NOTE

SMART CONTRACT ACCOUNTABILITY PROBLEMS: DEFAULT ORACLE LIABILITY AS THE SOLUTION

Leana Ter-Martirosyan*

Smart contracts have emerged as a transformative force in contract law, leveraging blockchain technology to automate transactions and reduce reliance on human intermediaries. However, their widespread adoption is hindered by significant legal challenges, particularly in determining liability for transaction failures. This Note examines the accountability problems inherent in smart contracts, focusing on the critical role of oracles—third-party entities that feed external data into blockchain-based agreements. While existing scholarship explores the theoretical foundations and potential applications of smart contracts, this Note shifts focus to liability allocation and proposes a novel framework: default oracle liability. Under this proposal, oracles bear primary responsibility for transaction errors arising from inaccurate data sourcing or validation failures. If oracles demonstrate that they functioned correctly, liability shifts to smart contract developers, who are responsible for ensuring secure and error-free code. By clarifying accountability, this framework incentivizes higher standards for data accuracy

* J.D. Candidate 2025, Columbia Law School; B.A. 2020, University of Southern California. I would like to express my deepest gratitude to Professor Dorothy Lund for her invaluable guidance and support throughout the process of writing this Note, as well as to the *Columbia Business Law Review* team for their meticulous edits and thoughtful feedback. Lastly, I am eternally grateful to my family and loved ones—my grandparents, parents, Stella, Hayk, and my fiancé Nshan—whose unwavering love, encouragement, and belief in me have been a constant source of strength. This work is as much theirs as it is mine.

and software integrity, ultimately fostering a more reliable and legally-viable environment for smart contracts to operate.

I. INTRODUCTION

In an era defined by relentless technological advancements, smart contracts have emerged as a disruptive force with the potential to transform legal agreements as we know it. Powered by blockchain technology, smart contracts are "models of legal efficiency, reducing the need for a complex court system to enforce transactions because the contracts themselves are self-enforcing."[1] This self-enforcement is perhaps the most unique element of smart contracts,

[1] Scott A. McKinney, Rachel Landy & Rachel Wilka, *Smart Contracts, Blockchain, and the Next Frontier of Transactional Law*, 13 WASH. J.L. TECH. & ARTS 313, 316 (2018).

distinguishing them from the traditional legal landscape where contracts are inked with human penmanship—negotiated, reviewed, and executed by licensed professionals under long-established principles of contract law. In contrast, smart contracts, operating as autonomous codes on blockchain networks, introduce a process that challenges conventional contracting norms. Their strictly technological operation, however, could face a myriad of challenges, many of which seem all the more relevant given the increasingly rapid introduction of such paradigm-shifting technologies.

This Note sets out to navigate the complex and topical issues pertaining to smart contracts, focusing primarily on the issue of legal liability and accountability. In the realm of smart contracts, determining liability—the cornerstone of our legal system—poses particularly intricate challenges. Specifically, as contracts become increasingly code-dependent, we encounter a legal landscape marked by reduced ambiguity, increased efficiency, and decreased human oversight. This shift prompts critical questions: How should fault be defined or perceived in a context where contracts are less prone to human error? Furthermore, when such errors do occur, who should bear responsibility—the lawyers representing the parties involved in "smart" transactions, or the developers who programmed the contracts themselves?

While there has been considerable scholarship dedicated to this topic, previous research has focused primarily on tracing the origins of smart contracts—elaborating upon their development and examining their status as a viable alternative to traditional contractual frameworks.[2] Researchers have also devoted significant attention to forecasting the potential challenges smart contracts may encounter, as well as the hurdles to achieving widespread

[2] *See, e.g.*, Farshad Ghodoosi, *Contracting in the Age of Smart Contracts*, 96 WASH. L. REV. 51 (2021). *See also* Max Raskin, *The Law and Legality of Smart Contracts*, 1 GEO. L. TECH. REV. 305 (2017); Morgan N. Temte, *Blockchain Challenges Traditional Contract Law: Just How Smart Are Smart Contracts?*, 19 WYO. L. REV. 88 (2019); Kevin Werbach & Nicholas Cornell, *Contracts Ex Machina*, 67 DUKE. L. J. 313 (2017); Jens Frankenreiter, *The Limits of Smart Contracts*, 175 JITE 149 (2019).

adoption.[3] Although this research has been incredibly useful in shedding light on the origins and regulatory issues of smart contracts, including both the advantages and drawbacks of their implementation, this Note shifts the focus toward specific issues of legal liability and accountability. More specifically, this Note proposes an innovative solution to the accountability problem—one premised on a system of default oracle liability.

As a foundational element of this discussion, smart contracts derive their "smartness" from an ability to autonomously execute predefined actions based on information available to them within the blockchain.[4] However, because smart contracts cannot access external data independently, oracles play a critical role by acting as intermediaries. These third-party entities gather, validate, and transmit real-world information to the blockchain, allowing smart contracts to register and respond to external events.[5] By bridging the gap between digital code and real-world conditions, oracles enable smart contracts to function similarly to traditional agreements—incorporating outside data such as economic indicators, weather patterns, and regulatory updates to inform contract execution.

However, smart contracts are not immune to error. When a smart contract fails to perform as intended, scenarios can emerge where oracles are found to be at fault. For one, an oracle may improperly rely on a single, centralized source containing inaccurate data—causing it to feed erroneous information into the smart contract and produce a flawed outcome. Alternatively, even if an oracle consults multiple

[3] *See* Temte, *supra* note 2.

[4] Reggie O'Shields, *Smart Contracts: Legal Agreements for the Blockchain*, 21 N.C. BANKING INST. 177, 179 (2017) ("Smart contracts are self-executing electronic instructions drafted in computer code. This allows a computer to 'read' the contract and, in many cases, effectuate the instruction—hence the 'smartness' of the contract." (quoting SAMUEL BOURQUE & SARA FUNG LING TSUI, A LAWYER'S INTRODUCTION TO SMART CONTRACTS 4 (2014)).

[5] *What Is a Blockchain Oracle?*, CHAINLINK (Jan. 12, 2024), https://chain.link/education/blockchain-oracles [https://perma.cc/CV6C-PSHY].

sources, it may nevertheless fail to verify the accuracy of the information, leading to a similarly compromised result. To illustrate, consider two parties entering into a smart contract wager on a horse race: Party 1 bets on Horse A, while Party 2 bets on Horse B. The oracle responsible for gathering race results relies solely on a single, centralized data source, www.horseraces.com, to determine the winner. However, the website inaccurately reports that Horse A won, resulting in an incorrect payout to Party 1. In such cases, oracles should assume liability when transactions fail due to their lack of cross-referencing multiple sources and verifying information accuracy.

However, in instances where oracles are found to have operated correctly, this liability model shifts its focus to smart contract developers. Much like oracle providers, developers occupy a critical role in the smart contract formation process. Entrusted with the meticulous task of programming a smart contract's code, they bear the responsibility of ensuring the reliability and security of their creations. Therefore, in instances where a smart contract falters due to a coding oversight rather than an information inaccuracy, it is reasonable to transfer liability from oracles onto the developers themselves.

The liability model proposed in this Note has great potential to mitigate the inherent risks associated with smart contract transactions. By incentivizing oracles to adopt a meticulous approach—consulting multiple sources and employing a rigorous, multi-step verification process—this framework reduces the likelihood of manipulation and errors, thereby improving transaction success rates. From a policy perspective, it also promotes greater accountability among developers, encouraging a stronger emphasis on code quality and accuracy. Ultimately, even if either party fails to uphold its coding or data-verification obligations, this model still fulfills its core objective: simplifying the assignment of liability in flawed smart contract transactions. By clarifying accountability, it addresses a fundamental challenge in smart contract adoption—the intricate web of involved parties—

thus creating a more viable path for widespread implementation.

II. WHAT ARE "SMART CONTRACTS"?

A. Blockchain Technology: The Foundation of Smart Contracts

In recent years, contract law has undergone a transformative evolution, propelling us into the era of "smart contracts." The concept of smart contracts was introduced in 1994 by cryptographer Nick Szabo, who described the idea of technologically-driven contracts in his seminal paper "The Idea of Smart Contracts."[6] Two years after introducing the idea, Szabo formalized it when he defined smart contracts as "a set of promises, specified in digital form, including protocols within which the parties perform on these promises."[7] Szabo proposed smart contracts as a computer code designed to autonomously enforce contractual terms when a number of predefined conditions are met.[8] Akin to a vending machine, where products are dispensed once a requisite amount of money is inserted, smart contracts were developed to perform a similar function: terms in, execution out—thereby rendering a quick and efficient contracting scheme.[9]

[6] Nick Szabo, *The Idea of Smart Contracts*, SATOSHI NAKAMOTO INST. (1997), https://nakamotoinstitute.org/the-idea-of-smart-contracts/ [https://perma.cc/N34C-58WJ].

[7] Nick Szabo, *Smart Contracts: Building Blocks for Digital Markets*, UNIVERSITAIT VAN AMSTERDAMN (1996), https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html [https://perma.cc/2AYU-KWXQ].

[8] *See* Alyssa Hertig, *How Do Ethereum Smart Contracts Work?*, COINDESK, https://www.coindesk.com/learn/how-do-ethereum-smart-contracts-work/ (Sept. 29, 2023, 11:50 AM).

[9] *See* John R. Storino et al., *Decrypting the Ethical Implications of Blockchain Technology*, LEGALTECH NEWS (Nov. 13, 2017, 8:00 AM), https://www.law.com/legaltechnews/sites/legaltechnews/2017/11/13/decrypting-theethical-implications-of-blockchain-technology/ [https://perma.cc/Q6FT-F3ND] ("To explain the technology, cryptographer Nick Szabo—who coined

What distinguishes smart contracts from this simple vending machine analogy lies in the integration of blockchain technology. This innovative concept can be traced back to Satoshi Nakamoto, the pseudonymous author of a 2008 whitepaper, in which he introduced the notion of cryptocurrency and the blockchain upon which it could be built. Specifically, Nakamoto's vision saw the blockchain as an ever-expanding registry of records, composed of individual "blocks."[10] Within each block was a timestamp, as well as a unique digital identifier known as a "hash."[11] The blockchain itself forms as each block establishes a cryptographic link with its predecessor in a peer-to-peer network, creating a chain. The end product is known as a distributed ledger, with the term "distributed" indicating that the information contained within it is not stored in a single location, but rather allocated across a decentralized network of participants.[12] As more members are added to the blockchain, each new user obtains their own copy of the unique ledger and thus contributes to the network's expansion.[13] This process not only fortifies the system's security but also establishes a strong foundation for the network's autonomy—realizing the potential for transactions that are able to act independently from the confines of human oversight.

the term 'smart contract'—analogized smart contracts to a vending machine: Vending machines are programmed to transfer ownership of delicious 'assets' (i.e., candy bars) once a predetermined amount of money is input.").

[10] Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, BITCOIN, at 3 (last visited Jan. 6, 2024), https://bitcoin.org/bitcoin.pdf [https://perma.cc/QYZ6-CEUQ].

[11] *Id.* at 2.

[12] *See Distributed Ledger Technology: Implications of Blockchain for the Securities Industry*, FINRA, at 2 (Jan. 2017), https://www.finra.org/sites/default/files/FINRA_Blockchain_Report.pdf [https://perma.cc/4NZ9-VBZY] ("Distributed ledger technology involves a distributed database maintained over a network of computers connected on a peer-to-peer basis, such that network participants can share and retain identical, cryptographically secured records in a decentralized manner.").

[13] *Id.*

Perhaps the most important contribution of blockchain technology in this discussion is its elevation of smart contracts from mere theoretical concepts to actual and compelling alternatives to traditional contracts. Previously, participants in "smart" transactions were forced to place an unwavering trust into their counterparty's computer code and network infrastructure. This required assuming that both parties' codes were not only identical but also executed uniformly across their respective computing environments.[14] Fortunately, the innovative technology used by the blockchain eliminates this reliance on blind trust. By embedding a given code into a decentralized ledger accessible by all parties to a smart contract transaction, the blockchain introduces a never-before-seen paradigm.[15] Essentially, the blockchain *carries* the code of a smart contract with it, ensuring that different users can safely access a given contract without concern about discrepancies in code versions. As a result, this process instills a newfound confidence in utilizing smart contracts, with blockchain technology not only enhancing user security but also rendering contracts practically immune to tampering.[16]

B. Elements of Smart Contracts: What Makes Them "Smart"?

Building on the foundational role of blockchain technology, this section explores what makes smart contracts truly "smart." By definition, smart contracts are "self-executing contracts with the terms of the agreements between buyer and seller directly written into lines of code. The code and the agreements contained therein exist across a distributed and

[14] McKinney et al., *supra* note 1, at 317.

[15] *See* Shafaq Naheed Khan et al., *Blockchain Smart Contracts: Applications, Challenges, and Future Trends*, 14 PEER TO PEER NETWORKING & APPLICATIONS 2901, 2901 (2021), https://doi.org/10.1007/s12083-021-01127-0 ("In order to prevent contract tampering, smart contracts are copied to each node of the blockchain network. By enabling the execution of the operations by computers and services provided by blockchain platforms, human error could be reduced to avoid disputes regarding such contracts.").

[16] Ghodoosi, *supra* note 2, at 60.

decentralized blockchain network."[17] Unlike traditional contracts, which require human oversight for enforcement, smart contracts autonomously execute predefined actions once specified conditions are met. Designed to streamline the transaction lifecycle, they also minimize reliance on intermediaries, reduce inefficiencies, and enhance transactional security.

To accomplish this purpose, an increased reliance is placed on mechanical actors—computers programmed to read inputted terms and execute actions once predefined conditions are met.[18] This fascinating ability to interpret and act on terms autonomously is made possible through the use of conditional logic—a process through which specific actions are triggered by the happening of predefined events.[19] The reasoning behind conditional logic is straightforward: "if X, then Y."[20] By reducing complex contract language into this structured framework, smart contracts can manage even the most intricate agreements without human intervention. Thus, the integration of conditional logic not only distinguishes smart contracts in the realm of transactions, but also creates

[17] Murat Kzildag, *DeFi Everything Soon?*, BOS. HOSP. REV., June 2021, at 6, https://www.bu.edu/bhr/2021/05/31/defi-everything-soon/ [https://perma.cc/V5FE-8V77].

[18] As some commentators put it:

> Although the term "smart contract" sounds like a legal instrument, a smart contract is actually a computer program that performs a task when triggered by the occurrence of a predetermined event. Smart contracts live on blockchain, which processes the terms of the smart contract, thereby enabling the smart contract to automatically execute the coded task when the triggering event occurs.

Jose A. Lazaro & Kathleen E. Wegrzyn, *Smart Supply Chains Using Smart Contracts*, NAT'L L. REV. (Sept. 23, 2021), https://www.natlawreview.com/article/smart-supply-chains-using-smart-contracts [https://perma.cc/N6AE-7S7W].

[19] Astrid Bulmer, *Smart Contracts – What Are They, And What Should You Look Out For?*, SIMKINS (Mar. 30, 2022), https://www.simkins.com/news/smart-contracts-what-are-they-and-what-should-you-look-out-for#:~:text=As%20with%20code%2C%20smart%20contracts,DLT)%2C%20although%20not%20always [https://perma.cc/LLA9-UBCP].

[20] *Id.*

a self-executing system that accelerates agreements and significantly reduces the potential for human error.

To illustrate the potential and ease of use of smart contracts, consider an analogy between smart contracts and iPhone applications. Much like familiar apps and services such as Apple Pay and Google Maps, which have become essential tools in our daily lives, smart contracts function as digital protocols designed to execute actions automatically. Envision the blockchain as akin to the App Store—a digital marketplace where users can select from and use a variety of smart contracts, each tailored to their individual needs and preferences. Just as iPhone applications eliminate the need for manual processes—allowing users to make payments or navigate routes with the tap of a finger—smart contracts remove the need for traditional intermediaries by autonomously executing agreements with speed, accuracy, and security. This automation not only reduces inefficiencies but also minimizes costs and human error, making smart contracts a powerful alternative to conventional contracting methods. Another key similarity is their participatory nature: just as App Store users can choose from existing applications or develop new ones themselves, blockchain users can also adopt or create smart contracts. This collaborative ecosystem enables continuous innovation, ensuring that smart contracts evolve to meet diverse and dynamic user needs.

C. Legal Enforceability of Smart Contracts

Having established smart contracts as viable entities due to their presence on the blockchain, the next inquiry is their enforceability. Put differently, can a smart contract be considered legally binding for the parties that engage with it?

a. Traditional Contractual Frameworks: Offer and Acceptance Requirements

In the absence of federal contract law in the United States, the interpretation and enforceability of contracts are matters

scrutinized at the state level.[21] To determine whether contracts are enforceable, state courts traditionally examine whether the common law requirements of offer, acceptance, and consideration are satisfied.[22] According to the Second Restatement of Contracts, an offer is defined as the "manifestation of willingness to enter into a bargain, so made as to justify another person in understanding that his assent to that bargain is invited and will conclude it."[23] Additionally, "acceptance of an offer is a manifestation of assent to the terms thereof made by the offeree in a manner invited or required by the offer."[24]

To determine whether an offeree has accepted a valid offer and effectively created a binding contract, state courts examine three key factors: (1) intent, (2) acceptance, and (3) communication.[25] First, courts explore whether an offeree genuinely intended to enter into a contract by assessing the sincerity and clarity of their statements and actions.[26] Second, they examine whether the offeree unconditionally accepted the offeror's proposed terms, corresponding exactly with the terms of the offer to reflect a meeting of the minds that is essential for contract formation.[27] Finally, courts evaluate whether the offeree sufficiently communicated acceptance to

[21] *Contract*, CORNELL L. SCH.: LEGAL INFO. INST., https://www.law.cornell.edu/wex/contract#:~:text=Contracts%20are%20mainly%20governed%20by,otherwise%20established%20by%20state%20law [https://perma.cc/YG3X-WWEV] (last visited Jan. 6, 2024) ("Contracts are mainly governed by state statutory and common (judge-made) law and private law (i.e. the private agreement).").

[22] Alex Lipton & Stuart Levi, *An Introduction to Smart Contracts and Their Potential and Inherent Limitations*, HARV. L. SCH. F. ON CORP. GOV. (May 26, 2018), https://corpgov.law.harvard.edu/2018/05/26/an-introduction-to-smart-contracts-and-their-potential-and-inherent-limitations/ [https://perma.cc/2KH9-N7UZ].

[23] RESTATEMENT (SECOND) OF CONTS. § 24 (AM. L. INST. 1981).

[24] *Id.* at § 50(1).

[25] *Understanding the Roles of Offer and Acceptance in the Formation of a Contract*, CAL. STATE UNIV., NORTHRIDGE, https://www.csun.edu/sites/default/files/blawaccept.pdf (last visited Jan. 8, 2024).

[26] *See id.*

[27] *See id.*

the offeror.[28] This third step highlights the importance of clear and unequivocal communication between parties, and demonstrates that a valid contract cannot be based on mere implications or assumptions. Assuming all three conditions are met, courts tend to respect the parties' intentions of entering into a valid agreement with one another, and thus acknowledge the existence of a fully formed contract.

b. Smart Contracts Sufficiently Meet Offer and Acceptance Requirements

As smart contracts introduce a transformative shift in contract law, it is important to reassess how legal agreements are created and enforced in order to determine their compliance with traditional offer and acceptance requirements. Unlike conventional, paper-based contracts, smart contracts exist solely in digital form and are defined by their nature as codes on a blockchain. This inherently redefines conventional concepts of offer and acceptance into intricate algorithms. In the context of smart contracts, the "offer" initiated by a party in a transaction is embedded within intricate lines of code that specify the terms and conditions of the agreement.[29] Parties can use computerized algorithms as negotiators to help determine and select the specific terms they wish to propose.[30] Once these terms are negotiated and finalized, the smart contract code becomes an official offer when "other participants on the ledger are entitled to interact with and execute on the code."[31] In other words, an offer is

[28] *See id.*

[29] *Smart Contract*, CORP. FIN. INST., https://corporatefinanceinstitute.com/resources/valuation/smart-contract/ [https://perma.cc/6566-CEYX] (last visited Feb. 14, 2024) ("A smart contract is a self-executing contract whose terms of the agreement between the contract's counterparties are embedded into lines of code.").

[30] Lauren H. Scholz, *Algorithmic Contracts*, 20 STAN. TECH. L. REV. 128, 146 (2017).

[31] MIREN APARICIO BIJUESCA ET AL., SMART CONTRACTS: IS THE LAW READY? 15 (2018), https://lowellmilkeninstitute.law.ucla.edu/wp-

considered valid only when a counterparty is able to connect its digital wallet—essentially its identity—to the smart contract, thereby unlocking the next step of acceptance.

Acceptance of a smart contract requires a party's intentional and voluntary interaction with the proposed digital code. The offeree, no longer a passive observer but an active participant, accepts the contract by engaging with its interface to trigger a blockchain transaction. For instance, a party could show assent to proposed terms by "providing its digital signature utilizing a cryptographic private key to sign the transaction before the offer expires."[32] In cryptocurrency transactions, acceptance can also occur by transferring the requisite amount of funds to a specified address to trigger an agreed-upon outcome.

Finally, for a contract to be legally binding, the exchanged promises must involve consideration.[33] This means that the terms must be "bargained for,"[34] with both parties exchanging something of value. This requirement is arguably inherent in the self-executing nature of smart contracts. Once terms are negotiated and agreed upon, parties are presumed to have knowingly consented to the value exchanged within the transaction. This is because smart contracts are only "triggered" when both parties fulfill the predefined conditions encoded into the contract—which typically require reciprocal commitments or actions. Put simply, the contract cannot execute unless each side performs its part, which functionally prevents one-sided or illusory promises from being carried out. Moreover, because smart contracts operate autonomously, acceptance and execution occur

content/uploads/2018/08/Smart-Contracts-Whitepaper.pdf [https://perma.cc/Q8XQ-YKCC].

[32] Anna Duke, *What Does the CISG Have to Say About Smart Contracts? A Legal Analysis*, 20 CHI. J. INT'L. L. 141, 169 (2019) (citing Alan Cohn et al., *Smart After All: Blockchain, Smart Contracts, Parametric Insurance, and Smart Energy Grids*, 1 GEO. L. TECH. REV. 273, 288 (2017)).

[33] May v. Anderson, 119 P.3d 1254, 1257 (Nev. 2005) ("Basic contract principles require, for an enforceable contract, an offer and acceptance, meeting of the minds, and consideration.").

[34] RESTATEMENT (SECOND) OF CONTS. § 70(1) (AM. L. INST. 1981).

simultaneously, which strengthens the legal validity of the agreement.[35] In other words, a meeting of the minds is established during the negotiation phase, and upon execution, both parties receive precisely what they bargained for—thus satisfying the consideration requirement. Finally, the decentralized and tamper-evident nature of the blockchain ensures transparency and immutability in recording these exchanges. Thus, smart contracts not only facilitate "bargained-for" transactions but also meticulously document them, satisfying the final element of a legally binding contract formation.

Alex Lipton and Stuart Levi of Skadden, Arps, Slate, Meagher & Flom LLP provide a helpful example that illustrates how the fundamental requirements of offer, acceptance, and consideration can be achieved through ancillary smart contracts:

> For example, an insurer might develop a flight insurance product that automatically provides the insured with a payout if a flight is delayed by more than two hours. The key terms, such as delineating how the delay is calculated, can be set forth in a text-based contract, with the actual formation of the contract (payment of the premium) and the execution (automatic payout upon a verifiable delay) handled through an ancillary smart contract. Here, the insurer has made a definite offer for a flight insurance product that is accepted by the insured upon payment of the premium as consideration.[36]

As this example demonstrates, smart contracts extend beyond a mere digital handshake. By embedding offer, acceptance, and consideration into self-executing code, smart contracts enable parties to form legally-binding agreements with greater speed, efficiency, and trust. Moreover, their transparency and tamper-resistant design enhance the

[35] *See* Zibin Zheng et al., *An Overview of Smart Contracts: Challenges, Advances and Platforms*, 105 FUTURE GENERATION COMPUT. SYS. 475, 475 (2020) ("In a smart contract, contract clauses written in computer programs will be automatically executed when predefined conditions are met.").

[36] Lipton & Levi, *supra* note 22.

integrity of these transactions, offering legal and practical benefits that complement traditional contract law principles.

III. ACCOUNTABILITY CHALLENGES IN SMART CONTRACTS: LEGAL AND PRACTICAL BARRIERS TO WIDESPREAD ADOPTION

This evolving frontier of contract law is driven by rapid technological advancement, with smart contracts at the forefront of innovation. According to an Allied Market Research report, "the global smart contracts market was valued at $192.7 million in 2022, and is projected to reach $2.5 billion by 2032, growing at a CAGR [compound annual growth rate] of 29.6% from 2023 to 2032."[37] Today, smart contracts have tapped into a wide range of industries, including healthcare, insurance, real estate, and eCommerce.[38] While these developments promise to enhance trust, security, and transparency in commercial transactions, smart contracts are not without challenges. As adoption increases, concerns surrounding accountability, enforceability, and operational risks continue to pose significant legal and practical obstacles.

One of the most pressing concerns facing smart contracts is accountability—the challenge of attributing fault or liability in cases of transactional error.[39] Unlike traditional contract models where allocating liability is typically

[37] Mayabrahmma Akhila & Onkar Sumant, *Smart Contracts Market Size, Share, Competitive Landscape and Trend Analysis Report, by Contract Type, by Platform, by Enterprise Size, by End User: Global Opportunity Analysis and Industry Forecast, 2023-2032*, ALLIED MKT. RSCH. (Sept. 2023), https://www.alliedmarketresearch.com/smart-contracts-market-A144098 [https://perma.cc/P938-4R3V].

[38] Pedro Ferreira, *How Smart Contracts Can Streamline Processes in Various Industries*, FIN. MAGNATES (Oct. 12, 2023, 10:04 AM), https://www.financemagnates.com/cryptocurrency/how-smart-contracts-can-streamline-processes-in-various-industries/ [https://perma.cc/5RNW-QA3U].

[39] Temte, *supra* note 2, at 89 ("The legal issues that will likely arise with this new form of contract, including the application of traditional contract law principles, the potential for unauthorized practice of law, jurisdictional challenges in drafting and enforcing smart contracts, and concerns regarding the potential liability for errors in smart contracts.").

straightforward, the intricate code underlying smart contracts and the complex web of involved parties complicate the process of determining fault when a transaction goes awry. As noted in the context of patent law, "this evolution . . . shows us that client lawsuits may be limited by the fact that smart contract complexity could make it difficult to attribute fault in the event that something goes wrong."[40] On a larger scale, these challenges raise serious doubts about the feasibility of smart contracts as a reliable alternative to traditional contractual frameworks, which have long been grounded in principles of accountability.[41] However, as smart contracts become increasingly embedded in modern commercial transactions, the U.S. legal landscape faces a critical question: should it embrace this new technology—one that promises to reduce transaction costs and minimize errors—despite unresolved accountaibility concerns? Or should the legal industry adhere to established norms and practices, prioritizing clarity and enforceability over innovation?

These questions will largely fall to the next generation of lawyers, who must navigate this ever-evolving digital legal landscape. This task can be daunting, especially when considering the decentralized nature of blockchain networks. Unlike traditional contract frameworks, where a central authority oversees compliance, blockchain transactions rely on a distributed network of nodes across several

[40] Ryan Hasting, *Smart Contracts: Implications on Liability and Competence*, 28 MIA. BUS. L. REV. 358, 376 (2020).

[41] Stuart Levi et al., *Legal Issues Surrounding the Use of Smart Contracts*, *in* GLOBAL LEGAL INSIGHTS, BLOCKCHAIN AND CRYPTOCURRENCY REGULATION 155, 162 (Josias N. Dewey ed., 2020) ("As noted above, in many cases, the parties to a smart contract will not have the technical capability to create a smart contract, and may therefore hire a third party to create the smart contract, or may rely on a smart contract "template" offered by a third party. In such cases, there is the possibility of programmer error or that the parties did not accurately convey what they intended to the developer. Parties will need to consider the ramifications of these situations and the appropriate allocation of risk and liability.").

jurisdictions.[42] With potentially millions of nodes participating in a single blockchain, determining a clear "regulatory access point"—an entity responsible for legal compliance—becomes much more difficult.[43] Legal scholars note that "this is further complicated by the fact that a decentralized ledger can span multiple locations around the world, making it unclear which laws would apply if a dispute were to arise."[44] Consequently, the absence of a single counterparty in each smart transaction raises significant concerns, as assigning liability in cases of contractual error could prove prohibitively challenging.[45]

With no clear regulatory access point, the responsibility for ensuring compliance may shift to those traditionally tasked with legal oversight. This raises the unsettling prospect that lawyers advising clients on smart contract transactions could bear the burden of liability when things go wrong. As officers of the court, attorneys maintain special relationships with their clients—relationships that are "fiduciary in the highest degree, with consequences that are diametrically opposed to the arm's length conception of a simple contract."[46] Their role

[42] *See* Shola Slick Akinrole, *Nodes… The Backbone of Blockchain Technology!*, MEDIUM (Feb. 3, 2023), https://meetslick.medium.com/nodes-the-backbone-of-blockchain-2632c3c0d168 [https://perma.cc/YWV6-WL6K].

[43] Predrag Cvetkovic, *Liability in the Context of Blockchain - Smart Contract Nexus*: *Introductory Considerations*, ZBORNIK RADOVA PRAVNOG FAKULTETA U NIŠU [COLLECTION OF PAPERS OF THE FACULTY OF L. IN NIŠ] 2020, at 83, 96–97, https://pdfs.semanticscholar.org/926a/bba7c5200a0a180d48375422ff2991fcefcc.pdf [https://perma.cc/7KRG-C68C].

[44] Elisabeth M.S. Frommelt, *Challenges in the Blockchain Ecosystem*, 21 UC DAVIS. BUS. L.J. 165 (2021).

[45] Cvetkovic, *supra* note 43, at 96 ("In decentralised networks, it can be burdensome to identify the actors liable for legal compliance (i.e. to define the so-called 'regulatory access point'). Identifying a regulatory access point is, however, more complicated where there is no centralised legal entity responsible for the network.").

[46] Nathan Isaacs, *Liability of the Lawyer for Bad Advice*, 24 CAL. L. REV. 39, 39 (1935). More than that,

> attorneys are very properly held to the same rule of liability for want of professional skill and diligence in practice, and for erroneous or negligent advice to those who employ them, as are physicians and surgeons, and other

in guiding clients through contract drafting and execution inherently suggests expertise not only in legal principles but also in the technological complexities of smart contracts. As a result, they may become primary targets in disputes over failed transactions. However, while attorneys do provide important legal guidance, their accountability does not necessarily extend to commercial disruptions or operational failures, which fall outside the scope of traditional legal counsel.

Beyond legal professionals, attention has also turned to the developers who build and maintain smart contracts. While attorneys may be scrutinized for advising on these transactions, developers bear direct responsibility for ensuring the integrity and security of the smart contracts they create. In this regard, "core developer groups that decide on software updates" function not only as "technology designers but also policy-makers shaping the world we live in."[47] Moreover, given the inherent complexity of smart contract development, even minor coding flaws can result in significant errors, security vulnerabilities, or compromised transactions. To mitigate these risks, developers must exercise meticulous attention to detail throughout the entire coding process. Thus, while developers do not share the fiduciary obligations of attorneys, their central role in the design, execution, and maintenance of smart contracts could suggest a level of accountability when programming oversights lead to transactional failures.

A. Case Study: Parity Multi-Sig Wallet

persons who hold themselves out to the world as possessing skill and qualification in their respective trades or professions. . . . An attorney who undertakes the management of business committed to his charge thereby impliedly represents that he possesses the skill, and that he will exhibit the diligence, ordinarily possessed and employed by well-informed members of his profession in the conduct of business such as he has undertaken.

Id. at 41 (citation omitted).

[47] MICHELLE FINCK, BLOCKCHAIN REGULATION AND GOVERNANCE IN EUROPE 52 (2018).

The Parity Multi-Sig Wallet serves as an informative case study illustrating the challenges of assigning liability in smart contracts operating on the blockchain. Parity Technologies, a prominent blockchain development company, created a multi-signature wallet using a smart contract designed to enhance security and user control over digital assets.[48] However, on November 6, 2017, a user known as *devops199* discovered a vulnerability in the smart contract's underlying code.[49] Exploiting this flaw, the user "made himself the 'owner' of the library contract."[50] The user then executed a self-destruct function, deleting the library content and "resulting in Ether tied to over 500 multi-sig wallets, then valued at over $150 million, becoming completely unusable."[51] Colloquially termed "the Freeze," this incident became a landmark example of how "a coding vulnerability in a smart contract (rather than a flaw in the underlying blockchain or cryptography) result[ed] in an exploit that compromise[d] cryptocurrency worth millions."[52]

The aftermath of the Parity Multi-Sig incident sparked fear and confusion within the blockchain community, raising critical questions about liability and accountability for smart contract vulnerabilities. While multiple parties suffered substantial losses in the Freeze—some totaling millions of

[48] *See* Wai Choy, *When Smart Contracts are Outsmarted: The Parity Wallet "Freeze" and the Software Liability in the Internet of Value*, Blockchain & L. (Dec. 22, 2017), https://www.blockchainandthelaw.com/2017/12/when-smart-contracts-are-outsmarted-the-parity-wallet-freeze-and-software-liability-in-the-internet-of-value/ [https://perma.cc/5H9H-MK4F] (noting that Parity Technologies offered open-source multi-signature wallets for Ether key storage, which operated as smart contracts on Ethereum and required multiple digital signatures for transactions—unlike standard Parity accounts).

[49] *See* Christof Ferreira Torres et al., *ÆGIS: Shielding Vulnerable Smart Contracts Against Attacks*, *in* THE ASSOCIATION FOR COMPUTING MACHINERY, ASIACCS '20: PROCEEDINGS OF THE 15TH ACM ASIA CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY, 2020, at 587 (2020).

[50] *A Postmortem on the Parity Multi-Sig Library Self-Destruct*, PARITY TECHS. (Nov. 15, 2017), https://www.parity.io/blog/a-postmortem-on-the-parity-multi-sig-library-self-destruct/ [https://perma.cc/F43X-6YDP].

[51] Choy, *supra* note 48.

[52] *Id.*

dollars—there was no clear consensus on who should bear responsibility. One side of the debate argued that Parity Technologies, the company that developed and deployed the smart contract code, should be held accountable for the failure. Proponents reasoned that, because users had placed significant trust in both the company's expertise and the security of its smart contract solutions, Parity should assume liability for any losses resulting from code-related vulnerabilities.[53] Prominent law firms, including Proskauer Rose LLP, even weighed in on the matter, suggesting that the company could face a lawsuit under negligence tort claims.[54] Conversely, others believed that that liability should not rest solely with Parity. Instead, Ethereum's original developers should share responsibility for the incident and take a more proactive role in advocating for enhanced security measures, such as comprehensive code audits, to prevent similar failures in the future.[55] However, Ethereum's core developers quickly distanced themselves from the controversy, rejecting claims that they bore any responsibility for ensuring the security of smart contract implementations.[56]

[53] *See Ethereum Community Split on Response to Parity Exploit*, COINBUREAU (Mar. 29, 2023), https://www.coinbureau.com/news/ethereum-community-split-response-parity-exploit/ [https://perma.cc/Y7KG-BYQF] ("Many in the Ethereum community are pointing to the fact that the problem was not with Ethereum but was the smart contract that was built on top of it. The Ethereum protocol worked just as intended.").

[54] Choy, *supra* note 48 ("[O]ne possible attempt for redress from Parity may be a negligence tort claim.").

[55] JP Buntinx, *Parity Hack Shows the Ethereum Ecosystem Is Flawed in Big Ways*, THE MERKLE (Nov. 26, 2017), https://themerkle.com/parity-hack-shows-the-ethereum-ecosystem-is-flawed-in-big-ways/ [https://perma.cc/HMG5-3PDU] ("We are not just pointing the finger at Parity, though. It's also up to the original Ethereum developers to step up and push for more code audits. Vitalik Buterin distanced himself from the Parity issue by stating that he 'won't comment on wallet issues.'").

[56] Christopher Durr, *Parity Hack: How it Happened, And Its Aftermath*, MEDIUM (Nov. 17, 2017), https://medium.com/solidified/parity-hack-how-it-happened-and-its-aftermath-9bffb2105c0#:~:text=On%20Twitter%2C%20Vitalik%20Buterin%20gave,verifying%20security%20of%20existing%20ones%E2%80%9D [https://perma.cc/4QH5-65KK] ("On Twitter, Vitalik Buterin gave a signal of impartiality by stating,

The Parity incident underscores the complexities of assigning liability in smart contract transactions and demonstrates the conflicting perspectives on who, if anyone, should be held accountable for contractual errors. More importantly, it highlights a key reason for legal professionals' reluctance to fully embrace smart contracts in everyday practice. Thus, addressing these concerns is essential to unlocking smart contracts' transformative potential and facilitating their widespread adoption within the legal sphere.

IV. SOLUTION: ESTABLISHING A FRAMEWORK OF DEFAULT ORACLE LIABILITY

Given the complex interplay between smart contracts and accountability, it is essential to develop a framework that clarifies liability when errors arise in "smart" transactions. This Note proposes a comprehensive yet practical solution to enhance accountability when a valid contract executed with proper guidance still fails. Specifically, it argues that (1) oracles should bear default liability for contractual failures, and (2) developers should assume secondary responsibility when failures stem from coding oversights rather than informational errors.

A. What are Oracles?

Oracles are the central pillar of this proposed liability framework, serving as the bridge between smart contracts and external networks.[57] Unlike traditional contracts, smart contracts are only "smart" to the extent that they can act

'I am deliberately refraining from comment on wallet issues, except to express strong support for those working hard on writing simpler, safer wallet contracts or auditing and formally verifying security of existing ones.'").

[57] Ammar Hassan et al., *From Trust to Truth: Advancement in Mitigating the Blockchain Oracle Problem*, J. NETWORK & COMPUT. APPLICATIONS, Apr. 2023, at 1, 1–2.

autonomously upon the information available within the blockchain. However, they lack the ability to access outside world data on their own. This limitation is addressed by oracles—third-party data agents that have the ability to "observe real-world events and report them back to the blockchain to be used by smart contracts."[58] To fulfill this role, oracles source off-chain data from Application Programming Interfaces (APIs), web services, Internet of Things (IoT) devices, and traditional databases.[59] Once acquired, the data undergoes a rigorous verification process to ensure its authenticity, integrity, and reliability—safeguarding the trustworthiness of the smart contract's inputs.[60] With the validated data in hand, the oracle then transmits this information to the blockchain, enabling the smart contract to execute predefined actions and seamlessly interact with real-world conditions.

B. Oracle Liability and Promising Solutions

Given the critical role oracles play in smart contract functionality, they should bear default responsibility in cases of transactional error. To fully appreciate this recommendation, it is essential to first examine the infamous "oracle problem." Widely studied among blockchain scholars, this issue stems from the tension between the foundational principles of blockchain technology—decentralization, transparency, and trustlessness—and those of oracles, which reintroduce elements of trust and reliance into smart contract transactions.[61]

[58] Hamada Al Breiki et al., *Trustworthy Blockchain Oracles: Review, Comparison, and Open Research Challenges*, IEEE ACCESS, 2020, at 85675, 85677.

[59] Andrew Kamsky, *Blockchain Oracles, Explained*, CCN (July 5, 2023, 8:24 AM), https://www.ccn.com/blockchain-oracles-explained/.

[60] *See id.*

[61] *See* Brian Curran, *What are Oracles? Smart Contracts, Chainlink & "The Oracle Problem"*, BLOCKONOMI (Sept. 19, 2018), https://blockonomi.com/oracles-guide [https://perma.cc/57AR-68ND] ("The Oracle Problem is defined as the security, authenticity, and trust conflict

At its core, the oracle problem arises from oracles' historic dependence on a single, centralized data source to feed information into smart contracts. This reliance on a readily-identifiable data source is problematic, as it reintroduces the notion of a single point-of-failure into an otherwise entirely decentralized system.[62] In other words, it offers a single entity upon which to place blame. If the oracle's chosen data source contains an inaccuracy or is subject to malicious manipulation, the smart contract will execute based on erroneous information—leading to a failed transaction and potential financial losses. Thus, what may seem like a minor reliability issue in data sourcing could carry significant repercussions, any one of which has the ability to compromise the integrity of the smart contract ecosystem.

To better understand the oracle problem, recall the scenario of two parties entering into a smart contract wager over a horse race. In this example, Party 1 bets on Horse A, while Party 2 bets on Horse B. To determine the outcome of the race and initiate a payout, the oracle retrieves data from a single, centralized data source called www.horseraces.com. However, the website contains an inaccuracy: it incorrectly reports that Horse A won the race, when in reality, Horse B was victorious. This erroneous data leads to an incorrect payout to Party 1, leaving Party 2, the true winner, with nothing. This scenario highlights a fundamental flaw in relying on a single oracle source: when that source is incorrect, the entire smart contract fails, completely contradicting the decentralized nature of blockchain technology. Moreover, the ability to trace the transaction failure back to a single point of failure—in this case, an unreliable data source—undermines

between third-party oracles and the trustless execution of smart contracts.").

[62] RedStone Oracles, *The Oracle Problem and its Implications for Blockchains*, MEDIUM (July 26, 2022), https://medium.com/@RedStone_Finance/the-oracle-problem-and-its-implications-for-blockchains-c0c0ad9cf5a7 [https://perma.cc/4SB8-X6PK] ("Because of [a singular entity's control of the oracle's connection to external networks], oracles often become a single point of failure in many web3 projects. Solving the Oracle Problem is not possible without eliminating this issue.").

the trustless, autonomous principles that smart contracts seek to uphold.

Fortunately, oracle companies like Chainlink have developed a solution to the oracle problem: the key lies in decentralization. To eliminate the single point of failure introduced by traditional information-gathering oracles, Chainlink mimics the blockchain model to employ "a decentralized network of independent entities (oracles) [to] collectively retrieve data from multiple sources, aggregate it, and deliver a validated, single data point to the smart contract to trigger its execution . . . ."[63] The solution is described in the example below:

> For instance, Chainlink provides the USD cost of Ethereum's native cryptocurrency, ETH, to blockchains via the ETH/USD Price Feed, which sources and delivers the price via a network of independent oracle nodes and data sources. The oracle of ETH/USD price can be utilized by a blockchain application to determine the current value of ETH when it is used as collateral for a loan or to settle a prediction about the value of ETH.[64]

In simpler terms, Chainlink's oracles gather data from multiple sources, rather than a single authority, and validate them all through a multi-step process. This significantly reduces the risk of erroneous data from a single source being fed into smart contracts, thereby mitigating the oracle problem and enhancing the reliability of smart contracts.

To better demonstrate this solution, consider a revised version of the horse race example. In a decentralized system, the oracle embedded within the smart contract no longer relies on a single source, such as www.horseraces.com, to

[63] *What is Chainlink? A Beginners Guide*, CHAINLINK (Jan. 25, 2021), https://blog.chain.link/what-is-chainlink/ [https://perma.cc/57QV-N224].

[64] Akash Takyar, *What is Blockchain Oracle Problem and How ChainLink Solves It?*, LEEWAYHERTZ, https://www.leewayhertz.com/chainlink-solving-blockchain-oracle-problem/#:~:text=ChainLink%20analyzes%20the%20issues%20with,trigger%20for%20a%20smart%20contract [https://perma.cc/XX67-KRMH] (last visited Jan. 18, 2024).

determine the race outcome. Instead, it consults a variety of different sources, including www.whichhorsewins.com, www.horseracevictories.com, and www.didyourhorsewin.com, to cross-verify the result. While the first website incorrectly reported that Horse A won the race, the other three correctly indicate Horse B's victory. Using its verification mechanisms, Chainlink's decentralized oracle discerns that the majority of data sources corroborate Horse B as the true winner. As a result, it initiates a correct payout to Part 2, preventing an erroneous transaction. Thus, by decentralizing the data-sourcing process, this solution eliminates reliance on incorrect data, enhancing the accuracy and reliability of smart contract executions. Importantly, it prevents failed transactions, reinforcing the integrity of "smart" agreements.

While decentralized oracles have significantly reduced the risks associated with erroneous data, they do not entirely eliminate the possibility of smart contract failures. As smart contracts continue to gain traction, the absence of a clear accountability framework remains a fundamental barrier to their widespread adoption. Thus, to ensure smart contracts function as viable contractual alternatives, a structured system of accountability must be implemented—giving rise to this Note's recommendation of default oracle liability. Specifically, in the event that a smart contract fails to perform as intended, lawyers must examine the functionality of the oracle embedded within the contract. Three possible scenarios may emerge from this analysis. First, if the oracle relied on a single, centralized source that provided inaccurate data, the oracle should be held liable for failing to ensure adequate validation. Second, if the oracle consulted multiple sources but still failed to deliver accurate data, it should likewise bear responsibility for flaws in its verification process. Third, however, if the inquiry confirms that the oracle did in fact perform properly—consulting multiple sources and undergoing thorough verification—liability then shifts to another party: the smart contract developers.

C. Developer Liability as a Backup

In scenarios where oracles function correctly, the accountability dynamics of smart contract transactions must undergo a crucial shift. When liability cannot be attributed to faulty data sourcing, attention turns to smart contract developers—the individuals entrusted with the meticulous task of programming smart contract code to accurately interpret and execute the information fed into it. Given the complex nature of smart contract programming, experts highlight that smart contract software is inherently prone to computing errors ("bugs"), which can disrupt contractual performance and increase vulnerability to cyber-attacks.[65] As a result, when a transaction deviates from its intended outcome due to a coding flaw rather than an information inaccuracy, the most reasonable allocation of liability falls on the core developers.[66] From a policy standpoint, imposing liability on developers for failed transactions would promote greater accountability, incentivize higher coding standards, and encourage prioritization of both security and accuracy in smart contract design.

Revisiting the Parity Multi-Sig hack, the incident demonstrated how a vulnerability in a smart contract's code enabled exploitation by a hacker, compromising transaction integrity and freezing millions of dollars in cryptocurrency assets. Under this Note's proposed accountability framework, Parity Technologies should bear liability for its oversight in the smart contract development process. As the sole entity responsible for crafting and deploying the code governing thousands of users' cryptocurrency holdings, Parity was entrusted with ensuring the security and proper functioning of its smart contract. In this scenario, Parity's role extended beyond mere technical development to one of heightened trust and expertise, where users relied on the company to safeguard their asses. Thus, given that a coding flaw directly led to

[65] *See* Angela Walch, *The Bitcoin Blockchain as Financial Market Infrastructure: A Consideration of Operational Risk*, 18 N.Y.U. J. LEGIS. & PUB. POL'Y 837, 856 (2015).

[66] Cvetkovic, *supra* note 43, at 96 ("Under the strict liability standard, code designers may be held liable for any default in the code which has been used to make the system operative.").

transaction failure and substantial financial losses for its users, liability should rightfully rest on the negligent developer.

Recent evidence further supports the growing trend of developer liability in cases where smart contracts fail to perform as intended.[67] In October 2018, Commissioner of the Commodity Futures Trading Commission ("CFTC"), Brian Quintenz, suggested that smart contract developers should be held liable in cases where smart contract users violated the laws of the United States if the developers "could reasonably foresee, at the time they created the code, that it would likely be used by U.S. persons in a manner violative of CFTC regulations."[68] Similarly, in November 2018, the Securities Exchange Commission ("SEC") found Zachary Coburn, founder and developer of digital trading platform EtherDelta, liable for violating the Securities Exchange Act of 1934.[69] Aside from the company's liability, Coburn himself was found in violation of the act because he "founded EtherDelta, wrote and deployed the EtherDelta smart contract to the Ethereum Blockchain, and exercised complete and sole control over EtherDelta's operations."[70]

V. CONCLUSION

The emergence of smart contracts signifies a profound shift in the legal landscape. As self-executing agreements which have the capacity to autonomously act on terms embedded into their code, smart contracts promise reduced ambiguity, enhanced efficiency, and minimized reliance on human intermediaries in the contract creation and execution process.

[67] *See id.*

[68] Brian Quintenz, Commissioner, CFTC, Remarks of Commissioner Brian D. Quintenz at the 38th Annual GITEX Technology Week Conference (Oct. 16, 2018), https://www.cftc.gov/PressRoom/SpeechesTestimony/opaquintenz16 [https://perma.cc/6VZ5-N8UE].

[69] Zachary Coburn, Exchange Act Release No. 84553, 2018 WL 5840155, at *8 (Nov. 8, 2018).

[70] *Id.* at *6.

However, their disruptive potential necessitates a clear regulatory framework to address liability in cases where smart contracts fail to perform as intended—particularly in these early developmental stages when such standards remain malleable.

This Note has examined the complexities of smart contract liability and proposed a novel framework centered on oracle and developer accountability. Implementing this solution will require collaboration among key stakeholders across the smart contract lifecycle. First, blockchain developers must integrate default oracle liability into their systems, ensuring robust accountability measures. Next, Oracle service providers, such as Chainlink, should refine and expand decentralized oracle solutions to improve reliability and accuracy. Finally, legal professionals must establish and enforce regulatory frameworks that govern liability and accountability in cases of smart contract failures.

Ultimately, this approach provides a comprehensive strategy for strengthening the blockchain ecosystem, reducing transaction failures, and increasing confidence in the legal viability of smart contracts. As blockchain adoption continues to accelerate, this proposed liability model establishes a critical foundation for a more secure, transparent, and reliable future—one in which smart contracts can fully realize their potential as a legitimate and enforceable alternative to traditional contractual frameworks.