Real Impact of the Blockchain in Securing a ToIP Network

Sekoude Jehovah-nis Pedrie Sonon, Institut d'Innovation Technologique, Université d'Abomey-Calavi, Benin*
https://orcid.org/0000-0003-2271-1631

Tahirou Djara, Institut d'Innovation Technologique, Université d'Abomey-Calavi, Benin

Matine Abdoul Ousmane, Institut d'Innovation Technologique, Université d'Abomey-Calavi, Benin

Abdou-Aziz Sobabe, Institut d'Innovation Technologique, Université d'Abomey-Calavi, Benin

ABSTRACT

Telephony over IP (ToIP) is a cost-saving communication technology based on voice over IP (VoIP) that enables enterprises to reduce communication fees. However, ToIP faces many security threats due to its IP-based nature. This work aims to improve ToIP security using cryptography and blockchain technology. The authors propose a secure approach to user registration, authentication, communication session establishment, and communication data storage. The proposed solution leverages blockchain technology to ensure the integrity, confidentiality, and availability of communication data. By implementing this solution, the researchers aim to enhance the security of ToIP networks and protect them from cyber threats. This approach provides a secure and reliable way to support ToIP services while preserving confidentiality and privacy.

KEYWORDS

Blockchain, Cryptography, Security, Telephony over IP (ToIP), Voice over IP (VoIP)

INTRODUCTION

Telephones are an important tool in the business world. It's the principal source of contact between enterprises and customers. Since its creation in 1876 by Alexander Graham Bell *(*https://www.history.com/this-day-in-history/alexander-graham-bell-patents-the-telephone***, 2022),*** telephone use hasn't ceased to increase. So telephonic communication takes a great place in enterprise development, and then, country development. The report is that, with traditional telephony, we spend more and more on our telephonic communications. The table below, published in November 2021 in the annual activities report of RAECP (Regulatory Authority for Electronic Communications, posts and Press distribution) in Benin, presents mobile telephonic traffic evolution from 2019 to 2020 in Benin Republic.

DOI: 10.4018/IJSPPC.324165

*Corresponding Author

Table 1. Mobile telephonic traffic evolution from 2019 to 2020 (RAECP BENIN, 2021)

Designations	2019	2020	Tendencies
Intra network traffic (in minutes)	3 795 312 233	3 913 566 886	3,1%
National outgoing traffic (in minutes)	1 617 239 901	1 642 941 183	1,6%
National incoming traffic (in minutes)	1 661 100 686	1 659 876 456	- 0,1%

Source: (Operators Data, 2020)

In 2020 in Benin Republic, the intra network traffic was 3 913 566 886 minutes (or 234 814 013 160 FCFA for 1 franc/s); in other words, intra network voice traffic and national outcoming voice traffic have known respectively increasing of 3.1% and 1.6% of volume comparatively to 2019. Although considerable efforts are done in order to improve telephonic communication fees, the question remains: How can we reduce telephonic communication fees ?

The merger of IT and telephonic networks that has been done since 17 years has considerably upset the telephony world. With this merger, we talk of Telephony over IP which needs, before all, great skills in systems, networks and telecommunication fields. Voice over IP is a complex field comprising a lot of essential concepts to know, before installing your own telephone system based on a free telephone switchboard. VoIP is a technology continuously used by a large number of users and businesses to transmit voice communications and multimedia sessions over the IP protocol. ***(Félix Meloche, 2016)***.

The American Center for Technological Innovation and the Brookings Institution have studied the use of free VoIP applications (whatsapp, messenger, etc.) and have found that the use of such applications adds 0.23% to national Gross National Product (GNP). Concerning Morocco, the American center assured that the non-use of VoIP applications (for around 11 months) caused the national economy to lose around 320 million dollars. ***(Center for Technology Innovation for Brooking, 2016)***

As)any technology is not without drawbacks, VoIP encounters security networks problems. The goal of our study is to use blockchain technology to enhance security in VoIP networks. The major problems encountered in IP telephony include vulnerable authentication which leads to identity theft, listening to the network and therefore calls through applications such as wireshark and ettercap (violation of user privacy) which can lead to the modification and deliberate falsification of information displayed on caller ID systems. ***(Félix Meloche, 2016)***

It is on this issue that we are working by strengthening security in an IP telephony network thanks to a revolutionary technology that is the blockchain.

OPERATION OF TOIP

Characteristics of ToIP

ToIP is a network based on VoIP technology and offers more advantages than Public Switched Telephone Network (PSTN):

Meaning

VoIP is a technique that allows communication by voice (or via multimedia streams: audio or video) on IP-compatible networks, whether private networks or the Internet, wired (cable/ADSL/optical) or not (satellite, Wi-Fi, GSM, UMTS or LTE). VoIP concerns the transmission of voice over an IP network. ***(Félix Meloche, 2016)***

Figure 1 below shows us how this data transport works on IP protocol. Indeed, the first step consists in capturing the voice using a microphone, whether it is a telephone or a headset microphone connected to a PC: we talk of signal acquisition. The second step is to digitize this signal using an ADC in 3 steps: sampling, quantization and coding. The signal once digitized can be processed by a DSP (Digital Signal Processor) which will compress it, i.e. reduce the amount of information necessary to express it. The advantage of compression is to reduce the bandwidth needed to transmit the signal. At this level, the data must still be enriched with information before being converted into data packets to be sent over the network: this is called header wrapping. The packets are then routed from the sending point to the receiving point. Of course, an autoswitch serves as an intermediary between these 2 points and allows the establishment or disconnection of the communication session. The protocols used for transport are RTP, RTCP or SRTP in some cases to provide more security. SIP and H.323 protocols are also used for signaling. When the packets arrive at their destination, it is essential to put them back in the right order and fairly quickly. Otherwise, a degradation of the voice will be felt. Digital-to-analog conversion is the reciprocal step of step 2. It brings back the analog signal. From then on, the voice can be transcribed by the loudspeaker of the helmet, the telephone handset or the computer: this is the restitution of the signal.

When in addition to transmitting voice (VoIP), we combine telephony services (messaging, call transfer, voicemail, etc.), we speak of Telephony over IP (ToIP).

Figure 2 shows ToIP over a set of networks. On the left, we can see the analog network, that is the Switched Telephone Network (RTC) with terminals connected to a local switch or PBx. On the right, we have IP terminals connected to an IPBx or IP auto switch which serves as a VoIP server in this network. The two networks are interconnected through the internet and a GSM gateway: with a similar infrastructure, we speak of Telephony over IP.

Lower communication fees

Before VoIP, everyone was heavily dependent on the good old telephone and its dial-up network for their communications, with no other choice. One of the advantages of VoIP is the immediate reduction in telephone bills. (***ToIP for Dummies, 2017***).

Figure 1. VoIP concept
(Félix Meloche, 2016)

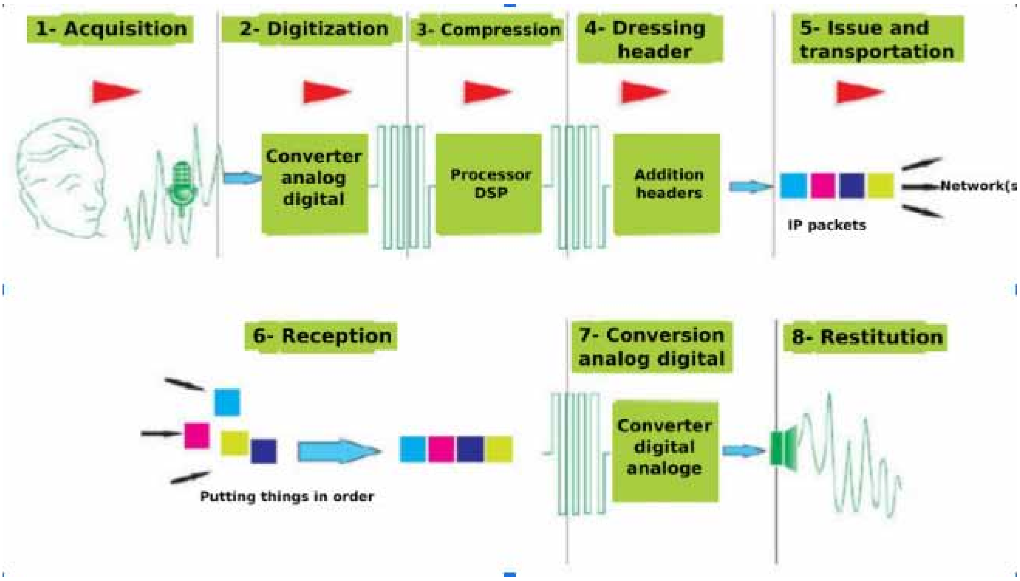
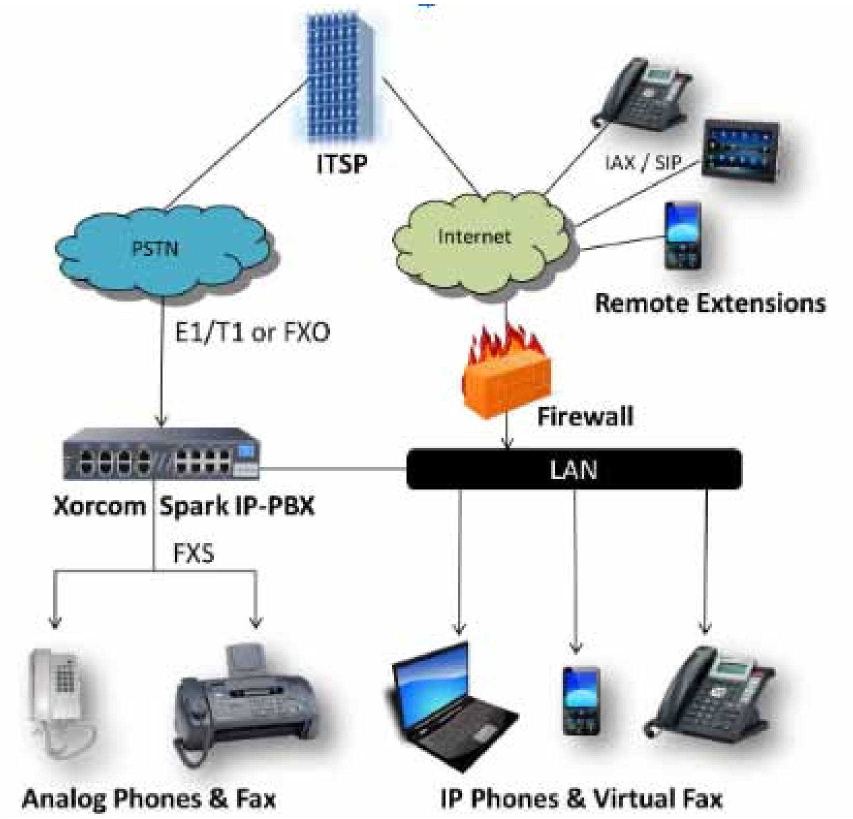


Figure 2. ToIP over set of networks
(https://www.xorcom.com/what-is-voip/, 2022)



Quality

Another most important feature of VoIP is its superior voice quality. On the switched telephone network, only the G.711 codec is accepted and it is strictly limited to audio. On the other hand, VoIP based phone systems allow a wide range of codecs, and hence VoIP offers a large rich features calling possibility.

Flexibility

The new features of VoIP, such as voicemail and call forwarding, have long been offered by traditional telephony. Furthermore, the integration of computer, voice and video applications so that they run on a single network and accommodate wireless telephony is a more recent innovation that has only been made possible by IP telephony. Like any new technological tool, VoIP and its many advantages tend to quickly replace the traditional telephone and even many old purely IT applications.

VoIP Standards

Here we highlight the most used VoIP standards: **SIP, H.323 and RTP**.

SIP (Session Initiation Protocol) is a signaling protocol defined by the IETF (Internet Engineering Task Force) allowing the establishment, release and modification of multimedia sessions **(*RFC 3261*)**. It inherits certain functionalities of the protocols HTTP (HyperText Transport Protocol) used to browse the WEB, and SMTP (Simple Mail Transport Protocol) used to transmit electronic messages (E-mails). SIP relies on a client/server transactional model like HTTP. Addressing uses the concept of SIP URL (Uniform

Resource Locator) which looks like an email address. Each participant in a SIP network can therefore be addressed by a SIP URL. Furthermore, SIP requests are acknowledged by responses identified by a numerical code. Moreover, most of the SIP response codes have been borrowed from the HTTP protocol.

For example, when the recipient is not located, a response code (404 Not Found) is returned. SIP defines two types of entities: clients and servers. (http://www.efort.com/r_tutoriels/SIP_EFORT.pdf **, 2014)**

The client UAC (User Agent Client) sends requests to the server which returns to him a response. The based methods used to send requests are:

ü **INVITE** permits a client to ask for a new session,
ü **ACK** confirms session establishment,
ü **CANCEL** cancels an INVITE outstanding,
ü **BYE** finishes an ongoing session,
ü **OPTIONS** permits users management capacities recovery without open a session,
ü **REGISTER** permits to register at a registrering server.

UAS (User Agent Server) server agents are classic devices that combine the services offered by SIP. Those are:

ü **Registration servers** used for locating users (Registrar)
ü **Delegation servers** (Proxy server) which manage SIP clients, receive and transmit requests to the NHS server (Next-Hop Server)
ü **Redirecting servers** which, on request, transmit the address of the NHS server to the client agent.

The response messages are also six. Those are:

ü **INFORMATIONAL**, simple service message;
ü **SUCCESSFUL**, message indicating that the action has been completed;
ü **REDIRECTION**, message indicating that another action must be taken to validate the request;
ü **CLIENT FAILURE**, message indicating a syntax error, the request cannot be processed;
ü **SERVER FAILURE**, message indicating an error on a server agent;
ü **GLOBAL FAILURE**, general error, the request cannot be processed by any server.

H.323 is a set of voice, image and data communication protocols over IP. More than a protocol, H.323 is more like an association of several different protocols that can be grouped into three categories: signaling, codec negotiation, and information transport. (https://wapiti.telecomlille.fr/commun/ens/peda/options/st/rio/pub/exposes/exposesrio2007/DesirScherpenseel/h323_presentation.html***, 2014***).

RTP - Real Time Transport Protocol - describes the standard packet format for audio and video transmission over the Internet (https://www.3cx.fr/voip-sip/rtp/**, 2018**). The first step in transporting voice over IP is the digitization of the analog signal picked up by the microphone.

Depending on the protocol used to transport the digital signal, an additional encoding step may be necessary (with A-law or µ-law), in particular to compress the signals. Then, the information is cut into frames that can circulate on a computer network. Various protocols can then be used to route the information to the recipient(s). Thus the **RTCP** protocol is used to control the transport of RTP packets.

Requirements for a VoIP System

Many companies have extensive knowledge of the feature richness of VoIP technology. Today, most voice calls are made using the Internet connection. In order to create a small local VoIP network to make calls, we just need smartphones or IP telephones, a wifi access point, an IPBx and a softphone.

THE BLOCKCHAIN

Blockchain is a shared and distributed ledger intended to facilitate the process of recording transactions and tracking assets in a business network. An asset can be tangible (house, car, cash, land), or intangible, such as intellectual property such as patents, copyrights or trademarks. Each block contains a hash (digital fingerprint or unique identifier), timestamped batches of recent valid transactions, and the hash of the previous block. The hash of the previous block links the blocks together and prevents a block from being modified or inserted between two existing blocks. Thus, each consecutive block strengthens the verification of the previous one, and, therefore, the entire Blockchain. The Blockchain therefore contains integrity witnesses which give it its essential characteristic of immutability. ***(John Wiley et al., 2020)***

$$B_{n+1} = E\left(Tx\right)_{n+1} + H\left(B_n\right) + H(B_{n+1}) \qquad (1)$$

$$H(B_{n+1}) = H\left(E\left(Tx\right)_{n+1} + H\left(B_n\right)\right) \qquad (2)$$

(1) : The block B_{n+1} is composed of the set E of transactions Tx, the hash of the previous block and the hash of the current block (n+1).

(2) : The hash of the block (n+1) $H(B_{n+1})$ is composed of the transactions of the block and the hash of the previous block.

Technically, the hash of a file or a block is a fixed length character string calculated from the file by the action of a function called "hash function". As can be seen in the diagram, as soon as the input message changes, the hash obtained at the output also changes. Even when only one letter is modified in the message as we see with the last 4 input messages, the hash changes automatically.

Here we present some characteristics of the blockchain:

- **Consensus**: For a transaction to be valid, all participants must agree on its validity.
- **Provenance**: Participants know where the asset came from and how its owners have changed over time.

Figure 3. The blockchain
(John Wiley et al., 2020)

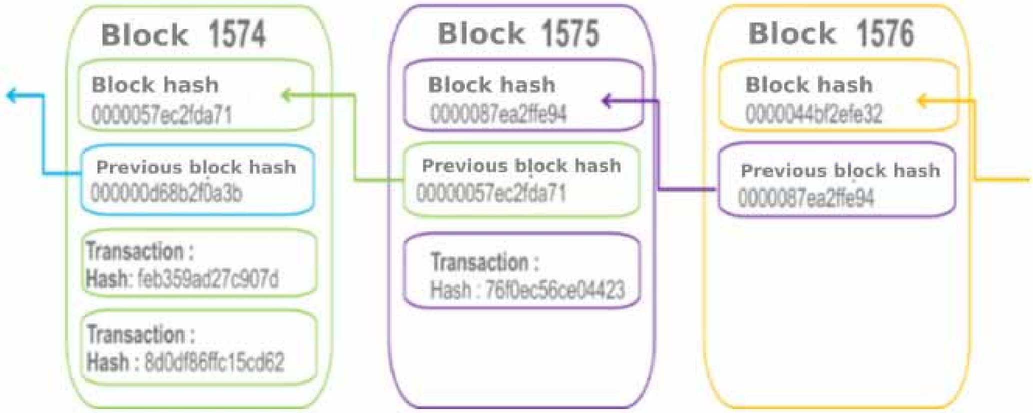
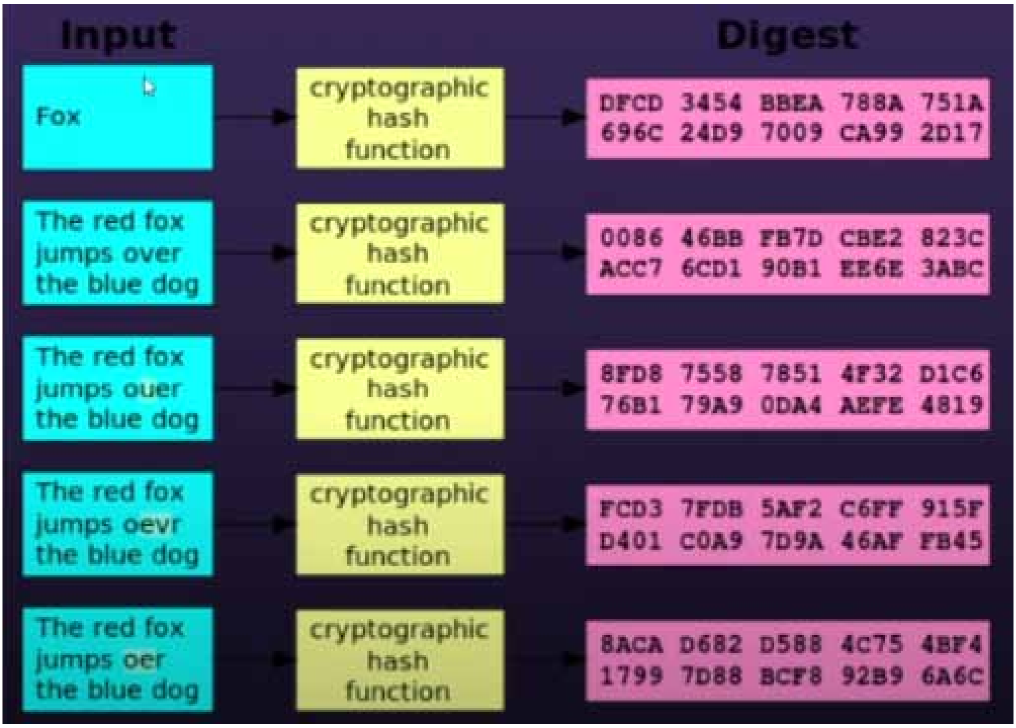


Figure 4. Cryptographic hash

(Ben BK, 2021)


Input
Digest
Fox
cryptographic hash function
DFCD 3454 BBEA 788A 751A 696C 24D9 7009 CA99 2D17
The red fox jumps over the blue dog
cryptographic hash function
0086 46BB FB7D CBE2 823C ACC7 6CD1 90B1 EE6E 3ABC
The red fox jumps ouer the blue dog
cryptographic hash function
8FD8 7558 7851 4F32 D1C6 76B1 79A9 0DA4 AEFE 4819
The red fox jumps oevr the blue dog
cryptographic hash function
FCD3 7FDB 5AF2 C6FF 915F D401 C0A9 7D9A 46AF FB45
The red fox jumps oer the blue dog
cryptographic hash function
8ACA D682 D588 4C75 4BF4 1799 7D88 BCF8 92B9 6A6C

- **Immutability**: No participant can falsify a transaction after it has been recorded in the ledger. If a transaction causes an error, it is necessary to perform a new transaction to reverse it. Both transactions are then visible.
- **Purpose**: A single, shared ledger provides a place everyone refers to when determining ownership of an asset or initiation of a transaction. (John Wiley et al., 2020)

The Blockchain also offers some advantages which are:

- **Time savings:** Settlement of transactions is faster, as it does not require verification by a central authority.
- **Costs reduction:** Supervision is reduced, because the network is autonomously controlled by its members. There are fewer intermediaries because members of the network can directly exchange valuable goods. The redundancy of actions disappears, because all members of the network have access to the shared ledger.
- **Greater Security:** Blockchain security features protect the network against falsification, fraud, and cybercrime. If it is a private Blockchain (permissioned), it allows the creation of a network reserved for members, with proofs guaranteeing their identity and the exact nature of the goods or assets exchanged as they are represented.
- **Increased privacy:** Through the use of credentials and permissions, users can define transaction details that other members can view
- **Ease of Audits:** Having a shared ledger as a single source of trust increases the ability to monitor and verify transactions.

- **Greater operational efficiency:** Purely digital processing of assets helps simplify the transfer of ownership and transactions can be completed at a speed closer to the pace of business. (John Wiley et al., 2020)

How Does It Work?

The diagram below shows the operating principle of MyEtherWallet (MEW) which allows transactions to be made. It is a wallet that can hold ethereum. First, we sign a transaction with the private key, then we send the transaction. After that, the transaction goes to a MEW node; it then arrives in what is called a pool of signed transactions. Subsequently, the miners will check its transactions to see if everything is fine. So, firstly, it checks the transactions that pay the most. Each transaction corresponds to an amount in GAS for minors. Gas can be considered as a fuel used to pay miners. Its value depends on several factors, the most important of them is the complexity of the operations to be carried out.

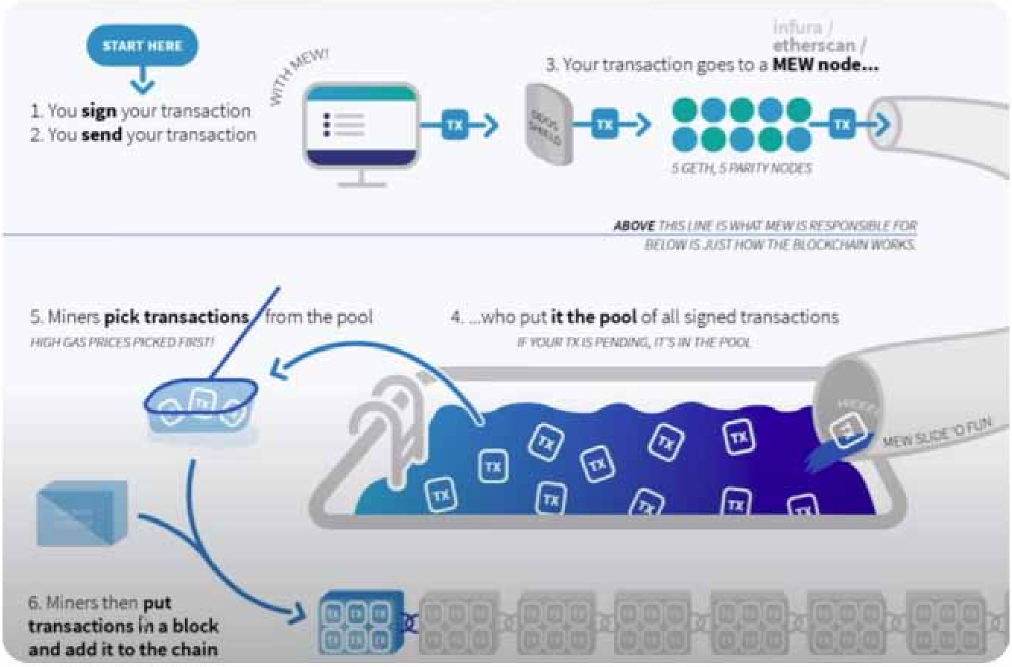
The GAS PRICE represents the price you are willing to pay for a unit of GAS. It is measured in "gwei", which represents 1 billion "wei". To make an ether, it is necessary to have 1 billion "gwei". So the miners, they are quite smart, process, first, the transactions that pay the most. Then they put the transactions in a block and add that block to the blockchain.

TOIP SECURITY

Threats and Risks of ToIP

Before citing a few threats that weigh on VoIP technology, we will come back to the difference between certain expressions in terms of the security of a computer system. These expressions are **Threat, Attack and Vulnerability**.

Figure 5. Operation of a transaction with the Blockchain
(Ben BK, 2021)


START HERE
1. You sign your transaction
2. You send your transaction
WITH MEW!
TX
DDOS SHIELD
infura / etherscan /
3. Your transaction goes to a MEW node...
5 GETH, 5 PARITY NODES
ABOVE THIS LINE IS WHAT MEW IS RESPONSIBLE FOR
BELOW IS JUST HOW THE BLOCKCHAIN WORKS.
5. Miners pick transactions from the pool
HIGH GAS PRICES PICKED FIRST!
4. ...who put it the pool of all signed transactions
IF YOUR TX IS PENDING, IT'S IN THE POOL
MEW SLIDE 'O FUN
6. Miners then put transactions in a block and add it to the chain

- An IT threat is a potential cause of an incident, which can result in damage to the system or to the organization. (***norme ISO/CEI 27000, 2018***)
- The attack is the act of trying to get around the security measures of a given system (**@ *waytolearnx, 2018***). An attack can be active or passive. When the attack is active, it attempts to modify system resources or affect their operation. When the attack attempts to read or use system information but does not influence system resources, it is called a passive attack.
- The vulnerability is a flaw in the system at the level of its design, or its implementation which can be exploited in order to violate its security. (***norme UIT-T X.1500, 2016***)

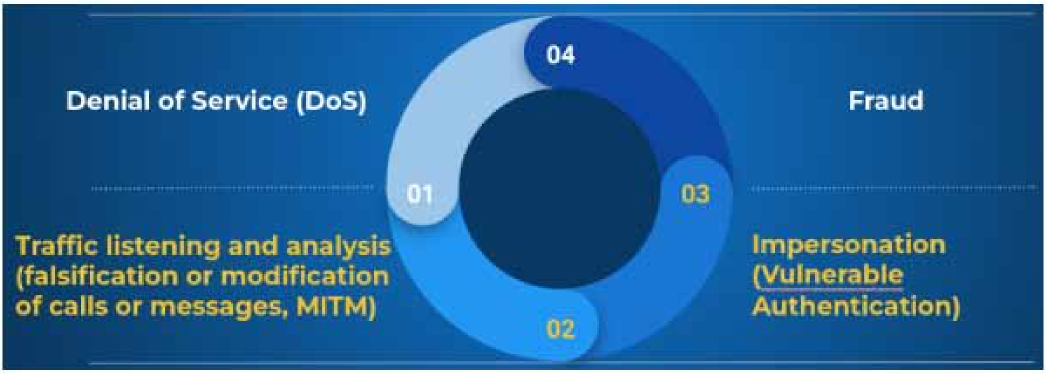
In the following figure, we have mentioned 4 of the main threats to VoIP:

- Denial of service whose purpose is to disrupt the normal operation of a VoIP component or service (memory, bandwidth, telephone, server, gateway, etc.), or even its total shutdown. How does it work? the attacker sends messages (valid or not) from a single source or from a large number of distributed sources (DDoS). The denial of service can be done on an IP phone or on a server. When it's on a server, we talk about distributed denial of service because the user uses several zombie PCs to achieve his ends.
- The purpose of listening to the network is to collect sensitive information in order to prepare other attacks or to have gains (as the case of credit card numbers). How does it work?: The hacker listens to unprotected signals or media streams exchanged between two interlocutors. In addition to confidential information, traffic analysis can reveal other information regarding the target person's profit, behavior and habits.
- The purpose of identity theft is to gain access to a network or one of its elements, a service or information. This attack can hide another (fraud, disruption of service, etc.). How does it work?: the hacker pretends to be another person, another element or another service of the VoIP infrastructure (Example: Hijacking). a Hijacking is an attack, using a Hijacker, consisting of the modification/corruption, by force, of certain settings or behaviors of a component of a computer.
- The purpose of fraud is to abuse VoIP services for personal gain. This category of attack is critical for telecom operators and providers. How does it work?: The hacker manipulates the configuration of certain elements of VoIP such as the billing system.

Considering the many studies carried out in relation to denial of service and fraud, we have chosen to focus our research on threats 2 and 3, i.e. listening to the network, and identity usurpation.

Figure 6. Some main ToIP threats

(Félix Meloche, 2016)


04
Denial of Service (DoS)
Fraud
01
03
Traffic listening and analysis (falsification or modification of calls or messages, MITM)
Impersonation (Vulnerable Authentication)
02

Blockchain in ToIP

In recent years, VoIP security vulnerabilities have made the headlines of various industry reports. The latest happened in 2020, when a group of hackers compromised the VoIP networks of nearly 1,200 organizations in 20 different countries (**Zdnet, 2020**). Sectors such as the military, finance, insurance, manufacturing and government have been affected by hacked systems, with more than half of the victims located in the UK.

To avoid similar hacks, VoIP providers should leverage stronger multi-layered security as part of 2022 VoIP trends. Blockchain technologies are now being explored as a way to decentralize control of VoIP platforms, which means cybercriminals will have a harder time to break the systems and steal confidential customers data. (**Nestor Gilbert, 2022**)

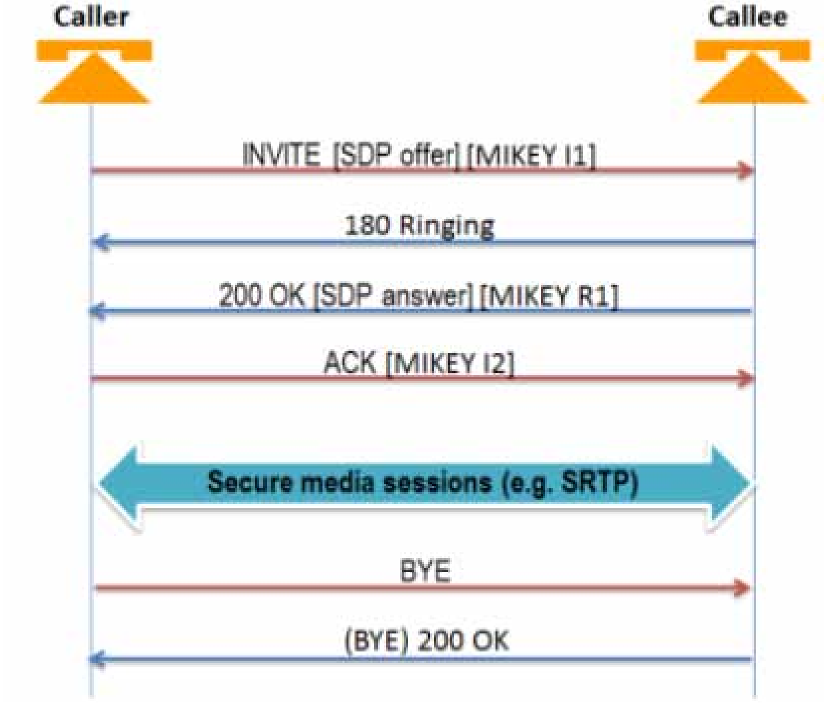
What must be remembered is, due to the vulnerable nature of VoIP platforms, service providers are constantly deploying better and improved security layers for VoIP systems. VoIP solutions are increasingly adopting multi-layered security and blockchain technologies to protect customers data sent over systems and networks.

State of the Art of ToIP Network Security Solutions Based on Blockchain and Cryptography

Triple Authentication Key Exchange Protocol for VoIP Applications (Riccardo Pecori et al, 2016)

The works of Riccardo Pecori *et al.* in 2016 aim to strengthen the security of a communication section between two users. For this, a 3-level authentication protocol is used. This protocol is called 3AKEP, which stands for "Triple-Authentication Keys Exchange Protocol". The purpose of this protocol is to ensure the exchange of keys between the participants involved in the communication session. How does it work?

Figure 7. SIP messages stream with MIKEY-3AKEP
(Riccardo Pecori et al, 2016)


Caller
Callee
INVITE [SDP offer] [MIKEY I1]
180 Ringing
200 OK [SDP answer] [MIKEY R1]
ACK [MIKEY I2]
Secure media sessions (e.g. SRTP)
BYE
(BYE) 200 OK

Indeed, when the caller calls the callee, an “INVITE” command is sent by the SIP server to the callee indicating to him that he is invited to a discussion. At this level, the proposed system sends a first key, i.e. the caller’s key to the callee. This key allows the callee to decrypt the caller’s messages at his terminal. When the callee’s device rings, a “180 Ringing” command is sent to notify the device is ringing. Then, the command “200 OK” is sent when the callee picks up. At this level, the proposed system sends a second key, i.e. the callee’s key to the caller. This key allows the caller to decrypt the messages of the callee at the level of his terminal as well. Then “ACK” is sent when the session is established between the two users. At this level, the 3rd key is used to encrypt the messages exchanged during this session. Finally, when the call is hung up, the command “BYE” is sent on both sides thus ending the communication session.

The advantage of encrypting the communication channel is that it avoids man-in-the-middle attacks (MITM) because the decryption keys are at the level of the two terminals only.

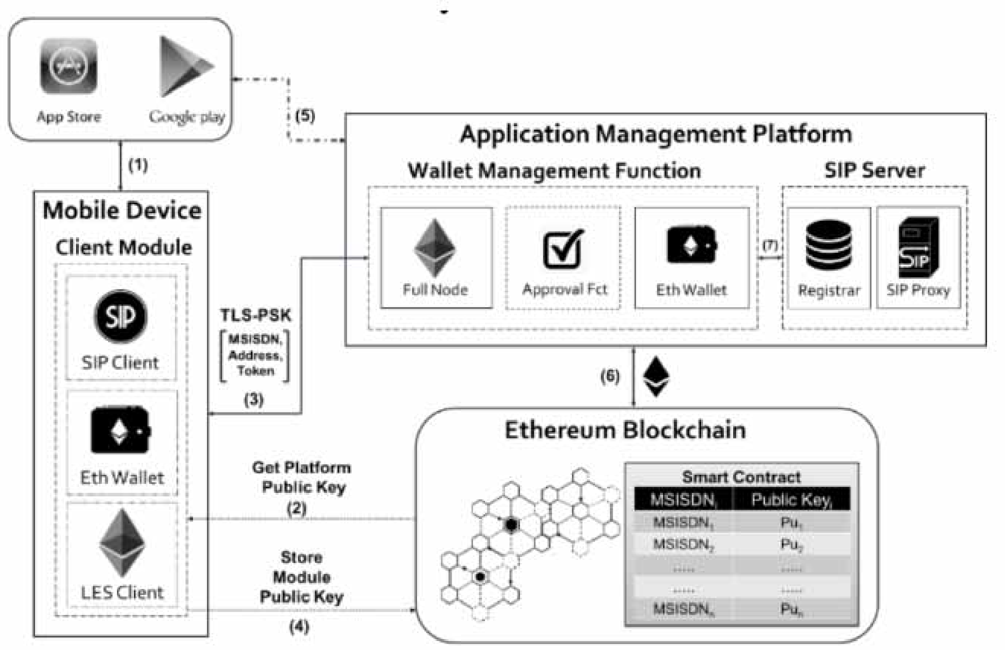
On the other hand, the system has some drawbacks such as the communication terminals themselves which are not authenticated before each call. The attacker can therefore impersonate a user in the system. Also, the keys exchanged in the system are generated from the identifier of the two users of a session. Thus, packet losses in the system can lead to the loss of the exchanged key and make the channel insecure.

End-to-end secure VoIP system based on the Ethereum blockchain (Elie Kfoury et al., 2018)

The goal of the work of Elie Kfoury and David Khoury in 2018 is to increase the security of application data at the level of VoIP applications by using a smart contract based on the Ethereum blockchain. How does it work ?

The proposed system consists of 3 parts: the mobile application, the application management server, and the smart contract. The application management server consists of the wallet management server and the SIP server. The application downloaded from the playstore or the app store by the user on his terminal consists of 3 modules: a SIP client responsible for making and receiving calls

Figure 8. System architecture and interfaces
(Elie Kfoury et al., 2018)



through a gateway, an empty etherium electronic wallet and a "LES" client responsible for verifying the effectiveness of a transaction. At the first connection of the user, a first transfer of ether is required. The smart contract verifies the effectiveness of this transaction thanks to the LES client which triggers the execution of the approval function at the portfolio management server level when the transfer is effective. Two keys are then generated and stored in the blockchain via the smart contract: a key for encrypting data at the application level and a key for encrypting data at the blockchain level. In the blockchain, each key pair is recorded according to the MSISDN (Mobile Station International Subscriber Directory Number), i.e. the user's telephone number.

The advantage of this system is that the security is reinforced at the level of the communication terminals because the data at the level of its terminals is encrypted. The fact that the keys are linked to the telephone number also reassures that two numbers cannot have the same keys.

The disadvantage is that a user who is not the owner of a number could also use it before the registration of the real owner thus preventing the real owner from using his number. Another disadvantage is that without a minimum of ether transfer, the system does not work.

Decentralized Blockchain-Based Authentication for Secure Voice Communication (Mustafa Kara et al., 2021)

The goal of the works of Mustafa Kara *et al.* in 2021 is to use a smart contract to secure communication between two users. How does it work ?

After registration in the SIP client and in the blockchain, a key pair is generated for the user. Then, the smart contract verifies the existence of the user's number in the blockchain and sends him a token when the number exists. When a user calls another user of the system and the session is already established, the smart contract again checks the existence of the caller's token, and this token is used as a certificate to secure the communication session.

The advantage of this system is that it makes it possible to secure the communication session between two users because the communication channel is secure. The system also allows the session information of a call such as the numbers of the participants involved in and the communication time to be recorded in the blockchain.

A limit of this system is that there is a latency between the message sending time and the message reception time since a verification is done after the establishment of the communication session between two users. Another limitation is that we cannot really know if the caller is really the originator of the number in case of theft of the login information.

DIGITAL IDENTITY

Thanks to the Internet, we are witnessing a growing increase in the number of connected terminals; online services are born and multiply; the world has become a global village as we say so well. In this dynamic and rapidly expanding ecosystem, the need to know with whom or with what we communicate becomes essential: this is how the concept of digital identity is born. This term was chosen to make the link between real entity and virtual entity in the digital ecosystem. Digital identity is, like real identity, faced with a number of threats.

Security: Threats

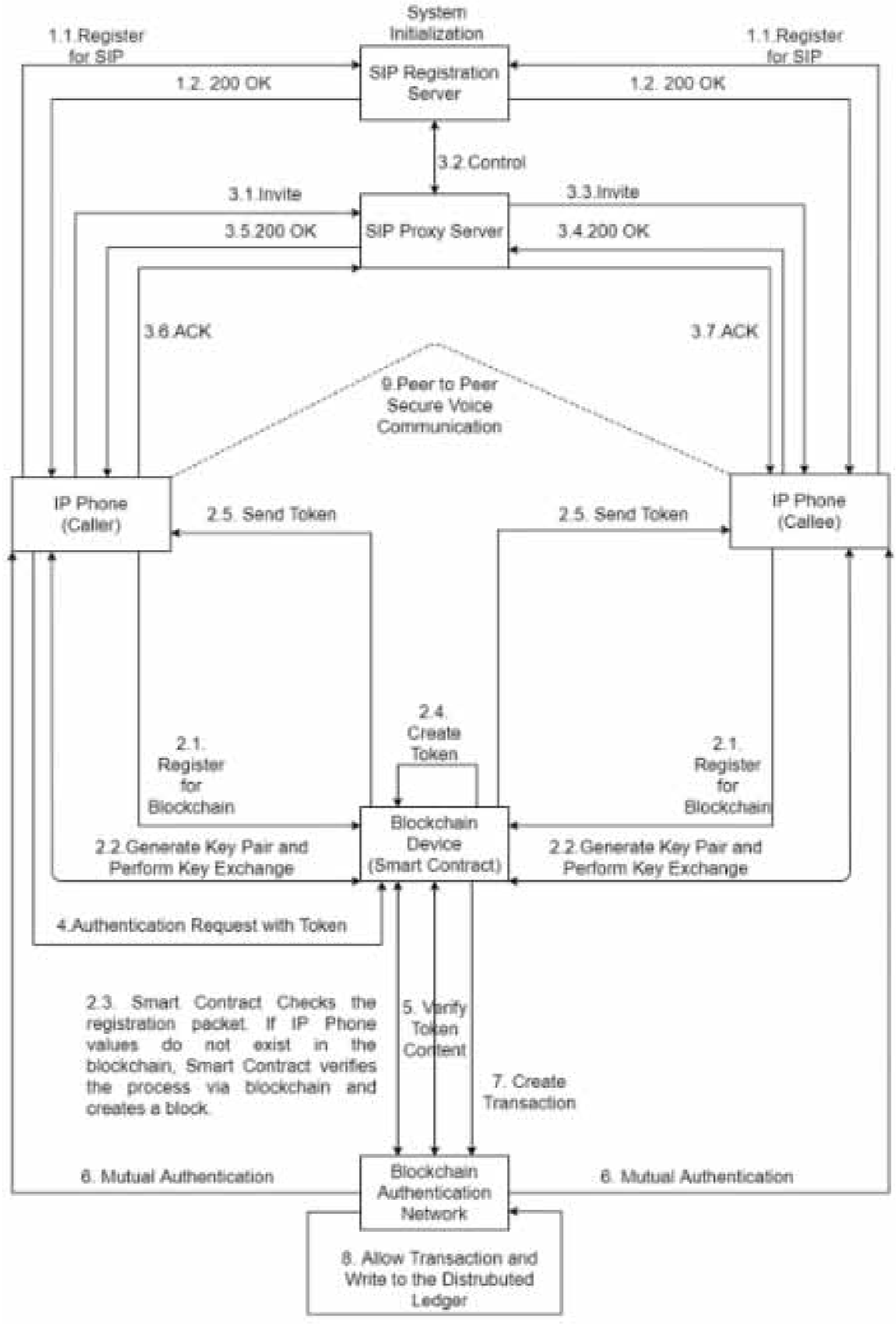
Identity Usurpation

The first threat to digital identity is impersonation by an attacker. This threat concerns more and more people. On a ToIP network, the attacker pretends to be a legitimate user by using the latter's credentials.

The key IT security concept that helps protect against identity theft is authentication. It consists of verifying the identity of an entity having access to the system. To do this verification, four classes are defined: what the entity knows, what the entity owns and what the entity is or does. To authenticate

Figure 9. Model diagram

(Mustafa Kara et al., 2021)


System Initialization
SIP Registration Server
1.1.Register for SIP
1.2. 200 OK
1.1.Register for SIP
1.2. 200 OK
3.2.Control
3.1.Invite
3.5.200 OK
SIP Proxy Server
3.3.Invite
3.4.200 OK
3.6.ACK
3.7.ACK
9.Peer to Peer Secure Voice Communication
IP Phone (Caller)
2.5. Send Token
2.5. Send Token
IP Phone (Callee)
2.4. Create Token
2.1. Register for Blockchain
2.1. Register for Blockchain
Blockchain Device (Smart Contract)
2.2.Generate Key Pair and Perform Key Exchange
2.2.Generate Key Pair and Perform Key Exchange
4.Authentication Request with Token
2.3. Smart Contract Checks the registration packet. If IP Phone values do not exist in the blockchain, Smart Contract verifies the process via blockchain and creates a block.
5. Verify Token Content
7. Create Transaction
6. Mutual Authentication
Blockchain Authentication Network
6. Mutual Authentication
8. Allow Transaction and Write to the Distrubuted Ledger

a digital identity, a subset of the claims composing it must be part of one of these classes. For the knowledge class for example, one of the claims can contain a password or a PIN code. Similarly, for the possession class, the identity will contain data relating to a digital certificate, a smart card, a telephone or an identity card. Finally, the claims can contain biometric data such as fingerprints, iris, face or the dynamics of keystrokes which are data specific to each individual. Authentication will then depend on the trust that an observer has in these claims. When claims are part of at least two of the authentication classes, it is called strong authentication. **(Johann Vincent, 2013)**

Information Theft

Another threat to identity is information theft. This process consists of collecting supposedly sensitive information from a user. This is the case, for example, of a password. The confidentiality property ensures that only authorized entities have access to information. In the information confidentiality process, there are two families of encryption algorithms: symmetric encryption algorithms and asymmetric encryption algorithms.

False Declarations or Change of Identity

Imagine an online sales platform, reserved only for adults. A teenager or an attacker, could change his age in order to pass access controls. We limit the threats related to digital identity to these three big points which constitute the flagship threats of digital identity.

Digital Identity Management Systems

Identity management systems (IMS) can be classified into three types as mentioned above. The purpose of the IMS is either to allow the use of a digital identity to establish a relationship of trust, or to monitor the use of a digital identity.

THE SOLUTION WE OFFER

To make a contribution to improving the security of the IP telephony network (ToIP), we offer a blockchain-based solution, and reinforcing the phases of enrolment, connection to the network, the communication session and the post-communication .

Indeed, ToIP networks face identity theft and false declarations of identity attributes. To strengthen security against these risks, we are developing identification and authentication systems that ensure the identity of the user. Identity verification methods such as KYC through facial recognition, character recognition (OCR: Optical Character Recognition), the use of one-time passwords (OTP: One Time Password), are means on which these systems are based. Finally, the blockchain makes it possible to provide a digital identity which will be the pledge of the unique and real identity of the users.

Authenticated network users must perform secure communication to ensure the confidentiality, privacy, and integrity of communication information. Therefore, we propose to further strengthen the communication sessions, by using cryptography.

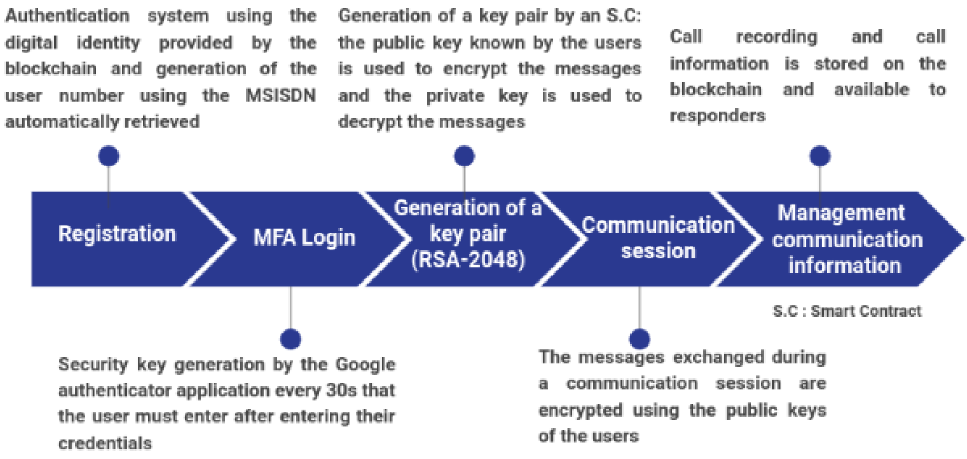
Finally, the management of communication information following the end of the session was also a point on which we worked throughout our study. Always relying on the blockchain, we intend to strengthen the confidentiality and integrity of communication data.

SOLUTION DESIGN

The Identification System

The identification system is the entry point for any new user of the system. Access to the ToIP network faces the validation problem of its identity by the system.

Figure 10. Proposed model diagram


Authentication system using the digital identity provided by the blockchain and generation of the user number using the MSISDN automatically retrieved
Generation of a key pair by an S.C: the public key known by the users is used to encrypt the messages and the private key is used to decrypt the messages
Call recording and call information is stored on the blockchain and available to responders
Registration
MFA Login
Generation of a key pair (RSA-2048)
Communication session
Management communication information
S.C : Smart Contract
Security key generation by the Google authenticator application every 30s that the user must enter after entering their credentials
The messages exchanged during a communication session are encrypted using the public keys of the users

- The user will have a mobile application to register (possibility will be to access the web interface of the system for registration). He is first invited to enter basic information constituting his pivotal identity. This includes the surname, first names, date and place of birth, sex, telephone, email, etc. An OTP is also sent to the telephone number for confirmation. He must also check his email by clicking on the link that would have been sent to him.
- The second step is for the user to submit official documents: photo of their passport or identity card. He must select the type of document to submit and then proceed. From the documents provided, we extract, by OCR, the content of the documents and we ask him to ensure the veracity of the information and to confirm. If confirmation is received, the OCR results are compared with the information provided manually by the user as well as that taken from the Machine Readable Zone of their part.
- The 3rd step is for the user to send a recent photo of himself, where he can be found alone, then to place himself in front of a live camera to verify his identity. First, he submits his photo and we generate a series of words that he will have to write on a support then stands in front of the live camera by presenting the support. We detect his face and we compare it with the photo sent, then with the OCR, we make sure that the written sentence is indeed the one requested. ***Emotion detection to define whether or not the user is forced into live video is an important phase that we plan to implement.*** At this stage, we can predict the age of the user, define his sex and compare the results with the information on the documents, then what he himself has defined. If everything is OK, it is assumed that at this level, the user's identity is confirmed and enrollment continues.
- The last step is to ask the user questions about his profession, and any other additional information. At the end of this step, we can certify a secure identity of the user and save his information in the blockchain. We send him his digital identity in his wallet.

Any other platform that would like to identify a user will no longer need to pass this same identification process to the user if that user already exists on the blockchain network: the process will be as with Google's authentication system.

Blockchain Network

Blockchain is a distributed ledger technology that is basically part of a decentralized system. As part of our study, we opted for a private blockchain in order to avoid the fees charged for processing transactions. Here is a comparative table of the two blockchains that we have the most studied:

Objective

- Ethereum is the platform for building B2C businesses and decentralized applications. It is created for the purpose of running smart contracts on the Ethereum Virtual Machine (EVM) and building decentralized applications for mass consumption using that.
- Hyperledger is designed to build B2B businesses and cross-industry applications. It helps companies or industries to collaborate with developers who work with Distributed Ledger Technology (DLT). Custom blockchain applications with limited access can be created with this.

Privacy

- Ethereum is a public network. All transactions are fully transparent and anyone with internet access can view these transactions.
- Hyperledger is a limited access or permissioned blockchain network. This is highly secure and confidential. Organizations or individuals with the Certificate of Authorization can only view all transactions on the network.

Governance

- The Ethereum network is governed solely by Ethereum developers. Vitalik Buterin is the main developer and founder of Ethereum. This is primarily an example of internal development rather than collaboration.
- The Hyperledger framework is governed by the Linux Foundation. IBM is also one of the main contributors to this framework. It is the product of the massive collaboration of these two companies which turned out to be a huge success.

Table 2. Comparison of Ethereum blockchains and Fabric Hyperledger

Features	Ethereum	Hyperledger Fabric
Privacy	Public Blockchain	Private Blockchain
Objective	Client-side B2C applications	Enterprise-side B2B applications
Governance	Ethereum developers	Linux Foundation
Participation	Any person	Organizations with a certificate of authorization
Programming languages	Solidity	Golang, JavaScript, or Java
Consensus mechanism	POW- Proof of Work Mechanism	Pluggable consensus mechanism
Transaction speed	Less	More
Cryptocurrency	Ether or Ethereum	None

(Nicolas Six et al., 2020)

Involvement

- Ethereum is a public and permissionless network. Anyone with internet access can download the software and start mining Ethereum.
- Hyperledger maintains strict control over participation in this network. Only Authorized Members and peers selected by Authorized Members may use the Hyperledger platform and its tools. It hides valuable and confidential information from external parties and prevents them from tampering with it.

Smart Contracts

- Ethereum first offered smart contracts. A smart contract is a computer program or condition written in code that automatically triggers when certain conditions are met. It controls the transfer of digital assets between parties involved in the contract. It is immutable, once the condition is created, it cannot be changed by any involved part.
- Like smart contracts, the Hyperledger framework also allows member organizations to execute code on peers that create the transactions under a specific condition. These are known as chaincodes.

Programming Language

- For writing smart contracts Ethereum uses solidity and for developing the application some high level languages like JavaScript, Python, Golang can be used.
- In Hyperledger, Go is widely used to write the blockchain code and a bit of Java and JavaScript is also used.

Proof of Work (POW) or Consensus Mechanism

- Since Ethereum is a decentralized network, a proof-of-work (POW) or consensus mechanism runs throughout the blockchain. It allows the participating nodes of the decentralized network to achieve a consensus or agreement on things like account balances and the order of transactions, which prevents users from making fake transactions and doubling up on spending.
- As Hyperledger is a private and authorized network, it does not need any POW or consensus mechanism to validate a transaction. If two participating parties agree to a specific transaction, no third party can see or intervene in the specific transaction. This helps improve scalability and transaction rates as well as overall network performance.

Speed of Transactions

- As Ethereum is a public domain, it has a POW mechanism, which reduces the transaction speed of Ethereum. That's about 20 transactions per second.
- To be an authorized blockchain network, the Hyperledger fabric does not need such a heavy POW mechanism as Ethereum. This increases transaction speed. This represents approximately 1000 transactions per second which is bigger than Ethereum.

Cryptocurrency

- Ethereum has its own native cryptocurrency called ETHEREUM (ETH). Any participating node can mine ETH by paying gas.
- Hyperledger does not have its native cryptocurrency and does not involve mining. This contributes to the speed of transactions.

Benefits of Hyperledger Fabric

- Open Source: Anyone can use the platform for the benefit of their business.
- Suitable for a wide range of industries: It covers sectors like healthcare, supply chain, insurance, media, cybersecurity, IoT, banking, government, real estate etc.
- Quality code
- High efficiency: Due to the architecture of the technology. Ability to process information without ever slowing down the platform simultaneously.
- Modular design: You can add as many features as you want. So, one can modify Hyperledger Fabric consensus, ledger types, add tokens, add other features.

It is for the advantages of the Hyperledger Fabric structure that we have opted for this technology as the blockchain to be used in the context of our work.

The Authentication System

Based on the immunity feature of the blockchain, this authentication system stores personal information (surname, first names, date and place of birth, online nickname, password, bank account, national identity card, passport, diplomas, telephone number ...) of each person. So to register on our platform, the individual can use this system by inserting his login credentials. Its other data will be retrieved automatically thanks to our chaincode.

Google Authenticator implements the one-time password algorithm defined in IETF RFC 623810, and the HMAC-SHA1-based one-time password generation algorithm defined in IETF RFC 422611. It generates six (06) characters every thirty (30) seconds (https://www.wikiwand.com/fr/Google_Authenticator**, 2020**). When the google authenticator account is linked to a system, a 16-characters backup code is generated and the user is asked to keep it in a safe place. This backup code allows you to keep access to our system even in the case of loss of login information. The HMAC function is defined as follows:

$$\mathbf{HMAC_K(m)= h((K\oplus opad) \parallel h((K\oplus ipad) \parallel m))} \quad (1)$$

h: an iterative hash function; K: the secret key; m: the message to authenticate; "||" denotes a concatenation; and ⊕ an 'exclusive or'; ipad and opad, each one block in size, are defined by: ipad = 0x363636...3636 and opad = 0x5c5c5c...5c5c. So if the block size of the hash function is 512, ipad and opad are 64 repeats of the bytes, respectively, 0x36 and 0x5c. **(Julien VANDENHAUTE, 2020)**

Communication Session

As far as the security of the communication session is concerned, we have planned to use a pair of keys per user: the public key known by the users is used to encrypt the messages and the private key is used to decrypt the messages. This key pair is generated only on the first login and is based on RSA-2048. The messages exchanged during a communication session are encrypted using the users' public keys.

RSA encryption is an asymmetric cryptography algorithm for exchanging confidential data over the Internet **(KERNOUF Yamina et al., 2020).** If M is a natural integer strictly less than n (product of 2 random prime numbers), representing a message, then the encrypted message will be represented by:

$$\mathbf{C=M^{e}\ (mod\ n)} \tag{2}$$

With RSA-2048, the integer n has a size of 2048. In February 2020, the 23rd smallest RSA digit (RSA-250) of the 54 numbers listed, was factored. **(RSA Laboratories, 2013)**

Managing Session Information After Communication

After each communication session, the call recording and call information is saved on the blockchain and available to session participants.

CONCLUSION AND PERSPECTIVES

In this document, we have covered the generalities of ToIP, in particular how it works, its key concepts and the protocols involved in a ToIP network. Although it has a lot of advantages, especially for companies, because it reduces or eliminates communication fees, ToIP networks present security problems. Solutions exist to reinforce security in ToIP networks. Some solutions are based on the blockchain, a current revolutionary technology which, by its characteristics, remains an important asset when it comes to securing ToIP networks. However, these solutions remain limited because they don't include all the stages of a ToIP session, i.e. from enrolling users to managing session communication information. To make a contribution to improving the security of ToIP, our perspectives concern the design and implementation of a blockchain-based solution, strengthening the phases of enrollment, connection to the network, the communication session and the post-communication. As an important benefit of this improvement and to allude to one of the current phenomena in the world, this solution could make working at home during pandemics less vulnerable to cyber attacks. Relying on the power of the blockchain, we intend to guarantee a secure and tamper-proof digital identity for each actor in the network.

REFERENCES

Abdurrahman, A., Christos, N. C., & Livio, F. (2017). *Malware analysis of wanacry ransomware*.

Alison, B. (2021). *The emergence of blockchain in contractual relations: Towards a new form of algorithmic trust?* HAL. https: //hal.archives-ouvertes.fr/hal-03210338.

Arshdeep, B., & Vijay, K. M. (2016). Blockchain platform for industrial internet of things. *Journal of Software Engineering and Applications*, *9*(10), 533–546. doi:10.4236/jsea.2016.910036

Asterisk Development Team. (2010) *Asterisk Administrator Guide 1.8.* Asterisk..

Asterisk Development Team. (2016). *Asterisk Administrator Guide 14*. Asterisk.

Brant, C., Giulio, R., Patricia, W., & Askhat, Z. (2018). *Blockchain beyond the hype: What is the strategic business value*. McKinsey & Company.

Butcher, D., Li, X., & Guo, J. (2007). Security challenge and defense in VoIP infrastructures. *IEEE Transactions on Systems, Man, and Cybernetics. Part C, Applications and Reviews*, *37*(6), 1152–1162. doi:10.1109/TSMCC.2007.905853

Dannen, C. (2017). *Introducing ethereum and solidity: Foundations of cryptocurrency and blockchain programming for beginners*. Apress. doi:10.1007/978-1-4842-2535-6

Darrell, M. W. (2016). Internet shutdowns cost countries $2.4 billion last year. Center for Technology Innovation at Brookings.

Elie, F. K. & David, J. K. (2018). *Secure End-to-End VoIP System Based on Ethereum Blockchain*.

Febro, A. (2013). Sipchain: Sip defense cluster with blockchain. In *2019 Principles, Systems and Applications of IP Telecommunications (IPTComm).* IEEE.

Formavision / Atrix. (2012). *Telephonic communication: 5 out of 5 !, Administrator guide, 2012*. Atrix.

Iddo, B., Charles, L., Alex, M., & Meni, R. (2014). Proof of activity: Extending bitcoin's proof of work via proof of stake [extended abstract] y. *Performance Evaluation Review*, *42*(3), 34–37. doi:10.1145/2695533.2695545

Jean-Pierre, F. (2017). Security and insecurity of blockchain and smart contracts. In *Annals of Mines- Industrial reality* (pp. 98–101). FFE. https://www.cairn.info/load_pdf.php?ID_ARTICLE=RINDU1_173_0098

Jiin-Chiou, C., Narn-Yih, L., Chien, C., & Yi-Hua, C. (2018). *Blockchain and smart contract for digital certificate. In 2018 IEEE international conference on applied system invention (ICASI)*. IEEE.

Johann V. (2013). *Digital identity in telecom context*.

Johnny L. (2007). *Asterisk Hacking, Tool kit and Live CD*.

La Corte, A., & Scatá, M. (2011, June). Security and qos analysis for next generation networks. In *International Conference on Information Society* (i-Society 2011) (pp. 248-253). IEEE, 2011. doi:10.1109/i-Society18435.2011.5978445

Mikael, M. & Felicia, S. (2017). *Using blockchain to solve the authentication problem in VoIP recordings*. Research Gate.

Mwrwan, A. (2021). *Blockchain-Based Authentication and Registration Mechanism for SIP-Based VoIP Systems, 2021*. IEEE.

Nakhoon, C., & Heeyoul, K. (2019). A blockchain-based user authentication model using metamask. *Journal of Internet Computing and Services*, *20*(6), 119–127. doi:10.7472/jksii.2019.20.6.119

Nelson, J. G. S. (2021). *Contributions to Data Security through Elliptic Curve Cryptography and Blockchain Technology*. MIT.

Niaz, C. (2019). *Inside blockchain, bitcoin, and cryptocurrencies*. CRC Press., doi:10.1201/9780429325533

Niaz, C. (2019). An iot and blockchain-based approach for ensuring transparency and accountability in regulatory compliance. In *Adjunct Proceedings of the 2019 ACM International Joint Conference on Pervasive and Ubiquitous Computing and Proceedings of the 2019 ACM International Symposium on Wearable Computers,* (pp. 957–962). ACM.

Nirupama, D. B., & David, L. K. C. (2015). Bitcoin mining technology. In *Handbook of digital currency* (pp. 45–65). Elsevier.

Omar, D., Kei-Leo, B., Antoine, D., Eric, T., & Elyes, B. H. (2018). Consortium blockchains: Overview, applications and challenges. *International Journal On Advances in Telecommunications*, *11*(1&2), 51–64.

Primavera, D. F., & Samer, H. (2018). Blockchain technology as a regulatory technology: From code is law to law is code. arXiv preprint arXiv:1801.02507.

RAECP BENIN. (2020). *Annual activities report 2017 - p 43, Table: Mobile telephonic traffic evolution in Bénin Republic from 2019 to 2020*. RAECP BENIN.

Rebecca, Y., Ron, W., Sainan, L., Sajani, J., Fengling, H., Xun, Y., Xuechao, Y., Gayashan, A., & Shiping, C. (2020). Public and private blockchain in construction business process and information integration. *Automation in construction, 118*, 103276.

Rishav, C., & Rajdeep, C. (2017). An overview of the emerging technology: Blockchain. In 2017 3rd International Conference on Computational Intelligence and Networks (CINE), pages 126–127. IEEE, 2017.

Rosenberg, J. (2002). *SIP: Session Initiation Protocol*. RFC 3261.

Russell B. et al. (2013). *Asterisk The Definitive Guide, 4ième édition*. Asterisk.

Scata, M. (2012). *Security Analysis of ICT Systems based on Bio-Inspired Models*.

Sebastian, G. (2021). A descriptive study on cybersecurity challenges of working from home during COVID-19 pandemic and a proposed 8 step WFH cyber-attack mitigation plan. *Communications of the IBIMA*, *2*, 2–7.

Sebastian, G. (2022). Cyber Kill Chain Analysis of Five Major US Data Breaches: Lessons Learnt and Prevention Plan. [IJCWT]. *International Journal of Cyber Warfare & Terrorism*, *12*(1), 1–15. doi:10.4018/IJCWT.315651

Sébastien, D. (2010) VoIP and ToIP: Asterisk, Business IP telephony. Asterisk.

Sloane, B., & Bhargav, P. (2018). Blockchain basics: Introduction to distributed ledgers. In *IBM Developer*. IBM.

Thierry, B. (2018). Blockchain unleashes questions. In *Annals of Mines - Manage and understand* (Vol. 131, pp. 83–85). FFE., doi:10.3917/geco1.131.0083.URL:https://www.cairn.info/revue-gerer-et-comprendre-2018-1-page-83.htm

Thomas, G. (2010). *Telephony over IP security. Networks and Telecommunications [cs.NI]*. Telecom Paris Tech.

Usman, W. C. (2017). The double spending problem and cryptocurrencies. *SSRN*, *3090174*, 2017.

Valeria, F., Claude, D. G., & Ronan, L. G. (2018). Understanding Blockchains: operation and challenges of these new technologies. Senat. http://www.senat.fr/rap/r17-584/r17-584_mono.html #fnref11

Victor, C., & Hossain, S. (2019). Blockchain development platform comparison. In *2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC),* (*vol. 1*, pages 922–923). IEEE.

Vitalik, B. (2014). A next-generation smart contract and decentralized application platform. *white paper, 3*(37).

Vitalik, B. (2015). On public and private blockchains. *Ethereum Blog*.

Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2019). Blockchain technology overview. arXiv preprint arXiv:1906.11078.

Yves, C., & Serge, S. (2016). *Blockchain, or distributed trust*. Foundation for political innovation.

Sekoude Jehovah-nis Pedrie SONON is a PhD student at the University of Abomey-Calavi, Benin. His research interests include IP telephony, blockchain, Internet of Things, industrial applications and symbolic programming. He is a member of the research laboratories: Lsaboratory of Electronics, Telecommunications and Applied Computing (LETIA / EPAC) and the Laboratory of Analysis and Processing of Image and Speech of the Institute of Technological Innovation (LATIP / IITECH). He graduated as a design engineer, Master degree, from the Polytechnic School of Abomey Calavi (EPAC) of the University of Abomey-Calavi in 2019. He is a consultant in the field of IP telephony, computer analysis, graphic design and web and mobile development.

Tahirou Djara is a Senior Lecturer at the Polytechnic School of Abomey-Calavi located in the University of Abomey-Calavi, Bénin. His research interests include: biometrics, signal and image processing, computational intelligence, industrial applications and symbolical programming. He is member of the research laboratory: Laboratory of Electronics, Telecommunications and Applied Data Processing Technology (Laboratoire d'Electrotechnique de Télécommunication et d'Informatique Appliquée– LETIA/EPAC). He received the PhD degree in signals and image processing from the University of Abomey-Calavi, in 2013. He is a consultant in quality assurance in higher education and consultant in the field of science and engineering technology.

Abdoul Matine OUSMANE holds PhD from the University of Abomey-Calavi, Benin. His research focuses on: biometrics, signal processing and images, computer intelligence, industrial applications and symbolic programming. He is a member of the research laboratory: Laboratory of Electronics, Telecommunications and Applied Data Processing (LETIA / EPAC). He graduated research master from the Institute of Training and Research in Computer Science (IFRI) at the University of Abomey-Calavi in 2012. He is a consultant in the field of computer analysis, web an mobile developer.

Abdou-Aziz Sobabe holds a PhD in Engineering Sciences from the University of Abomey-Calavi in Benin. He conducts his research at the Laboratory of Electrical Engineering, Telecommunications and Applied Computer Science (LETIA). His research interests include biometrics, signal and image processing, affective computing and software engineering. His areas of specialization include multimodal biometrics, non-contact biometrics, score fusion and user-specific parameters in biometric systems. In the area of software engineering, he is interested in object-oriented programming and relational databases for applications. In the field of artificial intelligence, he uses machine learning methods applied to computer security (biometric authentication), e-Agriculture, e-Health.