electronics

MDPI

Article

IoMT-Based Platform for E-Health Monitoring Based on the Blockchain

Jalel Ktari [1], Tarek Frikha [1], Nader Ben Amor [1], Leila Louraidh [2], Hela Elmannai [3] and Monia Hamdi [3,*]

[1] CES Lab, ENIS, University of Sfax, P.O. Box 3038, Sfax 3029, Tunisia; jalel.ktari@enis.tn (J.K.); tarek.frikha@enis.tn (T.F.); nader.benamor@enis.tn (N.B.A.)
[2] Department of Computer Sciences, Higher Institute of Management of Gabes, Gabes University, Gabes 6029, Tunisia; leila.louraidh97@gmail.com
[3] Department of Information Technology, College of Computer and Information Sciences, Princess Nourah Bint Abdulrahman University, P.O. Box 84428, Riyadh 11671, Saudi Arabia; hselmannai@pnu.edu.sa
* Correspondence: mshamdi@pnu.edu.sa

Abstract: With the evolution of information technology, the use of internet of things has increased. It affects several areas such as medical field, smart cities, and information systems. In this work, we will use this technological development in the context of health, particularly e-health. We present a platform based on IoMT to allow the monitoring of patient's health. To meet the constraint of medical secrecy and confidentiality of information, we will use the Blockchain as a secure system. Our system will use the data collected by several smart sensors such as blood pressure, SPO2 concentration, and EEG signals. These encrypted data will be collected by an embedded Raspberry PI 4 platform (working as a smart data relay) before being processed (on a backend server) and then saved in an embedded Blockchain node. The preliminary results show the effectiveness of the proposed platform as a candidate of a low-cost example of secured Electronic Health Record (EHR).

Keywords: EHR; blockchain; blood pressure; SPO2; EEG; Raspberry PI 4; FPGA

check for updates

Citation: Ktari, J.; Frikha, T.; Ben Amor, N.; Louraidh, L.; Elmannai, H.; Hamdi, M. IoMT-Based Platform for E-Health Monitoring Based on the Blockchain. *Electronics* **2022**, *11*, 2314. https://doi.org/10.3390/electronics11152314

Academic Editor: George Angelos Papadopoulos

Received: 10 June 2022
Accepted: 19 July 2022
Published: 25 July 2022

1. Introduction

The evolution of embedded systems has followed an ascending curve during the last decades. Indeed, we have seen the use of embedded systems touching such domains industry 4.0, agriculture, information systems, commerce, education, and the health domain. Because of its importance in the health and well-being of humans, the use of the new technologies in these fields has recently increased. Indeed, using artificial intelligence algorithms to process data from different sensors is an efficient new technique to detect anomalies, diseases, problems, or alerts. Indeed, it allows having an effective solution of medical diagnostic assistance based on embedded systems.

However, in the context of this type of application, we are confronted with an important problem—the confidentiality of the applications. To overcome this problem, several possibilities are available to secure the data, such as data encryption, elimination of personal information, etc. [1,2]. In this work, we will propose an approach based on Blockchain technology to secure information. The Blockchain is considered as a suitable technology since it allows making the encryption of information and preserving the confidentiality of data while allowing having immutable and irreversible traces.

Our paper consists of 4 parts. We start with a state of the art on the Blockchain in general and then the Blockchain applied to the medical field, and finally the embedded Blockchain. Then, we will propose the implemented approach. The results of the work will be revealed in part 3. We close our paper with a conclusion and some perspectives.

2. Blockchain Overview

Blockchain is a technology that allows information to be stored and transmitted transparently and securely. It consists of a database that contains the history of all exchanges made between its various users. This database is secure and distributed. It is somehow shared by its different users without intermediary, which allows everyone to verify the validity of the chain [1].

The Blockchain, which uses trustworthy and secure transaction, can be used in three ways:

- For the transfer of assets (money, securities, shares, etc.) [2]
- For a supply chain and a better traceability of assets and products [3]
- For securing confidential data (voting, health, diplomas, etc.) [4–7].

2.1. Blockchain Characteristics

Blockchain technology is characterized by:

- Disintermediation: The first property of Blockchain is to produce the trust necessary for users to exchange without the control of a trusted third party. The Blockchain allows trust to be based solely on technology and on the possibility for everyone to control transactions and their validation at any time. Trust is distributed here and no longer requires an intermediary [8].
- Transparency: Once a document is registered on the Blockchain, it exists at the moment and cannot be modified. Anyone can download the entire Blockchain and verify its reliability at any time. This is why the Blockchain is qualified by its transparency. All users of the Blockchain can see the present and past transactions. It also makes it possible to trace transactions and amounts when it comes to money [1].
- Security: Within a blockchain, all blocks are replicated in the network nodes and not in a single server. This decentralized architecture acts as a structural defense against the risks of data theft. Blockchain technology guarantees the security of recorded information. These records are said to be immutable: once stored, they become reserved forever and cannot be easily changed [1]. In order to overcome the security challenges, various solutions related to blockchain have been proposed in literature [9–15]. These solutions discuss the importance of security and privacy in healthcare system and suggest the advantages and challenges of utilizing blockchain as a solution in healthcare systems. Farouk et al. [16] illustrated the need of data privacy protection in IoT-enabled healthcare system and emphasized the way blockchain technology is used to achieve privacy goals. Kumar et al. [14] discussed Permissioned Blockchain and smart contract with Deep Learning (DL) techniques to design a novel secured and efficient data sharing framework. Turjman et al. [17] discussed different ways to integrate blockchain with the healthcare system in order to address issues like security, privacy, access control integrity, and ownership. Sengupta et al. [18] reviewed the benefits of smart contracts in terms of privacy protection and the ways they can extend the capabilities of blockchain. Other studies have focused on preventing unauthorized access [19] and protecting against eavesdropping [20]. Multiple means, such as efficient authentication [21], biometric authentication [22], user verification [23], and the use of dual signatures [24] have been suggested to achieve this objective. However, relatively less attention has been paid to the prevention of external attacks, such as attacks on sensor data [25], escrow, and collusion attacks [26]. In [15], Kumar et al., a Trustworthy Privacy-Preserving Secured Framework (TP2SF) for smart cities is presented. This framework includes three modules, namely: a trustworthiness module, a two-level privacy module, and an intrusion detection module. In trustworthiness module, address-based blockchain reputation system is designed. In the two-level privacy module, a blockchain-based enhanced Proof of Work (ePoW) technique is simultaneously applied with Principal Component Analysis (PCA) to transform data into a new reduced shape to prevent inference and poisoning attacks.
- Autonomy: The blockchain system is autonomous and independent, which means that each node of the blockchain system can access, update, transfer, and store data securely [8].

2.2. Different Blockchain Types

There are several types of blockchain dedicated to different use cases:

- Public Blockchain: The public blockchain is the historical blockchain. It is a blockchain that anyone throughout the world can read and send transactions to. Such transactions are expected to be included in the register, at least when they yield to the rules of the blockchain. It is a decentralized network that works as a Peer-to-Peer network, in the sense that it makes an exchange between two actors without intermediaries thanks to a trust relationship. It is a type of Blockchain that is free to access. Anyone can make transactions and/or verify them. The most known is Bitcoin [27].
- Private Blockchain: This type of Blockchain is considered a centralized network because it is completely controlled by an organization. In a private blockchain, a regulatory authority validates the introduction of new members and grants write and read rights. This authority can be in sole control or collegially governed by the different participants. Therefore, its access and use are limited to certain actors. No one can participate without being authorized, but anyone can consult it. This type of Blockchain is mainly used by companies such as banks. For the private Blockchain we can quote MultiChain, Hyperledger Fabric [28], etc.
- Permissioned Blockchain: A Consortium Blockchain brings together several private actors who have an interest in working together. Decisions or block validations are made by the most important members, and not by the whole network as in public Blockchains. The decision makers are the only ones who can verify the validity of the blocks. Consortium blockchain is the controlled blockchain, in which the approval process is controlled by a small and select number of nodes. The right to read the blockchain can then be public, reserved for participants, or hybrid. For the consortium type blockchain we know Corda, also known as R3, Ethereum, etc. [29].

2.3. Blockchain Applications

The blockchain technology can be used in several ways, as mentioned before. These include:

- For asset transfer (money, securities, stocks, etc.)
- For supply chain and better traceability of goods and products
- For securing confidential data (voting, health, diplomas, etc.)

As a result, using blockchain has become more and more common in such fields as the economy, industry, smart cities, and especially e-health. In the field of finance and entrepreneurship, the use of Blockchain is becoming more and more common. Larios-Hernández argued that "blockchain entrepreneurship can generate semi-formal financial services that bring people's financial aspirations closer together". Blockchain therefore enables a new type of inclusive entrepreneurship. It provides a suitable solution for financial inclusion at the bottom of the pyramid [30].

In [31], McKinsey et al. highlighted the importance of Blockchain technology. They presented several areas of use for this technology, such as:

- Tracking of containers during the shipping process
- Gift and ownership
- Digital assets
- Protection of intellectual property
- Peer-to-peer lending through bitcoin or Ethereum

Moreover, blockchain technology has great potential for a range of activities in the manufacturing industry. To make good use of blockchain in industry and especially in Industry 4.0, we will use data extracted from sensors. In this framework we talk about IoT technology, which becomes the source of different data that will be secured by the blockchain. In [32], Attran et al. presented an approach to highlight the potential of Blockchain in the industrial domain. Blockchain permits to give an efficient tracking of containers, to across multiple constituencies, to accurate recording of all important product information, but also supports security and compliance adherence, to expedite reconciliation of the contract and transfer of money [33].

For Industry 4.0, the Blockchain allows to:

- Act as a bridge between IoT devices.
- Sensor that timestamp data on the blockchain: it saves them from manipulation
- Reduce the vulnerability
- Formation of marketplace to enable customers to sell their data from IoT devices
- A platform to save IoT data on a private blockchain and share it with all business partners [34].

That is why Blockchain improves reliability, deals with IoT deployment challenges, handles big volumes of data, collaborates, communicates, and connects, including integration and communication, secures from cyber-attacks, and finally permits government regulations, particularly of privacy issues or within the framework of smart city.

In fact, smart cities use information and communication technologies to increase operational efficiency, share information with citizens, and improve both the quality of services and the well-being of citizens. Blockchains are suitable for autonomous transactions between networked devices and machines. For example, an electric car could pay for a charging station in order to get electrical energy or pay a toll to cross a toll gate. Thus, one idea adopted is to use blockchain-enabled smart charging stations. In [35] smart meter, users pay for electricity in cryptocurrencies (Velcoin). Another application in smart cities is presented. It is to use the Blockchain to book, pay, and manage smart parking lots. In [36], Badr et al. illustrated this use case of the Blockchain. In the next part, we will focus on the use of blockchain in the field of e-health.

2.4. Blockchain for E-Health

The sharing of data among different medical devices and healthcare providers plays a crucial role in an IMoT network. However, one of the major issues in secure data sharing is data fragmentation. Data fragmentation may lead to an information gap across healthcare providers who are associated with a single patient. Insufficient information may hinder the treatment process. Blockchain technology is used to solve the problem of data fragmentation and help the healthcare centers to establish a connection among the data repositories that are present in the network. This further ensures secure and protective sharing of sensitive medical information and increases transparency between the doctors and patients. Blockchain technology also promotes collaboration among healthcare providers and organizations to do qualitative research.

The secure transmission in blockchain technology can be due to three factors. First, it contains an immutable "ledger" that can be accessed and controlled by people. It ensures that once a record is stored in the ledger, it cannot be modified. Further, each transaction in the ledger must follow certain predefined rules. Second, blockchain is a distributed technology and operates simultaneously from multiple devices and computers. Third, blockchain follows the agreement rules and data exchange policies with a smart contract mechanism. The smart contract manages identity and sets out permissions to access different electronic medical reports (EMRs) that are stored in the blockchain. It means that doctors are only allowed to go through those EMRs to which they have been permitted. Over recent years, numerous blockchain projects have been established in the healthcare industry for the management of EMR, medicine prescription, and clinical pathways.

Healthcare and pharmaceutical companies are already vouching for its effectiveness by spending millions of dollars. According to a recent report, blockchain in the healthcare market is expected to reach $890.5 million by 2023 [37]. In healthcare, blockchain is recognized as an effective tool to avoid data breaches, increase the accuracy of medical records, and reduce costs. Some countries such as Australia and the United Kingdom have begun experimenting with Blockchain technology to manage medical records and transactions with patients, healthcare workers, and insurance companies. With a decentralized network of computers managing the Blockchain and simultaneously recording every transaction, conflicting information is automatically detected.

To modernize the analysis and care process, healthcare professionals are now embracing IoT. Billions of sensors and devices have been connected via the internet. Remote patient monitoring technology is now common for therapy and care offered to patients. However, these tools also pose serious privacy and security risks with respect to the transfer of information and the recording of data transactions. These security and confidentiality problems of medical information can result in a delay in the course of treatment and can even endanger the life of the patient. In [38], SimićMiloš et al. propose the use of Blockchain to provide secure management and analysis of important medical data.

By combining IoT with Blockchain, we could easily collect various patient data from different nodes, and perform real-time patient monitoring while storing the data more securely. Due to the current lack of database features in Blockchain technology, the data could be stored efficiently by using Big Data tools. Blockchain technology and big data have both experienced a quick growth. Coupling these two emerging technologies satisfies two important Big Data analysis requirements, which are security and efficient data organization. The proposed system in this paper targets various medical data and analysis exchanges between patients and doctors. As the proposed system is scalable, it must be able to fulfill both big data and blockchain technologies requirements while always being embedded. One of the possible key solutions is FPGA technology, which was already used in the work presented in this paper. Indeed, with its fine grain intrinsic parallelism, FPGA is well-tailored to serve as data center, while major FPGA vendors already propose data analytics frameworks and libraries.

Thus, we are able to reduce costs and improve collaboration between healthcare institutions using Blockchain. This will prevent hackers from storing or altering sensitive patient data. Blockchains provide robust, distributed systems and the ability to interact with nodes in a reliable and auditable manner. Blockchains offer smart contracts as a new mode of interaction. They enable the automation of complex multi-step processes. Devices in the IoT ecosystem are the touch points with the physical world [38,39].

2.5. Blockchain Constraints in Embedded Systems

As the use of embedded systems has become increasingly frequent, we find several works that implement the Blockchain despite its great greed in hardware and temporal resources. For example, in [7], Allouche et al. used the Blockchain to track documents and counteract plagiarism.

In [6], Frikha et al. used a Raspberry Pi 3 as a platform to be a Blockchain node for each patient and save both medial and confidential information as well as less secret data collected from a smartwatch (Blood pressure, steps count, walking time, and calories burned).

In [40], Falcone et al. proposed a blockchain-based mapping protocol for distributed robotic systems running on embedded hardware. This protocol was developed for a robotic system designed to locomote on lattice structures for space applications. They used proof of validity as consensus.

In [41], Dammak et al. proposed an IoT Architecture Integrating Blockchain and LoRa Network for Personal Health Care Data Monitoring. They used Arduino with Lora Shield and pulse heart sensor for ECG data. In [42], an embedded architecture was proposed to implement an HW IP for accelerating Proof of Work Consensus. This consensus is the most secure one. PoW is greedy, which is why Frikha et al. [42] proposed a Verilog IP implemented on FPGA (Field Programmable Gate Arrays) to improve system efficiency especially the real-time and the low power constraints [43–46]. In fact, most of the IoMT devices run on battery. Once a sensor is put on, the replacement of the battery is not easy. As such, a high-power battery was used to power such a system.

Moreover, as we mentioned in healthcare, real-time analysis of data is a trend that becomes a reality. In fact, doctors are able to consult the historical data assigned to patients.

They are also authorized to ask for real-time data before writing a report describing the health state and prescribing the right treatment.

Indeed, after the authentication, each one of the Medical Staff is able to handle all the application functionalities according to the permission given by the Healthcare Service Provider. For example, a doctor can consult all the patient data which are assigned to them and whose parameters are stored in the Blockchain platform. They can ask for real-time parameters using a communication protocol through the application server.

Finally, they are able to write a report about the patient's health state. This file will be uploaded by the doctor and stored into the platform. The Hash of the uploaded file is then added to the Blockchain platform. Moreover, nodes must allow data to be collected and locally processed and reduce recurring transmissions over the cloud between Cloud and device users, which ensures real-time computation and improved QoS.

On the other hand, concerning the overall performance evaluation of blockchain systems, some metrics cannot reflect the detailed performance in different process stages. Detailed performance information of blockchain is urgently required and metrics are lacking. Moreover, the overhead of real-time diagnostic, as well as scalability of the monitoring framework, need to be comprehensively investigated. Thus, the challenges of performance monitoring for blockchain systems can be summed up as to what and how to monitor. To attack the above challenges, some studies [47,48] focus on real-time performance monitoring framework for blockchain systems. The framework gets the performance data in real-time by log analysis and daemon process.

The feasibility of implementing Ethereum Blockchain with Proof of Work on an RPi, as well as the possibility of having a reliable IoT-based system, is shown in Reyna et al. [49]. For example, EthEmbedded enables the installation of Ethereum full nodes on embedded devices such as Raspberry Pi, Beaglebone Black, and Odroid. Raspnode and Ethraspbian both support the installation of Bitcoin, Ethereum, and Litecoin full nodes on a Raspberry Pi.

It should be noted that Ethereum uses ECDSA (Elliptic Curve Digital Signature Algorithm) for its public-key cryptography [50,51]. This is the same as bitcoin. The ECDSA signature assigned to an Ethereum transaction proves that the sender of the transaction had the required access to the private key, and the transaction has not been changed since it was signed.

It should also be noted that a transaction object needs to be signed using the sender's private key. With the signature hash, the transaction can be cryptographically proven that it came from the sender and submitted to the network. Moreover, ownership of Ethereum blockchain is established through private keys, addresses, and digital signatures. The private keys are at the center of all user interactions with Ethereum. In fact, account addresses are derived directly from private keys, which uniquely determine a single Ethereum address account.

In the next section, we will propose the implemented approach and the embedded platform for the collection, use, and management of medical and pharmaceutical data.

3. Proposed Approach

3.1. Generalized System

In the context of our platform, the proposed work is to implement an efficient embedded system for patient monitoring, analysis, and diagnostic support. Figure 1 represents a generalized embedded e-health system managed by different Raspberry PI (RPi).

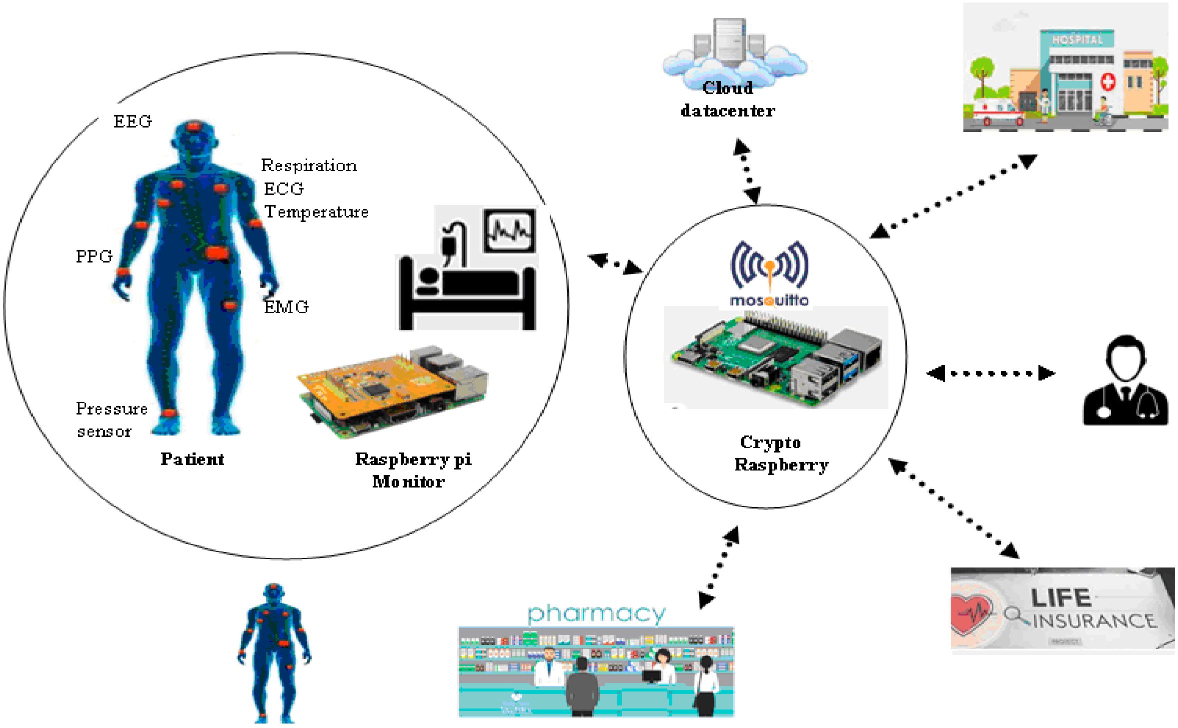


Figure 1. Embedded platform for the collection, use and management of medical and pharmaceutical data.

The following patient data are sent by different sensors: EEG (electroencephalogram), ECG (Electrocardiogram), PPG (Peak Pressure Gradient), EMG (Electromyography), blood pressure, and SPO2 (oxygen concentration). These sent data are then collected in a Raspberry PI “RPI” (mentioned as Raspberry pi Monitor in the Figure 1). The choice of the RPi is due to the fact that it is a low-cost multiprocessor embedded platform. Its low power consumption (less than 2 watts) makes it suitable for embedded computing.

The RPi is, indeed, more powerful than an Arduino platform, easier to program, and less complex than an FPGA. It also gives access to more peripherals than the STM 32. Raspberry can host a web server as well.

The patient data is then transferred to the Raspberry Crypto platform. This is a Raspberry PI responsible for sensor data encryption. Encryption can be done using the RPI itself or an add-on daughter board. The proposed platform is connected not only to the patient’s sensors but also to the hospitals that use this technology for the patient.

The proposed platform can be used by pharmacists to register the medicines bought by the different patients according to the prescriptions given either by structures (hospital, clinic, etc.) or directly from the doctor who is connected to our Blockchain system.

In parallel, insurance companies can also access our system to check the reimbursement forms that are sent by patients. Thus, in case of adequacy, the patient is reimbursed; otherwise, the system allows detecting fraud attempts. Indeed, the irreversibility of any data is recorded in the Blockchain, which makes it impossible to defraud or delete data that have been saved.

The use of the cloud is used to keep track not only of transactions but also of data that require a lot of space (MRIs, scans, medical reports, etc.).

Based on this platform, we designed a minimalist system as a proof of concept.

3.2. Proposed Minimalist System

This system is presented in Figure 2.

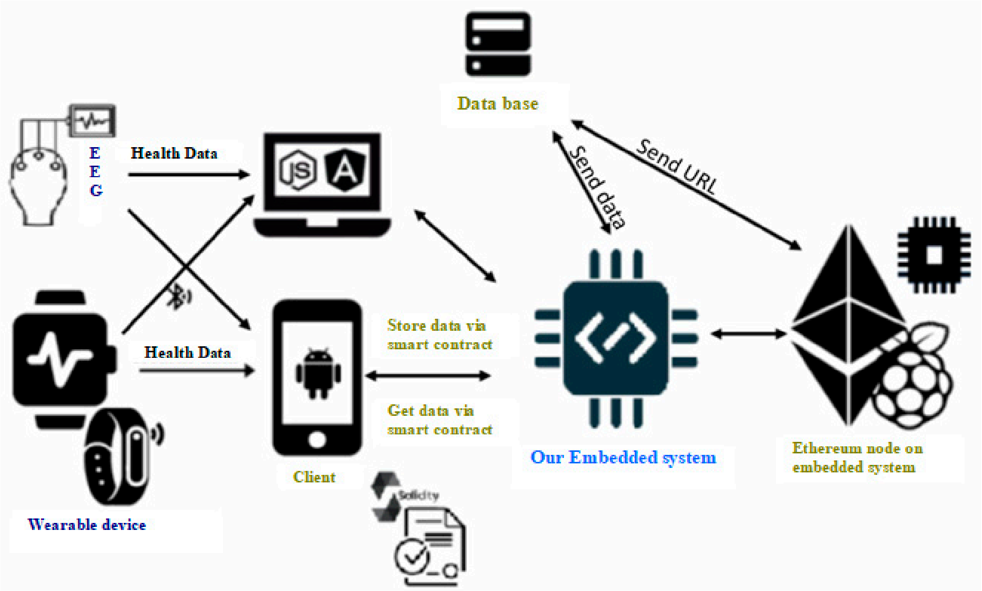


Figure 2. Proposed minimalist system.

Our minimalist system supports the use of wearable devices such as wristbands for number of steps count and number of pulses, smartwatches (SPO2, steps count, heart rate, sleep time and quality, stress indexes), and EEG headsets. When the wearable system option is used, a smartphone is used as a relay for sending data using Bluetooth or Wifi for the so-called "our embedded system" in Figure 2. It is a RPI 4 equipped with a powerful multiprocessor SoC and 2GB of RAM. All RPI 4 collected data are stored in a local Data Base. Stored data are accessed using a web server hosted on the RPI 4 that allows clear and simple access to different users (clients, doctors, etc.).

These data are then sent to the Blockchain in order to save the most voluminous ones (X-ray, MRI, CT images, etc.) and make the others as transactions in the Blockchain. We use an embedded hardware structure for the Ethereum Blockchain.

One of the main components of our system is the EEG headset. EEG is a process of monitoring and storing information about the electrical activity of the human brain. EEG signals consist of spontaneous and rhythmic impulses of the brain neurons. In neuroscience and psychology, it is suggested that EEG signals can describe affective brain states and human behavior or abnormal brain diseases and cognitive impairments such as Epilepsy [48], Parkinson's disease [52], and memory problems like Alzheimer's [53]. To track EEG signals, different headsets can be used. Wearable EEG headsets position non-invasive electrodes along the scalp. The collected data are sent to a computer or mobile device for storage and data processing, using wired or wireless connection. Wireless EEG headsets offer freedom of movement and are preferred to wired headsets. There are many different EEG wireless headsets that differ in price, electrodes numbers, availability of extra sensors (like gyroscope, magnetometer), the availability of a feature-rich software, and the required libraries and packages to build customized applications. We chose the Emotiv insight EEG headset [54,55] (white color model). With less than 500 US dollars in 2021, this headset offers a 5-channel, a gyroscope, and a rich software support [54].

Figure 3 represents an overview of the embedded Ethereum architecture.

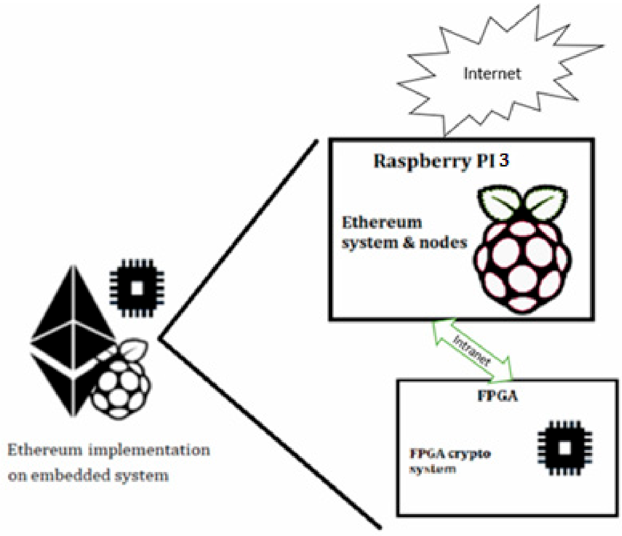


Figure 3. Permissioned Ethereum architecture implementation.

It is composed of two platforms:

- Raspberry PI 3 that executes the different nodes and which allows to set up the encrypted transactions. This platform was connected to the Raspberry Pi 4 via Internet (WiFi) [56]. It sends data to FPGA using RJ-45 link for encryption and then creates the different Blocs. That is why we do not to have a platform with high resources. We can consider the PI 3 as a master.
- The FPGA board that runs the complex encryption and mining Blockchain function using the Keccak algorithm [57], which is the algorithm used by the PoW. We used the Zedboard equipped with an AMD-Xilinx Zynq-7000 FPGA [58]. FPGA technology [59] is adopted here as it permits the creation of custom architecture tailored to the Keccak algorithm. For this aim, several custom and dedicated hardware accelerators (called IPs in the paper) are developed. These IPs allow mining based on the PoW.

The encrypted and mined data are then sent back to the Raspberry Pi 3 to be saved. The purpose of this task is to secure the Blockchain and keep the data confidential.

Once mined, the encrypted data are sent back to the Raspberry PI 4 so that the node can be validated.

The public and private key pair of the user is generated throughout the cryptographic algorithm, which enjoys a unique correspondence relation and is adopted in the smart contract to confirm the user's identity and authority. By checking the recorded certificate content and the public key used for signature, we can scrutinize whether the certificate data is fabricated or tampered.

This decentralized system allows the patient to add doctors, nurses, pharmacists etc. to this infrastructure. In order to accept the introduction of confidential medical data, the system must be secure. In this sense, the proposed system has two layers of security. Firstly, the various data stored are encrypted in the form of transactions. This is the first layer of security. The use of the PoW consensus during the mining process provides a second layer of security.

Therefore, only the doctor and the patient, respectively, can decrypt and thus access the information. This makes it possible to save the various sensitive data and only the patient owner or the attending physicians have the right to exchange them. This security is applied for patient data with low memory usage, heartbeat, respiratory rate, blood pressure, SPO2, and diabetes. Data are collected and sent every 5 min to be encrypted and used as a transaction. For more complex (2D) data like X-ray images, a database is used to store these data.

The patient's medical records are shared between doctor A and the patient. The patient, via the shared public key of doctor A and the doctor's private key, can have access to the data that the doctor will decrypt. These data will be encrypted by the same patient. The latter will do the encryption with the public key of doctor B and their private key. Doctor B will use their private key and the patient's public key to decrypt the file and have access to this information.

The minimalist proposed approach presented in this paper has been developed for a limited number of patients. Each patient runs their own private blockchain system, to which authorized medical stuff has access. A doctor can participate in several blockchain systems corresponding to his/her different patients. Since each one needs one RPI 3 and one FPGA board, it was not possible due to the limitation of available hardware kits, and we were constrained to show validation of a single patient (one node) blockchain architecture. The adoption of FPGA as a companion acceleration board allows us to successively map the blockchain on one low-cost RPI-based node. This makes it easy to migrate for a multi-node architecture. On the other hand, the flexible architecture of FPGA allows also the use of various computing hardware accelerators or multiprocessors architecture that make it suitable for other encryption schemes adopted by new updated blockchain protocol.

Using FPGA as a crypto-coprocessing unit has another important advantage over a solution like RPI-based software encryption. FPGA can give more security levels for stored data. Firstly, the architecture used can be highly customized using specific CPU cores that are neither popular nor hard to decrypt. The second level is the use of encrypted bitstreams which hardens the decryption process more.

Given that this system affects medical data as previously revealed, as well as data privacy, we opt for the PoW algorithm. Our Blockchain remains permissioned, and the data only needs to be kept and saved for traceability and security.

3.3. PoW Algorithm

Blockchain uses proof-of-work consensus to ensure that all participating nodes agree on the same branch. The main idea behind the protocol is to have nodes that solve a computationally expensive problem before they can suggest a new block. Proof of Work (PoW) is a way of protecting a decentralized network against attacks and data falsification. In a permissioned blockchain, miners do not usually receive a reward for their mining. Thus, the authors of [60] give arguments in favor of PoW, compared to Byzantine fault tolerance (BFT) based on voting.

In order to maintain the security and the confidentiality of the medical data, it is essential to use a powerful consensus. The permissioned Ethereum blockchain is used with PoW as a consensus.

Being greedy in execution time and CPU resources, the Keccak encryption algorithm is selected as a candidate for hardware acceleration on the FPGA platform. The first step for an efficient security is a careful analysis of the Keccak algorithm to ensure that the generated IP match as close as possible the internal characteristics of the algorithm. Figure 4 represents the flowchart of the PoW. The Keccak algorithm is located on the "256 bits hash" function. Indeed, if we find the nonce value that solves the Keccak problem, both the block, as well as a random value called nonce, will be mined. These values are combined and encrypted to get the hash number.

As soon as obtained, this value is compared to a source value which is the target value.

- If the hash is less than the target value, then the result is correct. Otherwise, the result is wrong.
- In case of error, you must insert a new nonce value and restart the process.
- This algorithm, after being profiled, is implemented in HW using the VHDL language.
- The obtained IPs are then embedded on FPGA to accelerate the PoW calculation.

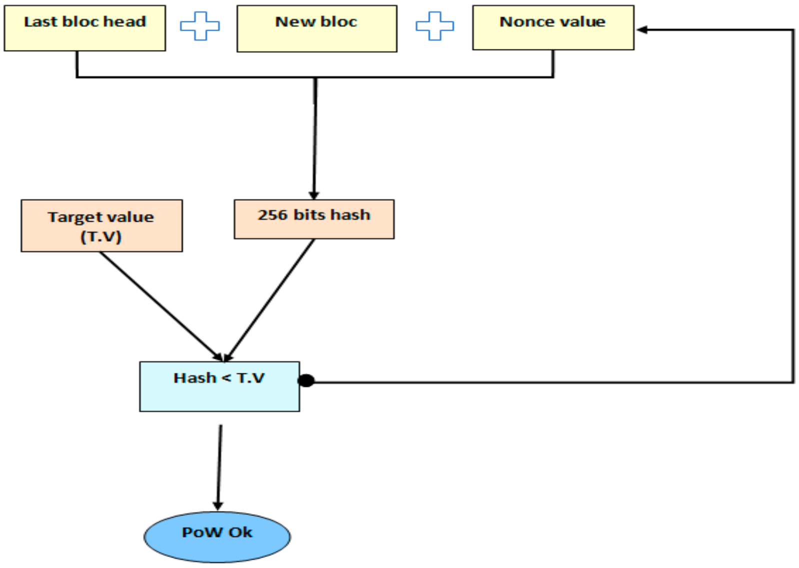


Figure 4. Keccak implementation algorithm.

4. Used Platform and Obtained Results

In this part, we will highlight the used platforms.

4.1. Hardware Used Platform

As system peripherals, we used a Smart watch Huawei GT 2 pro. This platform permits to have a lot of patient medical data (SPO2, heart rate), physical information (elevation, distance calories), stress rate, and sleep information.

We tested the SW platform (developed applications web and mobile) on different smartphones. This will be described in the next part. We used both an Iphone (IOS system) and a Samsung Smartphone (Android) to validate this approach

An illustration of our platform is provided in Figure 5.

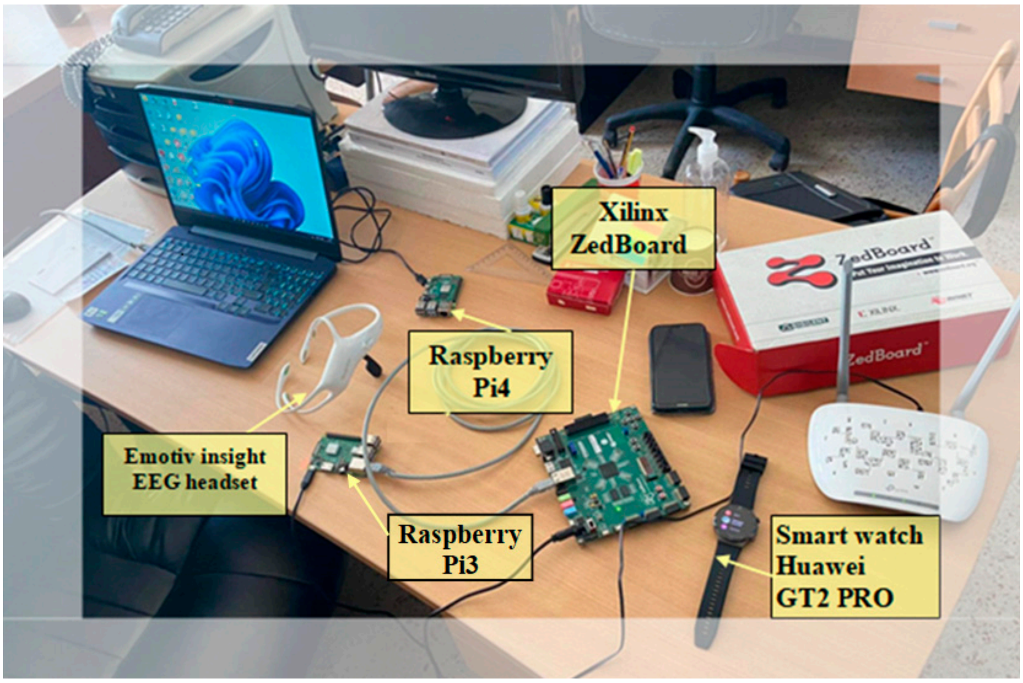


Figure 5. IoMT platform.

4.2. Hardware Implementation of the Keccak Algorithm

The hardware implementation of the Keccak algorithm uses 4 duplicated hardware components (IPs). These IPs help speed up the process. We only used 4 of them because the FPGA platform has limited resources. Therefore, we cannot implement more than 4 IPs that work in parallel.

Figure 6 describes the RTL implementation of one IP.

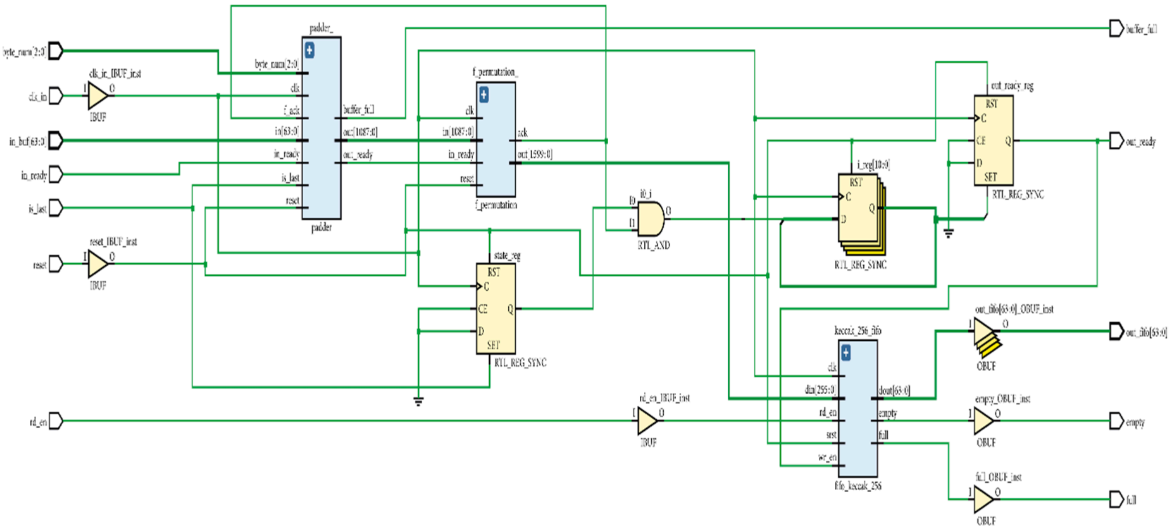


Figure 6. Internal architecture of one Keccak hardware accelerator (IP).

The implemented architecture is represented in Figure 7. We can see the 4 IPs connected to each other for the hardware architecture. The ARM processor is a scheduler that allows the allocation of one IP per transaction for hashing. If there is a need to mine, at least 3 IPs will be allocated for mining and the last one will be either allocated for mining or for hashing transactions. These encrypted data are the transactions that will be recorded on the blockchain and put online.

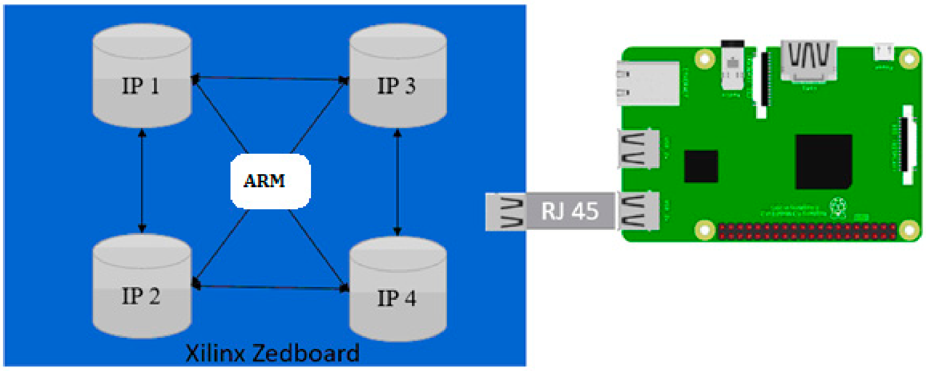


Figure 7. The proposed Intranet architecture.

The FPGA Zedboard is connected to the Raspberry PI 3 for mining and implementing the PoW consensus for our Ethereum FPGA. It is important to notice that the embedded CPU ARM available on the AMD-Xilinx Zedboard ensures the communication between Zedboard and PI 3 via RJ 45 communication.

A comparison between SW and HW implementation of the Keccak is illustrated in Table 1. As comparison metrics, we use energy consumption (obtained by Xilinx Power Estimator (XPE) and Vivado's power analysis tools) and real execution time. We have almost zero Watt as power consumption because we use the Xilinx Zedboard only when we need the accelerators. Otherwise, the Xilinx platform is placed in a standby low power state, contrary to a PC with high consumption graphic card (225W for the MSI Gaming Laptop with GeForce RTX 2070). HW implementation has a speed-up of about 7.5× times less than the SW one.

Table 1. Comparison of different HW/SW Keccak implementation.

	SW	HW
Execution time (ms)	21	2.78
Power consumption (W)	≈0	1.7

The energy study shows the efficiency of the proposed Keccak mixed hardware-software implementation. It ensures high speed-up without noticeable rise in power consumption. Indeed, it is common to have very high speed-up (execution time reduction of the mixed solutions over pure software solutions) results, but at the cost of an excessive use of hardware logics (and a consequent rise in power consumption).

4.3. Software Platform and Proposed Technologies

In this part, we will highlight the different technologies used.

4.3.1. Blockchain Application

We also used the Ethereum Blockchain. The choice of this Blockchain is due to two main reasons. Ethereum is a permissioned blockchain. It uses the most secure consensus: the PoW.

We also used the following software tools:

- Truffle: A world class development environment, testing framework and asset pipeline for blockchains using the Ethereum Virtual Machine (EVM).
- Ganache: Ganacheis used for setting up a personal Et4hereum Blockchain for testing the Solidity contracts [61].
- Metamask: it is a software cryptocurrency wallet used to interact with the Ethereum blockchain. It allows users to access their Ethereum wallet through a browser extension or mobile app [62].

4.3.2. SW Application

As represented in Figure 8, we present the different software used. We used NodeJS, reactJS, MongoDB, and Flutter.

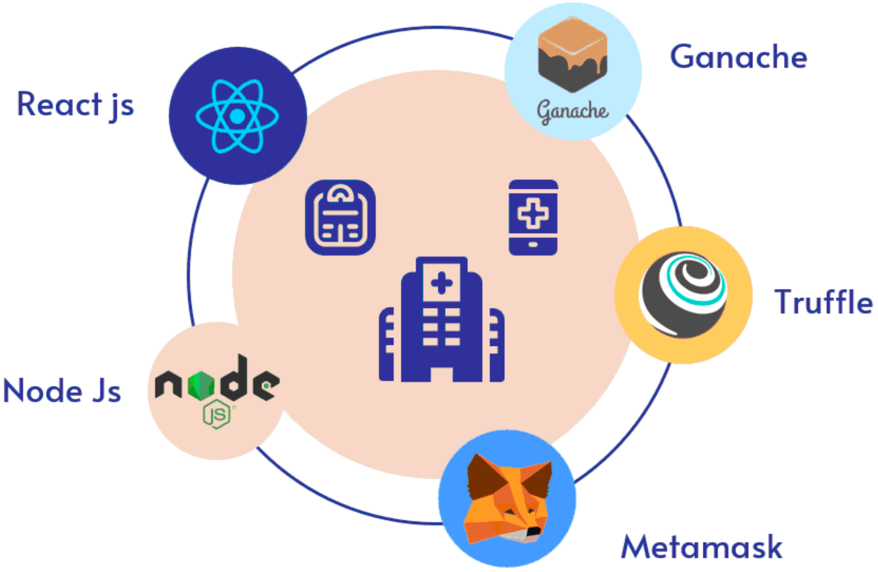
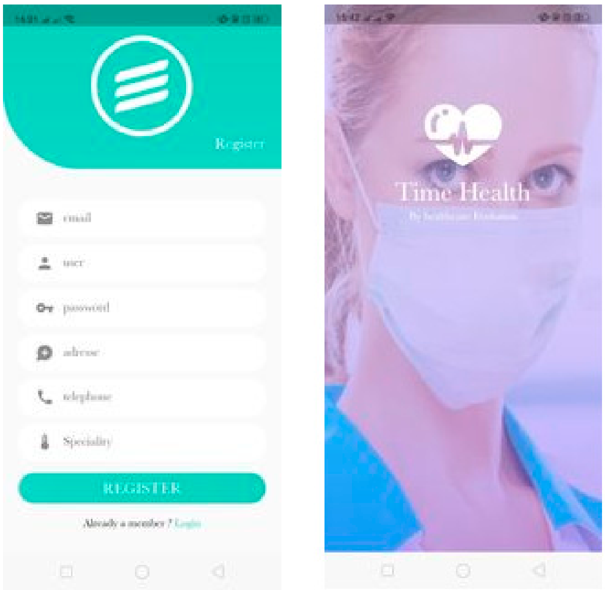


Figure 8. Used SW applications.

4.4. Obtained Results

4.4.1. Mobile Application

After implementing the architecture described in Section 4.3, and using the different tools (Truffle, Ganache, React JS, Flutter etc.), we show, in Figure 9a, the main page of the graphical interface of our Flutter application. Figure 9b describes the registration page allowing having access and becoming a client of our system.

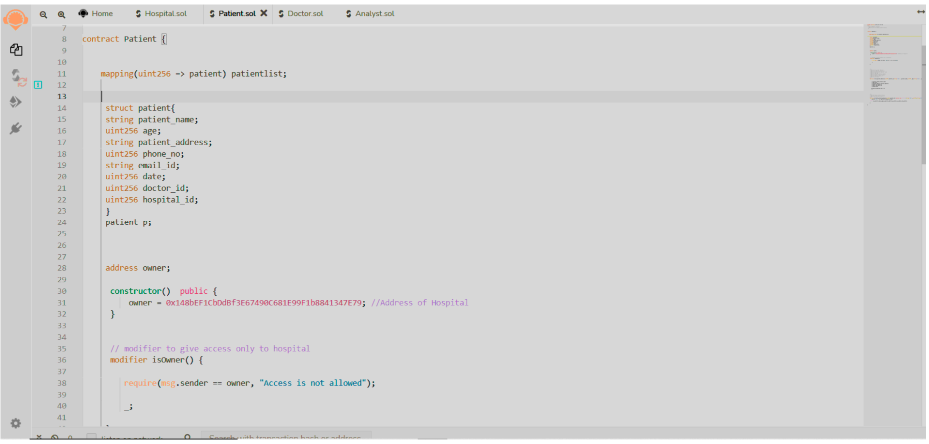


(**a**) (**b**)

Figure 9. (**a**) Registration interface; (**b**) Team Health welcome interface.

4.4.2. Blockchain Implementation

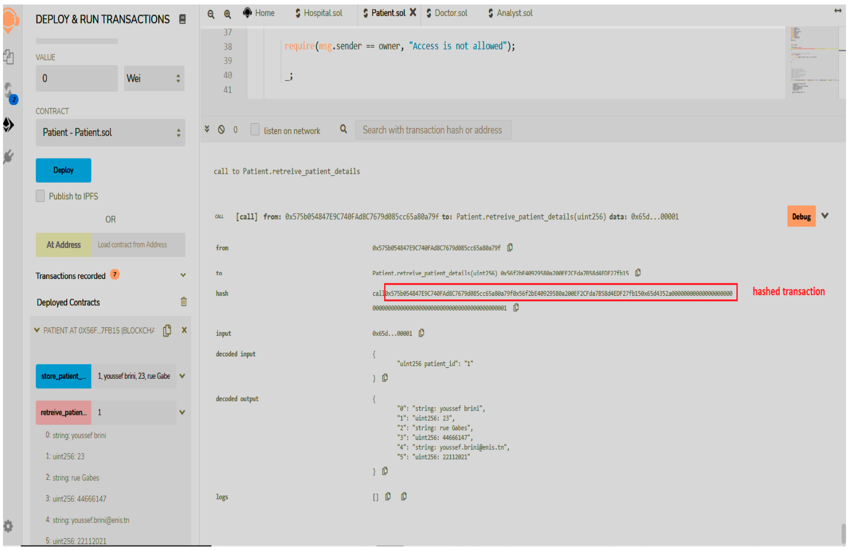
In Figure 10, we can see the solidity code representing characteristics of the patient and their inclusion to the hospital.



```
contract Patient {


    mapping(uint256 => patient) patientlist;


     struct patient{
     string patient_name;
     uint256 age;
     string patient_address;
     uint256 phone_no;
     string email_id;
     uint256 date;
     uint256 doctor_id;
     uint256 hospital_id;
     }
     patient p;



     address owner;

      constructor()  public {
          owner = 0x148bEF1CbDdBf3E67490C681E99F1b8841347E79; //Address of Hospital
      }


      // modifier to give access only to hospital
      modifier isOwner() {

         require(msg.sender == owner, "Access is not allowed");

         _;
```

Figure 10. Patient implementation using Solidity.

In Figure 11, we can find the deployment of the final transaction via Blockchain.



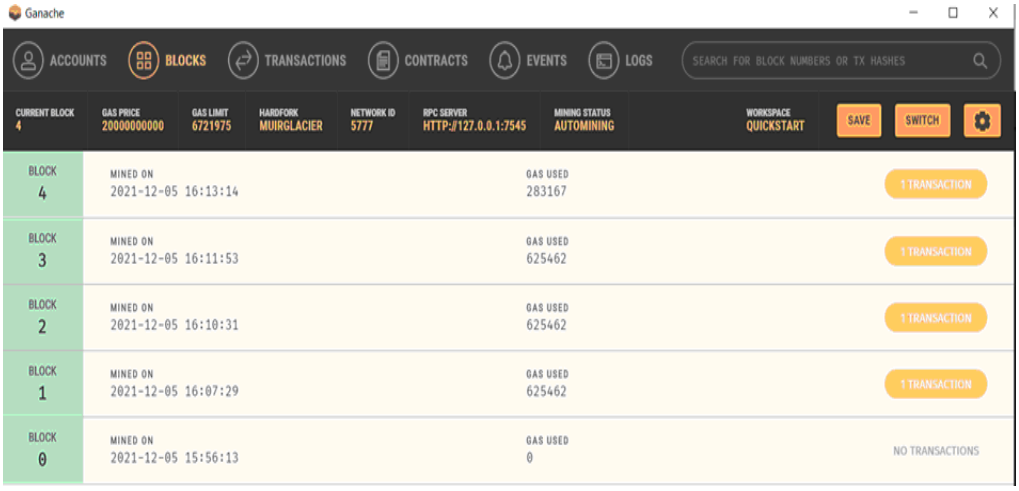
```
0: string: youssef brini
1: uint256: 23
2: string: rue Gabes
3: uint256: 44666147
4: string: youssef.brini@enis.tn
5: uint256: 22112021
```

```
        require(msg.sender == owner, "Access is not allowed");

        _;

```

```
call to Patient.retreive_patient_details

CALL  [call] from: 0x575b054847E9C740FAd8C7679d085cc65a80a79f to: Patient.retreive_patient_details(uint256) data: 0x65d...00001

from            0x575b054847E9C740FAd8C7679d085cc65a80a79f

to              Patient.retreive_patient_details(uint256) 0x56f2bE40929580a200EF2CFda7B58d4EDF27fb15

hash            call0x575b054847E9C740FAd8C7679d085cc65a80a79f0x56f2bE40929580a200EF2CFda7B58d4EDF27fb150x65d4352a00000000000000000000
                0000000000000000000000000000000000000000001

input           0x65d...00001

decoded input   {
                        "uint256 patient_id": "1"
                }

decoded output  {
                        "0": "string: youssef brini",
                        "1": "uint256: 23",
                        "2": "string: rue Gabes",
                        "3": "uint256: 44666147",
                        "4": "string: youssef.brini@enis.tn",
                        "5": "uint256: 22112021"
                }

logs            []
```

Figure 11. Deployment and running of transaction.

In Figure 12, we represent a simulation of blockchain and particularly paid transactions using virtual crypto currency. We can see 4 blocks. Each block contains one transaction. Block 0, which is the genesis block, does not contain transactions.



CURRENT BLOCK	GAS PRICE	GAS LIMIT	HARDFORK	NETWORK ID	RPC SERVER	MINING STATUS	WORKSPACE
4	20000000000	6721975	MUIRGLACIER	5777	HTTP://127.0.0.1:7545	AUTOMINING	QUICKSTART

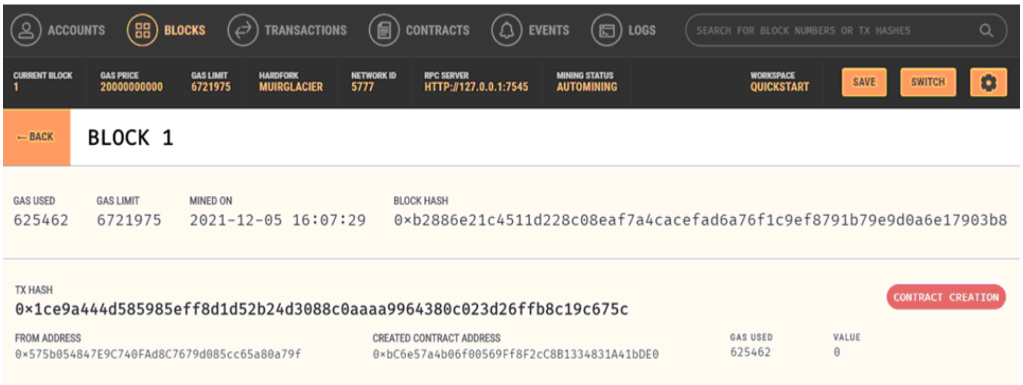
BLOCK	MINED ON	GAS USED	
4	2021-12-05 16:13:14	283167	1 TRANSACTION
3	2021-12-05 16:11:53	625462	1 TRANSACTION
2	2021-12-05 16:10:31	625462	1 TRANSACTION
1	2021-12-05 16:07:29	625462	1 TRANSACTION
0	2021-12-05 15:56:13	0	NO TRANSACTIONS

Figure 12. Paid transaction.

For example, the block 1 transaction used 625,462 Gas. In real Ethereum transactions, 283,167 gas corresponds to approximately 764 Ether. This result is obtained after implementation and result display from Ganache.

Figure 13 is obtained after displaying one of the blocks, especially Block 1. We notice the used Gas, the Gas limed, mining date, block hash, and transaction hash.

In this part, we have highlighted the mobile application, the blockchain implementation, and the different results obtained after implementing our SW application.



CURRENT BLOCK 1
GAS PRICE 20000000000
GAS LIMIT 6721975
HARDFORK MUIRGLACIER
NETWORK ID 5777
RPC SERVER HTTP://127.0.0.1:7545
MINING STATUS AUTOMINING
WORKSPACE QUICKSTART

BLOCK 1

GAS USED 625462
GAS LIMIT 6721975
MINED ON 2021-12-05 16:07:29
BLOCK HASH 0×b2886e21c4511d228c08eaf7a4cacefad6a76f1c9ef8791b79e9d0a6e17903b8

TX HASH 0×1ce9a444d585985eff8d1d52b24d3088c0aaaa9964380c023d26ffb8c19c675c
FROM ADDRESS 0×575b054847E9C740FAd8C7679d085cc65a80a79f
CREATED CONTRACT ADDRESS 0×bC6e57a4b06f00569Ff8F2cC8B1334831A41bDE0
GAS USED 625462
VALUE 0

Figure 13. Block 1 obtained result.

5. Discussion

As previously presented, in this paper, we presented a heterogeneous embedded platform to implement a multi-input EHR that uses different sensors connected via IoT. This platform secures the data doubly by using the Ethereum permissioned blockchain. In this work we chose to use PoW consensus. This choice was made to allow the securing of medical data. It is important that this data is not accessible or easy to hack.

As shown in the literature, the use of the Blockchain consumes a lot of energy. Thus, powerful computers, servers, and GPUs are used. In this work, we have proposed an efficient, secure, fast, and low energy consuming system compared to a classical PC. The energy study is presented to show the efficiency of the proposed Keccak mixed hardware-software implementation.

The use of the FPGA in our platform makes it possible to have a fast (multi-IP architecture totally parallel), secure (encryption based on Keccak transactions and mining), low energy (only the necessary resources for our application have been used) system.

Thus, our work proposes a rather complete system. We use different types of sensors that provide various data. These medical data are medical coming from very heterogeneous sources like health facility (hospital, radio center, clinic, etc.), patient data (SPO2, number of walking steps, etc.), and paramedical (pharmacy, para pharmacy etc.). These data are either used directly as transactions or stored in a database. The database link is encrypted and then used as a transaction to be secured. This approach is being tested with a single patient using FPGA and RPIs in order to validate the PoW.

This system can be enriched by using artificial intelligence to allow diagnostic assistance and therefore facilitate the work of doctors. On the architecture side, reconfigurable architectures can be used to save even more energy consumption and to have an even more reliable and optimized system.

6. Conclusions

In this paper, we have succeeded at setting a proof of concept of blockchain-based e-health as well as a real e-health platform based on embedded systems. Our system, unlike the works related to the Blockchain existing in the literature, allows us not only to use very limited hardware architecture (low-cost ZedBoard FPGA, Raspberry PI 3 and 4), but also offers efficient results in execution time and power consumption. Thus, we managed to have a heterogeneous platform that can represent a system which is usable in the context of personal data preservation and the safeguarding and securing of medical confidentiality. This work could be more enhanced by adding dynamic reconfiguration to further optimize the use of IPs and energy consumption. The technological transfer to make this platform more adequate can be achieved by implementing the Hyperledger Fabric Blockchain, which is a 100% private Blockchain.

Author Contributions: This paper is the result of a collaboration between different authors from different universities. Conceptualization, L.L., T.F., J.K.; methodology, N.B.A., T.F.; software.; validation, J.K. and N.B.A.; formal analysis, M.H.; investigation, L.L., H.E.; resources, M.H.; data curation, N.B.A.; writing—original draft preparation, J.K.; writing—review and editing, T.F.; visualization, M.H.; supervision, N.B.A.; project administration, T.F.; funding acquisition, M.H. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2022R125), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia.

Conflicts of Interest: There is no conflict of interest.

References

1. Huaqun, G.; Xingjie, Y. A survey on blockchain technology and its security. *Blockchain Res. Appl.* **2022**, *3*, 100067, ISSN 2096-7209. [CrossRef]
2. Cretarola, A.; Figà-Talamanca, G.; Grunspan, C. Blockchain and cryptocurrencies: Economic and financial research. *Decis. Econ. Financ.* **2021**, *44*, 781–787. [CrossRef]
3. Jabbar, S.; Lloyd, H.; Hammoudeh, M.; Adebisi, B.; Raza, U. Blockchain-enabled supply chain: Analysis, challenges, and future directions. *Multimed. Syst.* **2021**, *27*, 787–806. [CrossRef]
4. Jafar, U.; Aziz, M.J.A.; Shukur, Z. Blockchain for Electronic Voting System—Review and Open Research Challenges. *Sensors* **2021**, *21*, 5874. [CrossRef] [PubMed]
5. Ralston, S.J. Postdigital Prospects for Blockchain-Disrupted Higher Education: Beyond the Theater, Memes and Marketing Hype. *PostdigitSciEduc* **2020**, *2*, 280–288. [CrossRef]
6. Frikha, T.; Chaari, A.; Chaabane, F.; Cheikhrouhou, O.; Zaguia, A. Healthcare and Fitness Data Management Using the IoT-Based Blockchain Platform. *J. Healthc. Eng.* **2021**, *2021*, 9978863. [CrossRef] [PubMed]
7. Allouche, M.; Frikha, T.; Mitrea, M.; Memmi, G.; Chaabane, F. Lightweight Blockchain Processing. Case Study: Scanned Document Tracking on Tezos Blockchain. *Appl. Sci.* **2021**, *11*, 7169. [CrossRef]
8. Bhutta, M.N.M.; Khwaja, A.; Nadeem, A.; Ahmed, H.F.; Khan, M.K.; Hanif, M.A.; Song, H.; Alshamari, M.; Cao, Y. A Survey on Blockchain Technology: Evolution, Architecture and Security. *IEEE Access* **2021**, *9*, 61048–61073. [CrossRef]
9. Zhang, L.; Zou, Y.; Wang, W.; Jin, Z.; Su, Y.; Chen, H. Resource allocation and trust computing for blockchain-enabled edge computing system. *Comput. Secur.* **2021**, *105*, 102249. [CrossRef]
10. Liu, D.; Zhang, Y.; Wang, W.; Dev, K.; Khowaja, S.A. Flexible data integrity checking with original data recovery in iot-enabled maritime transportation systems. *IEEE Trans. Intell. Transp. Syst.* **2021**, *Early Access*, 1–12. [CrossRef]
11. Kumar, P.; Kumar, R.; Gupta, G.P.; Tripathi, R.; Srivastava, G. P2TIF: A Blockchain and Deep Learning Framework for Privacy-Preserved Threat Intelligence in Industrial IoT. *IEEE Trans. Ind. Inform.* **2022**, *18*, 6358–6367. [CrossRef]
12. Kumar, P.; Gupta, G.P.; Tripathi, R. An ensemble learning and fog-cloud architecture-driven cyber-attack detection framework for IoMT networks. *Comput. Commun.* **2021**, *166*, 110–124, ISSN 0140-3664. [CrossRef]
13. Kumar, P.; Kumar, R.; Gupta, G.P.; Tripathi, R. BDEdge: Blockchain and Deep-Learning for Secure Edge-Envisioned Green CAVs. *IEEE Trans. Green Commun. Netw.* **2022**, *Early Access*. [CrossRef]
14. Kumar, R.; Kumar, P.; Tripathi, R.; Gupta, G.P.; Islam, A.K.M.N.; Shorfuzzaman, M. Permissioned Blockchain and Deep-Learning for Secure and Efficient Data Sharing in Industrial Healthcare Systems. *IEEE Trans. Ind. Informatics* **2022**, *Early Access*. [CrossRef]
15. Kumar, P.; Gupta, G.P.; Tripathi, R. TP2SF: A Trustworthy Privacy-Preserving Secured Framework for sustainable smart cities by leveraging blockchain and machine learning. *J. Syst. Archit.* **2021**, *115*, 101954. [CrossRef]
16. Farouk, A.; Alahmadi, A.; Ghose, S.; Mashatan, A. Blockchain platform for industrial healthcare: Vision and future opportunities. *Comput. Commun.* **2020**, *154*, 223–235. [CrossRef]
17. Al-Turjman, F.; Nawaz, M.H.; Ulusar, U.D. Intelligence in the internet of medical things era: A systematic review of current and future trends. *Comput. Commun.* **2020**, *150*, 644–660. [CrossRef]
18. Sengupta, J.; Ruj, S.; Bit, S.D. A comprehensive survey on attacks, security issues and blockchain solutions for iot. *J. Netw. Comput. Appl.* **2020**, *149*, 102481. [CrossRef]
19. Nguyen, D.C.; Pathirana, P.N.; Ding, M.; Seneviratne, A. Blockchain for secure EHRs sharing of mobile cloud based e-health systems. *IEEE Access* **2019**, *7*, 66792–66806. [CrossRef]
20. Uddin, M.A.; Stranieri, A.; Gondal, I.; Balasubramanian, V. Continuous patient monitoring with a patient centric agent: A block architecture. *IEEE Access* **2018**, *6*, 32700–32726. [CrossRef]
21. Nagasubramanian, G.; Sakthivel, R.K.; Patan, R.; Gandomi, A.H.; Muthuramalingam, S.; Balamurugan, B. Securing e-health records using keyless signature infrastructure blockchain technology in the cloud. *Neural Comput. Applic* **2020**, *32*, 639–647. [CrossRef]
22. Dhagarra, D.; Goswami, M.; Sarma, P.R.S.; Choudhury, A. Big data and blockchain supported conceptual model for enhanced healthcare coverage: The Indian context. *Bus. Process. Manag. J.* **2019**, *25*, 1612–1632. [CrossRef]

23. Hussein, A.F.; Arun Kumar, N.; Ramirez-Gonzalez, G.; Abdulhay, E.; Tavares, J.M.R.S.; Albuquerque, V.H.C. A medical record managing and securing blockchain based system supported by a Genetic Algorithm and Discrete Wavelet Transform. *Cogn. Syst. Res.* **2018**, *52*, 1–11, ISSN 1389-0417. [CrossRef]
24. Li, X.; Huang, X.; Li, C.; Yu, R.; Shu, L. EdgeCare: Leveraging Edge Computing for Collaborative Data Management in Mobile Healthcare Systems. *IEEE Access* **2019**, *7*, 22011–22025. [CrossRef]
25. Brogan, J.; Baskaran, I.; Ramachandran, N. Authenticating Health Activity Data Using Distributed Ledger Technologies. *Comput. Struct. Biotechnol. J.* **2018**, *16*, 257–266, ISSN 2001-0370. [CrossRef]
26. Guo, R.; Shi, H.; Zhao, Q.; Zheng, D. Secure Attribute-Based Signature Scheme With Multiple Authorities for Blockchain in Electronic Health Records Systems. *IEEE Access* **2018**, *6*, 11676–11686. [CrossRef]
27. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. Available online: https://bitcoin.org/bitcoin.pdfhttps://bitcoin.org/bitcoin.pdf (accessed on 8 May 2022).
28. George, J.T. Hyperledger Fabric. In *Introducing Blockchain Applications*; Apress: Berkeley, CA, USA, 2022. [CrossRef]
29. Arslanian, H. Ethereum. In *The Book of Crypto*; Palgrave Macmillan: Cham, Switzerland, 2022. [CrossRef]
30. Larios-Hernández, J.G. Blockchain entrepreneurship opportunity in the practices of the unbanked. *Bus. Horiz.* **2017**, *6*, 865–874. [CrossRef]
31. McKinsey & Company Blockchain Technology in the Insurance Sector. Quarterly Meeting of the Federal Advisory Committee on Insurance (FACI). 11 January 2017. Retrieved 12 April 2018. Available online: https://www.treasury.gov/initiatives/fio/Documents/McKinsey_FACI_Blockchain_in_Insurance.pdf (accessed on 1 June 2022).
32. Attaran, M.; Gunasekaran, A. *Applications of Blockchain Technology in Business*, 1st ed.; Springer Nature: Berlin, Germany, 2019. [CrossRef]
33. Sandner, P. Application of Blockchain Technology in the Manufacturing Industry. Frankfurt School Blockchain Center, 18 November 2017. Available online: https://medium.com/@philippsandner/application-of-blockchain-technology-in-the-manufacturing-industryd03a8ed3ba5e (accessed on 12 April 2018).
34. Tanwar, S.; Parekh, K.; Khanpara, P.; Tyagi, S.; Kumar, N.; Alazab, M. Blockchain for Industry 4.0: A Comprehensive Review. *IEEE Access* **2020**, *8*, 79764–79800. [CrossRef]
35. Velasco-Castillo, E. Nineblockchain Opportunities that Telecoms Operators Should Explore. Knowledge Center. 13 June 2016. Retrieved 12 April 2019. Available online: http://www.analysysmason.com/Research/Content/Comments/nine-blockchain-opportunities-Jun2016-RDMY0/ (accessed on 1 June 2022).
36. Badr, M.; Amiri, W.A.; Fouda, M.M.; Mahmoud, M.M.E.A.; Aljohani, A.J.; Alasmary, W. Smart Parking System with Privacy Preservation and Reputation Management Using Blockchain. *IEEE Access* **2020**, *8*, 150823–150843. [CrossRef]
37. *Prescient& Strategic Intelligence, Blockchain in Healthcare Market by Application*; P&S Intelligence: New York, NY, USA, 2018.
38. SimićMiloš, M.; SladicGoran, S.; Milosavljević, B. A Case Study IoT and Blockchain powered. In Proceedings of the 8th PSU-UNS International Conference on Engineering, Novi Sad, Serbia, 8–10 June 2017.
39. Metcalf, D.; Milliard, S.; Gomez, S.D.; Schwartz, M. Wearables and the Internet of Things for Health: Wearable, Interconnected Devices Promise More Efficient and Comprehensive Health Care. *IEEE Pulse* **2016**, *7*, 35–39. [CrossRef]
40. Falcone, S.; Zhang, J.; Cameron, A.; Abdel-Rahman, A. Blockchain Design for an Embedded System. *Ledger* **2019**, *4*. [CrossRef]
41. Dammak, B.; Turki, M.; Cheikhrouhou, S.; Baklouti, M.; Mars, R.; Dhahbi, A. LoRaChainCare: An IoT Architecture Integrating Blockchain and LoRa Network for Personal Health Care Data Monitoring. *Sensors* **2022**, *22*, 1497. [CrossRef]
42. Frikha, T.; Chaabane, F.; Aouinti, N.; Cheikhrouhou, O.; Ben Amor, N.; Kerrouche, A. Implementation of Blockchain Consensus Algorithm on Embedded Architecture. *Secur. Commun. Netw.* **2021**, *2021*, 9918697. [CrossRef]
43. Tien Tuan Anh, D.; Ji, W.; Gang, C.; Rui, L.; Blockbench, A. Framework for Analyzing Private Blockchains. In Proceedings of the 2017 ACM International Conference on Management of Data, Chicago, IL, USA, 14–19 May 2017; pp. 1085–1100.
44. Ktari, J.; Abid, M. A Low Power Design Space Exploration Methodology Based on High Level Models and Confidence Intervals. *J. Low Power Electron.* **2009**, *5*, 17–30. [CrossRef]
45. Ktari, J.; Abid, M. System Level Power and Energy Modeling for Signal Processing Applications. In Proceedings of the 2007 2nd International Design and Test Workshop, Cairo, Egypt, 16–18 December 2007; pp. 218–221. [CrossRef]
46. Ktari, J.; Abid, M. *A Low Power Design Methodology Based on High Level Models*; ESA: Paris, France, 2008; pp. 10–15.
47. Ingo, W.; Vincent, G.; Ponomarev, A.; Staples, M.; Holz, R.; Tran, A.B.; Rimba, P. On availability for blockchain-based systems. In Proceedings of the 36th International Symposium on Reliable Distributed Systems (SRDS), Hong Kong, China, 26–29 September 2017.
48. Acharya, U.R.; Subbhuraam, V.S.; Goutham, S.; Martis, R.; Suri, J. Automated EEG analysis of epilepsy: A review. *Knowl. Based Syst.* **2013**, *45*, 147–165. [CrossRef]
49. Reyna, A.; Martín, C.; Chen, J.; Soler, E.; Díaz, M. On blockchain and its integration with IoT. Challenges and opportunities. *Future Gener. Comput. Syst.* **2018**, *88*, 173–190, ISSN 0167-739X. [CrossRef]
50. Yang, X.; Liu, M.; Luo, X.; Ye, Q. Efficient Verifiably Encrypted ECDSA-Like Signatures and Their Applications. *IEEE Trans. Inf. Forensics Secur.* **2022**, *17*, 1573–1582. [CrossRef]
51. Shbair, W.M.; Gavrilov, E.; State, R. HSM-based Key Management Solution for Ethereum Blockchain. In Proceedings of the 2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Sydney, Australia, 3–6 May 2022; pp. 1–3.

52. Klassen, B.T.; Hentz, J.G.; Shill, H.A.; Driver-Dunckley, E.; Evidente, V.G.; Sabbagh, M.N.; Adler, C.H.; Caviness, J.N. Quantitative EEG as a predictive biomarker for Parkinson disease dementia. *Neurology* **2011**, *77*, 118–124. [CrossRef] [PubMed]
53. Melissant, C.; Ypma, A.; Frietman, E.; Stam, C. A method for detection of Alzheimer's disease using ICA-enhanced EEG measurements. *Artif. Intell. Med.* **2005**, *33*, 209–222. [CrossRef]
54. Emotiv Insight EEG Headset. Available online: https://www.emotiv.com/product/emotiv-insight-5-channel-mobile-brainwear/ (accessed on 8 August 2021).
55. Frikha, T.; Abdennour, N.; Chaabane, F.; Ghorbel, O.; Ayedi, R.; Shahin, O.R.; Cheikhrouhou, O. Source Localization of EEG Brainwaves Activities via Mother Wavelets Families for SWT Decomposition. *J. Healthc. Eng.* **2021**, *2021*, 9938646. [CrossRef]
56. Ktari, J.; Frikha, T.; Hamdi, M.; Elmannai, H.; Hmam, H. Lightweight AI Framework for Industry 4.0 Case Study: Water Meter Recognition. *Big Data Cogn. Comput.* **2022**, *6*, 72. [CrossRef]
57. Ktari, J.; Frikha, T.; Yousfi, M.A.; Belghith, M.K.; Sanei, N. Embedded Keccak implementation on FPGA. In Proceedings of the 2022 IEEE International Conference on Design & Test of Integrated Micro & Nano-Systems (DTS), Cairo, Egypt, 6–9 June 2022; pp. 1–5. [CrossRef]
58. Available online: https://docs.xilinx.com/v/u/en-US/ug585-Zynq-7000-TRM (accessed on 1 June 2022).
59. Frikha, T.; Ben Amor, N.; Diguet, J.P. A novel Xilinx-based architecture for 3D-graphics. *Multimed. Tools Appl.* **2019**, *78*, 14947–14970. [CrossRef]
60. Malakhov, I.; Marin, A.; Rossi, S.; Smuseva, D. On the Use of Proof-of-Work in Permissioned Blockchains: Security and Fairness. *IEEE Access* **2022**, *10*, 1305–1316. [CrossRef]
61. Available online: https://trufflesuite.com/ (accessed on 10 October 2021).
62. Available online: https://metamask.io/ (accessed on 10 October 2021).