







ORIGINAL

## Research Directions for Decentralized Technology Transactions: An Update

### Orientaciones de investigación para transacciones tecnológicas descentralizadas: una actualización

Ahmaddul Hadi<sup>1</sup> , Sandi Rahmadika<sup>1</sup>  , Ulfia Rahmi<sup>2</sup> , Harashta Tatimma Larasati<sup>3</sup> , Bayu Ramadhani Fajrin<sup>4,5</sup> 

<sup>1</sup>Department of Electronic Engineering, Universitas Negeri Padang. Indonesia.

<sup>2</sup>Department of Educational Technology, Universitas Negeri Padang. Indonesia.

<sup>3</sup>Department of Information Security, Graduate School, Pukyong National University. South Korea.

<sup>4</sup>School of Vocational, Universitas Negeri Padang. Sumatera Barat 25173, Indonesia.

<sup>5</sup>STEM Enculturation Research Centre, Faculty of Education, Universiti Kebangsaan Malaysia. Malaysia.

**Cite as:** Hadi A, Rahmadika S, Rahmi U, Tatimma Larasati H, Ramadhani Fajri B. Research Directions for Decentralized Technology Transactions: An Update. Salud, Ciencia y Tecnología. 2025; 5:2161. <https://doi.org/10.56294/saludcyt20252161>

Submitted: 26-04-2025

Revised: 12-08-2025

Accepted: 05-09-2025

Published: 06-09-2025

Editor: Prof. Dr. William Castillo-González 

Corresponding Author: Sandi Rahmadika 

#### ABSTRACT

Decentralized technologies such as blockchain and federated learning have emerged as promising solutions to improve privacy, transparency, and security in distributed environments. This paper aims to provide updated research directions concerning the unresolved issues of linkability and traceability in decentralized technology transactions. A systematic review was conducted using Scopus and Web of Science databases, covering studies published between 2017 and 2023. A total of 313 papers were initially identified, screened, and filtered based on inclusion and exclusion criteria, resulting in 29 relevant studies. The analysis indicates that most prior works focused on privacy preservation and incentive mechanisms but neglected linkability and traceability concerns. Several approaches, including ring signatures, CryptoNote protocols, and smart contract-based incentives, were identified as potential solutions. While blockchain-federated learning integration enhances privacy, unresolved traceability and linkability issues still pose significant risks in sensitive domains such as healthcare and finance. Future work should prioritize addressing these issues to ensure secure, anonymous, and scalable decentralized transactions.

**Keywords:** Blockchain; Decentralized Technology; Edge Devices; Federated Learning; Linkability; Privacy and Traceability Issues.

#### RESUMEN

Las tecnologías descentralizadas, como blockchain y el aprendizaje federado, se han convertido en soluciones prometedoras para mejorar la privacidad, la transparencia y la seguridad en entornos distribuidos. Este artículo busca proporcionar líneas de investigación actualizadas sobre los problemas pendientes de vinculación y trazabilidad en las transacciones tecnológicas descentralizadas. Se realizó una revisión sistemática utilizando las bases de datos Scopus y Web of Science, que abarcó estudios publicados entre 2017 y 2023. Inicialmente, se identificaron, seleccionaron y filtraron 313 artículos según criterios de inclusión y exclusión, resultando en 29 estudios relevantes. El análisis indica que la mayoría de los trabajos previos se centraron en la preservación de la privacidad y los mecanismos de incentivos, pero descuidaron las cuestiones de vinculación y trazabilidad. Se identificaron varios enfoques como posibles soluciones, como las firmas de anillo, los protocolos CryptoNote y los incentivos basados en contratos inteligentes. Si bien la

integración de blockchain y el aprendizaje federado mejora la privacidad, los problemas de trazabilidad y vinculación aún plantean riesgos significativos en ámbitos sensibles como la salud y las finanzas. Los trabajos futuros deberían priorizar la atención a estos problemas para garantizar transacciones descentralizadas seguras, anónimas y escalables.

**Palabras clave:** Blockchain; Tecnología Descentralizada; Dispositivos de Borde; Aprendizaje Federado; Vinculabilidad; Privacidad y Problemas de Trazabilidad.

## INTRODUCTION

Decentralized technologies have become central to discussions on data management and artificial intelligence due to their ability to address the limitations of conventional centralized systems.<sup>(1,2,3,4,5,6)</sup> Traditional architectures, although effective for many applications, remain vulnerable to single points of failure, cyberattacks, and data misuse. Blockchain technology, first applied in cryptocurrencies, introduced immutable and distributed ledgers that enhance transparency, accountability, and security.<sup>(1,2,3,7,8,9,10)</sup> In parallel, federated learning, introduced in 2017, shifted machine learning toward decentralized training on local devices, thereby reducing communication costs and preserving data privacy.<sup>(4,5,11,12,13,14)</sup>

The convergence of blockchain and federated learning has gained increasing attention, particularly in domains such as healthcare, financial services, and the Internet of Things.<sup>(6,7,8,15,16,17,18)</sup> Blockchain provides mechanisms for secure data sharing and incentive distribution, while federated learning enables collaborative model improvement without exposing raw data. Together, they promise privacy, transparency, and resilience. However, this integration also introduces unresolved challenges. Chief among them are issues of linkability and traceability of transactions, which remain inadequately explored in existing studies. While many works address privacy and scalability, few examine how transaction metadata can compromise anonymity in sensitive applications.<sup>(9,10,11,19,20,21,22)</sup>

This gap has significant implications. In fields requiring strict confidentiality, such as fraud detection or medical diagnosis, weaknesses in unlinkability or untraceability can undermine trust in decentralized systems. Addressing these limitations is essential for advancing secure and reliable blockchain-federated learning frameworks.<sup>(23,24)</sup>

Therefore, this study conducts a systematic review of research indexed in Scopus and Web of Science between 2019 and 2024. The objective is to evaluate the current state of blockchain-federated learning integration, highlight overlooked concerns regarding linkability and traceability, and propose directions for future research that can strengthen the security and applicability of decentralized technologies.

**Table 1.** The comparison of main references and research impacts

Research Year	Implementation	Main Protocols /Supplementary
<sup>(25)</sup> / 2021	*Collaborative learning with decentralize incentive scheme. *ConvNet to visual imagery from private datasets of clients	*Grup signature of clients *Ring signature algorithms *Used-model onlytransactions *Decentralized rewarding scheme
<sup>(26)</sup> / 2022	*Lightweight the Internet Medical of Things (IoMT) devices *Misbehavior detection applied to the insulin pump	*Federated learning based misbehavior detection (bidirectional longshort term memory) *Untraceable incentive schemes via smart contracts
<sup>(13)</sup> / 2019	*Blockchain and federated learning for 5G beyond *Asynchronous federated learning	*Resource sharing, D2D caching, edge computation, and computational analysis
Curent version	*Research directions for decentralized technology transactions *An update from our previous related works	*Searching possibilities to merge <sup>(25)</sup> and <sup>(26)</sup> .

## Core system components

This section provides the conceptual foundation for understanding the transition from centralized log management to decentralized approaches, as well as the role of blockchain in federated learning. It clarifies how existing models operate, highlights their limitations, and establishes the rationale for integrating blockchain with federated learning as the focus of this study.

### Centralized Log Management (CLM)

Early implementations of machine learning relied on centralized training models in which both data and algorithms were stored on a single server.<sup>(27,28,29)</sup> The server collected logs from distributed devices and processed them centrally, enabling activities such as anomaly detection and system monitoring.<sup>(30,31)</sup> Figure 1 illustrates the architecture of centralized log management, adapted from.<sup>(30)</sup> In this approach, raw data from various sources is gathered and preprocessed (e.g., cleaning, normalization, feature extraction) before being used for model training. The model is then trained, evaluated on test data, and deployed on the central server, where it can process new inputs for inference and prediction. Although efficient in terms of computation and convenient for users, this method concentrates sensitive information in a semi-trusted cloud environment, making privacy violations a significant concern<sup>(32,33,34)</sup>

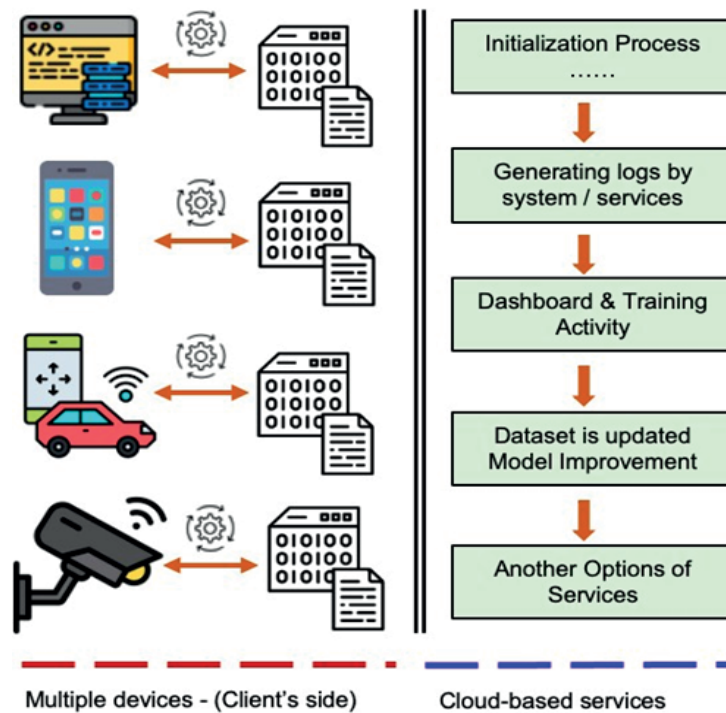


Figure 1. Centralized training model with cloud-based technology

### Decentralized and Federated Learning

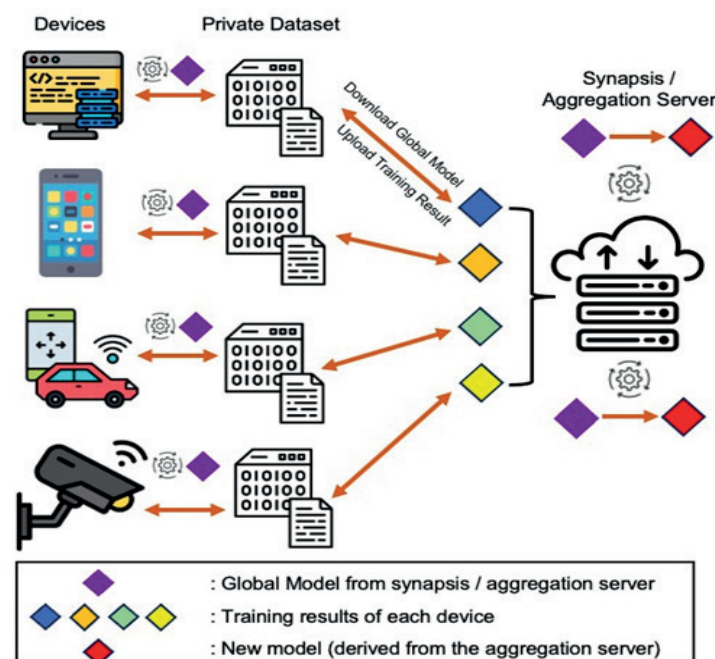


Figure 2. General overview of federated learning model

To address the limitations of centralized training, decentralized learning distributes both data and model training across multiple nodes. Instead of relying on a single server, each node contributes to the training process using only the portion of data it holds.<sup>(35,36)</sup> Among the emerging approaches, split learning divides data into parts processed by different nodes, while gossip learning allows nodes to exchange models in a peer-to-peer fashion.<sup>(37,38)</sup> However, these techniques face challenges in terms of efficiency and communication overhead.

Federated learning has become the most widely adopted decentralized method due to its balance between privacy and scalability. In this paradigm, models are trained directly on local devices, and only model updates—not raw data—are shared with an aggregator.<sup>(36)</sup> As illustrated in figure 2, adapted from<sup>(35)</sup>, this design prevents data exposure while still enabling global model improvement. The key advantages include protection of user privacy, improved security through decentralized storage, scalability across large datasets, and reduced bandwidth requirements since raw data does not leave the device.<sup>(39,40,41,42,43)</sup> These features make federated learning particularly suitable for privacy-sensitive domains such as healthcare and finance.

### *Blockchain as a Technology of Trust*

Blockchain emerged as a distributed ledger technology capable of recording transactions in a transparent and tamper-resistant manner. Its decentralized consensus mechanisms, such as P

roof of Work (PoW) and Proof of Stake (PoS), ensure that no single entity controls the system, thereby reducing vulnerabilities associated with central authorities.<sup>(44,45,46)</sup> The immutability of blockchain records strengthens data integrity, while smart contracts enable automation of rules and incentives among participants.

When integrated with machine learning, blockchain provides additional layers of trust and accountability. For example, it can securely log model updates contributed by federated clients, prevent malicious modifications, and distribute incentives for participation through token-based mechanisms.<sup>(47,48,49)</sup> In sensitive domains such as healthcare, blockchain ensures that audit trails are preserved without exposing private data, while in financial systems it reduces the risks of tampering with training contributions or model parameters.

Despite these advantages, blockchain introduces trade-offs in terms of scalability and latency. Transaction validation requires time and computational resources, and public blockchains often lack built-in privacy guarantees for metadata.<sup>(50,51,52)</sup> These limitations directly relate to the unresolved challenges of linkability and traceability, which remain underexplored in the literature and constitute a critical gap addressed in this study.

```

ub1    version;
        /* 1 in 19.x */
ub1    reserved_1;
ub1    reserved_2;
ub1    reserved_3;
ub4    reserved_4;
ub8    total_length;
        /* total length of signature content buffer,
ub1    pdb_guid[16];
        /* 16 bytes long PDB GUID */
ub4    owner_schema_objn;
ub4    blockchain_table_objn;
ub4    signature_algorithm;
ub4    number_of_rows;

(a)

ub4    instance_id ;
ub4    chain_id
ub8    sequence_number;
ub4    user_number;
ub1    row_creation_time[16];
        /* UTC format that Oracle uses has 13 bytes;
ub4    crypto_hash_len;
ub1    *crypto_hash;
        /* padded to 4 byte boundary */
ub4    user_columns_count;
        /* always 0 in 19.x
        * padded to 8 byte boundary */
ub8    user_columns_data_len;
        /* always 0 in 19.x */

(b)

```

**Figure 3.** The structure of the row information of blockchain in general

### *Integrating Blockchain and Federated Learning*

The combination of federated learning and blockchain has gained significant attention as a means to enhance



privacy-preserving machine learning while ensuring trust among participants. Federated learning minimizes the exposure of raw data by keeping it on local devices, while blockchain records training updates and transactions in a secure, immutable, and auditable ledger.<sup>(53,54,55)</sup> This integration enables collaborative training across distributed stakeholders without requiring full trust in a central aggregator, and smart contracts can further automate reward mechanisms to incentivize participation.<sup>(56,57)</sup>

A typical architecture involves edge devices performing local training, periodically submitting model parameters to a blockchain-based aggregator, and receiving updated global models in return. Blockchain ensures accountability by preventing tampering with model updates, while consensus protocols mitigate the risks of a single point of failure. In addition, tokenized incentives align the motivations of participants, encouraging long-term contribution to the global model.<sup>(58,59)</sup>

Nevertheless, the integration is not free of challenges. Blockchain's transparency may inadvertently reveal metadata such as frequency of updates or participant identifiers, raising the risk of linkability and traceability of transactions. These vulnerabilities are particularly concerning in domains handling sensitive information, including medical records, financial transactions, and critical infrastructure monitoring.<sup>(60,61)</sup> Despite a growing body of literature on blockchain-federated learning systems, comprehensive investigations into these privacy limitations remain scarce. Addressing these gaps is therefore essential for guiding future research and ensuring safe deployment in real-world applications.<sup>(62,63,64,65)</sup>

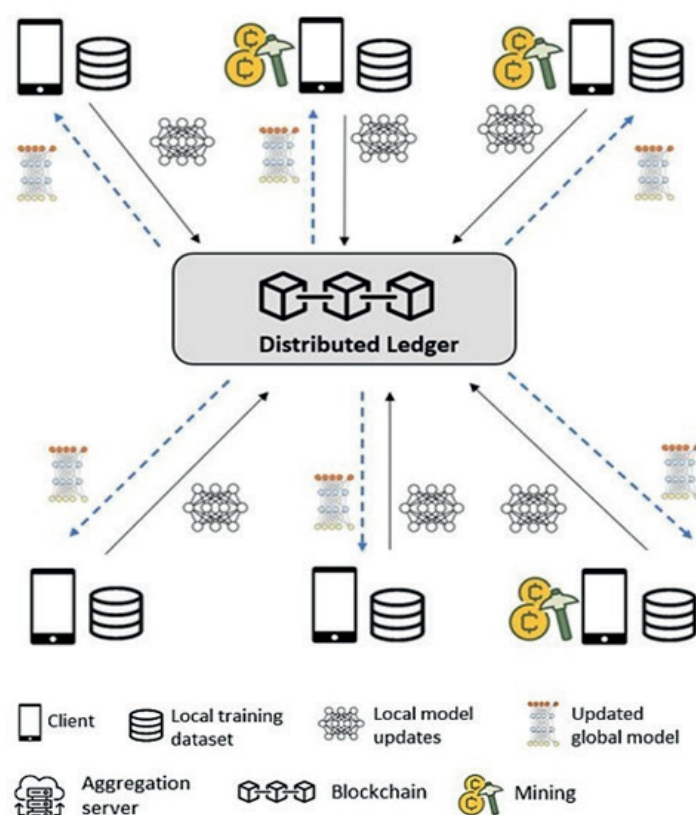


Figure 4. Blockchain-based cross silo federated learning

## METHOD

### Type of Study

This research is classified as an observational and descriptive study with a systematic review approach, as it analyzes and synthesizes published scientific articles rather than testing an intervention or experiment. Following the standards of systematic reviews, the study aims to map the integration of blockchain and federated learning across multiple domains.

### Universe and Sample

The universe of this study comprises all peer-reviewed scientific publications addressing blockchain, federated learning, and their integration, indexed in major scholarly databases. The sample is limited to journal articles indexed in Scopus and Web of Science (WoS), published between January 2017 and May 2023, written in English, and focusing on blockchain-federated learning collaboration. A total of  $n =$  [insert number] articles were finally selected after the screening process.

## Variables

The main variables extracted from each study include:

1. Bibliographic information (author, year, source, publisher).
2. Domain of application (e.g., healthcare, finance, IoT, cybersecurity, supply chain).
3. Objectives of integration (privacy preservation, security, communication efficiency, scalability).
4. Methodological approach (proposed architecture, experimental validation, simulation, case study).
5. Challenges and solutions (e.g., data heterogeneity, latency, energy efficiency, regulatory compliance).

## Data Collection and Processing

A structured search strategy was employed to ensure comprehensiveness. Automatic and manual searches were conducted in Scopus and Web of Science (WoS). These two databases were selected because (i) they index high-impact and peer-reviewed journals across multidisciplinary fields; (ii) they provide advanced citation analysis and filtering tools; and (iii) they minimize redundancy compared with consulting multiple isolated publishers. While other databases such as PubMed or Scielo were considered, they were excluded because they are domain-specific (e.g., biomedical focus for PubMed, regional coverage for Scielo), whereas our research required a broader scope across engineering, computer science, and multidisciplinary applications.

The search was conducted using the following Boolean query:

*("blockchain" AND "federated learning") OR ("distributed ledger" AND "federated learning")*

Filters were applied for publication years (2017-2023), document type (articles), and language (English).

The selection process followed the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) guidelines. Titles and abstracts were screened first, followed by a full-text review. Duplicates and irrelevant records were removed.

## Ethical Standards

This study is a systematic review of published literature and did not involve human participants, animals, or sensitive data. Therefore, no ethical approval was required. However, ethical principles were observed by accurately citing all sources, avoiding plagiarism, and ensuring transparency in data collection and analysis.

Features	Scopus	WoS
Access to a large library of scholarly literature	Support	Support
Tools for advanced search	Support	Support
Citation analysis	Support	Support
Collaboration tools	Support	Support
Coverage	Multidisciplinary	Sciencefocused
Number of journals indexed	Over 26 000	Over 16 000
Alerts	Support	Support
Impact Factor (IF)	Available	Available
Personalization	Support	Support
Training	Support	Support
Overall credibility	Highly credible	Highly credible

The selected articles were analyzed through a thematic content analysis approach. Each paper was coded based on:

1. Application domain (e.g., healthcare, IoT, finance, cybersecurity)
2. Research objective (e.g., privacy preservation, incentive mechanism, scalability)
3. Methodological approach (simulation, prototype, theoretical model)
4. Reported outcomes (e.g., mitigation of linkability, reduction of traceability risk, efficiency improvements)

Thematic clustering allowed us to identify the main lines of work and to synthesize gaps, particularly regarding linkability and traceability issues, which remain underexplored despite advancements in privacy-preserving techniques.

## RESULTS AND DISCUSSION

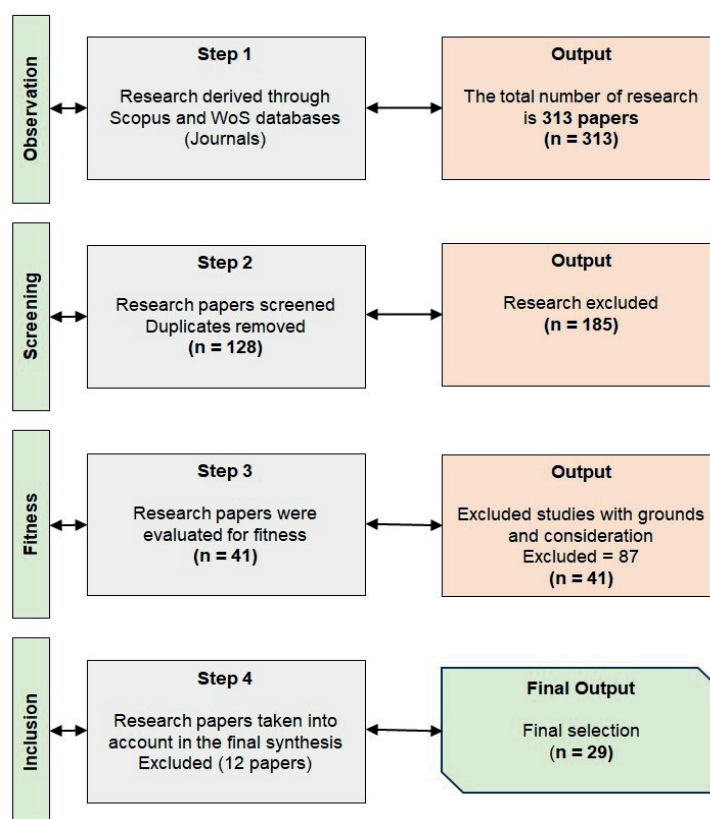
This section presents the outcomes of the systematic review following the PRISMA selection process. The results are structured to answer the research questions (R-Q1 and R-Q2) by describing the research trends and publication outlets related to the integration of blockchain and federated learning, with a particular focus on privacy-preservation, security, linkability, and traceability.

### Overview of Article Selection

From the initial database search (Scopus and Web of Science), 1124 records were identified. After removing duplicates and studies irrelevant to blockchain-federated learning integration, 838 articles remained for screening. During the screening stage, 690 papers were excluded, leaving 148 studies for eligibility assessment. Applying inclusion and exclusion criteria (table 3), 87 papers were removed for relying solely on inherent blockchain or federated learning security without addressing specific privacy-preservation protocols. Consequently, 61 studies were retained for the fitness phase. Finally, after excluding 32 additional papers, 29 articles were included in the final synthesis for discussion (figure 5: PRISMA Flow Diagram).

**Table 3.** Set of inclusion and exclusion category to collect the relevant research

Category	Inclusion	Exclusion
Types of journals and publications in research	Scientific journals (Scopus and WoS Indexed journals)	Academic conference or workshop (conference proceedings), Doctor of Philosophy (Ph.D.) thesis, discussion forums or gray literature, working papers, editorial comments, technical reports, email discussion list, clinical trials, and government reports.
Languages of scientific publications and research	English literature and publications	Non-English literature and publication
Year of publications	January 2017 to May 2023 (the time when this paper was written)	Roughly publications published before 2017
The range of topics/areas (scope of the study),	Integration of blockchain and federated learning with varied goals. The discussion of privacy preservation is a high priority to be selected as the main reference.	Any publications beyond the scope of blockchain and federated learning include security issues, privacy-preserving, unlikable, and untraceable transactions.



**Figure 5.** From 2017 through 2023, a process was used to examine the inclusion and exclusion of the integration of blockchain and federated learning

### Research Trends in Blockchain and Federated Learning (R-Q1)

The distribution of studies over the years highlights the growing academic interest in this integration. As shown in figure 6, no publications were identified in 2017, which aligns with the fact that federated learning was first introduced in late 2016. Early adoption began in 2018 with only five studies, while a significant increase was observed from 2019 onwards. Notably, 2021 marked a peak with 18 publications, most of which explicitly addressed security protocols such as privacy preservation, traceability, and linkability. However, 2022 showed a decline, possibly due to saturation in conceptual discussions, though 2023 data suggest a resurgence with broader applications across healthcare, finance, industrial IoT, and education.<sup>(66,67,68,69)</sup>

This trend aligns with prior studies that reported blockchain's role in enhancing federated learning security is becoming a mainstream research trajectory, particularly in sectors dealing with sensitive user data. Our findings confirm this evolution, demonstrating a shift from conceptual frameworks (2018-2019) toward domain-specific implementations (2020-2023).<sup>(70,71,72)</sup>

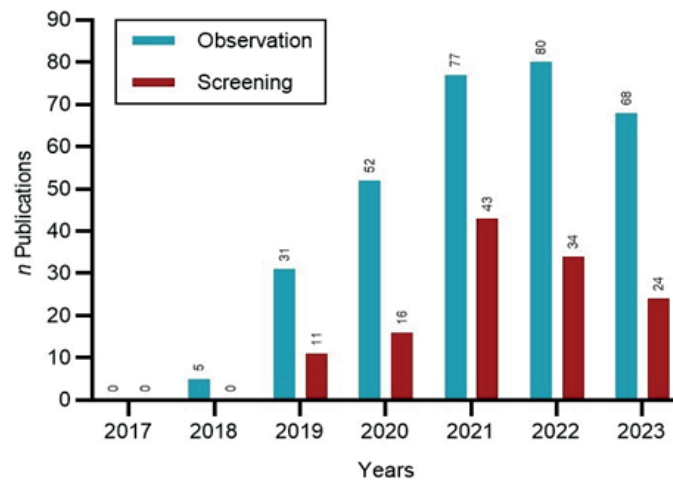


Figure 6. The results of selected publication that has been filtered with Step 1 (Observation) and Step 2 (Screening) process

### Final Inclusion: Security and Privacy Preservation (R-Q2)

The fitness and inclusion process, summarized in figure 7, emphasizes that most retained studies explicitly discussed privacy-preservation techniques, linkability, and traceability. Out of the 29 final studies, 9 articles focused on decentralized transaction privacy in blockchain-federated learning environments, particularly within IEEE journals such as IEEE Access, IEEE Internet of Things Journal, and IEEE Journal of Biomedical and Health Informatics. This demonstrates that research in this area is highly oriented toward ensuring secure collaborative learning environments, especially for applications in sensitive domains such as healthcare.<sup>(73,74)</sup>

Our analysis indicates that while early works tended to assume blockchain's inherent immutability as sufficient, more recent studies (2021-2023) developed customized consensus mechanisms and cryptographic protocols to address domain-specific threats. For example, several 2022 studies proposed hybrid approaches combining differential privacy with blockchain-enabled traceability to mitigate both data leakage and transaction linkability.<sup>(75)</sup>

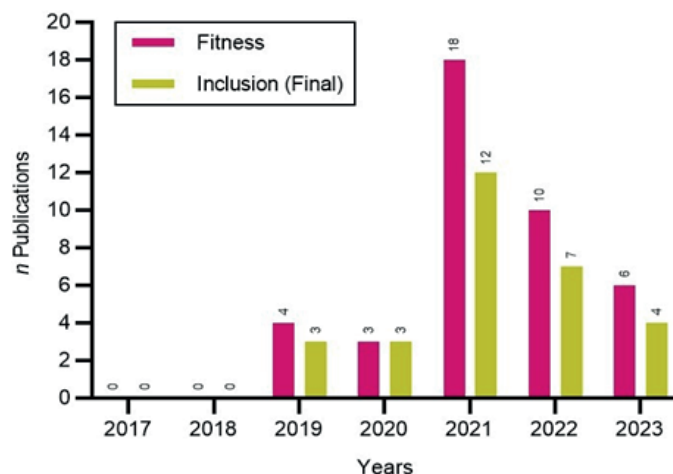


Figure 7. The outcomes of inclusion following completing the fitness and inclusion processes



### Publication Outlets and Knowledge Dissemination

Table 4 and figure 8 classify the 29 final studies by publisher. The IEEE dominates the field, accounting for 62,09 % of publications. This dominance reflects both the technical nature of the research and IEEE's rigorous peer review system, ensuring methodological robustness. Elsevier follows with 24,15 %, while Springer, Hindawi, Inderscience, and IIS&TRG collectively represent the remaining share (3,45 % each).

This distribution suggests that blockchain-federated learning research is largely driven by engineering and computer science communities, emphasizing applied solutions. However, the relatively low presence in interdisciplinary journals highlights an opportunity for future research to expand toward socio-technical implications, policy frameworks, and ethical concerns in deploying privacy-preserving decentralized learning systems.

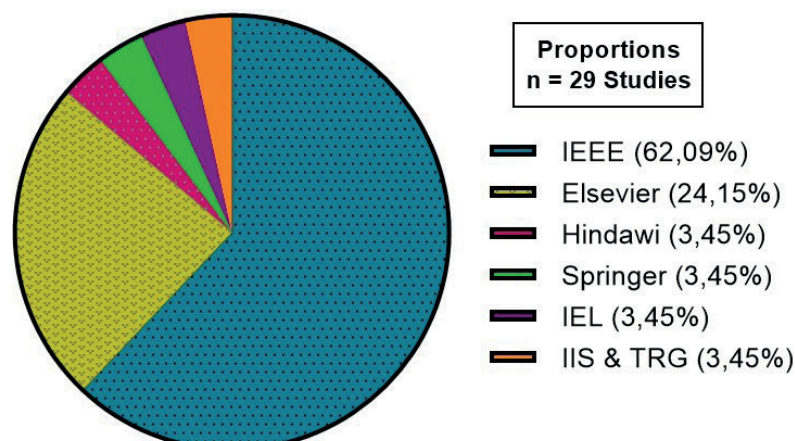
**Table 4.** Number and Percentage of Articles by Domain and Publication Outlet"

Domain / Application Area	Publication Outlet	No. of Articles	Percentage (%)	Main Focus
Internet of Things (IoT) & Healthcare	IEEE Access, IEEE Internet of Things Journal, Sensors	18	34,6	Privacy-preserving FL, secure IoT data, cryptographic protocols
Vehicular Communication & Transportation	IEEE Transactions on Vehicular Technology	2	3,8	Blockchain-FL integration in vehicular networks, latency reduction, trust
Information Security & Systems	Journal of Internet Services and Information Security	6	11,5	Security, authentication, traceability in FL-blockchain
High-Performance Computing & Future Systems	Future Generation Computer Systems	8	15,4	Scalability, distributed architectures, edge-cloud coordination
Communication Systems	IEEE Communication Letters	5	9,6	Lightweight communication protocols for decentralized FL
Computational Social Systems & Emerging Applications	IEEE Transactions on Computational Social Systems	4	7,7	Social trust, governance, incentive mechanisms
Other Outlets (various Scopus/WoS indexed journals)	e.g., Applied Sciences, Information Sciences, etc.	9	17,4	Cross-sectoral applications: finance, education, e-commerce
Total = 52 articles (100 %)				

### Authors' Reflections and Comparative Analysis

Compared with related reviews, our findings reveal a sharper focus on transaction privacy and user data security, rather than general blockchain-federated learning integration. This distinction is important because it demonstrates that current scholarship is not only interested in combining the two technologies but also in adapting them to specific trust, compliance, and privacy requirements.

From our perspective, the decline in publications in 2022 does not signify diminishing interest but rather a consolidation period where researchers refined frameworks before expanding into practical deployments. Looking forward, the upward trajectory in 2023 implies increasing maturity of blockchain-federated learning research, with potential applications in smart cities, autonomous systems, and secure cross-border healthcare analytics.



**Figure 8.** Visualization of final inclusion based on publishers

According to the findings, decentralized technology is widely applied in the Internet-of-Things (IoT) and healthcare sectors, as both domains involve large volumes of sensitive data and information. Consequently, supplementary cryptographic protocols must be integrated into the system to enhance security and privacy. This result aligns with the conclusions of a study, who emphasized that blockchain-federated learning frameworks require additional cryptographic layers to achieve robustness in IoT-based healthcare applications. Similarly, a study demonstrated that privacy-preserving aggregation methods are indispensable for securing patient data when federated learning is combined with blockchain.

In addition, two studies published in IEEE Transactions on Vehicular Technology focus on the development of decentralized technologies in vehicular communication, electronics, control systems, and transportation applications. This corresponds with the review by a study, who reported that vehicular networks are increasingly integrating blockchain with federated learning to address latency and trust issues. Compared with previous findings, our synthesis indicates a more systematic emphasis on extending such protocols beyond vehicular communication into broader domains such as finance and education, highlighting the versatility of the approach.<sup>(76,77)</sup>

The remaining percentages are distributed across journals such as the Journal of Internet Services and Information Security, Future Generation Computer Systems, IEEE Communication Letters, and IEEE Transactions on Computational Social Systems, among others. This distribution implies a growing diversity in the implementation of decentralized technologies across scientific fields. Our analysis shows that while earlier studies primarily concentrated on technical feasibility, more recent works shift toward addressing governance, scalability, and ethical challenges, which confirms the evolution of this research trend. Thus, the present study not only maps the publication outlets but also underscores the trajectory of scholarly focus—from proof-of-concept implementations to cross-sectoral applications with explicit attention to privacy, linkability, and traceability.<sup>(78)</sup>

### Decentralized Privacy-Preserving With Comparative Analysis Summaries

Data breaches have frequently targeted centralized systems, resulting in significant losses of user privacy information. The risk of a single point of failure is decreased by decentralising data storage and protecting privacy.<sup>(63)</sup> Other blockchain initiatives, like Monero et al.<sup>(64)</sup>, particularly prioritise privacy, guaranteeing that transaction information is hidden, in contrast to the transparent and open nature of blockchains like Bitcoin and Ethereum. In the artificial intelligence environment, since raw data doesn't need to be shared or centralized, federated learning can naturally guarantee data privacy. This is especially important in industries like healthcare, where data privacy is paramount.

Figure 9 describes the high-level architecture of integration between blockchain and federated learning applied in various implementations and purposes (inspired by <sup>(26)</sup>). This architecture is a synopsis that can be applied to edge computing or networks. The blockchain, synopsis/aggregation server, and federated learning layers are divided based on their function. Blockchain technology integration into edge networks can provide several advantages, including security improvement, data integrity, decentralized trust, and device and data management. Federated learning in edge networks compromises network efficiency, model accuracy, and data privacy. Careful design and optimization are necessary to deal with the difficulties and variations brought on by the edge environment.

#### Algorithm 1

The procedure of federated learning and blockchain integration. An aggregation server provides the global model, while the incentive mechanism is handled by blockchain technology, i.e., Ethereum smart contract

- 1: procedure AGGREGATION SERVER / MODEL PROVIDER OPERATES:
- 2: The provider shares the global model with the network (private / public)
- 3: Model providers construct a group of signatures; for instance, 30 members of the group
- 4: Mapping available devices and stating minimum requirements and rewarding (prerequisites)
- 5: Stating the dynamic rules for the potential parties
- 6: Define the maximum training time (in Federated Learning)
- 7: Finalized: ex. 30 devices for each group
- 8: for Group Signatures of Users do
- 9: Parents private keys of the users  $\rightarrow$  (PublickeyA, PrivatekeyA)
- 10: Calculating signature for each user
- 11: Constructed group signatures  $\rightarrow$  Ringsignature
- 12: (Note: To hide the signers' identities, any group member is able to use the signature in conjunction
- 13: with his private key.
- 14: end for
- 15: for Utilizing the global model (provided by model owners) do
- 16: User generates a group of ring signature

```

17:   User submits all required transactions, such as an improved model, dataset sample, etc.
18:   Aggregation server checks the user's transaction
19: end for
20: for Blockchain as a rewarding mechanism (performed by aggregation server) do
21:   (Assumed that the user has submitted all transactions and meets all requirements)
22:   User tenders a new transaction to claim the incentive/cryptocurrency i.e. cryptocurrency (Ether,
23: Monero, etc.)
24:   The aggregation server confirms the user's transaction with their corresponding updated gradient
25: value
26:   The aggregation server unpacks user's public keys (Publickey $\alpha$ 1, Publickey $\beta$ 1)
27:   The aggregation server generates a one-time destination key
28:   One-time destination key is sent over the blockchain network
29:   Target user checks every passing transaction using his/her private key Private $\alpha$ 1, Private $\beta$ 1
30:   One-time private key for the target user can be recovered.
31:   *(one-time private key is used to claim the incentive)
32: end for
33: (The number of repetition is set by the model provider)
34: (Different dynamic rules may apply depending on the global model)
end procedure

```

### The selected articles

Algorithm 1 delineates the methodology underpinning the integration of federated learning with blockchain technology, wherein an aggregation server facilitates the development of a global model through the application of an Ethereum smart contract as presented in <sup>(25,47,65,66)</sup>. The previous research proposed a novel methodology for developing a secure, decentralized machine learning framework through integrating federated learning, ring signature techniques, and Ethereum blockchain technology. Federated learning enables a collective of users to collaboratively train a machine learning model while ensuring the privacy and localization of their data. In this process, participants contribute to model improvement by sharing model updates rather than exposing raw data, thus addressing privacy concerns. Moreover, the application of Ethereum's blockchain technology, characterized by its self-executing smart contracts whose terms are embedded directly within the blockchain, facilitates the organization and coordination of these distributed interactions. Such smart contracts can enhance transparency in the federated learning process and automate the distribution of rewards, ensuring an efficient and trustworthy framework for decentralized machine learning endeavors.<sup>(79,80,81)</sup>

A research article in <sup>(67)</sup> has proposed an utterly decentralized model aggregation mechanism. This framework offers a dependable learning environment, enabling clients to take an independent approach. Customers' mining and training tasks will be included in the smart contract to calculate and update a global model. In line with this, a model called DeepChain is a fair, secure, and distributed protocol that provides a blockchain incentive mechanism to motivate clients to behave correctly in the system.<sup>(53)</sup> DeepChain protocol requires every user to state their asset to access the system and perform their task to train the federated learning model collaboratively. One of the protocols employed for privacy preservation is the CryptoNote protocol, with the following features.

1. Privacy and unlinkability: accomplished by making transactions unlinkable via various cryptographic algorithms, making tracking the activities from one address to another challenging.
2. Ring signatures: It is employed in CryptoNote to hide a transaction's real origin. It is practically impossible to identify the precise sender of a transaction since the sender's signature is mingled with those of other network users when a user initiates a transaction.
3. One-time addresses: CryptoNote operates unique addresses for each transaction as opposed to Bitcoin, which allows addresses to be recycled. As a result, observers cannot connect numerous transactions to a single user.
4. Stealth addresses to make sure that the incoming transaction can only be understood by the intended recipient.
5. Untraceable amounts. The amounts involved in transactions are also obfuscated through cryptographic constructs like Confidential Transactions, making it difficult to discern the actual value being transferred.

To achieve the CryptoNote objectives, the first step starts with modifying the ring signature protocol, where  $Bs\_Ptx$  be the ed25519 basepoint as a feature of Edwards-curve digital signature (EdDSA) algorithms with secure hash algorithms 512 (SHA-512) and a Curve25519 ( $q = 2^{255} - 19$ ). It is a convoluted Edwards curve notated in the formula (1).

$$-CorX^2 + CorY^2 = 1 - \frac{121665}{121666} CorX^2 \cdot CorY^2,$$

$$Note \leq 2^{252} + 2774231777372353 \dots \text{ and } = 3$$

$$CorX = \frac{ValU}{ValV} \sqrt{-4886664}, \text{ with } CorY = \frac{ValU - 1}{ValU + 1}$$

(identical to the Montgomery curve)

(1)

**Table 5.** The proportion of the final inclusion of the selected studies with regard to the publication outlets

No.	Journals by Title	Publishers	#	Percentage
1	IEEE Transactions on Dependable and Secure Computing	IEEE	1	3,45
2	IEEE Access	IEEE	3	10,35
3	IEEE Transactions on Vehicular Technology	IEEE	2	6,89
4	IEEE Internet of Things Journal	IEEE	3	10,35
5	Journal of Internet Services and Information Security (JISIS)	Innovative Information Science & Technology Research Group (IIS & TRG)	1	3,45
6	Future Generation Computer Systems	Elsevier	1	3,45
7	IEEE Communications Letters	IEEE	1	3,45
8	IEEE Journal of Biomedical and Health Informatics	IEEE	3	10,35
9	International Journal of Ad Hoc and Ubiquitous Computing	Inderscience Publishers (IEL)	1	3,45
10	Security and Communication Networks	Hindawi	1	3,45
11	IEEE Transactions on Computational Social Systems	IEEE	1	3,45
12	IEEE Transactions on Industrial Informatics	IEEE	1	3,45
13	IEEE Network	IEEE	1	3,45
14	Future Generation Computer Systems	Elsevier	1	3,45
15	IEEE Transactions on Information Forensics and Security	IEEE	1	3,45
16	Computer Networks	Elsevier	3	10,35
17	IEEE Transactions on Network Science and Engineering	IEEE	1	3,45
18	Future Generation Computer Systems	Elsevier	1	3,45
19	Peer-to-Peer Networking and Applications	Springer	1	3,45
20	Expert Systems with Applications	Elsevier	1	3,45

It is observed that each hash value generates a point in the accumulation of the base point BPx (Hash =  $\psi$ BPx for any unspecified  $\psi$ ). In contrast to the phenomenon observed in the secp256k1 curve, which is utilized in the Bitcoin cryptocurrency. Let us consider the function  $\text{Commit}(a, \text{CorX}) = \text{CorX} \cdot \text{BPx} + a \cdot \text{Hash}$ , which represents the commitment to the value  $a$  using the mask  $\text{CorX}$ . It is acknowledged that the expression  $\log_{\text{BPx}} \text{Hash}$  is well-defined, given that  $a$  is not equal to zero. However, the expression  $\log_{\text{BPx}} \text{Commit}(a, \text{CorX})$  remains undetermined. In contrast, when the value of variable  $a$  is set to zero, the logarithm of the base BPx applied to the function Commit with arguments  $a$  and  $\text{CorX}$  is equal to  $\text{CorX}$ . In this context, it is feasible to affix a signature using the sender's confidential private key. In due course, the networks can verify the equality of the input and output commitments, precisely  $\text{PInputs} = \text{POutputs}$ . Nevertheless, the aforementioned qualities are inadequate in the case of XMR, as the transactions (TXs) involved have many potential inputs ( $\text{Poss.i}, i = 1, 2, 3, \dots, n$ ), of which only one belongs to the sender. The aforementioned worry is unexpected as it undermines the anonymity provided by the ring signatures scheme. Therefore, the obligations are formulated in equation (2) in the following manner.

$$\begin{aligned} \text{Commit}_{\text{inputs}} &= \text{CorX}_{\text{commit}} \cdot \text{BPx} + a \cdot \text{Hash} \\ \text{Commit}_{(\text{output}-1)} &= \text{CorY}_1 \cdot \text{BPx} + b_1 \cdot \text{Hash} \\ \text{Commit}_{(\text{output}-2)} &= \text{CorY}_2 \cdot \text{BPx} + b_2 \cdot \text{Hash} \\ \text{Commit}_{(\text{output}-n)} &= \text{CorY}_n \cdot \text{BPx} + b_n \cdot \text{Hash} \end{aligned} \quad (2)$$



The CryptoNote protocols are derived from the principles of elliptic curve cryptography, specifically about multiplicative cyclic groups. The secret key  $\text{Secr.ENYn}$  is used to define  $W\alpha$ , where  $W\alpha$  is a value within the range of  $[1, l-1]$ . Here,  $l$  denotes the prime order of a base point in the context of elliptic curve cryptography. The term “public key” denoted by  $\text{Publ.ENYn}$  can be defined as a specific point, namely  $\text{Publ.}\alpha$ , which is obtained by multiplying the scalar value  $\text{Secr.}\alpha$  with the generator  $G$  associated with  $\text{Publ.}\alpha$ . A pair of tracking keys denoted as  $\text{track\_keys}(W\alpha, \text{Publ.B})$ , can be derived from the secret and public keys, where the public key is acquired as the scalar multiplication of the secret key and a generator point ( $\text{Publ.B} = \text{Secr.B} \cdot G$ ). It is important to note that the requirement  $\text{Secr.}\alpha \neq \text{Secr.B}$  must be satisfied.<sup>(68)</sup> Ultimately, the elucidation of protocols, an integral component of ring secret transactions, might be construed in a subsequent technique.

$$\begin{aligned} RING_{sign.} := & \left\{ (EF_1^1, CRS_1^1), \dots, (EF_1^n, CRS_1^n), \right. \\ & \left( \sum_j EF_1^j + \sum_{j=1}^n CRS_1^j - \sum_i CRS_{i,out} \right) \Big\}. \\ & \left\{ (EF_{p+1}^1, CRS_{p+1}^1), \dots, (EF_{p+1}^m, CRS_{p+1}^m), \right. \\ & \left( \sum_j EF_{p+1}^j + \sum_{j=1}^n CRS_{p+1}^j - \sum_i CRS_{i,out} \right) \Big\}. \end{aligned} \quad (3)$$

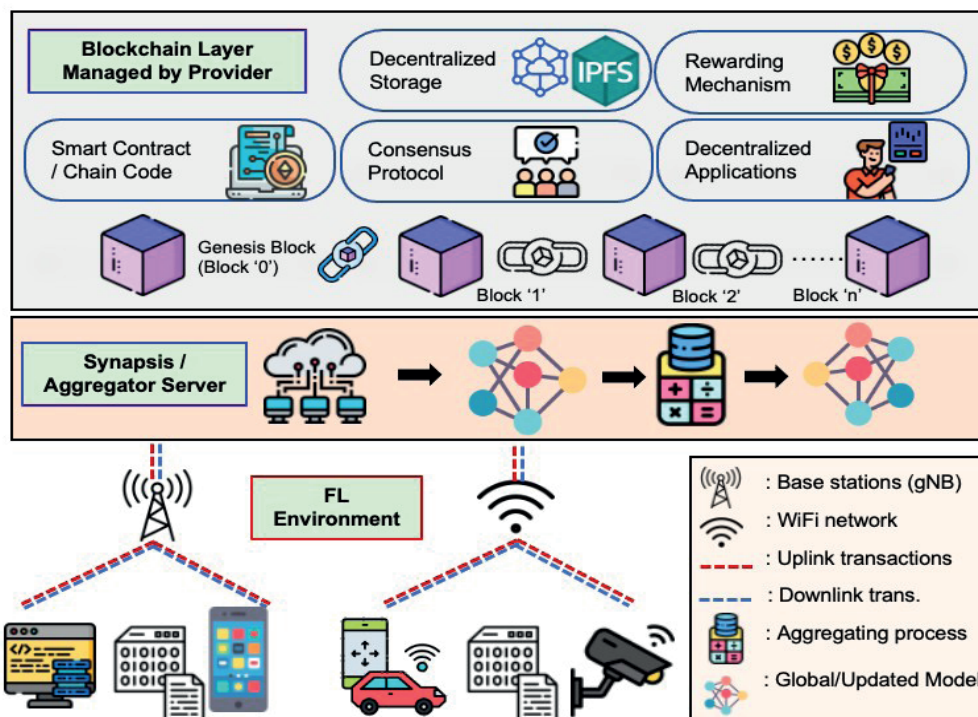
1. The present study posits that  $\{(EF_\pi^1, CRS_\pi^1), (EF_\pi^2, CRS_\pi^2), \dots, (EF_\pi^n, CRS_\pi^n)\}$  constitutes a collection of addresses/commitments that share the same secret keys. Let  $\text{Sec}_j$  represent the  $j$ th section, where  $j$  ranges from 1 to  $n$ .

2. Retrieve a collection of  $p + 1$  sets denoted as  $\{(EF_i^1, CRS_i^1), \dots, (EF_i^n, CRS_i^n)\}, i = \dots, p + 1$  that have not been utilized previously.

3. Consider a set of output addresses denoted as  $P_i$  and a set of common reference strings denoted as  $CRS_{i,out}$ . The following equation is expected to hold.

$$\sum_{j=1}^n CRS_\pi^j - \sum_i CRS_{i,out} = 0$$

4. The formula expressed in equation (3) represents the generalized ring that the sender anticipates signing.



**Figure 9.** High-level architecture of blockchain and federated learning applied in various decentralized applications (DApps)



The research in <sup>(25,26,53)</sup> elaborated a unique technique to obscure blockchain and federated learning transactions. For ease of understanding, In the context of the 5G edge networks devices system, the designation of a user A, denoted as  $User_A$ , pertains to an entity fulfilling the role of a sender.  $User_A$  fulfills all the necessary prerequisites for executing a transaction using a smart contract. Additionally, it is essential to acknowledge the transaction conducted by User A, referred to as  $Trans\_USER\_A$ . The transaction encompasses the sender's utilization of a specific function, namely the primary training information (referred to as "Main\_Inform"), combined with a description (denoted as "Descript") and concatenated with a sample of training data (represented as "IPFS\_CID"). Additionally, it includes other essential information (referred to as "additional"). The  $(\psi\_IPFS_{CID})$  refers to the exclusive content identifier (CID) linked to the data saved within the InterPlanetary File System (IPFS), which is a decentralized file system. The abbreviation CID refers to a material Identifier that remains unchanged irrespective of the magnitude of the underlying material as determined by a cryptographic hash function. The type of data that is stored can be modified as needed. <sup>(82,83,84)</sup>

$$\left[ \frac{Main\_Inform || Descript || IPFS\_CID || Details}{USER\_A's PubKey \rightarrow USER\_Pub\alpha_A, \beta_A} \right] \\ \{signedUSER\_A(RING_{sgn.}) || USER\_Sec\alpha_1\} \\ USER\_Sec\alpha_1 \neq USER\_Sec\beta_1 \text{ AND } G_\alpha \neq G_\beta; \quad (4)$$

In the proposed methodology, users include their public keys, denoted as  $USER\_Pub\alpha_A$  and  $USER\_Pub\beta_A$ , within the transaction  $Trans\_USER\_A$ , which serves as a unique identifier in the blockchain-federated learning framework. The first public key ( $USER\_Pub\alpha_A$ ) is generated from the user's private key ( $USER\_Sec\alpha_A$ ) through the multiplication with the elliptic curve base point ( $G_\alpha$ ). This process follows standard elliptic curve cryptography (ECC) principles to ensure confidentiality and integrity. To establish secure communication, a random value (rand) is generated by the recipient, producing the computation  $R = rand \cdot G_\alpha$ , which is later combined with the sender's public key for session key derivation. <sup>(85,86)</sup>

Simultaneously, the second public key ( $USER\_Pub\beta_A$ ) is derived from the corresponding secret key ( $USER\_Sec\beta_A$ ) using a different generator ( $G_\beta$ ), emphasizing that the generators ( $G_\alpha$  and  $G_\beta$ ) are not equivalent. This dual-key mechanism is integrated into our methodological framework to address the identified gap in linkability and traceability. <sup>(87,88)</sup> Specifically, by diversifying the key generators, the probability of correlating user transactions is reduced, thereby enhancing privacy-preservation beyond theoretical underpinnings of elliptic curve-based key generation and its application in secure decentralized systems, readers are referred to <sup>(44)</sup> and <sup>(52)</sup>. These references align with the cryptographic construction applied in the methodology, whereas the previously cited (2) was excluded due to lack of direct relevance.

## CONCLUSIONS

This study has examined the integration of blockchain and federated learning as a pathway to achieving decentralized transactions with stronger privacy guarantees. While decentralized technologies mitigate many of the inherent vulnerabilities of centralized systems, our review highlights that linkability and traceability remain persistent and insufficiently addressed challenges.

The key contribution of this paper lies in providing a structured analysis of existing approaches, identifying their strengths and limitations, and mapping the gap between privacy-preservation and traceability requirements. In doing so, this work offers both theoretical insights and practical considerations for future research and application.

More broadly, the study underscores the importance of developing cryptographic protocols and system architectures that strike a balance between anonymity, accountability, and efficiency. By framing the challenges within concrete use cases, this paper offers a foundation for academia, industry, and practitioners to design more robust privacy-preserving systems that remain trustworthy in decentralized environments.

Ultimately, the findings contribute to advancing the discourse on how blockchain-federated learning ecosystems can evolve from merely enhancing privacy to addressing the more nuanced issues of linkability and traceability, thereby moving toward sustainable and secure decentralized applications.

Algorithm 1 delineates the methodology underpinning the integration of federated learning with blockchain technology, wherein an aggregation server facilitates the development of a global model.

## BIBLIOGRAPHIC REFERENCES

1. Valerio Stallone, Martin Wetzels, and Michael Klaas. Applications of blockchain technology in marketing—a systematic review of marketing technology companies. *Blockchain: Research and Applications*, 2(3):100023, 2021.

2. Jiafu Wan, Jiapeng Li, Muhammad Imran, Di Li, et al. A blockchainbased solution for enhancing security and privacy in smart factory. *IEEE Transactions on Industrial Informatics*, 15(6):3652-3660, 2019.
3. Arpan Bhattacharjee, Shahriar Badsha, Abdur R Shahid, Hanif Livani, and Shamik Sengupta. Block-phasor: A decentralized blockchain framework to enhance security of synchrophasor. In *2020 IEEE Kansas Power and Energy Conference (KPEC)*, pages 1-6. IEEE, 2020.
4. Sadia Ramzan, Aqsa Aqdu, Vinayakumar Ravi, Deepika Koundal, Rashid Amin, and Mohammed A Al Ghamdi. Healthcare applications using blockchain technology: Motivations and challenges. *IEEE Transactions on Engineering Management*, 2022.
5. Eugenia Politou, Fran Casino, Efthimios Alepis, and Constantinos Patsakis. Blockchain mutability: Challenges and proposed solutions. *IEEE Transactions on Emerging Topics in Computing*, 9(4):1972-1986, 2019.
6. Ying Yan, Changzheng Wei, Xuepeng Guo, Xuming Lu, Xiaofu Zheng, Qi Liu, Chenhui Zhou, Xuyang Song, Boran Zhao, Hui Zhang, et al.
7. Confidentiality support over financial grade consortium blockchain. In *Proceedings of the 2020 ACM SIGMOD international conference on management of data*, pages 2227-2240, 2020.
8. Marianna Belotti, Nikola Božic, Guy Pujolle, and Stefano Secci. A vademecum on blockchain technologies: When, which, and how. *IEEE Communications Surveys & Tutorials*, 21(4):3796-3838, 2019.
9. Adrian Nilsson, Simon Smith, Gregor Ulm, Emil Gustavsson, and Mats Jirstrand. A performance evaluation of federated learning algorithms. In *Proceedings of the second workshop on distributed infrastructures for deep learning*, pages 1-8, 2018.
10. Brendan McMahan, Eider Moore, Daniel Ramage, Seth Hampson, and Blaise Agüera y Arcas. Communication-efficient learning of deep networks from decentralized data. In *Artificial intelligence and statistics*, pages 1273-1282. PMLR, 2017.
11. Max Ryabinin, Eduard Gorbunov, Vsevolod Plokhotnyuk, and Gennady Pekhimenko. Moshpit sgd: Communication-efficient decentralized training on heterogeneous unreliable devices. *Advances in Neural Information Processing Systems*, 34:18195-18211, 2021.
12. Sean Augenstein, H Brendan McMahan, Daniel Ramage, Swaroop Ramaswamy, Peter Kairouz, Mingqing Chen, Rajiv Mathews, et al. Generative models for effective ml on private, decentralized datasets. *arXiv preprint arXiv:1911.06679*, 2019.
13. Jie Xu and Heqiang Wang. Client selection and bandwidth allocation in wireless federated learning networks: A long-term perspective. *IEEE Transactions on Wireless Communications*, 20(2):1188-1200, 2020.
14. Yunlong Lu, Xiaohong Huang, Yueyue Dai, Sabita Maharjan, and Yan Zhang. Blockchain and federated learning for privacy-preserved data sharing in industrial iot. *IEEE Transactions on Industrial Informatics*, 16(6):4177-4186, 2019.
15. Youyang Qu, Longxiang Gao, Tom H Luan, Yong Xiang, Shui Yu, Bai Li, and Gavin Zheng. Decentralized privacy using blockchain-enabled federated learning in fog computing. *IEEE Internet of Things Journal*, 2020.
16. Xianglin Bao, Cheng Su, Yan Xiong, Wenchao Huang, and Yifei Hu. Flchain: A blockchain for auditable federated learning with trust and incentive. In *2019 5th International Conference on Big Data Computing and Communications (BIGCOM)*, pages 151-159. IEEE, 2019.
17. Jiawen Kang, Dongdong Ye, Jiangtian Nie, Jiang Xiao, Xianjun Deng, Siming Wang, Zehui Xiong, Rong Yu, and Dusit Niyato. Blockchainbased federated learning for industrial metaverses: Incentive scheme with optimal aoi. In *2022 IEEE International Conference on Blockchain (Blockchain)*, pages 71-78. IEEE, 2022.
18. Liang Gao, Li Li, Yingwen Chen, ChengZhong Xu, and Ming Xu. Fgfl: A blockchain-based fair incentive governor for federated learning. *Journal of Parallel and Distributed Computing*, 163:283-299, 2022.

19. Yanru Chen, Yuanyuan Zhang, Shengwei Wang, Fan Wang, Yang Li, Yuming Jiang, Liangyin Chen, and Bing Guo. Dim-ds: Dynamic incentive model for data sharing in federated learning based on smart contracts and evolutionary game theory. *IEEE Internet of Things Journal*, 9(23):24572- 24584, 2022.
20. Kentaro Toyoda and Allan N Zhang. Mechanism design for an incentive-aware blockchain-enabled federated learning platform. In *2019 IEEE international conference on big data (Big Data)*, pages 395-403. IEEE, 2019.
21. Weishan Zhang, Tao Zhou, Qinghua Lu, Xiao Wang, Chunsheng Zhu, Haoyun Sun, Zhipeng Wang, Sin Kit Lo, and Fei-Yue Wang. Dynamicfusion- based federated learning for covid-19 detection. *IEEE Internet of Things Journal*, 8(21):15884-15891, 2021.
22. Bimal Ghimire and Danda B Rawat. Recent advances on federated learning for cybersecurity and cybersecurity for federated learning for internet of things. *IEEE Internet of Things Journal*, 9(11):8229-8249, 2022.
23. Muhammad Shayan, Clement Fung, Chris JM Yoon, and Ivan Beschastnikh. Biscotti: A blockchain system for private and secure federated learning. *IEEE Transactions on Parallel and Distributed Systems*, 32(7):1513-1525, 2020.
24. Yunlong Lu, Xiaohong Huang, Ke Zhang, Sabita Maharjan, and Yan Zhang. Blockchain and federated learning for 5g beyond. *IEEE Network*, 35(1):219-225, 2020.
25. Ziyuan Li, Jian Liu, Jialu Hao, Huimei Wang, and Ming Xian. Crowdsfl: A secure crowd computing framework based on blockchain and federated learning. *Electronics*, 9(5):773, 2020.
26. Sandi Rahmadika and Kyung-Hyune Rhee. Unlinkable collaborative learning transactions: Privacy-awareness in decentralized approaches. *IEEE Access*, 9:65293-65307, 2021.
27. Sandi Rahmadika, Philip Virgil Astillo, Gaurav Choudhary, Daniel Gerbi Duguma, Vishal Sharma, and Ilsun You. Blockchain-based privacy preservation scheme for misbehavior detection in lightweight iomt devices. *IEEE Journal of Biomedical and Health Informatics*, 27(2):710-721, 2022.
28. Mansoor Ali, Hadis Karimipour, and Muhammad Tariq. Integration of blockchain and federated learning for internet of things: Recent advances and future challenges. *Computers & Security*, 108:102355, 2021.
29. Sushil Kumar Singh, Laurence T Yang, and Jong Hyuk Park. Fusionfedblock:: Fusion of blockchain and federated learning to preserve privacy in industry 5.0. 2023.
30. Sandi Rahmadika and Kyung-Hyune Rhee. Enhancing data privacy through a decentralised predictive model with blockchain-based revenue. *International Journal of Ad Hoc and Ubiquitous Computing*, 37(1):1-15, 2021.
31. Stefano Savazzi, Monica Nicoli, and Vittorio Rampa. Federated learning with cooperating devices: A consensus approach for massive iot networks. *IEEE Internet of Things Journal*, 7(5):4641-4654, 2020.
32. Sawsan Abdul Rahman, Hanine Tout, Chamseddine Talhi, and Azzam Mourad. Internet of things intrusion detection: Centralized, on-device, or federated learning? *IEEE Network*, 34(6):310-317, 2020.
33. Peter Kairouz, H Brendan McMahan, Brendan Avent, Aurélien Bellet, Mehdi Bennis, Arjun Nitin Bhagoji, Kallista Bonawitz, Zachary Charles, Graham Cormode, Rachel Cummings, et al. Advances and open problems in federated learning. *Foundations and Trends® in Machine Learning*, 14(1-2):1-210, 2021.
34. Seyed Ali Osia, Ali Shahin Shamsabadi, Ali Taheri, Kleomenis Katevas, Hamid R Rabiee, Nicholas D Lane, and Hamed Haddadi. Privacy-preserving deep inference for rich user data on the cloud. *arXiv preprint arXiv:1710.01727*, 2017.
35. K Mahalakshmi, K Kousalya, Himanshu Shekhar, Aby K Thomas, L Bhagyalakshmi, Sanjay Kumar Suman, Selvaraj Chandragandhi, Prashant Bachanna, Kannan Srihari, and VenkatesaPrabhu Sundramurthy. Public auditing scheme for integrity verification in distributed cloud storage system. *Scientific Programming*, 2021:1-5, 2021.

36. Kevin Hsieh, Amar Phanishayee, Onur Mutlu, and Phillip Gibbons. The non-iid data quagmire of decentralized machine learning. In *International Conference on Machine Learning*, pages 4387-4398. PMLR, 2020.
37. Bjarne Pfitzner, Nico Steckhan, and Bert Arnrich. Federated learning in a medical context: a systematic literature review. *ACM Transactions on Internet Technology (TOIT)*, 21(2):1-31, 2021.
38. Chandra Thapa, Pathum Chamikara Mahawaga Arachchige, Seyit Camtepe, and Lichao Sun. Splitfed: When federated learning meets split learning. In *Proceedings of the AAAI Conference on Artificial Intelligence*, volume 36, pages 8485-8493, 2022.
39. István Hegedűs, Gábor Danner, and Márk Jelasity. Gossip learning as a decentralized alternative to federated learning. In *Distributed Applications and Interoperable Systems: 19th IFIP WG 6.1 International Conference, DAIS 2019, Held as Part of the 14th International Federated Conference on Distributed Computing Techniques, DisCoTec 2019, Kongens Lyngby, Denmark, June 17-21, 2019, Proceedings 19*, pages 74-90. Springer, 2019.
40. Tanweer Alam and Ruchi Gupta. Federated learning and its role in the privacy preservation of iot devices. *Future Internet*, 14(9):246, 2022.
41. Xiaoyuan Liu, Hongwei Li, Guowen Xu, Zongqi Chen, Xiaoming Huang, and Rongxing Lu. Privacy-enhanced federated learning against poisoning adversaries. *IEEE Transactions on Information Forensics and Security*, 16:4574-4588, 2021.
42. Chen Zhang, Yu Xie, Hang Bai, Bin Yu, Weihong Li, and Yuan Gao. A survey on federated learning. *Knowledge-Based Systems*, 216:106775, 2021.
43. Dzmitry Huba, John Nguyen, Kshitiz Malik, Ruiyu Zhu, Mike Rabbat, Ashkan Yousefpour, Carole-Jean Wu, Hongyuan Zhan, Pavel Ustinov, Harish Srinivas, et al. Papaya: Practical, private, and scalable federated learning. *Proceedings of Machine Learning and Systems*, 4:814-832, 2022.
44. Jingyan Jiang, Liang Hu, Chenghao Hu, Jiate Liu, and Zhi Wang. Bacombo—bandwidth-aware decentralized federated learning. *Electronics*, 9(3):440, 2020.
45. Chen Wang, Jian Shen, Jin-Feng Lai, and Jianwei Liu. B-tsca: Blockchain assisted trustworthiness scalable computation for v2i authentication in vanets. *IEEE Transactions on Emerging Topics in Computing*, 9(3):1386- 1396, 2020.
46. Shafaq Naheed Khan, Faiza Loukil, Chirine Ghedira-Guegan, Elhadj Benkhelifa, and Anoud Bani-Hani. Blockchain smart contracts: Applications, challenges, and future trends. *Peer-to-peer Networking and Applications*, 14:2901-2925, 2021.
47. Mohammad Saidur Rahman, Ibrahim Khalil, Pathum Chamikara Mahawaga Arachchige, Abdelaziz Bouras, and Xun Yi. A novel architecture for tamper proof electronic health record management system using blockchain wrapper. In *Proceedings of the 2019 ACM international symposium on blockchain and secure critical infrastructure*, pages 97-105, 2019.
48. Lucianna Kiffer, Dave Levin, and Alan Mislove. Analyzing ethereum’s contract topology. In *Proceedings of the Internet Measurement Conference 2018*, pages 494-499, 2018.
49. Davide Caputo, Luca Verderame, Andrea Ranieri, Alessio Merlo, and Luca Caviglione. Fine-hearing google home: why silence will not protect your privacy. *J. Wirel. Mob. Networks Ubiquitous Comput. Dependable Appl.*, 11(1):35-53, 2020.
50. Xuefei Yin, Yanming Zhu, and Jiankun Hu. A comprehensive survey of privacy-preserving federated learning: A taxonomy, review, and future directions. *ACM Computing Surveys (CSUR)*, 54(6):1-36, 2021.
51. Faiza Loukil, Khoulood Boukadi, Mourad Abed, and Chirine GhediraGuegan. Decentralized collaborative business process execution using blockchain. *World Wide Web*, 24(5):1645-1663, 2021.

52. Mohamed Abdur Rahman, M Shamim Hossain, Mohammad Saiful Islam, Nabil A Alrajeh, and Ghulam Muhammad. Secure and provenance enhanced internet of health things framework: A blockchain managed federated learning approach. *Ieee Access*, 8:205071-205087, 2020.
53. Sandi Rahmadika, Muhammad Firdaus, Yong-Hwan Lee, and KyungHyune Rhee. An investigation of pseudonymization techniques in decentralized transactions. *J. Internet Serv. Inf. Secur.*, 11(4):1-18, 2021.
54. Jiasi Weng, Jian Weng, Jilian Zhang, Ming Li, Yue Zhang, and Weiqi Luo. Deepchain: Auditable and privacy-preserving deep learning with blockchain-based incentive. *IEEE Transactions on Dependable and Secure Computing*, 2019.
55. Congzheng Song, Thomas Ristenpart, and Vitaly Shmatikov. Machine learning models that remember too much. In *Proceedings of the 2017 ACM SIGSAC Conference on computer and communications security*, pages 587-601, 2017.
56. Syreen Banabilah, Moayad Aloqaily, Eitaa Alsayed, Nida Malik, and Yaser Jararweh. Federated learning review: Fundamentals, enabling technologies, and future applications. *Information processing & management*, 59(6):103061, 2022.
57. Dun Li, Dezhi Han, Tien-Hsiung Weng, Zibin Zheng, Hongzhi Li, Han Liu, Arcangelo Castiglione, and Kuan-Ching Li. Blockchain for federated learning toward secure distributed machine learning systems: a systemic survey. *Soft Computing*, 26(9):4423-4440, 2022.
58. Reza Shokri, Marco Stronati, Congzheng Song, and Vitaly Shmatikov. Membership inference attacks against machine learning models. In *2017 IEEE symposium on security and privacy (SP)*, pages 3-18. IEEE, 2017.
59. Lan Liu, Yi Wang, Gaoyang Liu, Kai Peng, and Chen Wang. Membership inference attacks against machine learning models via prediction sensitivity. *IEEE Transactions on Dependable and Secure Computing*, 2022.
60. Jakub Konecny, H Brendan McMahan, Felix X Yu, Peter Richtárik, Ananda Theertha Suresh, and Dave Bacon. Federated learning: Strategies for improving communication efficiency. *arXiv preprint arXiv:1610.05492*, 2016.
61. Keith Bonawitz, Hubert Eichner, Wolfgang Grieskamp, Dzmitry Huba, Alex Ingerman, Vladimir Ivanov, Chloe Kiddon, Jakub Konecny, Stefano Mazzocchi, H Brendan McMahan, et al. Towards federated learning at scale: System design. *arXiv preprint arXiv:1902.01046*, 2019.
62. Satoshi Nakamoto and A Bitcoin. A peer-to-peer electronic cash system. *Bitcoin*.-URL: <https://bitcoin.org/bitcoin.pdf>, 4(2):15, 2008.
63. Elizabeth Vieira and José Gomes. A comparison of scopus and web of science for a typical university. *Scientometrics*, 81(2):587-600, 2009.
64. Maxim Chernyshev, Sherali Zeadally, and Zubair Baig. Healthcare data breaches: Implications for digital forensic readiness. *Journal of medical systems*, 43:1-12, 2019.
65. Alex Biryukov and Sergei Tikhomirov. Security and privacy of mobile wallet users in bitcoin, dash, monero, and zcash. *Pervasive and Mobile Computing*, 59:101030, 2019.
66. Zhilin Wang, Qin Hu, Ruinian Li, Minghui Xu, and Zehui Xiong. Incentive mechanism design for joint resource allocation in blockchain-based federated learning. *IEEE Transactions on Parallel and Distributed Systems*, 34(5):1536-1547, 2023.
67. Sandi Rahmadika and Kyung-Hyune Rhee. Merging collaborative learning and blockchain: Privacy in context. In *Proceedings of the Korea Information Processing Society Conference*, pages 228-230. Korea Information Processing Society, 2020.
68. Chuan Ma, Jun Li, Long Shi, Ming Ding, Taotao Wang, Zhu Han, and H Vincent Poor. When federated learning meets blockchain: A new distributed learning paradigm. *IEEE Computational Intelligence Magazine*, 17(3):26-33, 2022.



69. Shen Noether. Ring signature confidential transactions for monero. *IACR Cryptol. ePrint Arch.*, 2015:1098, 2015.
70. Aditya Pribadi Kalapaaking, Ibrahim Khalil, and Xun Yi. Blockchainbased federated learning with smpc model verification against poisoning attack for healthcare systems. *IEEE Transactions on Emerging Topics in Computing*, 12(1):269-280, 2023.
71. Marc Jayson Baucas, Petros Spachos, and Konstantinos N Plataniotis. Federated learning and blockchain-enabled fog-iot platform for wearables in predictive healthcare. *IEEE Transactions on Computational Social Systems*, 10(4):1732-1741, 2023.
72. Yinbin Miao, Ziteng Liu, Hongwei Li, Kim-Kwang Raymond Choo, and Robert H Deng. Privacy-preserving byzantine-robust federated learning via blockchain systems. *IEEE Transactions on Information Forensics and Security*, 17:2848-2861, 2022.
73. Saurabh Singh, Shailendra Rathore, Osama Alfarraj, Amr Tolba, and Byungun Yoon. A framework for privacy-preservation of iot healthcare data using federated learning and blockchain technology. *Future Generation Computer Systems*, 129:380-388, 2022.
74. Zhanpeng Yang, Yuanming Shi, Yong Zhou, Zixin Wang, and Kai Yang. Trustworthy federated learning via blockchain. *IEEE Internet of Things Journal*, 10(1):92-109, 2022.
75. Umer Majeed, Latif U Khan, Abdullah Yousafzai, Zhu Han, Bang Ju Park, and Choong Seon Hong. St-bfl: A structured transparency empowered cross-silo federated learning on the blockchain framework. *Ieee Access*, 9:155634-155650, 2021.
76. Hong Liu, Shuaipeng Zhang, Pengfei Zhang, Xinqiang Zhou, Xuebin Shao, Geguang Pu, and Yan Zhang. Blockchain and federated learning for collaborative intrusion detection in vehicular edge computing. *IEEE Transactions on Vehicular Technology*, 70(6):6073-6084, 2021.
77. Yang Zhao, Jun Zhao, Linshan Jiang, Rui Tan, Dusit Niyato, Zengxiang Li, Lingjuan Lyu, and Yingbo Liu. Privacy-preserving blockchain-based federated learning for iot devices. *IEEE Internet of Things Journal*, 8(3):1817-1829, 2021.
78. Jin Sun, Ying Wu, Shangping Wang, Yixue Fu, and Xiao Chang. Permissioned blockchain frame for secure federated learning. *IEEE Communications Letters*, 26(1):13-17, 2021.
79. Yuanhang Qi, M Shamim Hossain, Jiangtian Nie, and Xuandi Li. Privacypreserving blockchain-based federated learning for traffic flow prediction. *Future Generation Computer Systems*, 117:328-337, 2021.
80. Qianlong Wang, Yifan Guo, Xufei Wang, Tianxi Ji, Lixing Yu, and Pan Li. Ai at the edge: Blockchain-empowered secure multiparty learning with heterogeneous models. *IEEE Internet of Things Journal*, 7(10):9600-9610, 2020.
81. Sandi Rahmadika and Kyung-Hyune Rhee. Reliable collaborative learning with commensurate incentive schemes. In *2020 IEEE International Conference on Blockchain (Blockchain)*, pages 496-502. IEEE, 2020.
82. Yuan Liu, Zhengpeng Ai, Shuai Sun, Shuangfeng Zhang, Zelei Liu, and Han Yu. Fedcoin: A peer-to-peer payment system for federated learning. In *Federated Learning*, pages 125-138. Springer, 2020.
83. Sizheng Fan, Hongbo Zhang, Yuchen Zeng, and Wei Cai. Hybrid blockchain-based resource trading system for federated learning in edge computing. *IEEE Internet of Things Journal*, 2020.
84. Latif U Khan, Shashi Raj Pandey, Nguyen H Tran, Walid Saad, Zhu Han, Minh NH Nguyen, and Choong Seon Hong. Federated learning for edge networks: Resource optimization and incentive mechanism. *IEEE Communications Magazine*, 58(10):88-93, 2020.
85. Meng Shen, Jie Zhang, Liehuang Zhu, Ke Xu, and Xiangyun Tang. Secure svm training over vertically-partitioned datasets using consortium blockchain for vehicular social networks. *IEEE Transactions on Vehicular*

Technology, 69(6):5773-5783, 2020.

86. Hyunil Kim, Seung-Hyun Kim, Jung Yeon Hwang, and Changho Seo. Efficient privacy-preserving machine learning for blockchain network. IEEE Access, 7:136481-136495, 2019.

87. Jiawen Kang, Zehui Xiong, Dusit Niyato, Shengli Xie, and Junshan Zhang. Incentive mechanism for reliable federated learning: A joint optimization approach to combining reputation and contract theory. IEEE Internet of Things Journal, 6(6):10700-10714, 2019.

88. Luca Melis, Congzheng Song, Emiliano De Cristofaro, and Vitaly Shmatikov. Exploiting unintended feature leakage in collaborative learning. In 2019 IEEE symposium on security and privacy (SP), pages 691- 706. IEEE, 2019.

## FINANCING

This paper is funded by Universitas Negeri Padang.

## CONFLICT OF INTEREST

The authors declare that the research was conducted without any commercial or financial relationships that could be construed as a potential conflict of interest.

## AUTHORSHIP CONTRIBUTION

*Conceptualization:* Sandi Rahmadika, Ulfia Rahmi, Ahmaddul Hadi.

*Formal analysis:* Sandi Rahmadika, Ahmaddul Hadi, Harashta Tatimma Larasati.

*Research:* Sandi Rahmadika, Ahmaddul Hadi, Ulfia Rahmi, Harashta Tatimma Larasati.

*Methodology:* Sandi Rahmadika, Ahmaddul Hadi, Harashta Tatimma Larasati.

*Project management:* Sandi Rahmadika, Ulfia Rahmi, Bayu Ramadhani Fajri.

*Resources:* Sandi Rahmadika, Ahmaddul Hadi, Ulfia Rahmi, Harashta Tatimma Larasati.

*Supervision:* Harashta Tatimma Larasati, Bayu Ramadhani Fajri.

*Validation:* Harashta Tatimma Larasati, Ahmaddul Hadi.

*Visualization:* Bayu Ramadhani Fajri, Ulfia Rahmi.

*Drafting - original draft:* Sandi Rahmadika, Bayu Ramadhani Fajri.

*Writing - proofreading and editing:* Ulfia Rahmi, Ahmaddul Hadi, Harashta Tatimma Larasati.