54] To utilize the benefits of smart contracts, input and output data needs to be accessible to other blockchain nodes.[55] Therefore, while tamper-resistant documentation can be achieved without major privacy challenges, how coordination and automation of processes that require multiple party inputs in smart contracts can be achieved without excessive transparency remains unclear.[56]

While public blockchains allow anyone to participate in the consensus process, private blockchains bound permissioned participants by terms and conditions, and therefore, it goes without saying that most legal issues, including privacy ones, arise in connection with public blockchains.[57] However, private blockchains only partially mitigate the fundamental legal challenges relating to transparency because exposing sensitive information to a few stakeholders

[52] Johannes Sedlmeir, et al., *The Transparency Challenges in Blockchain Organizations*, 32 ELECTRON MARKETS 1779–94 (2022), https://doi.org/10.1007/s12525-022-00536-0.
[53] *Id.* at 1785.
[54] *Id.*
[55] Kannengieber, *supra* note 44.
[56] Sedlmeir, *supra* note 52, at 1785.
[57] Voss, *supra* note 32, at 80.

can still be an inhibiting problem as it pertains to data privacy.[58] Additionally, restricted access to information offers less functionality for a smart contract or suggests that another communication layer must be added to distribute the underlying data between the contracting parties.[59] Consequently, private blockchains are not a full-fledged solution to the challenges associated with transparency and data handling.

Another approach to avoid excessive information exposure that has significantly evolved is verifiable computation using zero-knowledge proofs.[60] Zero-knowledge proofs are a cutting-edge technology that enable the validation of a statement without sharing the statement's contents or revealing how the validity was discovered.[61] This is done by allowing a prover to convince a verifier of the knowledge of data by providing a proof that can be verified to ensure that the statement is true without revealing any additional information about the statement.[62] Nonetheless, while relying on technological solutions such as zero-knowledge proofs to protect sensitive data is a start to addressing issues relating to data privacy, the question of what qualifies as protected data under current regulatory schemes is another issue that must be addressed because specific types of sensitive information is not protected by these regulations. Under the GDPR, citizens of the European Union have several rights with respect to their personal information, and since data has been pseudonymized, not anonymized, in the context of smart contracts, it remains personal data for purposes of the GDPR.[63] However, "personal data"

[58] Sedlmeir, *supra* note 52, at 1786.
[59] *Id.*
[60] *Id.*
[61] Andres Zunino, *What Are Zero-Knowledge Proofs*, FORBES (Feb. 7, 2023), https://www.forbes.com/sites/forbestechcouncil/2023/02/07/what-are-zero-knowledge-proofs/?sh=7cf5a4516b3e.
[62] *Id.*
[63] Madir, *supra* note 34.

refers solely to information relating to a natural person, not a legal person, so the data of corporations is not afforded protection under the GDPR.[64]

Similarly, the CCPA, CPRA, VCDPA, CPA, CDPA, and UCPA focus on protecting the privacy rights of individuals, whereas corporate data, including sensitive business and proprietary information, is typically governed by contractual agreements and/or other laws.[65] Since contract execution may involve confidential information governed by other regulations, such as in the healthcare and banking industries, exposure to information in smart contracts could trigger the applicability of other data privacy laws as well.[66] Therefore, the complexity of handling sensitive data within smart contracts and balancing the associated legal implications requires an understanding of what laws regulate the specific data, and in a general sense, robust data protection measures must be taken to avoid data exposure in smart contract transactions.

Needless to say, ensuring compliance with data privacy regulations remains a burden of its own on the path to adopting smart contracts as the norm in contracting. While neither the ADPPA nor state regulations (nor the GDPR, for that matter) explicitly mention blockchain technology, there are implications in the context of smart contracts when personal data is being processed. Under the ADPPA, similar to the GDPR, organizations would be prohibited from collecting, processing, or transferring personal data beyond what is necessary, proportionate, and limited to a purpose.[67] Essentially, it is built around some of the same data privacy principles as the GDPR, including data minimization. Additionally, the principle of privacy by design involves adoption at the outset of reasonable policies, practices, and procedures regarding data

[64] Voss, *supra* note 32, at 83.
[65] *Protecting Personal Information: A Guide for Business*, FED. TRADE COMM'N, https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business.
[66] Beldex, *Why is Privacy Vital to Smart Contracts*, MEDIUM (Oct. 20, 2023), https://beldexcoin.medium.com/why-is-privacy-vital-to-smart-contracts-94a63fc3ca08.
[67] American Data Privacy Protection Act, H.R. 8152, 118th Cong. (2022).

collection, processing, and transferring along with mitigation of data risks.[68] These principles require careful consideration of the data that is implicated within a smart contract and careful coding to ensure that data collection in the transaction is minimized to what is necessary for the purposes of the contract and that reasonable policies, practices, and procedures were followed.

While state regulations are already on the way to ensuring these data privacy principles for individuals, these principles are not enforced on a federal level until the ADPPA or another comprehensive data privacy bill passes Congress. Nonetheless, confidentiality is an integral part in contracting, and this poses significant issues in connection with smart contracts using blockchain technology due to their transparent nature. Not only is it important to consider what data is being collected in order to ensure compliance with current and upcoming regulation, but the transparency of smart contracts also triggers other legal considerations. The inherent degree of transparency of blockchain technology often conflicts with the level of security required when handling sensitive data, and this privacy challenge is a considerable reason as to why large-scale smart contract applications are still rare today.[69] Additionally, full transparency of private information is linked to another binary aspect of blockchain technology: if the technology is designed to ensure anonymity, then a smart contract is legally unreliable because the parties cannot be identified for liability purposes, but if it emphasizes transparency over personal information, then it clashes with privacy rights.[70]

B. Immutability and Rights Relating to Personal Data

The creation of immutable records in the blockchain context—both public and private—may potentially offend an individual's sense of entitlement, or their legal rights, to be

[68] *Id.*
[69] Sedlmeir, *supra* note 52, at 1790.
[70] Gianluigi Maria Riva, *What Happens in Blockchain Stays in Blockchain. A Legal Solution to Conflicts Between Digital Ledgers and Privacy Rights*, 3 FRONTIERS IN BLOCKCHAIN 36 (2022).

forgotten.[71] The concept of a right to be forgotten is a European one, as historically, the United States has placed a greater emphasis on the freedom of expression than on privacy.[72] Under the GDPR, the use of smart contracts in connection with personal data poses problems for compliance with the right to rectification, the right to opposition, and the right to erasure due to the immutability of blockchain technology.[73] In other words, the privacy rights of the GDPR conflict with blockchain technology's defining feature that it "never forgets" the information that it collects and that that information cannot be changed or deleted.[74] The fact that data cannot be modified once entered into a block clashes with the right to erasure, opposition, and rectification, and the fact that this data is stored forever clashes with the principles of purpose, necessity, and minimization.[75]

In the context of smart contracts, these rights create difficulties because blockchains are built to enable decentralized trust and ensure that transactions, including the parties to them, are never forgotten.[76] Restricting the use of smart contracts to private, permissioned blockchains does not mitigate those problems unless the network is designed in a way that each and every piece of data is accessible only by the parties that absolutely need access to the data and unless the data can be rectified or erased at the request of the data subject.[77] At this time, it remains virtually impossible to grant a request for erasure made by a data subject when that data is

---

[71] Andrew Neville, *Is It a Human Right to Be Forgotten? Conceptualizing the World View*, 15 S. CLARA J. INT'L L. 157 (2017).
[72] *Id.* at 167.
[73] Voss, *supra* note 32, at 90.
[74] Andrea Vittorio, *Blockchain's Forever Memory Confounds EU 'Right to be Forgotten'*, BLOOMBERG LAW (Aug. 3, 2022), https://www.bloomberglaw.com/product/blaw/bloombergterminalnews/bloomberg-terminal-news/RG17I5DWLU68?bc=W1siU2VhcmNoICYgQnJvd3NlIiwiaHR0cHM6Ly93d3cuYmxvb21iZXJnbGF3LmNvbS9wcm9kdWN0L2JsYXcvc2VhcmNoL3Jlc3VsdHMvMWU5ZDYwNDg3ZjQ5NTgzYjQwZTdhMDRhYTJmMmY2ZTUiXV0--7408a3b2b7e96909486125557837ad018f69122a&criteria_id=1e9d60487f49583b40e7a04aa2f2f6e5.
[75] Riva, *supra* note 70.
[76] Voss, *supra* note 32, at 92.
[77] TOM LYONS, LUDOVIC COURCELAS, & KEN TIMSIT, BLOCKCHAIN AND THE GDPR 25, (The European Union Blockchain Observatory and Forum, 2018)

registered on a blockchain, but technical solutions, such as making the data practically inaccessible through hashing, have been explored.[78] However, the right to be forgotten is not absolute under the GDPR, and a balancing test may need to be applied to determine whether the need for data protection trumps other fundamental rights, such as the right of innovation.[79] Nonetheless, a private, permissioned blockchain has less chance of prevailing over data protection than a public blockchain for several reasons, and where personal data is stored on a smart contract on the blockchain, and no exception to the regulation applies, the right to erasure is problematic, to say the least.[80]

In the United States, the CCPA and CPRA represent one model for comprehensive privacy laws, whereas the VCDPA, CPA, CDPA, and UCPA represent another model for comprehensive privacy laws. However, the rights to correction and to erasure are a common theme in each of these laws, paralleling those established in the GDPR.[81] As we shift from the "harms-prevention-based" hodgepodge of privacy protections into a more "rights-based" approach, determination on how to enforce these rights requires a careful analysis as to the scope, requirements, potential liabilities and penalties, and means of enforcement of each of the regulations.[82] For example, when dealing with smart contracts, who is responsible for enforcing data privacy rights and who is liable if there is personal data within a smart contract and that data contract cannot be erased or rectified upon assertion of the data subject's right to erasure or rectification?

[78] *Id.*
[79] Voss, *supra* note 32, at 92.
[80] *Id.*
[81] Bellamy, *supra* note 29.
[82] *Id.*

Under the GDPR, it must be possible to identify a data controller, who is defined as the "natural or legal person, public authority, agency or other body, which, alone or jointly with others, determines the purposes and means of the processing of personal data."[83] However, this is not a term that is used within the regulations of the United States. For example, the CCPA refers to the aspect of a data controller as a business, which is defined as an entity that "determines the purposes and means of the processing of consumers' personal information."[84] However, unlike the GDPR, the CCPA requires size and threshold requirements for an entity to be considered a "business," such as revenue in excess of $25 million, transaction of data relating to 50,000 subjects, or 50% revenue derived from selling personal information.[85] Similarly, under the ADPPA, a covered entity is "any entity or any person, other than an individual acting in a non-commercial context, that alone or jointly with others determines the purposes and means of collecting, processing, or transferring covered data . . ." with many exclusions.[86]

However, the importance of being able to identify a responsible party remains the same, which is not always easy in the blockchain context.[87] When technology is involved, it is entirely dependent on the specific use case and application to determine whether it is compliant with applicable regulations.[88] Understanding the interplay between blockchain technology in the context of smart contracts and regulatory compliance takes place on a case-by-case basis and requires determination of where the personal data appears, how it is processed, and who is responsible for the processing.[89] As mentioned, this can already be complicated enough under

[83] General Data Protection Regulation, art. 4(7), 2016/C 213/05, EUR.
[84] Cal. Civ. Code §1798.140 (2018).
[85] Bryan Cave Leighton Paisner, *CCPA FAQs: Does the CCPA Have Data "Controllers" and "Processors?",* JDSUPRA (Dec. 19, 2018), https://www.jdsupra.com/legalnews/ccpa-faqs-does-the-ccpa-have-data-98810/.
[86] American Data Privacy Protection Act, H.R. 8152, 118th Cong. (2022).
[87] LYONS, *supra* note 77, at 11.
[88] *Id.* at 16.
[89] *Id.*

the comprehensive GDPR, but the lack of regulatory clarity in the United States makes it all the more complicated, with its varied threshold requirements and exclusions. Additionally, in public blockchains, where the traditional model is replaced with one based on collective processing of data, the question of how to identify the controlling party is less straightforward and has been the object of debate as more and more use cases of blockchain technology develop.[90]

Furthermore, without centralization, there is little possibility of appointing a data controller, business, covered entity, or whatever the term is under applicable regulation. The clash between the immutability of blockchain technology and privacy rights encompasses that issue, along with the ambiguity in who performs the duty of informing data subjects about data that is collected and who defines the purposes for data processing or the legal basis on which it is based.[91] If there is no controlling entity, there is no way to ensure compliance with data privacy rights of data subjects, undermining data privacy regulation before the right to rectification and right to erasure can even be addressed.[92]

Addressing another issue of practicality, while the person who initially put the information within the smart contract, meaning the controlling entity, may be able to "erase" the relevant personal data in their records, this does not benefit the data subject because all the other blockchain records remain unchanged.[93] On a public blockchain, the operators of the other nodes cannot be practically compelled to update their records.[94] This issue has involved ongoing legal debate on whether the other nodes are acting as sub-processors of the personal data, which would place overall responsibility of their actions on the initial data controller, or if they are acting as

[90] *Id.* at 17.
[91] Riva, *supra* note 70.
[92] *Id.*
[93] BLOCKCHAIN: LEGAL IMPLICATIONS, QUESTIONS, OPPORTUNITIES AND RISKS 6, DELOITTE LEGAL (2022).
[94] *Id.*

controllers in their own regard.[95] This would be dependent on specific facts on a case-by-case basis, which creates a mess of liability in effect.

While mechanisms have been discussed in relation to smart chain immutability, such as mutating the smart contract to include a self-destruct opcode on Ethereum, these mechanisms only make sense for developers in terms of fixing a bug, patching, or employing new functionality.[96] They do not solve the data privacy rights issue of smart contracts because using and storing personal information on an immutable blockchain requires proper consent and an ability to withdraw that consent at any point. While the inclusion of kill switches within smart contracts is a start to addressing immutability as it pertains to the right to rectification and the right to erasure, consent mechanisms are another essential function, and that is just the beginning of addressing rights relating to personal data within smart contracts.

VI. PROPOSED RESOLUTION

It is evident that though there are several technological advances that are slowly addressing data privacy issues in the context of smart contracts, the lack of a comprehensive data privacy regulatory framework that imposes such rights in the United States is the biggest impediment in ensuring data privacy for its citizens in a decentralized world. If the ADPPA were to pass Congress, the United States would be taking a step in the right direction, but the fact that the bill does not directly address blockchain technology, in the same way that the GDPR does not, means that the same problems that arise with reconciling the use of personal data within smart contracts and the enforcements that the GDPR puts in place regarding data privacy would arise when there is personal data within a smart contract under ADPPA regulation. Additionally,

[95] *Id.*
[96] Matt Rickard, *Smart Chain Immutability*, BLOG (July 8, 2022) https://matt-rickard.com/smart-contract-immutability.

the fact that sensitive information that would not fall under ADPPA regulation but could fall under regulation of other laws, such as contract law or GLBA or HIPPA or COPPA, makes the use of transparent data within a smart contract an even more convoluted matter.

Earlier this year, the European Union voted to pass the European Data Act which has an express provision addressing data within smart contracts.[97] The Data Act was intended to promote fairness in the digital world, stimulate a competitive data market, open opportunities for data-driven innovation, and make data more accessible.[98] Two of its key requirements are access control mechanisms and a kill switch in smart contract code, which ultimately go against the permissionless nature of public blockchains and impact immutability.[99] However, this directly addresses some of the issues that arise in the context of smart contracts that were discussed in this paper, and though they do not serve as foolproof solutions, rigorous access control mechanisms and a high degree of robustness avoid errors in data handling and manipulation by third parties to a higher degree than what is now required.[100] Additionally, the requirement that smart contracts be designed to ensure the confidentiality of trade secrets addresses the issue of sensitive information that does not fall within personal data as defined by the GDPR, and the requirement of mechanisms in place to reset or instruct the contract to stop addresses the issue surrounding the right to rectification and right to erasure to some extent.[101] Although these provisions can be seen as an undermining of the benefits that blockchain technology offers, they are another step toward engaging with the legal implications of smart contracts, which shows

[97] Jordan Atkins, *EU Approves Data Law Requiring Kill Switch For Smart Contracts*, COINGEEK (Mar. 16, 2023), https://coingeek.com/eu-approves-data-law-requiring-kill-switch-for-smart-contracts/.
[98] *Data Act: Commission Proposes Measures for a Fair and Innovative Data Economy*, EUROPEAN COMMISSION (Feb. 23, 2022), https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1113.
[99] *EU Data Act Requires Smart Contracts to Have Kill Switch, Not Be Permissionless,* LEDGER INSIGHTS (Mar. 14, 2023), https://www.ledgerinsights.com/dressx-warner-music-backs-metaverse-fashion/.
[100] Atkins, *supra* note 97.
[101] *Id.*

that European Union lawmakers are keeping an eye on the world of blockchain as they consider how they should go about regulating data.[102]

The inability of Congress to enact federal data privacy legislation prevents the United States from establishing a baseline standard for data privacy.[103] Current data privacy legislation is insufficient, and the failure to pass comprehensive data privacy legislation in the United States has led to the European Union setting the standard, with individual U.S. states attempting to follow.[104] According to privacy experts, four areas that deserve basic protections are data collection and sharing rights, opt-in consent, data minimization, and nondiscrimination and no data-use discrimination.[105] This ties into the "privacy by design" model that the United States is attempting to move toward with the ADPPA. While there are several privacy laws in various states of legislation, the ADPPA is the closest that the United States has come to passing a comprehensive data privacy law, and therefore, it is likely that either a revised version of it or a similar proposed bill will go on to become the first federal comprehensive data privacy law in the United States. For the aforementioned reasons, that may not be enough to address the legal challenges associated with smart contracts, and therefore, it is essential that we consider the shortcomings of the GDPR and the European Union's attempts to mitigate those shortcomings in establishing our baseline standard for data privacy, keeping the advances that have been made in technology in mind.

Firstly, the ADPPA is not as expansive as it should be to deal with issues that may arise in terms of data privacy in the age of technology. Definitions in the ADPPA have limited

---

[102] *Id.*
[103] Jessica Rich, *After 20 Years of Debate, It's Time for Congress to Finally Pass a Baseline Privacy Law*, THE BROOKINGS INST. (Jan. 14, 2021), https://www.brookings.edu/blog/techtank/2021/01/14/after-20-years-of-debate-its-time-for-congress-to-finally-pass-a-baseline-privacy-law/.
[104] Heitz, *supra* note 17, at 292.
[105] Thorin Klosowski, *The State of Consumer Data Privacy Laws in the US (And Why It Matters)*, WIRECUTTER (Sept. 6, 2021), https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/.

effectiveness due to restrictions in when it applies and its many exclusions when compared to the GDPR.[106] Furthermore, while the ADPPA introduces rights to access, correct, and delete personal information, there are many exceptions that covered entities can rely on to not fulfill those requests.[107] The ADPPA is also intended to be enforced through the Federal Trade Commission and through the State Attorney General of each respective state, instead of through a specifically designated agency, and it fails to define what fines shall be imposed if there is a breach.[108] This, again, leaves much of the responsibility to individual states to make these determinations, burdening them while simultaneously taking away their regulatory authority since the ADPPA would preempt state law, rendering the state regulations discussed in this paper ineffective. It should be noted that that is a major point of opposition for the ADPPA, especially by California government officials who have expressed that the ADPPA weakens existing laws instead of strengthening them.[109] As such, while it is great that the ADPPA is attempting to provide regulatory clarity and private rights of action to all U.S. citizens, it should be adding to the data privacy rights that individuals have under current laws, not taking away from them. Moreover, an additional law that specifically addresses data in smart contracts should be enacted. Lastly, a data privacy authority that is independent of the government should be established to enforce these data privacy laws.

A. Improving the ADPPA

---

[106] Katherine Sainty & Aisling Hamilton, *International: Comparing the ADPPA and GDPR From An Australian Legal Perspective*, ONETRUST DATA GUIDANCE (Oct. 2022), https://www.dataguidance.com/opinion/international-comparing-adppa-and-gdpr-australian#:~:text=Key%20differences%20between%20the%20ADPPA%20and%20the%20GDPR&text=Exclusions%20include%20de%2Didentified%20data,data%20subjects%27%20has%20extraterritorial%20applicability..

[107] *Id.*

[108] *Id.*

[109] Shane Snider, *US Data Privacy Relationship Status: It's Complicated*, INFORMA (July 20, 2023), https://www.informationweek.com/data-management/us-data-privacy-relationship-status-it-s-complicated.

Perhaps the biggest issue with the ADPPA, apart from its many exclusions and exceptions, is that it sets a ceiling on general comprehensive data privacy standards in the United States, instead of setting a federal floor.[110] While this would be acceptable if the ADPPA were stronger than existing state privacy laws and resilient to future shifts in technology, it is debatable whether the ADPPA is stronger than the CCPA and CPRA and whether it factors in where we are in technology today, let alone where we will be in the future. It is inarguable that we need a strong baseline standard to protect the data privacy of all individuals, but the fact that no state would be permitted to enforce provisions of law that cover the same issues as the ADPPA and existing provisions of law that cover those issues would be superseded is concerning.[111] Not allowing states to go further when shifts in technology happen at the speed at which they do is problematic for several reasons, considering that the federal government still has not been able to pass a comprehensive federal data privacy legislation to this day whereas individual states have. Therefore, while the ADPPA should establish a national standard for data privacy, states should be able to establish stronger privacy protections as necessary to keep up with advances in technology.

B. Establishing a Smart Contract Data Privacy Act

In addition to a federal data privacy comprehensive scheme, it is important to establish a law that addresses the collection, usage, and storage of sensitive information, including personal data and confidential business information, within smart contracts. This act should contain provisions that address how to identify a controlling entity, how to obtain consent for data processing or storage, how to determine how much data needs to be collected for specific

[110] Alan Butler, *Evaluating the American Data Privacy and Protection Act*, TECH POLICY PRESS (Aug. 8, 2022), https://techpolicy.press/evaluating-the-american-data-privacy-and-protection-act/.
[111] *Id.*

purposes, how to enforce data correction and data erasure rights, and how to object to the processing of an individual's data. It should also address the need for compliance with other data privacy regulations and impose penalties for non-compliance that go beyond what the ADPPA establishes as a baseline, similar to how the European Data Act will function in relation to the GDPR. The Smart Contract Data Privacy Act should aim to protect privacy rights while promoting technological innovation through the responsible use of smart contracts.

C. Establishing a Data Privacy Authority

In the European Union, Data Protection Authorities (DPAs) are independent public authorities that supervise the application of data protection law.[112] Once we have established federal data privacy laws, the United States should have one of these authorities. Data privacy is a critical issue in the United States, and we should consider establishing a central authority to address the complex challenges of data privacy in the digital age. In an evolving landscape of data privacy regulation, a central authority could provide consistency in the enforcement of existing and future laws while simultaneously ensuring that data privacy rights are protected effectively and promoting trust. Establishing such an authority could be another crucial step toward safeguarding data privacy while continuing to promote innovation.

CONCLUSION

This paper has delved into the critical issue of data privacy in an increasingly decentralized world, focusing particularly on smart contracts and the associated legal challenges and implications. As technology continues to revolutionize the way that contracts are executed, it is increasingly important to address the effect that has on data privacy through effective regulatory frameworks. Smart contracts, with their reduced risk, reduced costs, and enhanced

[112] *What Are Data Protection Authorities (DPAs)?,* EUROPEAN COMMISSION, https://commission.europa.eu/law/law-topic/data-protection/reform/what-are-data-protection-authorities-dpas_en.

efficiency, can be transformative if the legal challenges surrounding the transparent and immutable nature of blockchain technology are effectively addressed through robust laws that balance the need to protect data privacy and promote innovation and the creation of a regulatory authority that enforces those laws.