Examining the Developing Legal Landscape for Healthcare Smart Contracts

Nodirakhon Abdurakhmanova

The lecturer of the Intellectual Property Law Department at Tashkent State University of Law

nodira2112@gmail.com

Abstract: Smart contracts are self-executing contractual logic encoded in software code deployed on blockchains. Smart contracts could transform efficiency, security, and transparency across healthcare by automating complex multi-party data exchanges and business workflows. However, uncertainties remain regarding the legal validity and healthcare regulatory compliance of blockchain-based smart contracts. This analysis reviews the current legal foundations supporting the enforceability of healthcare smart contracts under US contract law. Limits imposed by healthcare privacy regulations and medical device safety oversight are also examined. Standards development guiding compliant design is summarized. The overall landscape continues maturing, but further clarity is still needed to enable robust development of transformative healthcare smart contract applications.

Keywords: smart contracts, blockchain, healthcare, law, regulation, validity, HIPAA, CURES Act, standards.

Introduction

Smart contracts are blockchain-based self-executing contractual logic with potential to transform healthcare ecosystem efficiency, security and transparency. However, uncertainties around enforceability and healthcare regulatory constraints create adoption barriers. This analysis reviews the developing legal landscape to enable compliant smart contract healthcare integration.

Background

A smart contract encodes business terms as immutable software code executing deterministically on a tamper-proof blockchain ledger [1]. This allows trusted automation across workflows like medical claims adjudication, clinical trial data disclosure and precision medicine protocol enforcement [2].

Proposed applications include consolidating siloed health records, improving insurance claim processing, streamlining supply chain administration, enforcing prescription protocols and executing clinical trial contracts [3][4]. Benefits over fragmented healthcare data and process infrastructure include lower costs through automation, enhanced security via cryptography and increased trust through algorithmic transparency [5][6].

However, legal ambiguity exists around enforcing code-based agreements. Additionally, extensive healthcare regulations often conflict with blockchain architectures [7], presenting barriers to adoption. Hence realization of technological potential requiresnavigation of legal and compliance uncertainty.

Contract Law and Smart Contracts

Basic principles of common law contracts like demonstrated intent, consideration, contractual capacity and mutual assent do apply to software code agreements between parties [8]. U.S. courts also confirmed willingness to grant remedies when weaknesses cause contractual issues using principles like frustration of purpose and impossibility [9].

Areas of distinction remain regarding smart contract nuances. Immutability counters needed contractual flexibility as requirements evolve across long agreements [10]. Automation prevents human judgment for situational response [11]. Data integration necessitates risk management around counterparty dependence [12]. Reliance models contrast code integrity versus contracting party integrity [8].

Overall the American legal system demonstrated recognition of validity, emphasis of functionality over formality in enforcement and balance of code rigidity with legal fluidity [13]. Explicit opinions confirmed smart contracts can satisfy requirements for legal contracts [14]. Arizona, Tennessee and Nevada passed supportive legislation [15], while California, Ohio and North Dakota legislated limitations [16].

Healthcare Regulatory Barriers

Healthcare data usage faces regulations like HIPAA, HiTECH and state laws conflicting with blockchain's public transparency [17]. Encrypting sensitive data stored off-chain meets some privacy and security mandates but limits functionality [18]. Long term technical strategies like permissioned blockchains and zero-knowledge proofs manage access while upholding validity assurances [19].

The 21st Century CURES Act classified software like EHR systems and clinical support tools as medical devices needing FDA approval [20]. Existing FDA guidance covers clinical decision tools but not decentralized smart contract platforms [21], creating uncertainty. Software validation processes also burden agile development methods [22].

HL7, IEEE and ISO published healthcare blockchain best practices for access controls, identity management and responsible data sharing [23]. Following such guidance and architecting systems around published use cases and reference models accelerates compliant development [24]. State insurance regulators also began requiring IT infrastructure support for synchronized off-chain data inputs [25].

Early Adoption Trends

Highly segmented applications like genomic data access and patient consent management saw early deployment. Benefits around participants controlling data provenance audit trails outweighed integration overhead [26]. Industries with legacy transaction delays like pharmaceutical rebates and insurance claim reconciliations also began exploring use [27].

Consortium models brought competing health systems together in pilot programs to jointly assessimplementation paths aligning with emerging regulations [28]. Leading healthcare providers formed partnerships with blockchain technology companies and vendors to safely productize niche use cases [29].

Discussion

While basic contractual validity now exists in US law for smart agreements encoded in software, further legislative refinements and legal precedents confirming functional enforcement are still needed for widespread adoption. Healthcare regulations pose privacy, security and software safety challenges, although guidance documents increasingly provide design best practices. Consortia momentum and high value use cases are demonstrating legal and regulatory compliance in isolated implementations.

Conclusion

Progress continues across US contract law, healthcare policy making bodies and industry technology leadership in laying foundations to eventually enable transformative smart contract applications for efficiency, security and transparency gains. But fuller legal clarity, further regulatory guidance and ongoing prove vast technological utility are still needed to unlock the full disruptive potential of trustworthy automated contracting on blockchains across healthcare ecosystems.

References

[1] Ølnes, S., Ubacht, J., & Janssen, M. (2017). Blockchain in government: Benefits and implications of distributed ledger technology for information sharing. Government Information Quarterly, 34(3), 355-364.

[2] Zhang, P., White, J., Schmidt, D. C., Lenz, G., & Rosenbloom, S. T. (2018). FHIRChain: applying blockchain to securely and scalably share clinical data. Computational and structural biotechnology journal, 16, 267-278.

[3] Benchoufi, M., & Ravaud, P. (2017). Blockchain technology for improving clinical research quality. Trials, 18(1), 1-5.

[4] Wang, S., Ouyang, L., Yuan, Y., Ni, X., Han, X., & Wang, F. Y. (2019). Blockchain-enabled smart contracts: architecture, applications, and future trends. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 49(11), 2266-2277.

[5] Ølnes, S. (2016). Beyond Bitcoin Enabling Smart Government Using Blockchain Technology.

[6] Thompson, T. (2019). Closing the interoperability gap: Applying the Cures Act information blocking provisions to enable patient access and provider exchange of health data from wearable devices. Cornell L. Rev., 105, 1201.

[7] Roehrs A., da Costa C.A., da Rosa Righi R., da Silva V.F., Goldim J.R., Schmidt D.C. (2019) Analyzing the Performance of a Blockchain-based Personal Health Record Implementation. J. Biomed. Inform. 92 103140.

[8] Savelyev, A. (2017). Contract law 2.0: "Smart" contracts as the beginning of the end of classic contract law. Information & Communications Technology Law, 26(2), 116-134.

[9] O'Shields, R. (2017). Smart contracts: Legal agreements for the blockchain. North Carolina Banking Institute, 21, 177.

[10] Lee J. (2017) Smart Contracts and Legal Enforceability. Social Science Research Network. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2959166

[11] Reyes C. L. (2017) Moving Beyond Bitcoin to an Endogenous Theory of Decentralized Ledger Technology Regulation: An Initial Proposal. Social Science Research Network. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2930077

[12] Werbach K. D., Cornell N. (2017) Contracts Ex Machina. Duke L. & Tech. Rev. 67.

[13] Reyes C. L. (2021) Conceptualizing Cryptolaw. Neb. L. Rev. 100 977.

[14] Cohn A., West T., Parker C. (2017) Smart After All: Blockchain, Smart Contracts, Parametric Insurance, and Smart Energy Grids. Georgetown Law Technology Review 1 273-304.

[15] AZ Rev Stat § 44-7061 (2018); TN Pub Ch. 702 (2018); NV SB 398 (2017).

[16] An Act to Amend Section 1671 of the Civil Code, Relating to Smart Contracts, CA A.B. 2658 (2018); OH SB 220 (2020); ND H.B. 1045 (2021).

[17] Benchoufi, M., & Ravaud, P. (2017). Blockchain technology for improving clinical research quality. Trials, 18(1), 1-5.

[18] Zhang, P., White, J., Schmidt, D. C., Lenz, G., & Rosenbloom, S. T. (2018). FHIRChain: applying blockchain to securely and scalably share clinical data. Computational and structural biotechnology journal, 16, 267-278.

[19] Roehrs A., da Costa C.A., da Rosa Righi R., da Silva V.F., Goldim J.R., Schmidt D.C. (2019) Analyzing the Performance of a Blockchain-based Personal Health Record Implementation. J. Biomed. Inform. 92 103140.

[20] Thompson, T. (2019). Closing the interoperability gap: Applying the Cures Act information blocking provisions to enable patient access and provider exchange of health data from wearable devices. Cornell L. Rev., 105, 1201.

[21] U.S. Department of Health and Human Services, Food and Drug Administration. (2019) Clinical Decision Support Software. https://www.fda.gov/regulatory-information/search-fda-guidance-documents/clinical-decision-support-software

[22] Liu P.T.S. (2019) Legal and Regulatory Implications of Blockchain Health Records. Journal of Law and the Biosciences, 6(1), 185–235.

[23] IEEE Standards Association. (2017) Blockchain in Healthcare. Telehealth and Telemedicine Standards to Protect Sensitive Information. https://blockchain.ieee.org/images/files/pdf/ieee-blockchain-healthcare-pdf

[24] HL7 International. (2019) Blockchain in Healthcare Today. Version 1.0. http://hln.hl7.org/documentcenter/public_temp_9ACA3175-1C23-BA17-0C25DBB3181DAF59/wg/fhir/blockchain/HL7_Blockchain_in_Healthcare_Today_2019May.pdf

[25] NH H.B. 1685. (2021). https://gencourt.state.nh.us/bill_status/billText.aspx?sy=2021&id=923&txtForm at=html

[26] Benbunan-Fich R. (2021) An overview of the use of blockchain for consent management in biomedical research. Wiley Interdiscip Rev Data Min Knowl Discov. 2021;11:e1382. doi: 10.1002/widm.1382

[27] Agbo C.C., Mahmoud Q.H., Eklund J.M. (2019) Blockchain Technology in Healthcare: A Systematic Review. Healthcare 2019; 7(2):56. https://doi.org/10.3390/healthcare7020056

[28] Ekblaw A., Azaria A., Halamka J.D., Lippman A. (2016) A Case Study for Blockchain in Healthcare: MedRec prototype for electronic health records and medical research data. Proceedings of IEEE Open & Big Data Conference. https://doi.org/10.13140/RG.2.2.36632.08448/1

[29] Miller R. (2022) Cleveland Clinic, IBM forge 10-year partnership to establish healthcare accelerator. https://www.beckershospitalreview.com/digital-transformation/cleveland-clinic-ibm-forge-10-year-partnership-to-establish-healthcare-accelerator.html