Computer Communications 198 (2023) 247–261

Contents lists available at ScienceDirect

Computer Communications

journal homepage: www.elsevier.com/locate/comcom

VoIPChain: A decentralized identity authentication in Voice over IP using Blockchain

Mustafa Kara [a,*], Hisham R.J. Merzeh [b], Muhammed Ali Aydın [c], Hasan Hüseyin Balık [b]

[a] Department of Computer Engineering, Air Force Academy, National Defence University, Istanbul, Turkey
[b] Department of Computer Engineering, Yıldız Technical University, Istanbul, Turkey
[c] Department of Computer Engineering, Istanbul University-Cerrahpaşa, Istanbul, Turkey

ARTICLE INFO

Keywords:
Blockchain
VoIP
Authentication
Security

ABSTRACT

Confidentiality, availability, integrity, authentication, and non-repudiation when together became the top priority for secure communication. However, authentication is the first line of defense in all these security parameters. Unfortunately, several authentication mechanisms in the traditional methods cannot provide secure communication due to various vulnerabilities such as single point of failure and privacy issues. Furthermore, key distribution mechanisms such as Certificate Authority (CA) and Trusted Third Party (TTP) distribute keys over the central architecture fail, thus secure communication cannot occur. As a solution to these drawbacks, this paper proposes a new decentralized blockchain-based identity authentication mechanism for VoIP networks, VoIPChain. The proposed scheme utilizes the main features of the blockchain platform, such as immutability, transparency, and fault tolerance, to provide data privacy and secure communication in VoIP applications. The proposed scheme is evaluated as an actual implementation using the virtual Ethereum platform and Python language. The experimental results show that the proposed scheme is an efficient and cost-effective solution for the call process as a decentralized identity authentication system in VoIP. In addition, end-to-end secure call performance outperforms the existing blockchain-based authentication mechanisms by 30%–70% in terms of average time delay. The proposed scheme is almost ten times faster than the TLS process to authenticate between parties. Moreover, compared to fast but less secure basic methods over the SIP authentication the proposed scheme has an acceptable time delay in a call process.

1. Introduction

Voice over Internet Protocol (VoIP) is an internet multimedia application that connects parties over a public network and offers a cost-effective, flexible, reliable and scalable communication infrastructure against early/traditional phone services such as Public Switched Telephone Network (PSTN). It is the most widely used communication module for calls using an internet connection. However, the VoIP application, which is a real-time technology, is exposed to severe attacks because it provides data flow over the public network (Internet) [1–4]. Therefore, security is an important issue, and every VoIP user in the system is a potential vulnerability point [5]. Furthermore, because of the well-known threats of the public network, such as Man in the Middle (MITM) attacks in VoIP applications, there is a reliability issue between parties [6]. Authentication as a security requirement is at the core of secure communication in real-time applications, and due to various vulnerabilities in the public network, it plays a significant role [7]. Moreover, privacy and reliability issues must be revised in VoIP communication [5]. Reliability and privacy may be at greater risk in VoIP communications unless critical management is enforced and maintained because VoIP communications are still improving and do not have dominant standards. Also, the Internet is unreliable, and VoIP cannot function without the Internet. Therefore, the telephony networks will be at greater risk if based on VoIP unless carefully designed and deployed. In this regard, the reliability issues among users regarding security and privacy should be enhanced via authentication. In the call process, the VoIP telephony system must provide privacy, and the system can do so by encrypting all telephony traffic. Furthermore, the key exchange process must be done after a robust authentication among parties.

The first step in VoIP communication setup is ensured by Session Initiation Protocol (SIP), which starts and ends real-time sessions. However, the authentication protocol of SIP is vulnerable to eavesdropping, brute force like password guessing, or server-based spoofing attacks, and it can be exposed to attacks easily [3]. Moreover, SIP cannot provide a validation process sufficient for VoIP networks. One of the

* Corresponding author.
E-mail addresses: mkara@hho.msu.edu.tr (M. Kara), hisham.raad.jafer.al-assedy@std.yildiz.edu.tr (H.R.J. Merzeh), aydinali@istanbul.edu.tr (M.A. Aydın), balik@yildiz.edu.tr (H.H. Balık).

https://doi.org/10.1016/j.comcom.2022.11.019
Received 4 June 2022; Received in revised form 13 September 2022; Accepted 29 November 2022
Available online 5 December 2022

most critical aspects of ensuring SIP security is authentication. Authentication, confidentiality, and integrity in SIP messages are generally provided by using Transport Layer Security (TLS) or other methods like Secure/Multipurpose Internet Mail Extensions (S/MIME) that use a centralized architecture model [2]. These protocols are employed to protect the end-to-end secure communication by using Public Key Infrastructure (PKI) [8].

Traditional centralized security methods such as TLS provide authentication with encryption methods for the trusted networks by performing Trusted Third Party (TTP) or Certificate Authority (CA). Thus, authentication is based on a single-server architecture, in other words, centralized architecture [9]. The centralized architecture is isolated, inconsistent, and lacks privacy and anonymity [10,11]. If the authentication process is centralized, some shortcomings, including fault tolerance and single point of failure, occur in the VoIP network [12]. Moreover, scalability, which is very important for authentication, is the ability of architecture to operate a growing process [13]. Unfortunately, centralized authentication is prone to scalability issues and is not a suitable solution for privacy [14]. In addition, TLS, which is based on a TCP connection between two end hosts, is an end-to-end secure channel, not peer-to-peer encryption to the media session. TLS uses certificates from TTP as an authentication way and can prevent MITM attacks since an attacker should not be able to forge a valid certificate. However, in the case of preferring TLS protocol for the confidentiality and authentication process, the MITM attack could still be a crucial issue for key exchange if the server also needs to support an older version of the protocol.

In the media transport layer, the Secure Real-Time Transport Protocol (SRTP) is the most widely used in the transmission of encrypted multimedia packets. However, the most critical problem in using SRTP is public key distribution after unreliable authentication. Unlike SIP, there is another solution called composed of Z and Real-time Transport Protocol (ZRTP) that utilizes Short Authentication String (SAS) for media over Real-time Transport Protocol (RTP). SAS authentication is a method of authenticating by reading a value between VoIP users. However, this method is ineffective and vulnerable to MITM attacks or forgery threats [15]. For this reason, both users in a call must be authenticated by a robust platform to provide secure key distribution for SRTP protocol. Therefore, the key distribution between legitimate users can only be achieved by authentication, which is the first step of security.

In order to ensure identity authentication between VoIP users in a call without a single-server architecture, this paper integrates the VoIP application with the blockchain environment. Blockchain is preferred because of its qualifications such as transparency, security, immutability, and reliability. The blockchain is a distributed technology that uses cryptographic algorithms, hash methods, and a shared ledger. Due to the blockchain immutable environment [16], identity authentication is tamper-proof. Moreover, unlike single-server authentication architecture, decentralized authentication supplies fault tolerance and withstands deleted credential data. This paper proposes a novel decentralized authentication scheme called VoIPChain using the Ethereum blockchain. VoIPChain is employed to prevent failures and weaknesses in single-server authentication architecture. However, the required security infrastructure must be provided before communication over the insecure public network using robust mutual authentication. The main contributions of this study could be summarized as below.

- This study achieves identity authentication between parties in a call by eliminating centralized architecture such as TTP and CA. Thus, the single point of failure is removed and high fault tolerance is provided. Moreover, the scheme maintains a distributed ledger to prevent unreliability and privacy issues.
- The proposed decentralized authentication mechanism prevents multiple potential attacks in the public networks and guarantees trusted authentication among VoIP users in a call.
- The proposed scheme is compared with the existing single-server architecture process, TLS, and the existing SIP authentication scheme in the literature. Moreover, the end-to-end secure call performance is evaluated between blockchain-based authentication schemes regarding average time delay and security requirements.

This study is organized as follows. Section 2 reviews the related works. Section 3 provides the related background to understand the proposed scheme. Then, the proposed decentralized identity authentication scheme is presented in Section 4. Section 5 explains the implementation part. Experimental results and discussion are given in Section 6. Finally, Section 7 concludes this paper.

2. Related work

In order to provide robust data immutability and reliable verification of identity between entities without the need for a third party in the authentication mechanism, blockchain technology has already been utilized in different areas such as Wireless Sensor Networks (WSNs), Smart Grids, Internet of Things (IoT) and VoIP. In [17], Sheron et al. provide security within the WSN and IoT structure by dividing the direct inter-device decentralized authentication method into two parts device verification and message verification. It provides the security provided by the central authority at the device level with the tree-based (three-based hash) method in blockchain technology. However, it uses CA, which does not scale very well. The single system can become busy processing requests. Having a single system also denotes a potential single point of failure. Also, there is no guarantee for user privacy in the network based on the open channel (internet). Zhihua Cui et al. [18] simplify the network administration by using a hybrid blockchain. The hybrid blockchain model consists of two parts: local blockchain and public blockchain and local means private blockchain. It is also designed for an IoT-based architecture. This model divides the network into parts to prevent single point of failure. However, this model has communication delay. Experimental results show that the time cost is high. Communication delay may not be tolerated in real-time applications like VoIP. Pankaj Kumar and Lokesh Chouhan [19] present a secure authentication method in a smart home system. It shares a predetermined secret key with all the device owners who will access the network by storing it on smart cards and the ID of the person registered in the system. However, central authentication centers are still needed in this case. Debiao He et al. [20], applying a similar study in a different field, VANET architecture, perform the vehicle registration with a value-loaded during the production of the vehicles. Therefore, it needs a central authority for the first key distribution with the pre-loaded values. Although these studies are based on a distributed structure, there is still a need for a centralized system in the first place with decentralized solutions in blockchain solutions.

With cloud-based solutions, authentication becomes slow and less secure. For this reason, [10], which is one of the studies supporting faster computation and distributed structure, proposes an effective model by combining blockchain technology with edge computing. Abdullah Al-Noman Patwary et al. [16] proposed a model suitable for a structure with a high-speed requirement during real-time data transmission. It builds on blockchain technology and device location-based authentication. Since these studies are implemented via energy-constrained devices, the blockchain authentication structure has been created instead of getting approval from a central structure every time.

Digital devices can also access the network without any authentication in open systems. Therefore, [21], which proposes a new evidence-based, secure, and authenticated keyless scheme for smart grids, use blockchain technology for key management. Using blockchain-based smart contracts deployed on a distributed ledger prevents data tampering attacks. Akash Suresh Patil et al. [22] offer a privacy-protected architecture in a similar structure. Authentication in peer-to-peer networks is an element that has increased security in recent years. Sungh-

yuck Hong [23] performs end-to-end authentication between IoT sensor nodes with blockchain technology. This work, which reduces the workload in the blockchain by using the Lightweight protocol, offers a more secure architecture. In addition, some studies show the predisposition of the basic architecture to authentication technology by doing a general review of blockchain studies [24].

It is not easy to compare VoIPChain with other related works for identity authentication in VoIP networks using blockchain due to the scarcity of studies in the related field. Kfoury and Khoury [25], which is one of the few studies, retrieve the public key of the VoIP users using blockchain and provide the authenticity of the retrieved public key. However, every authentication process creates a new block. For this reason, the total call setup time is high. Another identity authentication method using blockchain known as "CallChain" was proposed in [4], which provides end-to-end verification for the caller's real identity. However, their approach is not sufficient in terms of average time delay as it takes about 2 s.

In our previous work in [26], a general peer-to-peer blockchain-based mutual authentication scheme for VoIP applications is proposed. However, this paper proposed a novel decentralized identity authentication for VoIP networks and evaluated it for real-life scenarios with acceptable fault tolerance to provide higher security using Ethereum. Further, providing secure identity authentication is an issue that needs to be analyzed in VoIP networks. SIP original authentication protocol is vulnerable. Therefore, reliable authentication via SIP is not an acceptable level for VoIP. In order to realize fast and secure authentication in a VoIP network, the identity credentials are performed by SIP protocol using a SIP server. Unfortunately, their methods are vulnerable to single-point failure and low fault tolerance [3,27].

3. Preliminaries

This section describes the basic background information needed to explain and analyze the proposed model. The topics are Blockchain and attacks against authentication mechanisms in VoIP, respectively.

3.1. Blockchain

Blockchain is a list of records that provides permanent storage and management of data [28]. The structure of blockchain offers a transparent and decentralized solution [29]. Data is stored in structures called blocks [30]. After the first block record (genesis), all blocks follow. The longer this chain is, the stronger the blockchain system is. The data in the network are kept as peer-to-peer copies over all of the devices as a system [31]. In the blockchain architecture, hiding the information contained in the blocks against attackers is not the main task. Instead, it is the prevention of unauthorized and secret modification of the data kept in the blocks in the blockchain. In this respect, the blockchain, which uses cryptographic hashing functions, provides non-repudiation with its timestamp structure [32].

Approval of every device in the blockchain other than the device that created the transaction must be obtained for transaction validation. The transaction that is not approved within the relevant consensus mechanism algorithm is destroyed. As a result, the requested transaction cannot be performed. This process is called verification in the blockchain. Transactions approved by the consensus mechanism are recorded in blocks with a timestamp. A one-time value is obtained through the relevant consensus mechanism, and this value is associated with the relevant block. The device that finds this value first broadcasts the information to other devices. This process is called mining. In addition, each block creates a chain by keeping the previous block's hash in its structure [33]. The blockchain, which works in a kind of hashed linked list data structure logic, prevents backward transaction changes in this way [25]. Smart contracts are pieces of software code that cannot be changed within the created structure [24]. They run automatically once created. It confirms and validates the transactions on the blockchain during the transaction. It works interactively with block structures in the blockchain.

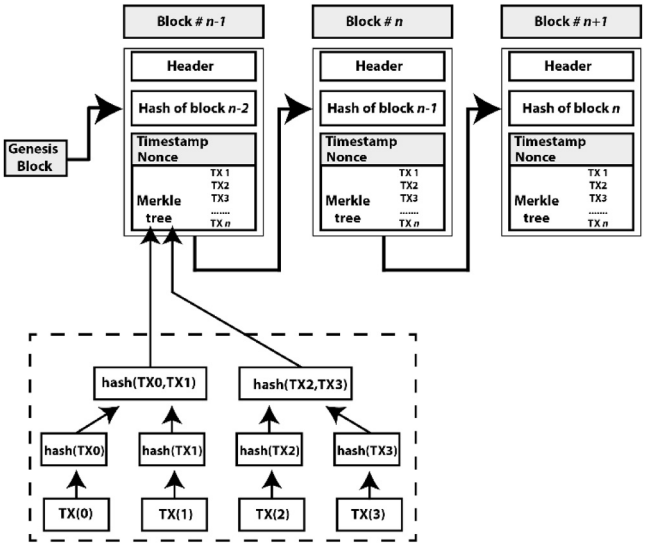

Fig. 1. Basic design of Blockchain: Merkle tree, blocks, and cryptographic techniques.

The basic design of blockchain consists of a Merkle tree where *TX* represents a transaction, blocks, and cryptographic techniques implemented on the network, as shown in Fig. 1.

The blockchain is made of a sequentially connected chain of blocks, in which each relation is an inverse hash point of the previous block. All generated blocks are invalidated if an adversary modifies any previous block in the blockchain. In addition, the Merkle tree has a Merkle root, the hash of all the hashes of all the transactions part of a block. Merkle tree provides data integrity by using Merkle root. Any modifications on any transactions disrupt the original Merkle root and produce a new Merkle root.

Blockchain types are categorized according to scalability, flexibility, permission, and consensus mechanism. There are three types of blockchain. These are, respectively, Public, Private, and Permissioned blockchain. A suitable blockchain type is selected depending on the application requirements. A public blockchain is decentralized. The private blockchain is centralized and partially decentralized is the permissioned blockchain [28].

The preferred blockchain is Ethereum in the proposed VoIPChain. The benefits of using Ethereum are high-performance thanks to the preferred consensus mechanism and low energy consumption. Ethereum allows the system to deploy Smart Contracts, which provide digital agreements. Ethereum dramatically enhances the proposed mechanism because it is a decentralized autonomous digital system, and proof of the transaction is tamper-proof. In addition, the Ethereum blockchain operates with very high transaction throughput as Ethereum has an upper bound on the transaction time, which is achieved by altering the complexity level of the consensus mechanism [14]. The Bitcoin system could perform decentralized authentication for the proposed mechanism in real-life scenarios. However, a round of block generation time in the Bitcoin blockchain network is almost 10 min because of the consensus mechanism known as Proof of Work. The block-generation time is approximately 12–14 s in Ethereum because Ethereum is used through a consensus mechanism called the Proof of Stake.

In this paper, blockchain solves the PKI problem for VoIP. Although authentication exists in VoIP, it is based on single-server architecture models, introducing technical weaknesses in providing security validation. Protocols like MIKEY, SDES, ZRTP and TLS typically perform authentication through an online trusted third-party server. This situation raises the threat of a single point of failure. Blockchain is a decentralized technology that does not require a third party.

3.2. Attacks against authentication mechanism

Detection of attacks against authentication mechanisms allows us to identify every possible threat to the VoIP network [34]. While performing the threat model, it is necessary to correctly categorize the possible attacks and analyze their possible capabilities. This study assumes that an attacker can make the following attack patterns against the proposed system.

Interruption of service: Distributed denial-of-service (DDoS) attack on a system causes a loss of service to users of that system. That is difficult to prevent service interruption against denial of service attacks on certificate authority or authentication servers. On the other hand, the blockchain network provides a secure environment for DDoS prevention [10].

Interception: MITM attack is a cyberattack in which a malicious user secretly transmits and possibly alters the communication between two parties who believe they are communicating directly [16]. Unless the key securely distributes between peers through an authenticated channel, it is a dangerous attack pattern. Eavesdropping defines a method in which an attacker can monitor all signals and flow between two or more VoIP endpoints but cannot modify or alter the data itself. Monitoring for abnormal activity or traffic within the network is a fundamental cybersecurity practice. However, eavesdropping security, a passive attack model, uses some form of authentication for incoming network packets with S/MIME and TLS-like protocols [35].

Modification: A malicious user impersonates an authorized user to steal data, spread malware, or access control systems in Spoofing attack [36]. It is an attack model on unauthorized access, especially in communication systems and multimedia systems such as voice mail. A substitution attack is the modification of the sent message content by the attacker. Changing the content by the attacker causes the communication channel to become unusable. Sybil attack is an attack based on creating fake identities by impersonating original users so that the attacker sends false information to the system. It creates serious damage with an unauthorized access on the authorization side. An impersonation attack typically involves a message that appears to come from a trusted source. A replay attack occurs when the attacker intercepts and uses a message previously used by a legitimate user within the system to infiltrate the communication network [18]. In this attack model, valid data transmission (voice message) is repeated maliciously or fraudulently. For the proposed model, the storage of possible private keys in VoIP application users is carried out by summarizing with hash algorithms. Thus, the study assumes that this private key cannot be obtained even if it is physically compromised and also each object is protected against physical attacks. There are already various methods such as password-based authentication and biotechnology-based authentication to protect them from such attacks by making these private data readable only by the device itself [12].

4. VoIPChain: Decentralized authentication mechanism in VoIP

VoIP provides lower cost and more flexibility in transmission and minimizes communication overhead. The digitized voice data is transmitted over an IP network via VoIP architecture, communication technology. The calling system's full functionality provides a scalable, flexible, and cost-effective communication infrastructure wherever connected to the IP network with this technology. Nevertheless, the connection to the IP network exposes security and privacy vulnerabilities and malicious attacks. In the signaling layer of the VoIP network, ensuring end-to-end authentication between parties (caller and callee) is challenging because of numerous network intermediate devices such as SIP servers. The main purpose of this study is to establish a blockchain-based decentralized authentication system to provide end-to-end secure communication in VoIP applications that realize a call between parties. In addition to calling, any user in a VoIP application can also receive a voice message. For this reason, in the proposed VoIPChain, there are two kinds of authentication processes. The first is the single VoIP user authentication responsible for authenticating users to read the message inbox. The second one is mutual authentication which is the decentralized identity authentication. Mutual authentication is accountable for authenticating two VoIP users to make calls. As a result, the proposed scheme provides a fast, secure, and cost-effective authentication mechanism to the associated users.

In all cases, the first step in a secure VoIP application must authenticate the users and meet VoIP security requirements. Any VoIP user who is not registered on the blockchain network is considered malicious in the proposed scheme. If a VoIP application user is enrolled in the VoIPChain, identity authentication can efficiently occur in real-time. The blockchain platform is the most crucial part of the scheme, including distributed ledger, smart contracts, consensus mechanisms, transparency, scalability, trust management, etc. With this proposed scheme, identity authentication becomes flexible and scalable. The security need of VoIP constitutes an important step in authentication with blockchain integration. The chosen platform for realizing identity authentication is Ethereum as blockchain technology due to its robust structure against data alteration and identity falsification.

4.1. System architecture

This section explains the main components of the proposed authentication method using blockchain. Fig. 2 depicts a summary of the VoIPChain using the blockchain network for authentication in general terms. The caller initializes a transaction to authenticate both callee and its own identity. The blockchain components such as consensus mechanism, distributed ledger, and smart contract are used to authenticate the corresponding VoIP users for setting up a secure IP call. As a general summary of the flow, the VoIPChain scheme lets VoIP users send a registration request to a smart contract to register VoIP user information. The smart contract in blockchain verifies the user information. The blockchain is where pieces of information are stored, and it stores the hash in a secure smart contract. The distributed ledger is used for storing VoIP user information permanently and unalterably.

4.1.1. System components

The VoIPChain comprises six distinct components. These are VoIP Network, Admin, VoIP Users, Blockchain Network, Smart Contracts and Miners.

VoIP network: VoIP network is an IP network that transmits multimedia packets such as voice or video. VoIP enables VoIP users to make voice calls from an IP phone, sometimes called SIP Phone or a VoIP phone. If the VoIP application is installed, any computer, mobile device, or smartphone could be a VoIP Phone.

Admin: Admin is the management device that generates an ID and Ticket for a group of VoIP users to register on the blockchain securely. Each activity is realized by Admin that initializes the smart contract. In addition, an Admin is nominated in the VoIP network among associated VoIP users and the others are called VoIP users. The Admin is a member of the VoIP Network and is not involved in the authentication process in the blockchain after the registration process. Therefore, when Admin is disrupted, the registration process stops in the VoIP network for new users. However, the authentication process is not affected and continues for all registered users.

VoIP Users: A VoIP user is an end system with a SIP phone residing in it. They are called caller and callee. VoIP users' purpose is to make a secure call in an IP network (VoIP network).

Blockchain Network: The proposed scheme's main point is that all VoIP users must be matchlessly identified for secure authentication. In VoIPChain, the blockchain platform is a private blockchain for the sake of simplicity. While evaluating the proposed scheme, the private

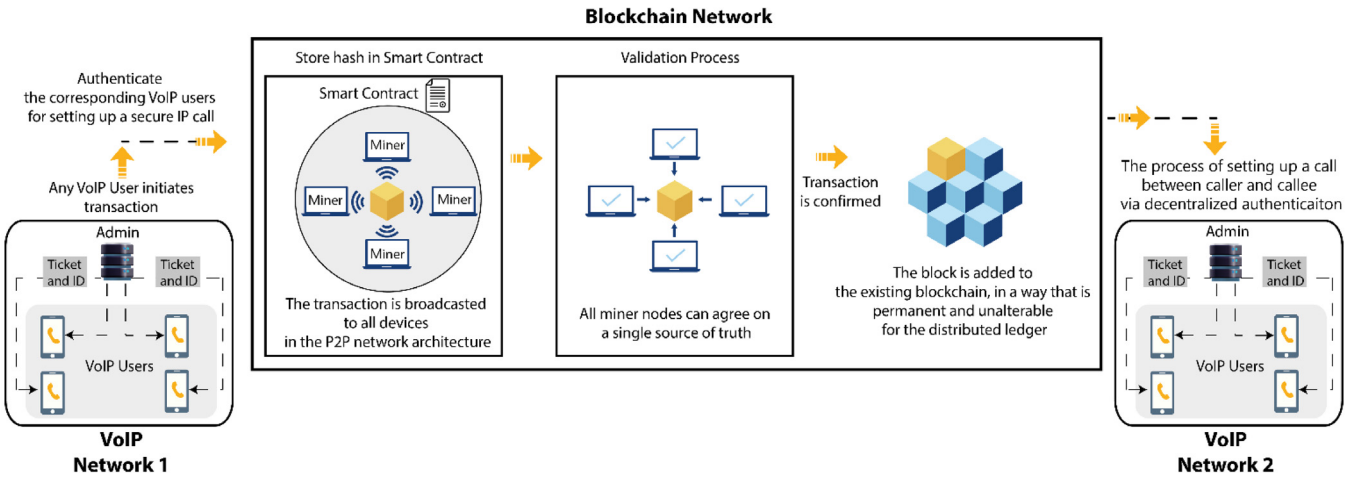

Fig. 2. Architecture of VoIPChain.

blockchain is chosen as it gives more reliable results. However, in the real communication process, public blockchain could be more effective. The public blockchain network is a platform that anyone can join without restrictions. On the other hand, a private blockchain is a platform that can be read by every user but is just written by authorized nodes.

Smart Contract: The piece of code called smart contracts makes blockchain a network for decentralized applications. Once the smart contract validates the content of the message sent by the VoIP user, it will authorize the VoIP user to make transactions in the system.

Miner: There are typically two kinds of nodes in the blockchain. The first kind of node is an inactive node responsible for storing and reading the block data. Inactive nodes cannot construct a new block or initiate a transaction. The second kind of node is the miners which creates a block and validates transactions. Miners in blockchain networks protect the system's security and stability by confirming transactions and keeping copies of the blockchain. All miners can agree on a single source of truth in the network using a consensus algorithm. Through the miners in the blockchain network, the data is fully decentralized, immutable, and reliable. The consensus algorithm needs to provide that all miners in the mechanism accept a single source of validity, even if some miners fail. It ensures fault tolerant. According to the blockchain types, the system selects miners to participate in the network, execute the consensus mechanism and maintain the distributed ledger. The selection of miners is variable for different blockchain types. For example, in the Public blockchain, any node can participate, and the system supports participants joining as miners. On the other hand, in Private blockchain, private deployment chooses the different consensus mechanisms and generally does not need encouragement for participants. Finally, there are restrictions on participating in the blockchain network. In this research, we prefer the private blockchain to test the system. However, the system is built to simulate the public blockchain. For this reason, all participants are accepted as a miner in the VoIP network. The system allows for all participants to join as a miner. However, the user who initiates the transaction has not joined the process as a miner.

In addition, the security and robustness of a blockchain come from its innovative use of hash functions and consensus algorithms. The structure of blockchain allows VoIP users to coordinate in a distributed environment. Thus, a consensus mechanism prevents tampering with a block and recalculates all the hashes of other blocks.

4.1.2. Assumptions

Before explaining the proposed model, it is helpful to examine some assumptions in depth. The following assumptions are considered;

- One VoIP user in the VoIP network is designed as an Admin. Besides, Admin is not a particular VoIP user.
- Admin must be reliable and legitimate to produce reliable tickets and IDs for all VoIP users. In addition, Admin initializes the smart contract for the system function's inception.
- Admin can securely share the signature with this mechanism's legitimate VoIP user device.

4.2. System authentication process

VoIPChain consists of four phases and these are respectively; blockchain association, initialization, registration, and authentication. In this study, a typical smart contract for identity authentication of the VoIP application users, all required functions, and mapping lists for implementing the decentralized authentication system are designed. VoIPChain proposes a corresponding Ticket to verify the VoIP user identity signed information. VoIPChain is a cost-effective and fast authentication scheme is presented, and the total call setup time is not high compared to schemes using blockchain. Also, the single point of failure is the weak connections in the chain that can disrupt the system's operations. Typically, the solution to a single point of failure is to modify the crucial process to not rely on a centralized structure. To solve this limitation, VoIPChain uses blockchain.

As explained below, a list of methods defines the VoIP users communicating with each other and the checking functions and parameters that manage these operations.

A list of methods

//Parameters and functions definition.
Parameter:
Admin: Object //Blockchain's Admin object
Caller: Object// This is a user that request for call
Callee: Object// This is a user that receive for call
Ids : mapping (address=> integer)//mapping table of address to ID (trusted list)
TrustedMember: mapping (integer=> address)// mapping table of ID to address
MsgBox: mapping (integer=> string)// mapping table of ID to message (Inbox of VoIP user)

Function: BcAdminInit(Object Admin)// initialization Blockchain's Admin object

Function: ObjIdExists(Integer ObjId)// check if the object identifier is used in the blockchain or not

Function: ObjAddrExists(Address ObjAddr)// check if the object address is used in the blockchain or not

Function: ControlofTrust(Object Caller, Object Callee)// check if the caller and callee are in the trusted list or not

Function: TicketVerify(Object Caller, Integer Ticket)// check if the Ticket is valid or not

Function: AddTrustedObject (Object Caller)// add new object (VoIP user information) to the trusted list

Function: sendMSG (Object Caller, Object Callee, Text Msg)// add the message to callee's MsgBox

Function: readMSG(Object Caller)// read message from concerned trusted object

Function: Error (String Err)// returns an error message

4.2.1. Flow of VoIPChain

This sub-section offers all the steps in the VoIPChain scheme, which ensures robust, secure, and reliable authentication between VoIP users. All phases of the proposed VoIPChain are depicted in Fig. 3. The overall flow of the proposed identity authentication mechanism is shown in detail. The authentication scheme consists of 6 steps.

Step 1: SIP is utilized for signaling and managing voice communication sessions in IP phones for voice calls. After setting up the VoIP network using SIP, the VoIP users of the VoIPChain scheme first send an association request.

One VoIP user in the VoIP network is designed as an Admin (It owns a private/public key-pair), which can be considered similar to a certification authority. Except for Admin, other users of the VoIP network are called VoIP users (caller or callee). In this paper, we assume that Admin is reliable and legitimate. For this reason, the Admin's certificate is self-signed. After the initialization of the smart contract by Admin, the smart contract authenticates the certificates.

Then, each VoIP user generates its own public–private key pairs in the blockchain association phase. The public/private key pairs are generated using Elliptic Curve Digital Signature Algorithm (ECDSA). The public and private keys generated here are mainly used to verify the integrity of messages sent in the process of registration and authentication. Each VoIP user is provided with a structure called a ticket, representing a lightweight certificate containing a hash form of signed related VoIP user' public key and ID. Admin generates a ticket for each VoIP user to verify their identification, and also, the ticket is generated by a self-signed CA model. The signature certificate represents ECDSA signature using the private key of the VoIP network's Admin. If the Admin fails in the VoIP network, the registration is interrupted for a short time, but the authentication process is not affected for the VoIP users.

Step 2: If the association is successfully completed, the initialization process is done. First, Admin sends an initialization request to a smart contract that validates and checks VoIP user information in the distributed ledger in the blockchain. Smart contracts execute the transactions and agreements between users reliably and consistently by providing flexibility. In addition, the smart contract controls the execution. Transactions in blockchain are traceable and irreversible by all blockchain miners.

Miners handle the verification of the transactions within the block respecting the defined rules. Miners realize the Proof of Stake (PoS) consensus mechanism to validate the added block. After initializing the smart contract, Admin sends a registration request to it. If the request is accepted, the smart contract broadcasts the public key of Admin in the blockchain. The Admin registers the blockchain platform after initiating the smart contract, and the Admin public key is stored in a new block.

Step 3: All VoIP users can send Tickets and ID requests to Admin because Admin is associated and registered in blockchain as a secure device. Therefore, the Admin is an accepted, secure entity by the other VoIP users and creates a new unique ID for every new VoIP user, then generates a relevant Ticket based on the VoIP user's new ID and the public key. After generation, the Admin creates a response to send Ticket and ID information to corresponding VoIP users.

Step 4: After initialization, the registration process begins. All VoIP user information is stored in the blockchain's distributed ledger. A blockchain utilizes two-level cryptography that keeps the data secure. The first is the key-encryption method, and the other is hash functions. Key encryption, a kind of external layer of protection, provides the secure transmission of information from one entity to another. The blockchain cryptographic methods are hash functions, a procedure of irreversible data encryption in a block. All the data in the block is encrypted using the SHA-256 hashing algorithm. Therefore, using two-level cryptography in a blockchain makes the system safer.

The system also uses the hashed data via the smart contract. For registration, a VoIP user sends a Ticket and an ID to the miners in the blockchain network and signs them with a digital signature. Then, the miners send the VoIP user credentials to the smart contract for a verification request. The smart contract checks the VoIP user's credentials to verify the registration. If the VoIP user's information verification is successful, the VoIP user information is stored and added to the trusted list. After registration is complete, the public key of the VoIP user is broadcasted on the blockchain network by miners.

Step 5: After the registration, the authentication process begins. There are two types of authentications in the proposed scheme. The first one is the single VoIP user authentication model. The VoIP user would send a single VoIP user authentication request with the Caller ID signed with a digital key to the Blockchain network to read its voice messages. Smart contract validates and checks the information. If it matches the registered data in the distributed ledger, authentication is done. After the verification process, the authentication information is broadcasted between the miners.

Step 6: Mutual authentication must be done among the VoIP users before an IP call over the public channel. First, the caller creates a signed transaction with the caller's private key. Then, the smart contract validates the caller and callee information with the registered information. The smart contract is responsible for validating the VoIP user by checking its information in the trusted list. Therefore, there is no need for a new block to be created. If the verification is successful, the mapping (trusted list) is broadcasted between miners transparently. Finally, mutual authentication is done, and secure communication is established if the callee agrees with the call.

With these six steps, we presented a brief explanation of the VoIPChain. The VoIPChain comprises four main phases that represent the technical infrastructure of the decentralized authentication mechanism in detail. These phases are (1) Blockchain association, (2) Initialization, (3) Registration, and (4) Authentication.

Phase 1: Blockchain association In Fig. 4 the authors introduced a new layer, the signaling layer which contains the blockchain, key exchange, and authentication phases. All these components are application-based. The SIP protocol is also an application layer protocol. In VoIPChain, the first step is setting up the structure, which consists of a blockchain network and a VoIP network. As shown in Fig. 4, the VoIPChain protocol stack is divided into two layers: Blockchain and SIP signaling phases. The authentication process is performed over the Blockchain network after the SIP protocol establishes the connection between parties in the VoIP application. In VoIP, the signaling layer is an application-layer control system to modify, create, and terminate VoIP sessions with one or more participants and generally uses the SIP protocol for the session process. All the IP phone devices need to be registered to the SIP server to provide calling functions. Then, the SIP protocol initiates the session and establishes the connection among VoIP users. In the proposed

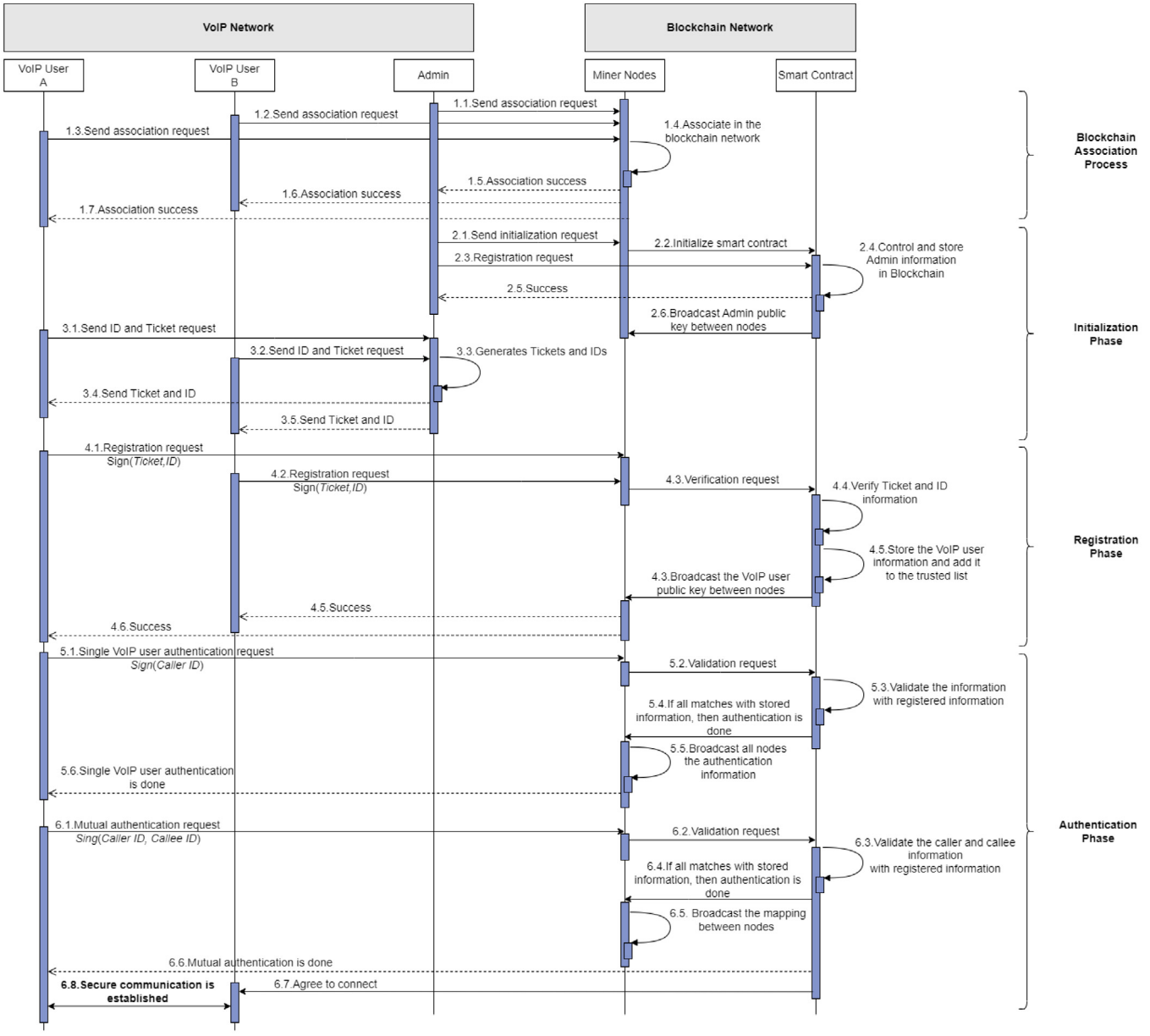

Fig. 3. Overall flow of the proposed authentication scheme.

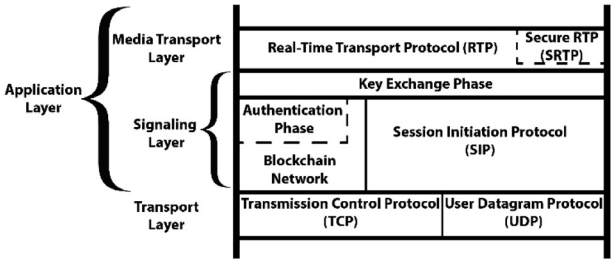

Fig. 4. VoIPChain protocol stack.

VoIPChain, first, the VoIP network processes are realized, such as inviting and trying. Authentication in VoIP calls plays a significant role in establishing trust among VoIP users in the VoIP network. The proposed VoIPChain ensured secure authentication among VoIP users using a blockchain network, simultaneously with the signaling layer. Thus, the key exchange process can be done. The proposed scheme prefers the Elliptic Curve Diffie–Hellman Key Exchange (ECDH) algorithm to establish a secret key. The primary reason to choose ECDH is that it has better performance than other algorithms like Diffie–Hellman in memory usage and execution times. Then SRTP generates a symmetric key for secure peer-to-peer communication in the media transport layer. During the call process, messages are transmitted securely with the RTP protocol.

Each VoIP user initializes the association process to the blockchain network. Admin is the first entity that demands an association with the blockchain network among all VoIP users. All VoIP users and Admin generate an Elliptic Curve (EC) private/public key-pair using ECDSA. ECDSA provides a proper number of benefits according to conventional

signature algorithms such as Rivest Shamir Adleman (RSA) in terms of signature time and key size. ECDSA is a type of the Digital Signature Algorithm (DSA) used on the elliptic curve and sends a signed message between VoIP users, two VoIP users agree on Elliptic Curve domain parameters.

As public-key cryptography, ECC (Elliptic Curve Cryptography) provides security due to its ability to calculate a dot product with an arbitrary point and the inability to find the product given the original curve and multiplication points [10]. ECC is based on how elliptic curves are constructed algebraically over finite fields. Like all asymmetric encryption infrastructures, the ECC method is based on mathematical functions that are simple to compute in one direction but difficult to obtain keys by reversing the process. Therefore, it makes sense to adopt ECC, which performs well in both speed and security, between asymmetric encryption methods using fewer parameters. It provides the same level of security as asymmetric encryption methods, despite the smaller key size, less energy requirement, and fewer parameters used in total encryption. The ECC algorithm is based on the domain parameters. P is a field that the curve is defined over, a and b are the curve's values, G is the generator point, and n is the prime order of G. Then, $n \times G = 0$. Finally, the private key (P_{rk}) is a random value that can be calculated as:

$$1 \leq P_{rk} \leq n - 1 \tag{1}$$

The public key is the elliptic curve dot product of the private key and the base point. The public key is (P_{uk}):

$$P_{uk} = P_{rk} \times G \tag{2}$$

After generating the elliptic-curve public/private key pair, the signed transaction in the registration and authentication processes can be implemented by the VoIP users.

The Admin public key is A_{puk} and the private key is A_{prk}. Admin generates an identity ID_{admin}, as the first 5 digit of the public key. Admin keeps A_{prk} safely and demands registering its identity with the related public key into the blockchain after it is confirmed and validated by the blockchain network. Each public key has an associated timestamp. Admin signs transaction with the related private key and send this transaction to the miners in the blockchain. The signed transaction is given below:

$$Sign_{A_{prk}}(ID_{admin},\ \ Sign_{A_{prk}}(A_{puk},\ timestamp)) \tag{3}$$

When the miners receive the transaction, they verify its integrity by verifying the signature with the Admin public's key:

$$A_{puk}(ID_{admin},\ \ Sign_{A_{prk}}(A_{puk},\ timestamp)) \tag{4}$$

The miners check if the ID_{admin} is used in the blockchain or not. If ID_{admin} has never previously been registered in the blockchain, the information of Admin (ID_{admin}, A_{puk} *and timestamp*) is stored on the blockchain. So, the Admin association process is done.

Phase 2: Initialization. The proposed scheme can be implemented for numerous VoIP users. However, some pre-steps are needed. These steps are;

i. After the successful association process in VoIPChain, Admin initializes the smart contract. The smart contract stores the Admin information in the distributed ledger in the blockchain. The blockchain creates a transaction to broadcasts the Admin public key among the miners in the blockchain network.
ii. In the initialization phase, every VoIP user who requests and takes a ticket from the Admin can register via the smart contract in the blockchain using its public key, ID and ticket.
iii. All public keys of the registered VoIP users are stored in the trusted list. The smart contract contains a set of rules for the data immutability of the trusted list.
iv. The fact that the smart contract manages the trusted list does not mean it can interfere with and change its content. On the contrary, it makes the trusted list transparent for all VoIP users, creates an interface, and makes it available.

Algorithm 1 describes the smart contract initialization rules by Admin that start the smart contract as a manager in the VoIP network. *BcAdmin* represents the Admin. In the initialization phase, the address associated with this BcAdmin object must be empty. In other words, address equals null. If so, the smart contract will store the address of the smart contract initializer (Admin) in the BcAdmin object. Next, the Admin must initialize the smart contract to register by itself. The smart contract will not allow another Admin to register if the Admin is already registered by calling the initialization function, which checks the condition. If the condition is not satisfied, the Admin will not be stored.

Algorithm 1. Initialization rules for smart contract

```
Begin
    if (BcAdmin.address = null) then
            BcAdminInit(Admin)
    else
        return Error ("BlockChain's Admin object is
    already initialized")
End
```

Once initializing these rules via smart contract, Admin is determined, and from this moment, other VoIP users cannot be Admin, and no rule can be modified. In Algorithm 1, the address means the public key.

Phase 3: Registration. As mentioned in the initialization phase, the Admin is determined and registered securely. After the Admin registration, the VoIP users start their registration process. First, each VoIP user sends a ticket request to the Admin using its public key. ECDSA is used to generate the ticket for the VoIP users by Admin. Then, Admin generates a unique ID (ID_{user}) for the corresponding VoIP user. A unique ID is:

$$ID_{user} = universally\ unique\ ID \tag{5}$$

After generating the unique ID, the Admin concatenates the public key and ID. Then, the Admin hashes the concatenation by using the SHA-256 algorithm. P_{uk_u} is the related VoIP user public key and A_{prk} is the private key of Admin. Finally, the Ticket is rendered as:

$$Ticket = Sign_{A_{prk}}\left(hash(P_{uk_u} \parallel ID_{user})\right) \tag{6}$$

The ticket is a hash of the public key and VoIP user ID signed by the Admin. The Admin signs the hash with its private key, and the hash is signed using the ECDSA algorithm. Each ticket is unique per VoIP user. Then, the VoIP user receives the ticket and ID from the Admin and initiates a transaction for a registration request by sending them to the smart contract in the blockchain. The smart contract checks whether the VoIP user's public key and ID are registered before or not. If not, the smart contract checks the ticket for validation with the Admin signature. The smart contract adds the corresponding VoIP user's ID and public key to the trusted list if the ticket is valid. Besides, a response message is sent to acknowledge the related VoIP user about

the registration approval. Finally, the VoIP user is registered and the new VoIP user's information is added to the trusted list. A new block is created to add the transaction report to the block. Algorithm 2 describes the smart contract association rules for registration. This algorithm checks the new VoIP user address (public key) and ID if they are already taken or not, finally checking the validity of the user's ticket to add the users to the trusted list.

Algorithm 2. Association Rules for Smart Contract

```
Begin
    if (BcAdmin.address = 0) then
        return Error ("Admin object is not initialized")

    if (ObjIdExists (obj.id) = true) then
        return Error ("Object Id is used")

    if ObjAddrExists (obj.address) then
        return Error ("Object address is used")

    if (TicketVerify(obj.id, obj.ticket) = failed) then
        return Error ("The Ticket is not valid")

    AddTrustedObject(obj) // if no error appears, add
                new trusted object
End
    // Association finished with success
```

Phase 4: Authentication. In this proposed scheme, some processes are accomplished to perform decentralized authentication between the parties in a VoIP call securely. This study ensures two types of authentication; single VoIP user authentication and mutual authentication. Single VoIP user authentication is a one-sided authentication through the blockchain platform to read voicemail messages. A blockchain-based smart contract validates the voicemail message owner identity before the VoIP user reads the message when a voicemail message is received. In this authentication type, the VoIP user sends the signed public key (P_{uk_u}) and caller ID that is displayed as ID_{user} to the blockchain. When the blockchain receives the transaction, it validates its integrity by validating the signature with the VoIP user's public key. The smart contract controls the ID and public key in the trusted list if the signature is valid to check whether the public key and ID value corresponds. As a consequence, T is accepted as the trusted list, and the authentication process is decided as follows:

$$Auth\left(P_{uk_u}, ID_{user}\right) = \begin{cases} 1, & if\ P_{uk_u}\ and\ ID_{user} \in T \\ 0, & Otherwise \end{cases} \tag{7}$$

The smart contract responds to the VoIP user according to the authentication result. The response can be accepted or rejected.

The second type of authentication is mutual authentication. The caller and callee's credentials must be verified in the blockchain for mutual authentication to ensure a secure voice call. First, the caller sends a transaction that contains the ECDSA signature of the caller's ID and callee's ID using the caller's private key. Then, the smart contract validates the signature and checks the information in the trusted list. If both are registered in the blockchain, mutual authentication is established. The smart contract communication rules to ensure secure authentication in the proposed VoIPChain are described in Algorithm 3.

Algorithm 3. Smart Contract Communication Rules

```
Begin
    if (ObjAddrExists (caller.address) = True AND
ObjIdExists (caller.id) = True AND (ObjIdExists
(callee.id) = True) then

        sendMSG(caller, callee, msg)
    else
      return Error ("Sending Message Error")

    if (ObjAddrExists (callee.address) = True AND
       ObjIdExists (callee.id) = True) then

        readMSG(callee)
    else
     return Error ("Reading Message Error")
End
   // secure data exchange finished with success
```

At the beginning of the call process, the caller does not know the public key of the callee. All public keys of the VoIP users are stored on the blockchain, a robust and immutable storage environment. Thus, a secure key distribution via blockchain is provided for authentication. After the authentication, the blockchain offers the callee's public key with a response message for the approval authentication request. In summary, it is a mutual check process for parties' data (caller and callee) in the trusted list stored in the blockchain network.

The overall authentication process between blockchain and SIP entities in VoIP is shown in Fig. 5. In the proposed VoIPChain, the signaling layer is executed independently of the blockchain network. VoIP network needs a SIP server to set up a call establishment. After the call is initiated by the caller and accepted by the callee with a 200 OK message via the SIP server, identity authentication occurs just before the media transport phase in the blockchain. If the authentication request is validated, mutual authentication is established, and then the caller sends SIP ACK to the callee via the SIP server. The SIP ACK message ensures that the VoIP user receives the last response to an INVITE request. Until now, SIP has established a multimedia session, and the parties have established mutual authentication. Then, the mechanism needs key exchange performed via RTP packets between authenticated parties before calling. The caller utilizes callee's public key and the caller's private key to generate a shared secret. The shared secret can be performed using the ECDH and produces a symmetric key to encrypt data between parties. After a successful key exchange, the secret key is generated [37], and it is used to encrypt messages using a symmetric key algorithm via SRTP [5].

4.2.2. Fault tolerance of VoIPChain

Unlike the single server architecture, the data is stored inside a block in the blockchain network. Computers can calculate hundreds of thousands of hashes per second. Hence, anybody can tamper with a block or recalculate all the hashes of other blocks. Blockchain can mitigate tampering or recalculating the block using a consensus algorithm (Proof of Stake, PoS or Proof of Work, PoW, etc.). Ethereum is generally based on the PoS algorithm to provide consensus between miner nodes. The consensus algorithms set up the nodes making the network more decentralized and secure because the system must be approved by the majority of the network. Malicious people who want to corrupt or manipulate data should have most of the network. Therefore, methods such as the 51% attack are theoretically almost impossible. The fault-tolerance of PoS defined in Eq. (8) shows that VoIPChain is secure against manipulation.

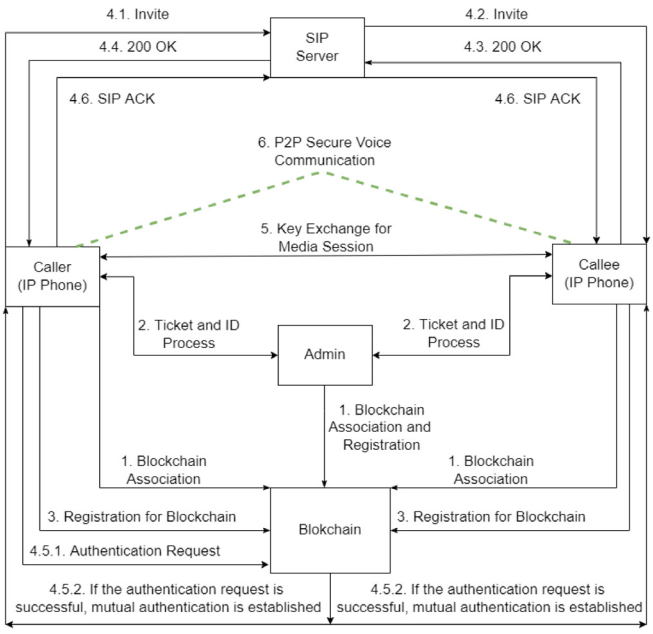

Fig. 5. VoIPChain flowchart.

The consensus process needs an agreement between several agent nodes for a single data value. Some agent nodes could be faulty or unreliable in other ways, so consensus protocols must be fault-tolerant. Each agent node must somehow put forth its candidate values, peer-to-peer communication should be established, and every node agrees on a single consensus value. According to this process, fault tolerance must be calculated to determine the proposed scheme's reliability and scalability. The proposed scheme ensures a relationship between the total nodes (n) and the fault nodes (f). The fault tolerance is given below:

$$f \leq \frac{n-1}{2} \tag{8}$$

5. Implementation

The implementation of VoIPChain, which is the proposed blockchain-based decentralized identity authentication scheme, is explained in this section. This study includes a proof of principle template to demonstrate the VoIPChain scheme's feasibility for VoIP applications. The experimental results and performance are shown in detail in the evaluation results. The preferred technology for the proof of principle implementation was Ethereum as a blockchain [38].

The Ethereum deployment environment was selected to implement our approach and validate the processes. The proposed scheme was developed in a private platform called Ganache as a virtual Ethereum environment to create dummy accounts. Ganache provides an Ethereum environment that simulates the real scenario. Furthermore, the private blockchain, which gives us more accurate experimental results, was preferred instead of the public blockchain platform. In other words, the goal of this implementation is to indicate the usability of the public blockchain network with VoIP applications in the real environment. The smart contract was designed using the Solidity programming language. To compile and deploy the smart contract, we utilized the Truffle, which supports the last version of the Solidity compiler. Moreover, Node.js was used to provide a back-end runtime environment that can run Javascript code outside of a web browser, communication processes, and data transfer between VoIP users. In addition, a collection of libraries was used called Web3 that allows nodes to interact with another Ethereum node through RPC calls. Jason API was preferred to provide an independent platform communication data format. Node.js Express provided the back end for the web application framework that supports Node.js.

6. Evaluation and discussion

This section presents the experimental setup and the performance metrics for the proposed scheme. In this study, experiments were implemented in a simulated scenario to evaluate the performance of the VoIPChain phases, such as ticket generation, registration, and authentication. In addition, the average time delay with different schemes that are both single server architecture and using blockchain in VoIP network was compared. It is noted that the average time delay is related to the Random Access Memory (RAM) size of the test components and the network speed of the test environment. However, the proper test environment was provided to understand its suitability for public blockchain in real-life scenarios. The experiment runs 100 different times and eliminates the effect of external factors by means of employing the test conditions in a virtual environment.

6.1. Experimental setup

The experiments were implemented on a Windows 10 Pro 64-bit operating system with 3 GB Memory and Intel(R) Core (TM)2 Duo CPU T6600 @2.20 GHz. We simulated and tested the proposed scheme in the Ganache-GUI in order to perform the authentication method tests. Ganache is a virtual Ethereum platform to generate virtual Eth Accounts. Ganache is used to test our smart contract during development. In addition, Ganache provides suitable tools like a built-in block explorer and improved mining controls. Truffle is a development platform that can run tests for smart contracts. The default number of accounts in Ganache is 10. On the other hand, the maximum number of accounts that can be generated is 100. The test environment with different 100 accounts to show average times and time delays was implemented. Python language was used in order to show performance evaluation tests between them.

6.2. Performance evaluation

The proposed scheme is evaluated regarding ticket generation, registration, and authentication phases. In addition, the financial cost of the proposed scheme is described.

6.2.1. Ticket generation process

Ticket generation is a lightweight process using a one-way hash function and ECDSA. The hashing data process uses the SHA-256 algorithm, and the ECDSA algorithm is used to sign the Ticket information with Admin's private key. Therefore, ticket generation is not a part of the blockchain platform. For this reason, it does not cost any Ethereum gas. Furthermore, this operation does not need a new block in the blockchain network, which means 0 gas cost. The timing test for requesting and generating the ticket for 100 iterations. The ticket generation process is related to the registration phase. The ticket is a lightweight certificate that proves the identity of the trusted VoIP user.Fig. 6 shows the experimental results for Ticket generation when we ran the experiment with 100 different VoIP users' requests, respectively. Of course, this variation in the ticket request is up to network and hardware performance and response. However, it is variable within an acceptable range, and the average generation time is concise. Also, the ticket generation process is related to the registration phase. The average time of this operation is around 36 ms (ms). The ticket generation time is short compared to all processes in our proposed scheme, which means its approach is proper for VoIP applications.

6.2.2. Registration process

Fig. 7 depicts the experimental results for the registration process in the Blockchain environment. The registration test ran the experiment with 100 different nodes. The registration process creates transactions to store in distributed ledger and requires gas costs. The registration cost is 73,381 gas for each VoIP user, and the registration timing was tested for 100 different nodes. The average registration time is about 1422 ms. Compared with other steps in VoIPChain phases, the registration process requires more time since this operation is based on Blockchain mining. On the other hand, the VoIP user registration data is stored in the blockchain network, immutable and secure. The block-generation time is approximately 12–14 s in Ethereum because Ethereum is used through a consensus mechanism called the Proof of Stake. Besides, the block generation for the registration process does not cause communication delays in a call.

6.2.3. Authentication process

The timing test for a single VoIP user authentication request is tested for 100 iterations. As shown in Fig. 8, the changes in elapsed time with different VoIP users, ranging from 1 to 100, are demonstrated. The VoIPChain authentication process does not need any financial (gas) cost because of not store authentication process information in a blockchain network. The authentication process is 0 gas because there are no transaction blocks for storing data in the blockchain network. The average time for single VoIP user authentication is about 162 ms. In this operation, there is no need for a new blockchain mining process. If the VoIP user is registered to the blockchain platform once, it can authenticate multiple times. It is a process to check for VoIP users' registered data in the trusted list that is the storage field in the blockchain network. The smart contract of the blockchain provides this control.

The second authentication type is the mutual authentication performed between the caller and callee. The timing test for mutual authentication is computed over 100 iterations, and the result is shown in Fig. 9. The average authentication time between caller and callee is about 184 ms. On the other hand, the standard deviation is low in both authentication types, which witnesses the stability of computations. Mutual authentication was run 100 times with a VoIP user and the increase ratio was approximately 13.5% according to single VoIP user authentication. As a result, in VoIPChain, authentication performance does not increase linearly at the same rate as the number of VoIP users increases.

As shown in Figs. 7–9, we evaluated the relationship between the elapsed time and the VoIP User for Transaction Requests. VoIPChain is independent of the VoIP user number since the approach is a peer-to-peer authentication mechanism. The proposed approach serves multiple VoIP users and multiple connections simultaneously. The authentication elapsed time does not increase linearly at the same rate as the number of VoIP users increases. For this reason, any security approach serving this type of real-time system cannot be affected by the number of VoIP users. The proposed method serves multiple VoIP users and connections simultaneously without creating time delays in real-time data transmission. As a result, the VoIP user numbers may not affect the elapsed time.

6.2.4. Financial cost

In this section, the financial cost of the proposed scheme is described. The values of the registration process were obtained using Algorithm 4, which defines the estimated financial cost of the registration process regarding the number of registration transactions for each VoIP user. Ethereum has a currency called Ether (ETH). In the Ethereum blockchain environment, Gas fees are paid with ETH.

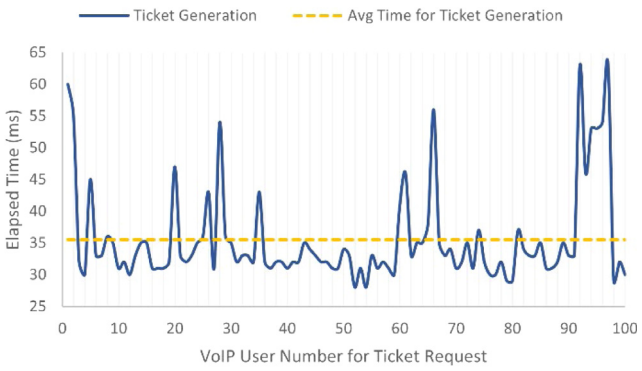

Fig. 6. Experimental result of VoIPChain for ticket generation.

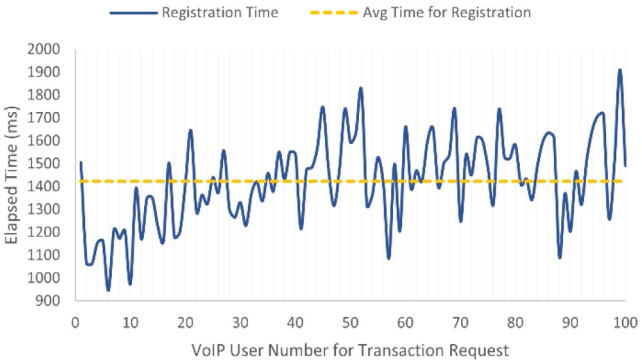

Fig. 7. Experimental result of VoIPChain for registration.

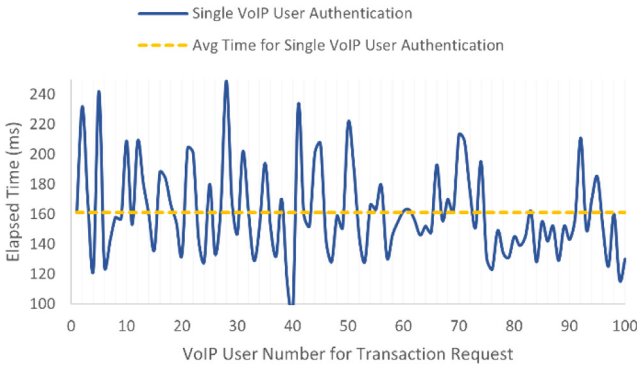

Fig. 8. Single VoIP user authentication results of VoIPChain.

Algorithm 4. VoIPChain Cost Calculator

```
const registration_cost =73381     // gas
const gas_in_Eth = 0.000000001   // gas
const Eth_in_Dollar = $ // current price ETH to Dollar

Function: FinancialCost (double transaction_number)

Begin
    return ((transaction_number * registration_cost) *
gas_in_Eth * Eth_in_Dollar)

End
```

Besides, Gas prices are indicated in Gwei, which is a denomination of ETH. Each Gwei is equal to 0.000000001 ETH (10^{-9} ETH). The real

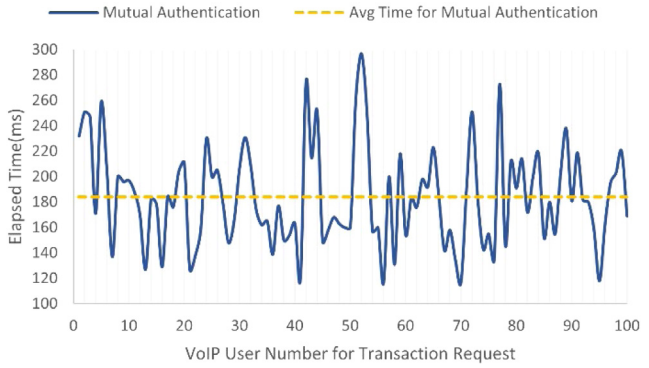

Fig. 9. Mutual authentication results of VoIPChain.

cost is calculated in the dollar by converting the real value of ETH to the dollar. The registration transaction cost of VoIPChain is 73,381 gas which is equal to ETH is calculated as:

$$Eth = Gwei * 10^{-9}$$
$$Eth = 73381 * 10^{-9} \quad (9)$$

According to the current price of ETH ($Eth = 0.000073381$) in the dollar, it is calculated as about (8 Cents at the current price) for each VoIP user registration. The Gas cost is used as a registration fee for any VoIP user. In addition, it is used for mining blocks when the system needs to create a new block for any transaction. The proposed scheme prevents spoofing IDs by charging a fee for all calculations executed in the registration phase. Briefly, Gas fees contribute to blockchain network security, but Gas does not mean keeping the system secure. For example, the attacker will pay Gas if they want to launch the attack. The financial cost system is meant to keep VoIP users reliable and legitimate in the blockchain.

6.3. comparison

This section compares VoIPChain with other schemes according to time delay. These schemes use single-server authentication methods and blockchain-based methods. The proposed VoIPChain is compared with the SIP-TLS process, which uses the centralized structure, and the existing schemes using the SIP authentication method. In addition, the effectiveness of VoIPChain is demonstrated by comparing it to the blockchain-based methods in VoIP.

6.3.1. Comparison with single-server authentication methods

VoIPChain can avoid some limitations of the centralized system, like a single point of failure or privacy, and improve the VoIP system security. The proposed decentralized authentication mechanism prevents multiple potential attacks in the public networks and guarantees trusted authentication among VoIP users in a call.

TLS ensures confidentiality, integrity, and authenticity. With the confidentiality is provided that no entity (CA or TTP) can know what is being sent. With the integrity is provided that no entity (CA or TTP) can change the messages without being detected. With the authenticity is provided that no entity (CA or TTP) can impersonate one of the communicating parties. TLS provides an end-to-end security channel and combines a series of cryptographic functions. However, it does not mean TLS is peer-to-peer technology. TLS protects the exchange end-to-end when transmitting voice data. The structure of TLS for a secure VoIP network is shown in Fig. 10. TLS does not afford complete peer-to-peer confidentiality to the media transport layer for the voice packets.

One of the best options is using the SIP-TLS process to confirm that the identity data has not been tampered with and destroyed in

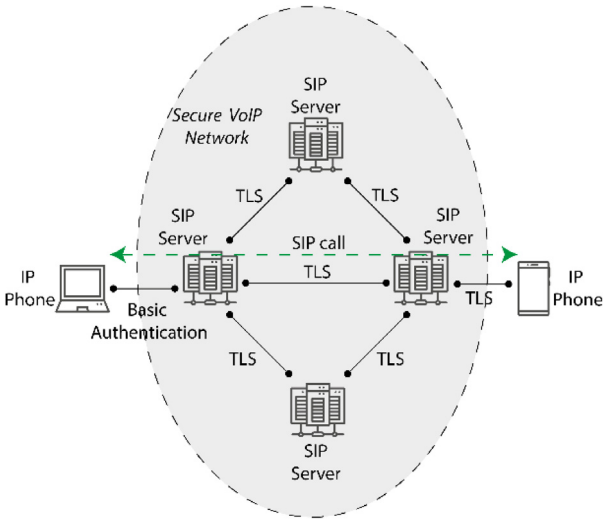

Fig. 10. The structure of TLS for secure VoIP network.

a VoIP call. Mutual authentication is a part of the TLS process. In this experiment, TLS v.1.3, the highest TLS certificate that could be set up on the VoIP user device, was used. The average time delay for TLS certificate validation is about 2056 ms. In addition, if the system prefers the TLS process for identity authentication, this validation must also be realized in each call process. This process causes a time delay in VoIP applications that transmit real-time data.

The upper line in Fig. 11 shows the experimental result for the TLS process. Authentication average time delay of the TLS process is about 2217 ms for 100 different nodes. Fig. 11 shows the experimental result of the authentication process comparison between the TLS process and the proposed scheme, VoIPChain. The result demonstrates that VoIPChain is about 10 times faster in terms of average time delay than TLS, which is the equivalent process. In addition to increased fault tolerance, elapsed time for the authentication process is also increased in the TLS process.

VoIPChain average registration time is about 1422 ms, and any VoIP user can register once in the system. TLS requires a registration for every authentication. Unlike TLS, VoIP users can authenticate multiple times after successful registration in VoIPChain. Moreover, the registration process does not occur during the call process. Therefore, the required time for registration operation is not related to the following authentication processes, and registration time is not added to the authentication time. Also, the call time is an acceptable range for VoIP calls. For this reason, the average authentication time of the proposed VoIPChain is 184 ms and is faster than TLS.

As shown in Fig. 12, compared with methods in the literature using SIP authentication, the average authentication time of the Yeh et al. [27] scheme is about 110 ms. In comparison, Zhang et al. [3] scheme is about 70 ms. However, the average time for a single VoIP user authentication is about 162 ms in VoIPChain. According to these results, Zhang's protocol utilizes only a one-way hash function and exclusive-or operations during the authentication process, achieving the best performance. Although the protocol of Yeh et al. [27] and Zhang et al. [3] reduces average authentication time significantly, their protocol has some security weaknesses such as single point of failure, poor fault tolerance, and privacy issues. The proposed scheme is slightly slower than Yeh et al. [27] and Zhang et al. [3] schemes that used single server authentication methods over SIP but it is still an acceptable range in a call process. The results (shown in Figs. 11 and 12) show that the TLS protocol is the slowest authentication method among compared schemes because TLS is composed of two-part, the Record part and the Handshake part. The Record part is used for encryption, and the three-way handshake part is used for authentication.

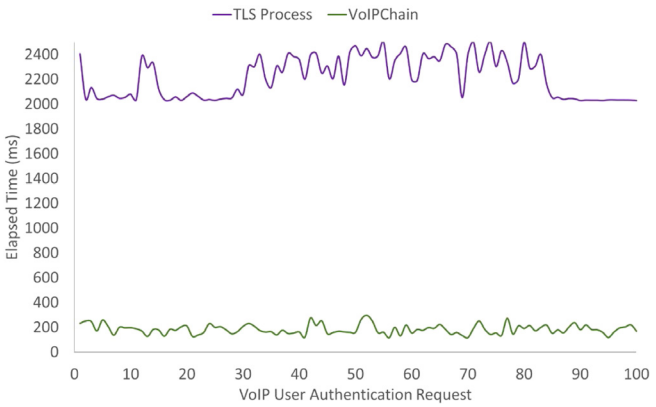

Fig. 11. Comparison between TLS and VoIPChain.

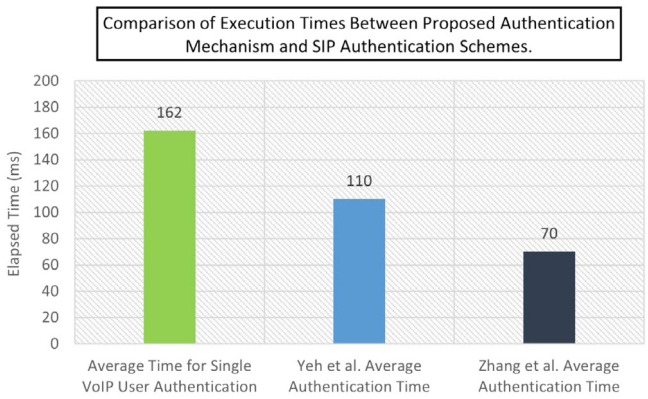

Fig. 12. Comparison with existing SIP authentication schemes.

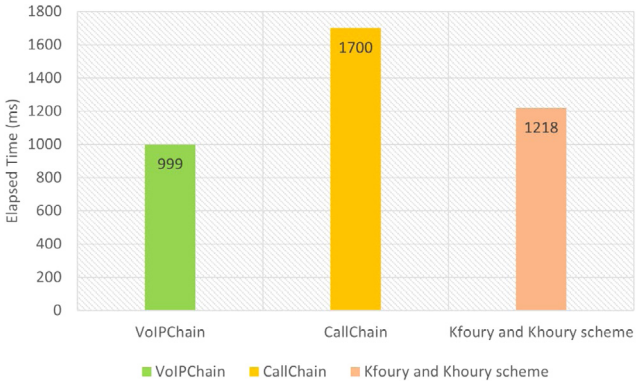

Fig. 13. Average call establishment time comparison with authentication schemes using blockchain.

The main reason for the massive difference between VoIPChain and TLS protocol is that the handshake part performs cipher suite (public key), block cipher encryption, hashing, and compression methods. Moreover, the Record part fulfills ZIP for data compression, Hash with Message Authentication Code (HMAC), and the block cipher's cipher block chaining (CBC) mode, contributing to the highest time delay. In addition, TLS utilizes certificates (X.509) from a single server for mutual authentication. Moreover, its robustness, reliability, security, and fault tolerance are more appropriate for VoIP applications with higher reliability requirements. The proposed scheme eliminates the complexity of SIP security and the CA or TTP issues.

VoIPChain is a decentralized, fast and reliable method with low energy consumption. Although the proposed VoIPChain scheme's time complexity ($O(n)$) is higher than the centralized scheme ($O(1)$), its security and robustness are reliable and more suitable for real-time application scenarios with higher security requirements. Because the decision strategy or consensus of VoIPChain is PoW, the centralized scheme uses the single server system. Moreover, VoIPChain's fault tolerance is $2f + 1 \leq n$. However, the centralized fault tolerance is 1 and is not acceptable for VoIP.

Blockchain rapidly distributes public keys between VoIP users and excludes the threat of data manipulation. This is its main advantage over the present PKI. Traditional key distribution mechanisms often store revoked certificates, making it difficult to inform other users that a given certificate is no longer valid. However, the proposed authentication mechanism significantly simplifies this. VoIPChain can quickly share public keys encrypted using ECDH while eliminating the risks of public channels. This unique key distribution environment is based on the Ethereum blockchain platform. For the public key information, a keyring is created and stored on the blockchain, which is immutable, and all VoIP users can check the public key on the chain.

6.3.2. Comparison with blockchain-based methods

As shown in Fig. 13, schemes that perform identity authentication using blockchain in the VoIP network are compared with the VoIPChain. For example, Kfoury and Khoury [25] scheme's total call setup time is calculated as 1218 ms to set up an end-to-end secure call process between VoIP users. In this scheme, in a call setup time, key retrieval from the blockchain, asymmetric encryption (encryption with public key and decryption with private key), SIP signaling, symmetric key generation, and symmetric key generation for SRTP protocol are performed step by step. Callchain total call setup time is 1700 ms for 4G and 1600 ms for WIFI to set up an end-to-end secure call process between parties using Ethereum. The time latency of these schemes is mainly affected by the overall flow of the proposed authentication design with the blockchain network. For example, generating a new block in a blockchain network by miners takes time and slows down all the processes.

In the signaling layer, the order of operations is significant because the correct sequence of steps minimizes time delay while integrating blockchain for authentication. Also, the flow of call establishment should be handled carefully. In VoIPChain, SIP signaling works independently of the blockchain network. After the call is initiated by the caller and accepted by the callee, the authentication occurs just before the media transport phase in VoIPChain. VoIPChain does not create a new block for every authentication process. Only the registration process generates transactions for storing data in a distributed ledger. Thus, a cost-effective and fast authentication scheme is presented, and the total call setup time is not high compared to schemes using blockchain. Call setup is composed of two parts in the signaling layer of VoIP networks. The first part is the SIP INVITE phase, after which the callee accepts the call request. Next, the second part is started. Thus, a call process is established from OK messages to ACK messages between VoIP users. These two parts need a SIP server to set up a call establishment. According to experimental results, VoIPChain average total call setup time takes about 999 ms to set up an end-to-end secure call process between VoIP users. The average time from Invite to Ringing is about 295 ms, and from OK to ACK, the average time is about 350 ms in the signaling layer. The average mutual authentication time between caller and callee is about 184 ms in the blockchain network. The average time of the ECDH algorithm is taken about 170 ms for key exchange. As a result, the total average time in VoIPChain is approximately 28% faster than Kfoury and Khoury's scheme as the time delay for VOIP call setup. Likewise, CallChain is approximately 70% slower than the VoIPChain scheme. 70% ratio increase in the call setup time could be perceptible to the end-user. Real-time application availability like VoIP is up to internet bandwidth and RAM size. For this reason, security methods such as authentication must be done as soon as possible in the application.

7. Conclusion

The use of VoIP applications is increasing due to their convenience in communication. As a result, the reliance mechanism between caller and callee should be performed securely. This study proposed a decentralized identity authentication model by combining VoIP and Ethereum blockchain. Thus, the proposed VoIPChain realizes a robust and secure identity authentication by ensuring public key distribution among users. VoIPChain scheme solves the privacy and reliability issues in the centralized authentication model. It provides scalable and fault-tolerant authentication solutions with a decentralized blockchain architecture in VoIP networks. In this study, the blockchain platform is combined with the VoIP network. Thus, a key distribution was provided to ensure secure authentication. Using smart contracts, consensus algorithms, distributed ledgers, and cryptographic algorithms, which are the key features of the blockchain, a robust authentication model against well-known threats was presented.

VoIP calls and voicemail messages are data packets susceptible to IP network attacks. In VoIPChain, the authentication is secure because the proposed mechanism uses the trusted list, the tamper-proof record list in the distributed ledger, as a reference for all registered VoIP users. The smart contract manages the trusted list to check the VoIP users' information validation. Also, it verifies the digital signature of the transaction for authentication. Therefore, the block is not created for calling information between VoIP users in the blockchain. This makes our system faster and more practical. Furthermore, the security system is not affected because the trusted list is used by nodes when a transaction is sent to the blockchain, and nodes check the transaction information using consensus mechanisms. Every node uses consensus mechanisms to prove transactions by themselves.

Furthermore, the proposed model is compared to the single-server authentication methods and blockchain-based schemes. According to the experimental results, the VoIPChain mechanism is more flexible and resistant to attacks than centralized authentication models and emerges as a cost-effective solution for the VoIP application. Time delay and fault tolerance is the effective parameter in a secure call establishment. VoIPChain is more successful than similar schemes using blockchain in terms of time delay. Moreover, this study reduces fault tolerance without compromising time complexity.

Many mechanisms can provide offline authentication, like the certificate-based approach. The trusted third party can be either online or offline. TTP can be offline with this approach, and there will be no single point of failure issue. Undoubtedly, TTP should be trusted, and the proposed approach also needs Admin to be trusted. However, the proposed approach is an obvious advantage over current solutions. An online TTP intervenes in every transaction between the parties, while an offline TTP intervenes only in the case of a conflict. In addition, an online TTP can become a communications bottleneck, adding more tasks and calculations to the protocol. On the other hand, a single point of failure limitation is another issue in the case of using an online TTP server. This is not acceptable for VoIP provides real-time conversation syncing. It might also be challenging to find an offline TTP for both the caller and the callee. A single point of failure refers to a system element that can interrupt the whole network from executing if it crashes, which is undesirable in any structure for performing high availability and reliability. The distributed structure of blockchain is a potential solution to issues with a single point of failure and bottleneck.

VoIP users create a signed transaction containing a timestamp and public key with VoIP user ID. The information is verified and distributed across all the miners and linked to previous blocks stored on the trusted list as a distributed ledger. The digital signature is used to determine if someone edits a piece of information after the VoIP user signs it and is a mathematical method used to check the authenticity and integrity of a transaction on the blockchain. An adversary cannot retrieve a VoIP user's ID and Ticket. Therefore, it is almost impossible to spoof the cryptographic method like digital signature and hashing that made the blockchain immutable. The basic structure of the proposed VoIPChain ensure a secure platform against attacks such as DDoS, Spoofing, Substitution, Sybil, Impersonation, and Replay attack. Furthermore, VoIP users' key exchange is provided successfully before the media sessions were encrypted, making MITM or Eavesdropping attacks almost impossible.

In the future, we intend to extend VoIPChain and apply multiple authentication processes to be enhanced secure connection establishment between parties in conference calls.

CRediT authorship contribution statement

Mustafa Kara: Conception and design of study, Acquisition of data, Analysis and/or interpretation of data, Writing – original draft, Writing – review & editing. **Hisham R.J. Merzeh:** Conception and design of study, Acquisition of data, Analysis and/or interpretation of data, Writing – original draft, Writing – review & editing. **Muhammed Ali Aydın:** Conception and design of study, Analysis and/or interpretation of data, Writing – original draft, Writing – review & editing. **Hasan Hüseyin Balık:** Conception and design of study, Writing – original draft, Writing – review & editing.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article.

Acknowledgments

All authors approved version of the manuscript to be published.

References

[1] G. Bella, P. Biondi, S. Bognanni, Multi-service threats: Attacking and protecting network printers and VoIP phones alike, Internet Things (2022) 100507.

[2] P.K. Dhillon, S. Kalra, Secure and efficient ECC based SIP authentication scheme for VoIP communications in internet of things, Multimedia Tools Appl. 78 (16) (2019) 22199–22222.

[3] L. Zhang, S. Tang, S. Zhu, An energy efficient authenticated key agreement protocol for SIP-based green VoIP networks, J. Netw. Comput. Appl. 59 (2016) 126–133, http://dx.doi.org/10.1016/j.jnca.2015.06.022.

[4] Y. Chen, Y. Wang, Y. Wang, M. Li, G. Dong, C. Liu, CallChain: Identity authentication based on blockchain for telephony networks, in: 2021 IEEE 24th International Conference on Computer Supported Cooperative Work in Design, no. Did, CSCWD, May 2021, pp. 416–421, http://dx.doi.org/10.1109/CSCWD49262.2021.9437650.

[5] R. Dantu, S. Fahmy, H. Schulzrinne, J. Cangussu, Issues and challenges in securing voip, Comput. Secur. 28 (8) (2009) 743–753, http://dx.doi.org/10.1016/j.cose.2009.05.003.

[6] R. Pecori, L. Veltri, 3AKEP: Triple-authenticated key exchange protocol for peer-to-peer VoIP applications, Comput. Commun. 85 (2016) 28–40, http://dx.doi.org/10.1016/j.comcom.2016.04.005.

[7] I. Alqassem, D. Svetinovic, A taxonomy of security and privacy requirements for the internet of things (IoT), in: 2014 IEEE International Conference on Industrial Engineering and Engineering Management, Dec. 2014, Vol. 2015-Janua, pp. 1244–1248, http://dx.doi.org/10.1109/IEEM.2014.7058837.

[8] Y.P. Liao, S.S. Wang, A new secure password authenticated key agreement scheme for SIP using self-certified public keys on elliptic curves, Comput. Commun. 33 (3) (2010) 372–380, http://dx.doi.org/10.1016/j.comcom.2009.10.005.

[9] K. Khacef, G. Pujolle, Secure peer-to-peer communication based on blockchain, in: Advances in Intelligent Systems and Computing, vol. 927, Springer International Publishing, 2019, pp. 662–672.

[10] S. Guo, X. Hu, S. Guo, X. Qiu, F. Qi, Blockchain meets edge computing: A distributed and trusted authentication system, IEEE Trans. Ind. Inform. 16 (3) (2020) 1972–1983, http://dx.doi.org/10.1109/TII.2019.2938001.

[11] C. Lin, D. He, N. Kumar, X. Huang, P. Vijayakumar, K.-K.R. Choo, HomeChain: A blockchain-based secure mutual authentication system for smart homes, IEEE Internet Things J. 7 (2) (2020) 818–829, http://dx.doi.org/10.1109/JIOT.2019.2944400.

[12] M. Zhaofeng, M. Jialin, W. Jihui, S. Zhiguang, Blockchain-based decentralized authentication modeling scheme in edge and IoT environment, IEEE Internet Things J. 8 (4) (2021) 2116–2123, http://dx.doi.org/10.1109/JIOT.2020.3037733.

[13] M.T. Hammi, B. Hammi, P. Bellot, A. Serhrouchni, Bubbles of trust: A decentralized blockchain-based authentication system for IoT, Comput. Secur. 78 (2018) (2018) 126–142, http://dx.doi.org/10.1016/j.cose.2018.06.004.

[14] U. Khalid, M. Asim, T. Baker, P.C.K. Hung, M.A. Tariq, L. Rafferty, A decentralized lightweight blockchain-based authentication mechanism for IoT systems, Cluster Comput. (2020) 1–21.

[15] Christoforos Ntantogian, et al., A survey of voice and communication protection solutions against wiretapping, Comput. Electr. Eng. 77 (2019) 163–178.

[16] A.A.N. Patwary, A. Fu, S.K. Battula, R.K. Naha, S. Garg, A. Mahanti, FogAuthChain: A secure location-based authentication scheme in fog computing environments using blockchain, Comput. Commun. 162 (December 2019) (2020) 212–224, http://dx.doi.org/10.1016/j.comcom.2020.08.021.

[17] P.S.F. Sheron, K.P. Sridhar, S. Baskar, P.M. Shakeel, A decentralized scalable security framework for end-to-end authentication of future IoT communication, Trans. Emerg. Telecommun. Technol. 31 (12) (2020) 1–12, http://dx.doi.org/10.1002/ett.3815.

[18] Z. Cui, et al., A hybrid BlockChain-based identity authentication scheme for multi-WSN, IEEE Trans. Serv. Comput. 13 (2) (2020) 241–251.

[19] P. Kumar, L. Chouhan, A secure authentication scheme for IoT application in smart home, Peer-To-Peer Netw. Appl. 14 (1) (2021) 420–438, http://dx.doi.org/10.1007/s12083-020-00973-8.

[20] Q. Feng, D. He, S. Zeadally, K. Liang, BPAS: Blockchain-assisted privacy-preserving authentication system for vehicular Ad Hoc networks, IEEE Trans. Ind. Inform. 16 (6) (2020) 4146–4155, http://dx.doi.org/10.1109/TII.2019.2948053.

[21] H. Zhang, J. Wang, Y. Ding, Blockchain-based decentralized and secure Keyless signature scheme for smart grid, Energy 180 (2019) 955–967, http://dx.doi.org/10.1016/j.energy.2019.05.127.

[22] A.S. Patil, R. Hamza, A. Hassan, N. Jiang, H. Yan, J. Li, Efficient privacy-preserving authentication protocol using PUFs with blockchain smart contracts, Comput. Secur. 97 (2020) 101958, http://dx.doi.org/10.1016/j.cose.2020.101958.

[23] S. Hong, P2P networking based internet of things (IoT) sensor node authentication by blockchain, Peer-To-Peer Netw. Appl. 13 (2) (2020) 579–589, http://dx.doi.org/10.1007/s12083-019-00739.

[24] D. Minoli, B. Occhiogrosso, Blockchain mechanisms for IoT security, Internet Things (Netherlands) 1–2 (2018) 1–13, http://dx.doi.org/10.1016/j.iot.2018.05.002.

[25] E.F. Kfoury, D.J. Khoury, Secure end-to-end VoIP system based on ethereum blockchain, J. Commun. 13 (8) (2018) 450–455, http://dx.doi.org/10.12720/jcm.13.8.450-455.

[26] M. Kara, M. Ali Aydın, H. Hüseyin Balık, Bcvop2p: Decentralized blockchain-based authentication scheme for secure voice communication, Intell. Autom. Soft Comput. 31 (3) (2021) 1901–1918, http://dx.doi.org/10.32604/iasc.2022.021309.

[27] H. Yeh, T. Chen, W. Shih, Robust smart card secured authentication scheme on SIP using elliptic curve cryptography, Comput. Stand. Interfaces 36 (2) (2014) 397–402, http://dx.doi.org/10.1016/j.csi.2013.08.010.

[28] H.N. Dai, Z. Zheng, Y. Zhang, Blockchain for internet of things: A survey, IEEE Internet Things J. 6 (5) (2019) 8076–8094.

[29] M. DI Pierro, What is the blockchain? Comput. Sci. Eng. 19 (5) (2017) 92–95, http://dx.doi.org/10.1109/MCSE.2017.3421554.

[30] T. Ahram, A. Sargolzaei, S. Sargolzaei, J. Daniels, B. Amaba, Blockchain technology innovations, in: 2017 IEEE Technology and Engineering Management Society Conference, TEMSCON 2017, Jul. 2017, pp. 137–141, http://dx.doi.org/10.1109/TEMSCON.2017.7998367.

[31] T. Salman, M. Zolanvari, A. Erbad, R. Jain, M. Samaka, Security services using blockchains: A state of the art survey, IEEE Commun. Surv. Tutor. 21 (1) (2019) 858–880, http://dx.doi.org/10.1109/COMST.2018.2863956.

[32] A.I. Sanka, M. Irfan, I. Huang, R.C.C. Cheung, A survey of breakthrough in blockchain technology: Adoptions, applications, challenges and future research, Comput. Commun. 169 (January) (2021) 179–201, http://dx.doi.org/10.1016/j.comcom.2020.12.028.

[33] O. Novo, Blockchain meets IoT: An architecture for scalable access management in IoT, IEEE Internet Things J. 5 (2) (2018) 1184–1195, http://dx.doi.org/10.1109/JIOT.2018.2812239.

[34] U.U. Rehman, A.G. Abbasi, Security analysis of VoIP architecture for identifying SIP vulnerabilities, in: 2014 International Conference on Emerging Technologies, no. ii, ICET, Dec. 2014, pp. 87–93, http://dx.doi.org/10.1109/ICET.2014.7021022.

[35] M.Z. Gunduz, R. Das, Cyber-security on smart grid: Threats and potential solutions, Comput. Netw. 169 (2020) 107094, http://dx.doi.org/10.1016/j.comnet.2019.107094.

[36] J. Carrillo-Mondéjar, J.L. Martinez, G. Suarez-Tangil, On how VoIP attacks foster the malicious call ecosystem, Comput. Secur. (2022) 102758.

[37] F. Hendaoui, H. Eltaief, H. Youssef, UAP: A unified authentication platform for IoT environment, Comput. Netw. 188 (2021) 107811.

[38] Gavin Wood, Ethereum: A secure decentralised generalised transaction ledger, Ethereum Proj. Yellow Pap. 151 (2014) 1–32.