Privacy Preservation Techniques for Smart Contracts in Blockchain

***Abstract*—The widespread adoption of smart contracts on blockchain platforms has introduced significant advantages in terms of transparency and efficiency for digital transactions. This paper presents an extensive exploration of the data privacy landscape specifically in the context of smart contracts, aiming to move beyond the inherent transparency associated with blockchain technology. By navigating this privacy landscape, our objective is to identify existing privacy-preserving mechanisms, assess their efficacy, and propose potential research directions to address privacy concerns in smart contracts.**

Keywords— Smart contracts, Data privacy, Blockchain technology, Privacy challenges, sensitive data.

I. Introduction

Blockchain is decentralized technology that uses distributed digital ledgers to record transactions across computer networks. Each "block" in the chain contains unique identifiers such as timestamp, version, nonce, previous hash etc. that are specific to a transaction. Once a block is inserted to the chain, it cannot be removed making it immutable [1]. The decentralized nature of blockchain provides high degree of security and resistance to hacking.

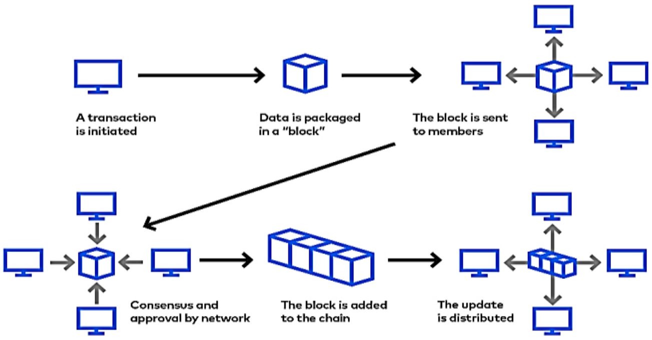
A transaction is initiated
Data is packaged in a "block"
The block is sent to members
Consensus and approval by network
The block is added to the chain
The update is distributed

Figure1: Overview of Blockchain

Since the ledger is distributed across many computers, any changes made to it would require the consensus of the network. To permanently record the well-structured and organized data of a new transaction, a "block" is created. This block contains references to the adjacent blocks, creating a "chain" of interconnected blocks, as depicted in Figure 1. The creation of a blockchain begins with the initiation of a transaction, where the data is packed into a block and sent to the network members. The network members collaborate to verify the precision and validity of the data within the block [1]. Every block is added to the chain once approved and the rationalized version of the chain is shared across the network. This ensures that all participants have access to the most current version of the blockchain, preserving the integrity of the system

Industries in various domains like supply chain[10], real estate[5], healthcare [1],insurance [2], financial [3], [4], government [6], real estate [7], social media [8], [9], and education [11] etc are revolutionized by the Blockchain technology (BC). A number of real-world problems can be solved logically and efficiently using BC technology. With the help of 3 main characteristics like decentralization, point-to-point network and immutability, BC describes how the data is gathered, stored and delivered. The first generation of BC technology purely focused on crypto currencies like Bitcoin. Author Andreas Antonopoulos, described Bitcoin as un-banks the banked or banks the un-banked [12], [13], the 2nd generation, demonstrated by Ethereum, enables a new computing paradigm which is decentralized and opensource [14], [15]. Bitcoin is pure monetary system whereas these systems introduce enormous amount of security faults that don't exist in Bitcoins. An account holder can exchange, buy and sell cryptocurrencies using smart contracts which are executed automatically when a transaction occurs on Ethereum platform and these are maintained in BC. These contracts are capable of transferring ether to and from various contracts as well as users. Transactions are submitted on Ethereum Network by the users for creating new contracts, perform contract functionalities, and send ether to participants or other contracts. A distributed ledger records the transactions which is public and allows to add the state of transaction on a data structure. The state of every contract and user's balance is established based on the order in which transactions are recorded in blockchain. The security of the smart contracts is one of the main topics of research among various security agencies as it contains a huge amount of cryptocurrency worth billions of dollars as displayed in Figure 2.

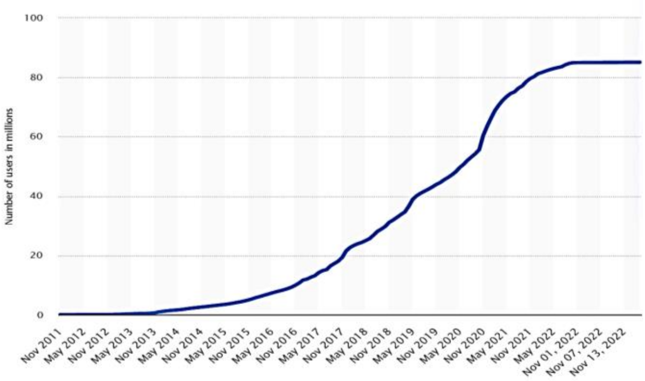

Figure 2: Number of Blockchain Users [15]

1.1 Smart Contract

Smart Contracts (SCs) automate the execution based on the terms agreed by the contract parties to check whether the conditions are met, thus removing the dependency on a central server and this code is built in as a part of the contract. Once signed off, even the creator cannot alter the content or prevent execution. However, while validating the contracts in blockchain the terms and conditions are revealed thereby affecting their privacy. Additionally, the transaction fees and timing can increase the overall spending for a contract depending on the steps taken for validation . The blockchain network replicates the code and agreement stored. Based on specific terms of the contract a wide range of information can be enclosed in smart contract data. For example, it might include information about the parties involved in the contract, the goods or services being exchanged, the terms of payment, and any other relevant details.

1.2 Privacy Preservation

In general: Privacy preserving techniques are methods used to safeguard the privacy of an individual or organizations while still allowing for the collection and analysis of data. These techniques can be applied in a variety of contexts, including the storage and handling of personal information, the use of data in research and analytics, and the sharing of information with third parties. The general framework of privacy preservation is shown in Figure 3.

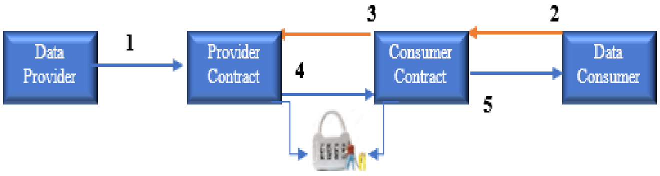

Figure 3: Privacy-Preserving Smart Contract in Blockchain

The steps of privacy protection are as follows.

1) A data provider, stores encrypted data on a centralized or decentralized storage service (such as AWS, IPFS, or Swarm). He creates a smart contract, that includes the address of the data and any payment or privacy requirements.
2) The contract is also provisioned with a data decryption key, which is kept private.
3) The data consumer, who wants to use the provided data creates a smart contract, that meets the constraints of the data provider.
4) The data provider contract activates the consumer contract, which sends a signed request that verifies its identity.
5) The data provider Contract provides a secure data decryption key on successful verification of the consumer contract.
6) Consumer contract uses the decryption key to access and perform required operations on decrypted data.

There are various approaches to privacy preservation, and the specific techniques used will rely on the particular needs and requirements of the situation. Some common methods include the use of anonymization and de-identification techniques, the implementation of access controls and permissions, the use of encryption and secure communication protocols, and the adoption of privacy-enhancing technologies.

In Specific: A privacy protection model for smart contracts is a collection of techniques or methods used to protect the privacy of organizations or individuals while still allowing for the execution of smart contracts [16]. Smart contracts are tiny programs that are self-executing, directly written into lines of code. They are basically designed to support and verify the correctness of transaction between 2 communicating parties. There are several approaches to protecting privacy in the context of smart contracts. One common method is to perform the verification of a statement or claim without revealing any additional information using zero-knowledge proofs. This can be used to prove that a specific condition has been met, without disclosing the underlying data that led to the condition being satisfied.

1.3 Approaches for Privacy Protection:

There are several ways that could be used to protect a smart contract under a privacy protection model:

1. De-identification: Machine learning can be used to remove and modify information in smart contract data, making it difficult to backtrace to its individuals through De-identification. While de-identification can be an effective privacy preserving technique, it may not always be sufficient to protect the privacy of individuals, as it is possible to re-identify using other data sources or by combining multiple datasets. Smart contracts often rely on the ability to identify and authenticate the parties involved in the contract, if personal identifiers are removed or modified in the data used in a smart contract, it can become difficult or impossible to verify the identity of the parties involved, which can undermine the integrity and security of the contract.
2. Homomorphic Encryption: Machine learning could be used to encrypt the data used in a smart contract, so that it will be difficult for unauthorized parties to access the data [18]. Homomorphic encryption allows performs computations on encoded data without first decoding it, thereby preserving the privacy of the sensitive information. One specific algorithm that can be used for homomorphic encryption in smart contracts is the Paillier cryptosystem [19].

3. Federated learning is a technique for training machine learning models on decentralized data without disclosing the raw data. A popular federated learning algorithm is the federated averaging algorithm, which trains the model by aggregating updates from multiple parties. In a study by Shokri et al. (2015), the federated averaging algorithm was applied to the classification of images in a decentralized manner, and the results showed that the algorithm achieved high accuracy rates of up to 90%.
4. Machine learning algorithms such as Paillier cryptosystem for homomorphic encryption, Laplace mechanism for differential privacy, and federated averaging algorithm for federated learning can be used for privacy protection in Ethereum-based smart contracts of blockchain. These algorithms have been shown to achieve high accuracy rates while preserving the privacy of sensitive information.

A. Privacy Challenges in Smart Contracts

Smart contracts are immutable and transparent as mentioned above, which means that once deployed, their code and data are publicly accessible [17]. This characteristic poses several challenges to privacy protection, including:

a. Data Leakage: Smart contracts may inadvertently expose sensitive data, such as private keys, financial transactions, or user identities [18].

b. Anonymity: The public nature of blockchain networks raises questions about maintaining user privacy while ensuring regulatory compliance [19].

c. Off-Chain Data Integration: Off-chain data sources, can interact with Smart contracts which may introduce privacy risks if not handled properly [20].

II. RELATED WORK

The motivation of this survey is to provide assistance to developers, students and researchers who are interested in understanding privacy preservation techniques for smart contracts.

Author Desai et. al [21] combined private and public blockchains to create a hybrid blockchain architecture that allows bids which are sensitive to be disclosed on a private blockchain so that bids are learnt only by the auctioneer, and no one else. Patil et. al [22] proposed a PUF model which is a secret computational model of physically unclonable function based on blockchain technology. Off-chain storage interact via Oracle-based mechanisms, to build an effective connection between real assets and distributed database was demonstrated by Chen et. al [23] . Li et. al [24] proposed a systematic study on scientific databases that deals with privacy and security in the field of blockchain-based FL methodologies Sipek et. al [25] demonstrated an educational learning platform which is designed as a distributed system that can make the educational system more versatile and transparent. Steffen et. al [26] demonstrated the expressiveness of the ZeeStar compiler by integrating non-interactive ZkPs and adding homomorphic encryption by encoding 12 example contracts, including oblivious transfer and a private payment system like Zether. Subathra et. al [27] study ipfs-based data aggregation and decentralized consensus blockchain for efficient data storage scheme. The PoW-enabled scheme along with Elgamal-based data aggregation is employed in the blockchain consensus algorithm. Zhou et. al [28] proposed a tree-based training network for abstract syntax trees (AST) for TMLVD prediction.

Kosba et. al [29] presented Hawk, a smart contract system that does not store financial transactions in transparent on the blockchain and is decentralized, thus transactional privacy is retained from the public's view. The subject of Dagher et. al [30] focused security and privacy concerns in the healthcare industry by analyzing the interaction of Ancile with different needs of patients, providers, and third parties. Cheng et.al [31] analyzed the pitfalls arising from harmonizing Trusted Execution Environments and blockchains. The TEEs are fragmented across hospitals which are decentralized and hinders data sharing and put patient's privacy at risks. To address these issues Liu et. al [32] proposed preserving data sharing which uses Blockchain for EMRs, called BPDS. By fusing edge computing and blockchain technologies, Gai et al. [33] implemented a permissioned blockchain edge model for smart grid networks (PBEM-SGN) and addressed important smart grid, privacy, and energy security challenges. "Privy Sharing," a blockchain-based novel framework for safe and private IoT data exchange in a smart city setting, is presented by Makhdoom et al. [34]. Arachchige et. al [35] introduced a framework to enforces privacy and trustworthiness on IoT data named PriModChain by amalgamating differential privacy, Ethereum blockchain, federated ML and smart contracts. Alkadi et. al [36] designed a security-based distributed intrusion detection and privacy-based blockchain through a deep blockchain framework (DBF) with smart contracts in IoT networks.

With the increase in the usage of blockchain technology, that provides a way to manage assets in a decentralized way for example Bitcoin, Ayoade et. al., 2018 enforced a decentralized system of data management for IoT devices where all audit trail of data access and data access permission is stored in blockchain

The Table 1: below describes the existing techniques utilizing blockchain technology in Ethereum for privacy preservation: approaches and drawbacks.

Methods	Factors	Limitations	Ref
PPChain	Efficient protection of personal data and Security of a high standard privacy are guaranteed.	Lacks confidentiality, regulation, transparency or anonymity.	[37]
	The emphasis on optimizing training performance takes precedence over considering the correlation between variables.	High Computational Cost	

BiLSTM	Increases Storage Expenses.	Additional training time is needed, and the pace is slower in comparison to alternative methods.	[38]
	Exceptional accuracy in prediction, precision, and F1 score.	Does not possess costly hardware for executing intricate mathematical computations.	
SGINs	False Positive rate is High.	No universal accessibility to the service.	[39]
	Affordable storage expenses and minimal communication delays	The absence of an all-encompassing security system for communication and privacy protection leads to certain vulnerabilities in terms of security	
Federated Learning	It intensifies functionality attributes related to signaling, communication overheads, and computations, resulting in increased efficiency.	The efficiency decreases when compressing a large number of devices within the security system.	[40]
	It provides efficient authentication even with limited resources and replica storage.	Federated communication system is costly.	
Data encryption	It effectively enables strict rights management, making it suitable for various applications.	It provides limited computation for compatibility.	[41]
	It enhances data integrity at a low implementation cost.	The scalability is very poor.	
Raspberry Pi network	The cost of implementation is reasonably priced.	Managing a substantial volume of data requires extra storage within this network.	[42]
	The suggested remedy is more practical and dependable.	It fails to attain an ideal equilibrium between connectivity and storage needs.	
peer-to-peer	It improves computation rationality and ensures identity anonymity.	Data confidentiality is significantly compromised.	[43]
	It simplifies the setup of client data without requiring specialized knowledge.	The resources of file are not centrally organized, resulting in longer processing times.	
EdDSA	It enhances privacy by improving immutability, transparency, and the overall privacy system.	When dealing with extensive data, there is a risk of private key leakage.	[44]
	It diminishes the computational intricacy of decentralization algorithms.	It lacks the capability to combine complex data.	

III. PRIVACY PRESERVING TECHNIQUES AND TOOLS

A. Privacy-Preserving Techniques for Smart Contracts

Several techniques and approaches have been proposed to address the challenges associated with privacy in smart contracts. Some notable techniques are:

a. Zero-Knowledge Proofs (ZKPs): ZKP is a technique using which One entity (the prover) proves the validity of a statement to another entity (the verifier) without disclosing any additional information. ZKPs have been employed to enhance privacy in smart contracts by verifying computations without exposing sensitive data.

b. Secure Multi-Party Computation (MPC): MPC protocols allow multiple parties to collaborate to calculate a function on their private inputs without revealing those inputs to each other. MPC can be used in smart contracts to perform operations on sensitive data without exposing it.

c. Off-Chain Confidentiality: Off-chain solutions, such as trusted execution environments (TEEs) or secure enclaves, can be utilized to process sensitive data outside the blockchain while ensuring its confidentiality. The results are subsequently validated and recorded on the blockchain.

B. Privacy Enhancing Tools

Researchers and developers have also proposed various tools and frameworks specifically designed to increase privacy in smart contracts. These include:

a. Solidity Enhancements: Ethereum smart contracts are written using a programming language called Solidity. To address privacy concerns, researchers have proposed extensions to Solidity, such as access control mechanisms, encryption primitives, and privacy-aware data types.
b. Smart Contract Auditing: Auditing tools have been developed to identify potential privacy vulnerabilities in

smart contracts. These tools analyze the contract's code and data flow to detect potential data leaks or privacy breaches.

c. Privacy-Focused Blockchains: Alternative blockchain platforms have emerged that prioritize privacy, such as Monero, Zcash, and Quorum. These platforms offer enhanced privacy features, including anonymous transactions, shielded addresses, and confidential smart contracts.

C. Case Studies and Implementation Examples

Privacy protection techniques in real-world scenarios are demonstrated with various case studies and implementation examples. These studies demonstrate the feasibility and effectiveness of privacy-enhancing solutions in smart contracts.

a. Private Voting Systems: Privacy-preserving smart contracts have been deployed to enable anonymous and verifiable voting systems, where individual votes remain private while ensuring the integrity of the overall process.

b. Confidential Data Sharing: Smart contracts with privacy-enhancing techniques have been used to facilitate secure and confidential data sharing between organizations, enabling secure collaboration without exposing sensitive information.

c. Decentralized Finance (DeFi): Privacy concerns have emerged in the context of decentralized finance applications. Many other privacy-preserving mechanisms, such as confidential transactions, zero-knowledge asset swaps and private lending platforms, have been proposed to address these concerns

IV. CONCLUSION

Privacy protection of sensitive data from smart contract .sol files is an essential aspect of blockchain technology. The literature survey reveals a range of challenges, techniques, tools, and frameworks that have been developed to enhance privacy in smart contracts. However, it is still an active area of research, and further advancements are needed to address the evolving privacy requirements of blockchain-based systems. Future research should focus on scalability, usability, and compatibility of privacy-enhancing techniques within the smart contract ecosystem.

REFERENCES

[1] O Budzinski, , S Gaenssle, & Lindstädt-Dreusicke, N" Data (r) evolution: the economics of algorithmic search and recommender services. In Handbook on Digital Business Ecosystems. Edward Elgar Publishing" 2022.

[2] S. Parthasarathy, A. Harikrishna, G. Narayanan, K. Singh et al., "Secure distributed medical record storage using blockchain and emergency sharing using multi-party computation," 11th IFIP International Conference on New Technologies, Mobility and Security (NTMS). IEEE, pp. 1–5,2021.

[3] L. Zhang, Y. Xie, Y. Zheng, W. Xue, X. Zheng, and X. Xu, "The challenges and countermeasures of blockchain in finance and economics," Systems Research and Behavioral Science, vol. 37, no. 4, pp. 691–698, 2020.

[4] P. Treleaven, R. G. Brown, and D. Yang, "Blockchain technology in finance," Computer, vol. 50, no. 9, pp. 14–17, 2017.

[5] A. K. Kar and L. Navin, "Diffusion of blockchain in insurance industry: An analysis through the review of academic and trade literature," Telematics and Informatics, vol. 58, p. 101532, 2021.

[6] S. Olnes, J. Ubacht, and M. Janssen, "Blockchain in government: Benefits and implications of distributed ledger technology for information sharing," pp. 355–364, 2017.

[7] V. Thakur, M. Doja, Y. K. Dwivedi, T. Ahmad, and G. Khadanga, "Land records on blockchain for implementation of land titling in india," International Journal of Information Management, vol. 52, p. 101940, 2020.

[8] C. Li and B. Palanisamy, "Incentivized blockchain-based social media platforms: A case study of steemit," in Proceedings of the 10th ACM conference on web science, pp. 145–154,2019.

[9] T. W. Jing and R. K. Murugesan, "A theoretical framework to build trust and prevent fake news in social media using blockchain," in International conference of reliable information and communication technology. Springer, pp. 955–962,2018.

[10] F. Longo, L. Nicoletti, A. Padovano, G. d'Atri, and M. Forte, "Blockchain-enabled supply chain: An experimental study," Computers & Industrial Engineering, vol. 136, pp. 57–69, 2019.

[11] A. Alammary, S. Alhazmi, M. Almasri, and S. Gillani, "Blockchain-based applications in education: A systematic re- view," Applied Sciences, vol. 9, pp 12, 2400, 2019.

[12] A. M. Antonopoulos, Mastering Bitcoin: Programming the open blockchain. " O'Reilly Media, Inc.", 2017.

[13] M. Thombs and A. A. Tillman, "Designing 21st century curricu- lum for bitcoin and blockchain studies," International Journal of Global Business, vol. 11, no. 1, pp. 67–80, 2018.

[14] M. Swan, Blockchain: Blueprint for a new economy. " O'Reilly Media, Inc.", 2015.

[15] M. Nofer, P. Gomber, O. Hinz, and D. Schiereck, "Blockchain," Business & Information Systems Engineering, vol. 59, no. 3, pp. 183–187, 2017.

[16] A. Bogner, M. Chanson, and A. Meeuw, "A decentralised sharing app running a smart contract on the ethereum blockchain," in Proceedings of the 6th International Conference on the Internet of Things, 2016, pp. 177–178.

[17] Gupta, R., Tanwar, S., Al-Turjman, F., Italiya, P., Nauman, A., & Kim, S. W. (2020). Smart contract privacy protection using AI in cyber-physical systems: tools, techniques and challenges. IEEE access, 8, 24746-24772.

[18] Steffen, S., Bichsel, B., Gersbach, M., Melchior, N., Tsankov, P., & Vechev, M. (2019, November). zkay: Specifying and enforcing data privacy in smart contracts. In Proceedings of the 2019 ACM SIGSAC conference on computer and communications security (pp. 1759-1776).

[19] Juels, A., Kosba, A., & Shi, E. (2016, October). The ring of gyges: Investigating the future of criminal smart contracts. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (pp. 283-295).

[20] Singh, S. K., Jenamani, M., Dasgupta, D., & Das, S. (2021). A conceptual model for Indian public distribution system using consortium blockchain with on-chain and off-chain trusted data. Information Technology for Development, 27(3), 499-523.

[21] Gaur, R.; Prakash, S.; Kumar, S.; Abhishek, K.; Msahli, M.; Wahid, A. A Machine-Learning– Blockchain-Based Authentication Using Smart Contracts for an IoHT System. Sensors 23 Nov,2022, 9074. https://doi.org/10.3390/s22239074.

[22] Zhang Xihua , S. B. Goyal , Miretab Tesfayohanis ,and Chaman Verma Blockchain-Based Privacy-Preserving Approach Using SVML for Encrypted Smart City Data ,30 July 2022

[23] Tahmid Hasan Pranto , Kazi Tamzid Akhter Md. Hasib, Tahsinur Rahman, Akm Bahalul Haque , A. K. M. Najmul Islam , And Rashedur M. Rahman Blockchain and Machine Learning for Fraud Detection: A Privacy-Preserving and Adaptive Incentive Based Approach 24 August 2022.Digital Object Identifier 10.1109/ACCESS.2022.3198956

[24] R. Cheng, F. Zhang, J. Kos, W. He, N. Hynes, N. Johnson, A. Juels, A. Miller, and D. Song, ``Ekiden: A platform for condentiality preserving, trustworthy, and performant smart contracts," in Proc. IEEE Eur. Symp. Secur. Privacy, Jun. 2019, pp. 185200.

[25] K. Salah, M. H. U. Rehman, N. Nizamuddin, and A. Al-Fuqaha, ``Blockchain for AI: Review and open research challenges," *IEEE Access*, vol. 7, pp. 1012710149, 2019.

[26] C. Li, B. Palanisamy, and R. Xu, ``Scalable and privacy-preserving design of ON/OFF-chain smart contracts," in *Proc. IEEE 35th Int. Conf. Data Eng. Workshops (ICDEW)*, Apr. 2019, pp. 712.

[27] Weng, J.-S., Weng, J., Li, M., Zhang, Y., Luo, W.: DeepChain: Auditable and privacy preserving deep learning with blockchain-based incentive. IACR Cryptology ePrint Archive, vol. 2018, p. 679. (2019)

[28] P. Tasatanattakool and C. Techapanupreeda, ``Blockchain: Challenges and applications," in Proc. Int. Conf. Inf. Netw. (ICOIN), Jan. 2018, pp. 473475

[29] S.Wang, Y. Yuan, X.Wang, J. Li, R. Qin, and F.-Y.Wang, ``An overview of smart contract: Architecture, applications, and future trends," in Proc. IEEE Intell. Vehicles Symp. (IV), Jun. 2018, pp. 108-113.

[30] A. B. Kurtulmus and K. Daniel, ``Trustless machine learning contracts; Evaluating and exchanging machine learning models on the Ethereum blockchain," *CoRR*, vol. abs/1802.10185, pp. 111, Feb. 2018.

[31] .Marwala and B. Xing, ``Blockchain and artificial intelligence,'' Feb. 2018, *arXiv:1802.04451*. [Online]. Available: https://arxiv. org/abs/1802.04451

[32] T. N. Dinh and M. T. Thai, ``AI and blockchain: A disruptive integration,'' *Computer*, vol. 51, no. 9, pp. 4853, Sep. 2018.

[33] Z. Geng, Y. He, T. Niu, H. Li, L. Sun, W. Cheng, and X. Li, ``Poster: Smart-contract based incentive mechanism for *K*-anonymity privacy protection in LBSs,'' in *Proc. IEEE Symp. Privacy-Aware Comput. (PAC)*, Aug. 2017, pp. 200201

[34] D. Kim, D. Shin, and D. Shin, ``Unauthorized access point detection using machine learning algorithms for information protection," in *Proc. 17th IEEE Int. Conf. Trust, Secur. Privacy Comput. Commun.*, Aug. 2018, pp. 18761878.

[35] N. Senavirathne and V. Torra, ``Approximating robust linear regression with an integral privacy guarantee," in *Proc. 16th Annu. Conf. Privacy, Secur. Trust (PST)*, Aug. 2018, pp. 1-10.

[36] Arachchige, P. C. M., Bertok, P., Khalil, I., Liu, D., Camtepe, S., & Atiquzzaman, M. (2020). A trustworthy privacy preserving framework for machine learning in industrial IoT systems. IEEE Transactions on Industrial Informatics, 16(9), 6092-6102.

[37] Alkadi, O., Moustafa, N., Turnbull, B., & Choo, K. K. R. (2020). A deep blockchain framework-enabled collaborative intrusion detection for protecting IoT and cloud networks. IEEE Internet of Things Journal, 8(12), 9463-9472.

[38] Garg, L., Chukwu, E., Nasser, N., Chakraborty, C., & Garg, G. (2020). Anonymity preserving IoT-based COVID-19 and other infectious disease contact tracing model. Ieee Access, 8, 159402-159414.

[39] Lin, C., He, D., Huang, X., Xie, X., & Choo, K. K. R. (2020). Ppchain: A privacy-preserving permissioned blockchain architecture for cryptocurrency and other regulated applications. IEEE Systems Journal, 15(3), 4367-4378.

[40] Rahmadika, S.; Astillo, P.V.; Choudhary, G.; Duguma, D.G.; Sharma, V.; You, I. Blockchain-Based Privacy Preservation Scheme for Misbehavior Detection in Lightweight IoMT Devices. IEEE J. Biomed. Health Inform. 2022, 27, 710–721. [Google Scholar] [CrossRef]

[41] Xiong, T.; Zhang, R.; Liu, J.; Huang, T.; Liu, Y.; Yu, F.R. A blockchain-based and privacy-preserved authentication scheme for inter-constellation collaboration in Space-Ground Integrated Networks. Comput. Netw. 2022, 206, 108793. [Google Scholar] [CrossRef]

[42] Singh, S.; Rathore, S.; Alfarraj, O.; Tolba, A.; Yoon, B. A framework for privacy-preservation of IoT healthcare data using Federated Learning and blockchain technology. Futur. Gener. Comput. Syst. 2021, 129, 380–388. [Google Scholar] [CrossRef]

[43] Guo, L.; Xie, H.; Li, Y. Data encryption based blockchain and privacy preserving mechanisms towards big data. J. Vis. Commun. Image Represent. 2019, 70, 102741. [Google Scholar] [CrossRef]

[44] Mohan, D.; Alwin, L.; Neeraja, P.; Lawrence, K.D.; Pathari, V. A private Ethereum blockchain implementation for secure data handling in Internet of Medical Things. J. Reliab. Intell. Environ. 2021, 8, 379–396. [Google Scholar] [CrossRef]