Indonesian Journal of Electrical Engineering and Computer Science
Vol. 42, No. 1, April 2026, pp. 164~173
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v42.i1.pp164-173

A decentralized call recording in voice over IP based on blockchain using smart contracts

Abdelhadi Rachad, Lotfi Gaiz, Khalid Bouragba, Mohammed Ouzzif
Computer Science and Smart Systems (C3S) Laboratory, Higher School of Technology Casablanca (ESTC), University of Hassan II Casablanca, Casablanca, Morocco

Article Info

Article history:

Received Jun 27, 2025
Revised Feb 26, 2026
Accepted Mar 4, 2026

Keywords:

Agent
Blockchain
Decentralized call recording
VoIP Security
Smart Contracts

ABSTRACT

Although voice over IP (VoIP) has established itself as the new paradigm for universal telecommunications, its massive deployment within businesses and government agencies has paradoxically increased the attack surface for cyber threats: stream injection fraud, identity theft, and, more recently, the emergence of voice deepfakes, rendering traditional security architectures obsolete. At the same time, conventional centralized recording systems raise trust issues, as they are vulnerable to data manipulation, unauthorized access, and single points of failure. This article presents a new architecture that decentralizes the recording and securing of VoIP calls by combining three key technologies: blockchain for immutability; smart contracts to automate communications governance and ensure the transition from a centralized to an algorithmic trust model; and artificial intelligence (AI) agents that analyze audio streams in real time. This approach transforms VoIP recording from a simple passive file into a secure, auditable, and confidential digital asset. By removing centralized control and strengthening identity verification, this architecture provides a concrete response to security requirements.

This is an open access article under the CC BY-SA license.

Corresponding Author:

Abdelhadi Rachad
Computer Science and Smart Systems (C3S) Laboratory
Higher School of Technology Casablanca (ESTC), University of Hassan II Casablanca
Casablanca, Morocco
Email: rachad.abdelhadi@gmail.com

1. INTRODUCTION

Voice over IP based (VoIP) [1] is a technology that allows voice calls to be made over the internet instead of the traditional private branch exchange (PBX) network. VoIP is a type of virtual phone system that uses the internet, not physical copper wiring, to manage incoming and outgoing calls. VoIP is also known as virtual telephony, online calling, and IP telephony. VoIP is a technology that allows voice calls and other communication services to be transmitted over IP networks such as the internet. It converts analog voice signals into digital data packets, which are then transmitted over the network. This conversion allows users to make phone calls over an internet connection, without the need for a traditional phone line. Figure 1 shows an architecture diagram using SIP trunking [2]. This system allows businesses to move from a traditional private branch exchange PBX to an intelligent, cloud-based system. The key features of most providers: Inbound and outbound call management; advanced routing (time-and location-based); simultaneous routing; international forwarding; call flow generator; voicemail; fax; call screening; speed dialing; caller ID management, and much more.

The global VoIP market size [3] is expected to reach $108.5 billion by 2032. With increasing adoption in businesses and the integration of new technologies like AI, cloud, and 5G networks to provide

faster internet speeds and more reliable connections, VoIP also allows businesses to reduce their telecom bills. Businesses can save up to 30% on their communication costs, especially on international communications, by benefiting from much more advantageous plans. Some of the major challenges associated with VoIP implementation include call quality issues, security concerns, reliability and uptime complications, and compatibility and integration challenges. VoIP is an increasingly common target for cybercriminals. Effective measures, such as data encryption, ensure that even if information is intercepted, it remains indecipherable to hackers. Strong and varied passwords and regular network testing further enhance security. It is essential that VoIP providers and customers are aware of potential security risks and take appropriate measures to protect sensitive information.

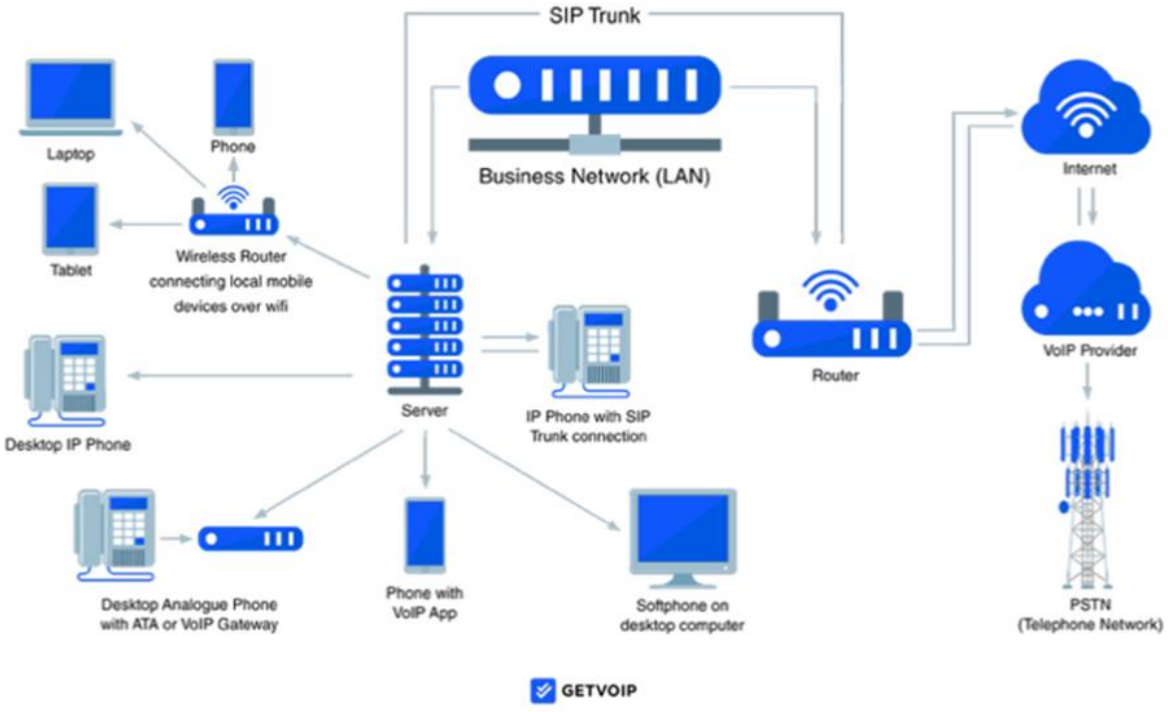

Figure 1. VoIP architecture [2]

Call detail records (CRD) is a database that concerns the information provided by call detail records, we can generally include [4]: date and time; call duration (minutes); caller ID; Location of call origination and destination; destination number or number dialed; completion status or reason for call termination; type of call (toll-free, local, etc.); cost per call and total charge; features used (SMS forwarding, call recording, etc.); call journey (extensions, IVR, etc.). It is important to note that a call detail record and thanks to AI today the content of a call. Additionally, CDRs may contain data related to your VoIP network, such as IP address or port number. In a broader context, CDR data contributes to network optimization, helping telecommunications providers improve service delivery and reduce congestion. This results in better customer satisfaction and better resource allocation. Managing CDR data is not without its challenges.

Figure 2 [5] shows a diagram analyzing detailed CDR call recordings. The Neo4j solution transforms raw telecommunications data into an interconnected network, revealing social structures and behavioral patterns. By modeling subscribers as nodes and calls as relationships, this approach facilitates the immediate identification of customer communities, key influencers, and complex fraud patterns.

The evolution of VoIP towards 5G and AI paradoxically increases its vulnerability to cyber threats. Current infrastructures remain susceptible to critical attacks [5]-[8] such as voice over misconfigured internet telephones (VOMIT), which enables the extraction of sensitive data, call interception (eavesdropping), and SPIT (spam over IP telephony). In this context, the traditional management of call recordings on centralized servers represents a single point of failure, where call logs can be falsified to conceal fraudulent activity or line hijacking. Despite recent advances, CDRs management within decentralized VoIP infrastructures [9] faces a major challenge: the trade-off between immutability and scalability. According to Table 1 in the current systems, the static structure of CDRs does not allow for dynamic responses to emerging threats or

complex real-time billing requirements. Locking data in centralized databases not only creates a single point of failure conducive to fraud but also limits interoperability between peer-to-peer nodes.

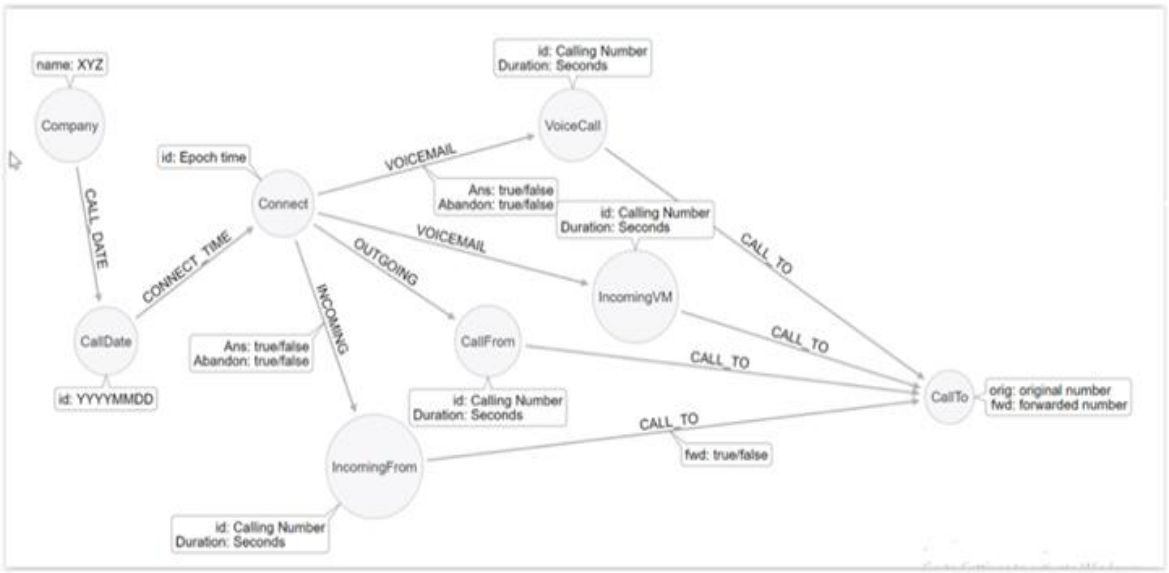

Figure 2. Graph data model stores call detail records [5]

Table 1 Comparison between traditional VoIP and blockchain recording [10]-[13]

Category	Enregistrement VoIP traditionnel	Enregistrement VoIP basé sur blockchain
Architecture	Centralized (Client-Server).	Decentralized (Peer-to-Peer / Nodes).
Data integrity	Low (Risk of audio file tampering).	Immuable (Hash cryptographic ancré in chain).
Proof of consent	Stockée dans une base de données modifiable.	Smart Contract (Horodatage certifié et irréfutable).
Log security (CDR)	Sensible aux ransomwares et accès non autorisés.	Résilient (Accès contrôlé par clé privée via Smart Contract).
General data protection regulation (GDPR)	Audit difficile et manuel.	Conformité par conception (Privacy by Design)
Hardware requirements	Téléphones IP, adaptateurs ou softphones; nécessite un serveur central de stockage.	Téléphones IP, mobiles ou PC; Nœuds de validation légers (Edge); stockage hybride IPFS.
International calls	Tarifs réduits par rapport au RTC classique, mais dépendants des passerelles opérateurs.	Coût quasi-nul sur réseaux privés; interconnexion directe via Smart Contracts sans intermédiaires.

The goal of this research is to transform the CDR from a simple, passive log susceptible to falsification into a dynamic entity governed by smart contracts. The challenge then lies in designing smart contracts capable of processing a massive volume of metadata without degrading communication latency, while ensuring tamper-proof traceability and automated compliance, thus addressing the security and governance challenges of today's networks. The integration of blockchain technology into VoIP networks [10]-[13] marks a major evolution compared to centralized systems. While current literature has mainly focused on the call setup phase, our research identifies and fills a critical gap: securing audio content after the call.

The integration of blockchain and smart contracts is redefining security and operational efficiency across multiple technology domains. Recent work demonstrates their usefulness in securing sensitive data records in communication systems [14], while also proposing consortium networks for managing SMEs via the intelligence of things (AIoT) [15]. This synergy extends to the architecture of 5G telecom networks [16] and the Internet of Things, where hybrid and scalable authentication frameworks ensure the confidentiality of sensitive data [17]. Finally, the application of smart contracts is proving crucial for automating predictive maintenance in Industry 4.0 [18] as well as for modernizing business processes in several sectors [19].

Our work builds upon promising research aimed at securing modern communication infrastructures. Initiatives such as VoIPChain, Bcvop2p, and BBCA [20], [21] have already demonstrated the technical feasibility of primary blockchain integration into P2P VoIP networks. Recent literature supports this approach [22]-[27]. The shortcomings of centralized storage in the face of strict regulations regarding data privacy and integrity justify this technological advancement. Similarly, the hybrid architectural model (blockchain for metadata, decentralized storage for multimedia content) validates our proposal.

2. METHOD

This section presents our decentralized architecture and key details of our blockchain-based VoIP call recording, which consists of four main elements: a smart contract, a SIP VoIP client, a VoIP server, and a decentralized administration interface. These components are independent but can communicate with each other. Our goal is to create a distributed call log, broadcast to every node on the network, verified, and stored within the network. Call recordings will thus be more secure, similar to a Bitcoin transaction: a call will be treated as a transaction. Indeed, they are added to a ledger encrypted with a digital security code, guaranteeing their inviolability and permanence. The structure is generally organized into blocks. Each block contains an index, a timestamp, and information related to the transactions: the status of the calls (incoming or outgoing), their duration, their type, network details, and the hash of the previous block. The system structure is shown in Figure 3. The blocks represent metadata. Call detail records collect specific data related to telecommunications activities. They include key information about where, when, and how VoIP is used. Call detail records databases store calls in distributed databases in the form of smart contracts. A smart contract is a detailed record of telecommunications activity, including metadata such as: call logs; call recordings; call history.

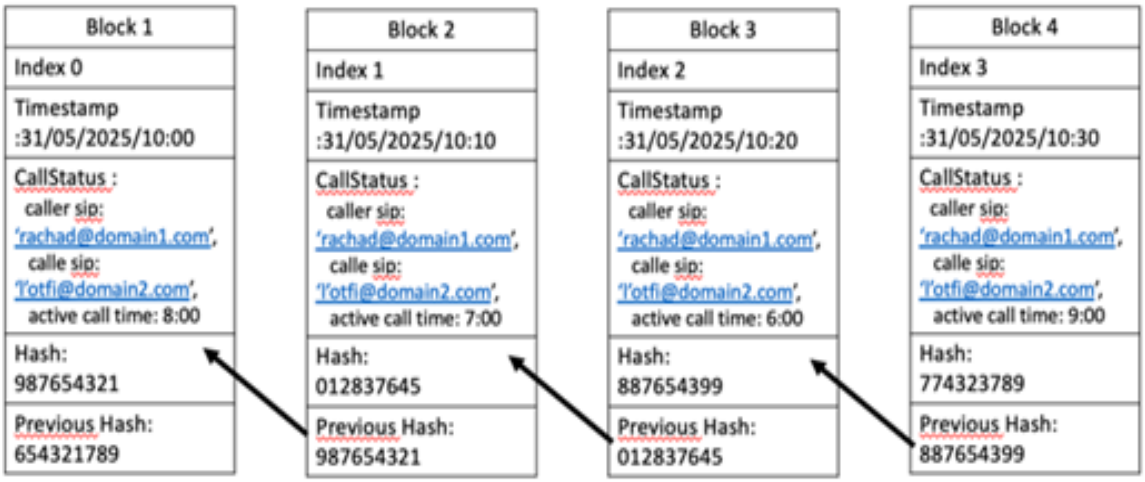

Figure 3. Example VOIP registration in the blockchain

These smart contracts can contain more than a dozen attributes. Here are some of the most common:

- Originating number: The number that placed the call.
- Receiving number: The number that received the call.
- Date of call: The time the call was placed.
- Time of call: The time it was placed.
- Call duration: The duration of each call.
- Call type: Whether it was an inbound or outbound call.
- Location: The geographical origin of the call.
- Recording: Encrypted call storage path (Local Storage, Cloud Storage: AWS, Google Drive, Dropbox, etc.);

Considering the business requirements, several technical aspects were then considered. They can be summarized as follows:

- VoIP client: A VoIP compatible device/software, in our model we have chosen the SIP client. The SIP client is an application installed in smartphones or laptop/desktop. Which can send and receive SIP messages and provide traditional phone call functions, such as dialing, answering, rejecting, holding, call transfer, etc. the VOIP client will be a blockchain node that will create or receive a new block, it adds it to its copy of the ledger and then transmits it to its peer nodes. When they receive it, they check that this new block is valid they ensure that the sum of the transactions is equal in input and output. If the block is valid, they then integrate it into their ledger and transmit it in turn to their peers. In our implementation we will develop an application programming interface (API) that will connect the SIP client with Ethereum blockchain.
- VOIP server(s): In our model, a VoIP server is a system that allows telephone calls to be made over the Internet. There are several types of VoIP servers: a) Cloud-based servers, such as cloud IPBX, are popular because they do not require complex installation and offer great flexibility. And b) Local device-based

VoIP servers require the purchase of IP phones that connect via Wi-Fi or Ethernet. In our implementation, an open-source Asterisk VoIP server is used.

- Smart contract: Using smart contracts to record VoIP call audio data and store call metadata (customer number, agent number, date, time, etc.) on the blockchain is an innovative approach to ensure the security and integrity of decentralized audio data, unlike existing CRD management solutions. Call recording data would be recorded on a blockchain, making it difficult or impossible to tamper with or delete it. In our implementation, we will use the Ethereum blockchain.

In our proposal, a blockchain-based call recording architecture is designed on a secure end-to-end decentralized model and is established over the IP network during the call and after the transfer of multimedia data. Thus, encrypted keys that change dynamically during conversations can be obtained. Any device not registered on the blockchain in the proposed system architecture is considered a malicious device. The verification process is performed transparently through the blockchain, and flow control is ensured, thus ensuring a secure and reliable communication structure. The implementation of our proposal for secure, decentralized blockchain-based call recording is explained in this section. The preferred technology for the proof-of-principle implementation was Ethereum as the blockchain and Asterisk as VoIP.

The call recording workflow goes through 4 phases is shown in Figure 4:

- Phase 1: Authentication and call routing via VoIP and blockchain encrypts all telephone communications end-to-end. Authentication is based on the SIP protocol and smart contracts, allowing user identification and call authenticity verification, while call recording includes transfer, hold, and other standard features offered by traditional VoIP.
- Phase 2: After the end of Phase 1, the call status is automatically updated in the smart contract, using intelligent agents. The latter is an immutable program stored on a cloud blockchain that executes automatically when the coded conditions defined by VOIP and blockchain servers are met.

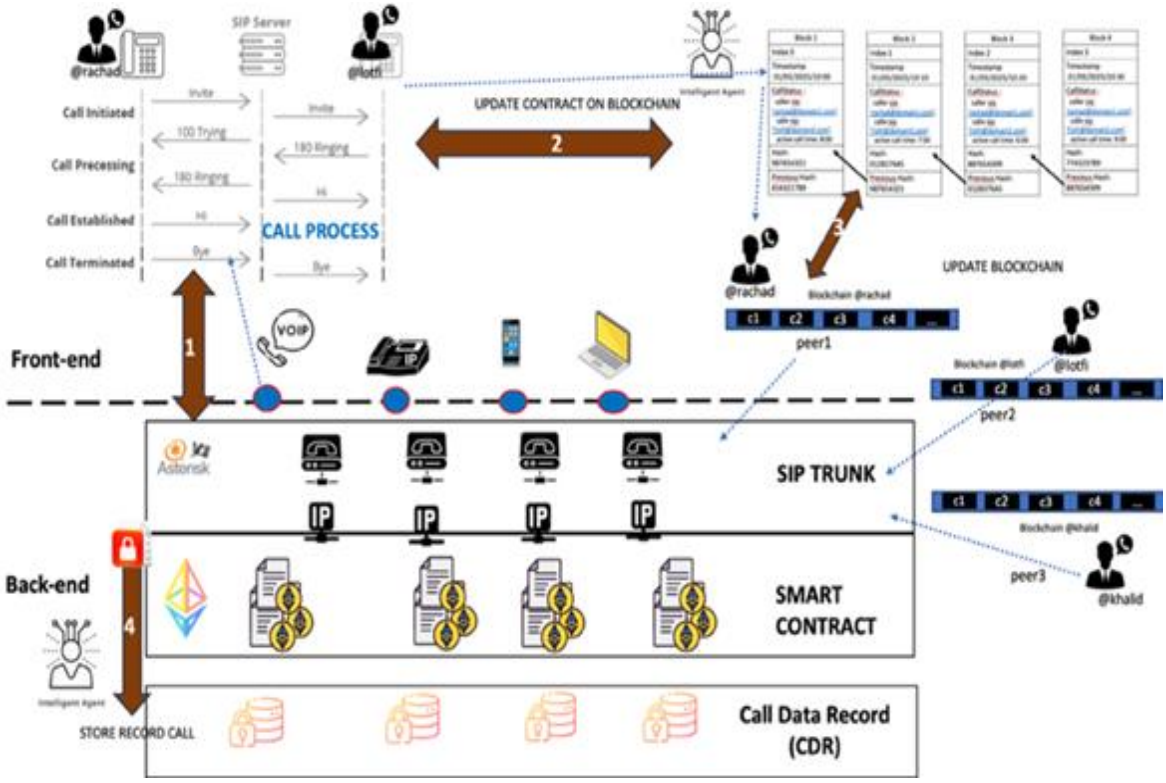

Figure 4. Decentralized call data record system model based on blockchain technology

- Phase 3: After the end of Phase 2, updating the blockchain in the network involves several steps, including the validation of new blocks by network nodes and the addition of these blocks to the existing chain.

- Phase 4: Aggregate transactional call CDRs and record encrypted calls in distributed cloud databases using smart agents, the latter is a program defined in VOIP and blockchain servers that contains: the call recording and a copy of the smart contract

Our solution relies on applications hosted in distributed cloud computing. Our current architecture, based on peer-to-peer networks, offers several advantages: No risk of traditional hacking thanks to the security offered by blockchain technology; Easy maintenance thanks to its distributed architecture; Evidence of data cannot be modified. Our implementation of the call recording system will be based on the Asterisk solution (Table 2). The Ethereum blockchain-integrated VoIP system will consist of three main components.

Table 2. The components of our implementation

Component	Solution	Function
VoIP server	Asterisk	Manages VoIP call routing and sessions
Smart contract	Ethereum	Automates authentication & log validation
Decentralized call recording	Multi Storage	P2P Database Management Systems Stores call logs as immutable records Store call recording
VoIP client	SIP	Smartphones: Android; iPhone
Network	VPNs	Encrypts VoIP communication channels
Monitoring	Grafana	Dashboard provides a high-level overview of the Asterisk instance

Our implementation environment (Figure 5) will be based on Asterisk version 22.4 installed on a Debian 12 server with FreePBX 17 as the management interface.

Stapes 1 and 3: All VoIP client (SIP client) authentication is secure and encrypted through the immutable blockchain environment. Identity authentication is tamper-proof, decentralized authentication provides fault tolerance and resists deletion of authentication data.

Stapes 2: An ETHEREUM instance deployed on multiple distributed nodes to manage smart contracts and authentication. All data entering/leaving the VoIP server Asterisk and FreePBX is transformed and managed in the ETHEREUM servers.

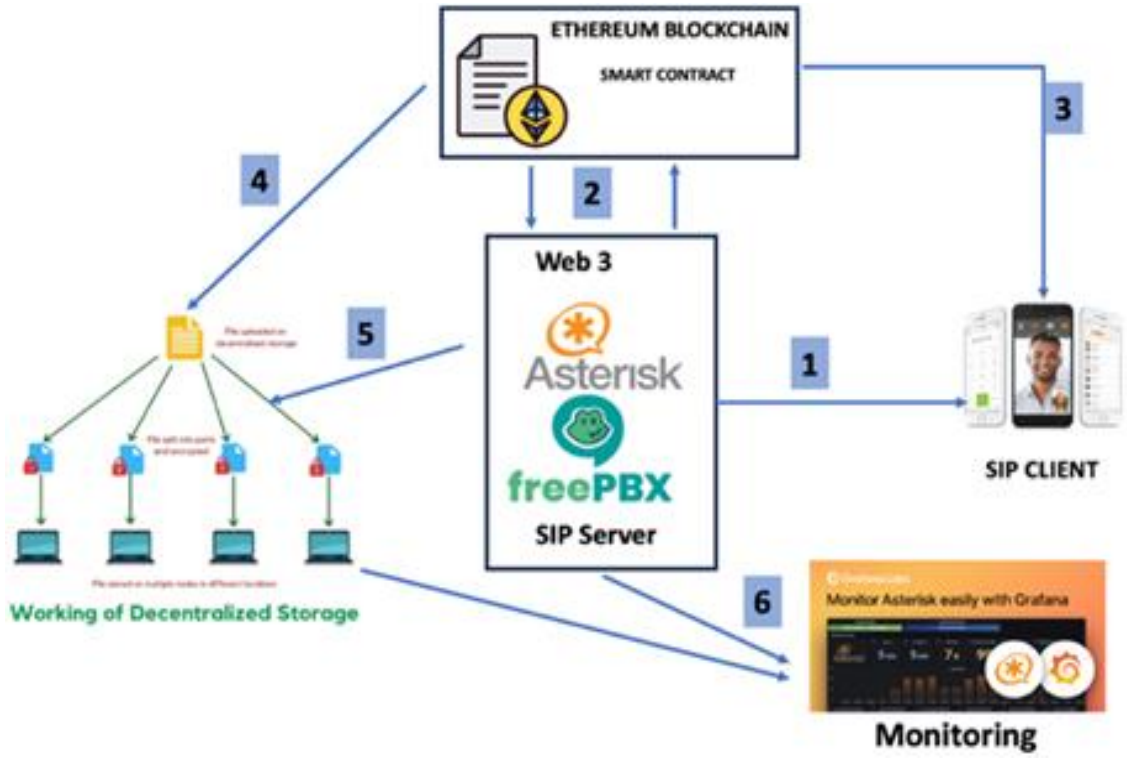

Figure 5. Our test implementation: Asterisk, FreePBX, Grafana and Ethereum

Stapes 4 and 5: After the call ends, the call record will be saved along with the call details, and the call recording will be uploaded to decentralized storage using the following process: The files are split into several parts; All elements are secured with strong encryption; Each element is stored in a different location.

Stapes 6: Grafana is an open-source solution that allows us to easily monitor our Asterisk deployment and store distributed data. This dashboard provides a high-level overview of the Asterisk instance based on all metrics exposed by the Prometheus exporter built into Asterisk.

3. RESULTS AND DISCUSSION

Our proposed architecture relies on an asynchronous coupling between the Asterisk switching plane and a decentralized trust layer based on Ethereum. When a media stream terminates (audio call, video call), the FreePBX server executes a hang-up manager that extracts metadata from the CDR and generates a SHA-256 cryptographic hash of the associated audio file. This hash, acting as a unique and immutable identifier, is transmitted to a smart contract via a programmatic transaction. Unlike centralized storage approaches vulnerable to administrative manipulation, our method guarantees the integrity of the proofs through on-chain anchoring. To validate the scalability of this model, we correlated the most relevant performance metrics with the block finality latency on the blockchain, all visualized in real time on Grafana. This hybrid approach maintains the high availability required for VoIP while ensuring mathematical non-repudiation of the recordings. Here is a typical results structure, based on a simulation with Asterisk, Ethereum (Layer 2), and Grafana:

3.1. System performance analysis (CPU/RAM Impact)

Tests performed with SIPp demonstrate that the SHA-256 hashing process and the sending of CDRs to the blockchain do not impact the quality of service (QoS) of voice.

- CPU usage: A marginal increase of 7% to 10% is observed when calling the Astersk AGI script after hanging up.
- RAM usage: Stable at approximately 190 MB additional for the transaction management daemon (Python Pusher).

3.2. Blockchain validation latency

The time elapsed between the end of the call and the recording of the hash on the registry is a critical metric visualized on Grafana (Figure 6):

- Network: Average confirmation time of 1.75 to 3.5 seconds.
- Interpretation: This delay is considered acceptable for an auditing system because it is asynchronous and does not interfere with the establishment of subsequent calls.

Figure 6. Grafana: blockchain validation latency

3.3. Economic viability

Using Ethereum-optimized Smart Contracts (Layer 2) with Solidity reduces operational costs.

- Cost per CDR: Approximately 37,000 to 50,000 Gas per transaction.
- Simulation: On a Layer 2 architecture, this represents a cost of less than $0.001 per record, making the solution economically viable for high-volume call centers.

3.4. Effectiveness of alteration detection

During the attack simulation, we manually modified a .wav file and an SQL entry. The result: the system showed a 100% detection rate. Any discrepancy between the hash stored on Ethereum and the locally recalculated hash triggers an immediate alert on the Grafana dashboard, proving the system's immutability.

3.5. Discussion

Experimental results confirm that integrating a decentralized registry for CDRs and VoIP recordings does not impair PBX transaction performance. With a validation latency of less than 4 seconds on a Layer 2 network and a negligible cost per transaction, our architecture offers a robust and scalable alternative to traditional centralized archiving systems, guaranteeing absolute integrity of communication data. After this study, the combination of the two technologies of VoIP and blockchain will be the right choice that will guarantee the security and confidentiality of VoIP communications, while offering transparent and secure payment solutions. By integrating cutting-edge technologies to secure telecommunications, SMEs can protect their data and prevent intrusions at several levels: Decentralization, Enhanced security of communications, Traceability of transactions, and call recording.

4. CONCLUSION

Beyond a simple technical upgrade, the convergence of blockchain and VoIP foreshadows the future of digital sovereignty in internet communications. Our approach transforms call recordings into digital assets protected by decentralized governance. By eliminating single points of failure, we establish an ecosystem where trust no longer relies on a third party, but on the robustness of the smart contract code. This resilient infrastructure lays the foundation for a global communications network where confidentiality and authenticity are guaranteed by design.

FUNDING INFORMATION

The authors state that no external funding was received for this research work.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Abdelhadi Rachad	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Lotfi Gaiz			✓		✓			✓						
Khalid Bouragba				✓						✓	✓	✓	✓	
Mohammed Ouzzif										✓	✓	✓	✓	

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal analysis
I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting
Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject administration
Fu : **Fu**nding acquisition

CONFLICT OF INTEREST STATEMENT

The authors have no conflict of interest relevant to this paper.

DATA AVAILABILITY

Data availability is not applicable to this paper as no new data were created or analyzed in this study.

REFERENCES

[1] B. Goode, "Voice over IP Networks." 2nd ed. New York, NY, USA: McGraw-Hill Education, ch. 2, sec. 4, pp. 45–82, 2024.
[2] K. Stone, "What is VoIP (Voice over Internet Protocol)?," GetVoIP Library. Accessed: Jan. 15, 2026. [Online]. Available: https://getvoip.com/library/what-is-voip/
[3] Global Market Insights Inc., "Voice over internet protocol (VoIP) market – global forecast 2023–2032," 2023.

[4] K. Murthy, "Call Detail Records (CDR) Analytics," GitHub Gist. Accessed: Jan. 15, 2026. [Online]. Available: https://gist.github.com/kaisesha/bd10fd299a3bed2b12ff031c937cdd4c
[5] A. M. Ramly, Z. W. Ng, Y. Khamayseh, C. S. C. Kwan, A. Amphawan, and T. K. Neo, "Review and enhancement of VoIP security: identifying vulnerabilities and proposing integrated solutions," *Journal of Telecommunications and the Digital Economy*, vol. 12, no. 4, pp. 109–136, Dec. 2024, doi: 10.18080/jtde.v12n4.1022.
[6] Washima Tuleun, "Design of an asterisk-based VoIP system and the implementation of security solution across the VoIP network," *World Journal of Advanced Research and Reviews*, vol. 23, no. 1, pp. 875–906, Jul. 2024, doi: 10.30574/wjarr.2024.23.1.2048.
[7] M. Abdul Jabbar and Suharjito, "Fraud detection call detail record using machine learning in telecommunications company," *Advances in Science, Technology and Engineering Systems*, vol. 5, no. 4, pp. 63–69, Jul. 2020, doi: 10.25046/aj050409.
[8] T. Porter, *VoIP security: concepts and practice*. Burlington, MA, USA: Syngress Publishing, 2023.
[9] S. Abdulrahman and M. Useng, "Blockchain and distributed ledger technologies for IoT security: a survey paper," *Mesopotamian Journal of Computer Science*, vol. 2022, pp. 5–9, Apr. 2022, doi: 10.58496/MJCSC/2022/006.
[10] R. Dantas, C. Exton, and A. Le Gear, "Blockchain voip authentication of text-to-speech conversations," *IEEE Transactions on Network and Service Management*, vol. 22, no. 1, pp. 415–430, 2025.
[11] V. Sreenivasulu and C. Ravikumar, "FractalNet-based key generation for authentication in voice over IP using blockchain," *Ain Shams Engineering Journal*, vol. 16, no. 3, p. 103286, Mar. 2025, doi: 10.1016/j.asej.2025.103286.
[12] M. K. Siam *et al.*, "Securing decentralized ecosystems: a comprehensive systematic review of blockchain vulnerabilities, attacks, and countermeasures and mitigation strategies," *Future Internet*, vol. 17, no. 4, p. 183, Apr. 2025, doi: 10.3390/fi17040183.
[13] R. Gupta and M. S. Obaidat, "A privacy-preserving blockchain framework for secure VoIP signaling in 6G networks," *IEEE Transactions on Cognitive Communications and Networking*, vol. 11, no. 2, pp. 312–325, 2025.
[14] M. Kara, "Securing call detail records (CDR) in Asterisk-based PBX systems using private blockchain," *Journal of Information Security and Applications*, vol. 81, no. 103712, 2025.
[15] A. A. Khan *et al.*, "BAIoT-EMS: consortium network for small-medium enterprises management system with blockchain and augmented intelligence of things," *Engineering Applications of Artificial Intelligence*, vol. 141, p. 109838, Feb. 2025, doi: 10.1016/j.engappai.2024.109838.
[16] A. Ayub Khan *et al.*, "ORAN-B5G: a next-generation open radio access network architecture with machine learning for beyond 5G in Industrial 5.0," *IEEE Transactions on Green Communications and Networking*, vol. 8, no. 3, pp. 1026–1036, Sep. 2024, doi: 10.1109/TGCN.2024.3396454.
[17] A. A. Khan *et al.*, "A lightweight scalable hybrid authentication framework for internet of medical things (IoMT) using blockchain hyperledger consortium network with edge computing," *Scientific Reports*, vol. 15, no. 1, p. 19856, Jun. 2025, doi: 10.1038/s41598-025-05130-w.
[18] A. Rachad, L. Gaiz, K. Bouragba, and M. Ouzzif, "Predictive maintenance-as-a-service (PdMaaS) in industry 4.0 using blockchain," in *2023 10th International Conference on Wireless Networks and Mobile Communications (WINCOM)*, IEEE, Oct. 2023, pp. 1–6. doi: 10.1109/WINCOM59760.2023.10322922.
[19] A. Rachad, L. Gaiz, K. Bouragba, and M. Ouzzif, "A smart contract architecture framework for insurance industry using blockchain and business process management technology," *IEEE Engineering Management Review*, vol. 52, no. 2, pp. 55–68, Apr. 2024, doi: 10.1109/EMR.2023.3348431.
[20] M. Kara, H. R. J. Merzeh, M. A. Aydın, and H. H. Balık, "VoIPChain: a decentralized identity authentication in voice over IP using blockchain," *Computer Communications*, vol. 198, pp. 247–261, Jan. 2023, doi: 10.1016/j.comcom.2022.11.019.
[21] I. M. Tas and S. Baktir, "Blockchain-based caller-ID authentication (BBCA): a novel solution to prevent spoofing attacks in VoIP/SIP networks," *IEEE Access*, vol. 12, pp. 60123–60137, 2024, doi: 10.1109/ACCESS.2024.3393487.
[22] M. Kara, M. Aydın, and H. H. Balık, "Enhanced Bcvop2p: optimization of decentralized authentication for large-scale VoIP networks," *Intelligent Automation & Soft Computing*, vol. 39, no. 1, pp. 210–228, 2025.
[23] S. Das and R. C. Barik, "A comparative analysis of Bcvop2p and VoIPChain in 5G-enabled communication systems," *IEEE Access*, vol. 13, pp. 4412–4430, 2025.
[24] K. Sharma and P. Tyagi, "Decentralized anti-spam framework for SIP-based VoIP using hyperledger fabric," *International Journal of Information Security*, vol. 25, no. 1, pp. 45–62, 2026.
[25] Y. Qi and M. S. Hossain, "Harnessing federated generative learning for green and sustainable internet of things," *Journal of Network and Computer Applications*, vol. 222, p. 103812, Feb. 2024, doi: 10.1016/j.jnca.2023.103812.
[26] N. Khan *et al.*, "An efficient blockchain-enhanced protocol for securing real-time IoT data in public cloud environments," *Human-centric Computing and Information Sciences*, vol. 15, no. 69, 2025, doi: 10.22967/HCIS.2025.15.069.
[27] S. Kumar and J. Singh, "Smart contract-based fraud prevention in decentralized VoIP peering," *Journal of Cyber Security Technology*, vol. 9, no. 1, pp. 12–28, 2025, doi: 10.1080/23742917.2024.2301542.

BIOGRAPHIES OF AUTHORS

Abdelhadi Rachad received the Research Master's degree in Computer Engineering in 2010 from the National School of Computer Science and Systems Analysis (ENSIAS), Rabat, Morocco. and currently a Ph.D. student in the Research Laboratory Computer Science and Smart System (C3S) of the High School of Technology (ESTC), in Hassan II University of Casablanca, Morocco. Since 2012, he has served as head of IT projects in the private sector. His research interests include blockchain and smart contract, cloud computing, service-oriented architecture (SOA), business process management (BPM), enterprise resource planning (ERP) and artificial intelligence (AI). He is a member of the Computer Science and Smart System (C3S) laboratory in Hassan II University of Casablanca. He can be contacted at email: rachad.abdelhadi@gmail.com.

Lotfi Gaiz was born in Ouazzane, Morocco. 1990. He received his Master's degree in Computer from the Faculty of Science Kénitra, Ibn-Tofail University, Kénitra, Morocco. Currently a Ph.D. student in the Research Laboratory in Computer Science and Smart System (C3S) of the High School of Technology (ESTC), in Hassan II University of Casablanca, Morocco. His research interests include BigData, Blockchain, Cloud Computing and Analytics. He can be contacted at email: lotfigaiz@gmail.com.

Prof. Dr. Khalid Bouragba received the DESS degree in network and telecom From the University of Chouaib, El jadida, Morocco, in 2002, and Phd degree in informatics (computer science) from the Hassan II University of Casablanca, Morocco, in 2012. Currently, he is a professor and DUT coordinator in the Department of Computer Engineering at the superior School of Technology in Hassan II University of Casablanca, Morocco. He has served as a TPC Co-Chair in SysCoBIoTS 2019, and TPC member in several leading conferences in the field of mobile and wireless communications and collaborative system workflow (WINCOM'23, WINCOM'22, COCIA'2023, COC'2019). He has coauthored several papers published in international journals and conference proceedings. His research interests include distributed computing, workflow interoperability, network and systems management, requirement engineering, and sensor networks. He is a member of the Computer Science and Smart System (C3S) laboratory in Hassan II University of Casablanca. Also, Member of the Moroccan Association of Information Technologies (AMTI). He can be contacted at email: khalid.bouragba@etu.univh2c.ma.

Prof. Dr. Mohammed Ouzzif joined the Higher School of Technology in 1996 as assistant professor. He got his postgraduate doctorate in 1999 at the Faculty of Science of Rabat. In 2005, he defended his Ph.D. in the National Doctorate at the National School of Computer Science and Systems Analysis. His principal's contributions was in the dynamic management of resource sharing in a collaborative system with distributed algorithms allowing the extension of static distributed mutual exclusion algorithms for the support of new joins and departures dynamically. Currently, Mr. Mohammed OUZZIF's research interests concern distributed systems and networks. He has published a considerable number of scientific articles in various journals, conferences and workshops. He is a Steering Committee member of the SYSCO-BIOTS conference, and he served on the Technical Program Committees of several international conferences and workshops, most of which were related to wireless network and distributed systems. In 2021, he founded the C3S laboratory (Computer Science & Smart Systems). He is currently the head of this laboratory and he is a professional member of the IEEE Computer Society. He can be contacted at email: ouzzif@gmail.com.