

Article

Secure and Fast Emergency Road Healthcare Service Based on Blockchain Technology for Smart Cities

Amel Ksibi ¹, Halima Mhamdi ², Manel Ayadi ¹, Latifah Almuqren ^{1,*}, Mohammed S. Alqahtani ^{3,4}, Mohd Dilshad Ansari ⁵, Ashutosh Sharma ⁶ and Sakli Hedi ^{2,7}

¹ Department of Information Systems, College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University, P.O. Box 84428, Riyadh 11671, Saudi Arabia

² MACS Research Laboratory RL16ES22, National Engineering School of Gabes, Zrig Gabes 6029, Tunisia

³ Radiological Sciences Department, College of Applied Medical Sciences, King Khalid University, Abha 61421, Saudi Arabia

⁴ BioImaging Unit, Space Research Centre, Michael Atiyah Building, University of Leicester, Leicester LE1 7RH, UK

⁵ Department of Computer Science & Engineering, University Institute of Engineering & Technology, Guru Nanak University, Ibrahimpattam, Hyderabad 501506, India

⁶ School of Computer Science, University of Petroleum and Energy Studies, Dehradun 248007, India

⁷ EITA Consulting, 5 Rue Du Chant des Oiseaux, 78360 Montesson, France

* Correspondence: laalmuqren@pnu.edu.sa

Abstract: Road accidents occur everywhere in the world and the numbers of people dead or injured increase from time to time. People hope that emergency vehicles and medical staff will arrive as soon as possible at the scene of the accident. The development of recent technologies such as the Internet of Things (IoT) allows us to find solutions to ensure rapid movement by road in emergencies. Integrating the healthcare sector and smart vehicles, IoT ensures this objective. This integration gives rise to two paradigms: the Internet of Vehicles (IoV) and the Internet of Medical Things (IoMT), where smart devices collect medical data from patients and transmit them to medical staff in real time. These data are extremely sensitive and must be managed securely. This paper proposes a system design that brings together the three concepts of Blockchain technology (BC), IoMT and IoV to address the problem mentioned above. The designed system is composed of three main parts: a list of hospitals, patient electronic medical record (EMR) and a network of connected ambulances. It allows the road user in the case of an accident to report their position to the nearby health services and ambulances.

Keywords: Blockchain; smart contract; emergency healthcare services; IoMT; IoV; road accident



check for updates

Citation: Ksibi, A.; Mhamdi, H.; Ayadi, M.; Almuqren, L.; Alqahtani, M.S.; Ansari, M.D.; Sharma, A.; Hedi, S. Secure and Fast Emergency Road Healthcare Service Based on Blockchain Technology for Smart Cities. *Sustainability* **2023**, *15*, 5748. <https://doi.org/10.3390/su15075748>

Academic Editors: Juneyoung Park and Jun (Justin) Li

Received: 20 January 2023

Revised: 7 March 2023

Accepted: 16 March 2023

Published: 25 March 2023



Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

According to the World Health Organization (WHO), 1.3 million people die because of car crashes annually. In Tunisia, 616 people lost their lives, and 4873 others were injured in road accidents during the first 8 months of 2022, according to data from the National Observatory of Road Safety under the Ministry of the Interior.

The United Nations General Assembly has set an ambitious target for road safety to halve the total number of road traffic deaths and injuries by 2030 (A/RES/74/299). Several factors can contribute to reducing this number. Among them are the timely arrival of ambulances at the scene of the accident and the recognition of the medical data of the injured in advance by the medical staff. However, the questions here are how to determine the nearest available emergency vehicle and how to inform the emergency services of patient information. Therefore, two strategies are possible responses to these two questions. The first is the use of connected ambulances and the second is the sending of vital signals of injured people to the appropriate service in real time. In this case, emergent technology such as the Internet of Things is seen as a prominent solution to manipulate the components mentioned above.

The Internet of Things (IoT) has invaded several areas, including connected vehicles and healthcare [1–3]. As a result, a new paradigm named the Internet of Medical Things (IoMT) is arising. IoMT proposes to radically transform healthcare delivery. Through machine-to-machine (M2M) interaction and real-time intervention solutions, IoMT solves accessibility and reliability issues [4,5]. In addition, increased patient engagement in decision making will drive healthcare compliance. IoMT enables faster disease diagnosis and decision making by compiling large amounts of medical data in a timely manner. IoMT increases human–machine interaction, which improves medical record keeping. We are talking about the exchange of medical data that require a prominent level of confidentiality, security, and rapid intervention.

The convergence of IoT and Intelligent transportation system (ITS) gave rise to the concept of Internet of Vehicles (IoV) [6]. Over the past decade, the concept of the smart vehicle has grown considerably. It plays an especially key role in several application areas such as smart cities, healthcare, and intelligent transportation systems, since vehicles can communicate with each other and with their surroundings. Through vehicular communication, many data are manipulated that require extremely high security, confidentiality, and availability.

Blockchain technology has recently become important in systems that handle security and privacy concerns. In its report, published in December 2018, the National Assembly’s joint information mission on the uses of BC and other register certification technologies, defined BC technology as follows [7]: “A BC is a register, a large database that has the particularity of being shared simultaneously with all its users, all of whom are also holders of this register, and all of whom also have the ability to enter data into it, according to specific rules set by a computer protocol that is very well secured thanks to cryptography”. It is indeed a connection of nodes that communicate and save transactions. So, every entity in the network records a copy to mitigate a single failure point. The record from the BC is arranged in blocks to construct a distributed ledger (DLT). Cryptographic processes guarantee the confidentiality and integrity of data. Satoshi Nakamoto introduced the idea of BC for the first time in 2008 [8]. Numerous key characteristics highlight BC technology, such as decentralization, integrity, autonomy, confidentiality, and immutability [9,10]. These characteristics increase the demand for BC in a wide range of sectors [11,12].

The fusion between IoV and IoMT gives a fantastic opportunity to reduce the number of people losing their lives due to road accidents. However, the data managed in such cases are highly sensitive. They need a dependable, decentralized, and secure system. To ensure these properties, BC technology is highly recommended. The integration of blockchain technology, IoV, and IoMT is a crucial solution to these issues with decentralized, efficiency, privacy, and partner trust management. In the form of a distributed and secure register that enables emergency medical personnel in addition to have admission to harmed vital signs but also to change them, blockchain technology offers just such a solution. Hence, we guarantee the compatibility of the platform used by the various actors of the proposed system using Blockchain technology. To cut maintenance costs and get rid of legacy threats from centralized systems, this approach removes the central authority (CA). The fundamental goal is to build autonomous interaction without human involvement through smart contracts, ensuring security and trust amongst the agents in the system. To guarantee the security of patient data, the following criteria must be taken into consideration: authentication and access control.

Based on smart contracts, we propose a system for the treatment of road accidents. This system is composed of two subsystems. The first one includes an IoV part that takes care of the search for the nearest available ambulance and the nearest emergency service. On the other side, the second sub-system deals with the transfer of the vital signs of injured people to the appropriate emergency service staff.

The following are the most significant contributions of this manuscript:

- (1) Designing a system for road safety emergencies.

- (2) Proposing a subsystem to search for available rescue vehicles and the nearest emergency service, using IoV.
- (3) Suggesting a sub-system to transfer the patient's health data to the appropriate service.
- (4) To ensure the security and confidentiality of the exchanged information, smart contracts are provided in each part of the total system.

The rest of this manuscript is structured as follows. The second section covers the fundamental concepts of BC technology, IoMT, and IoV. Section 3 shows how BC technology is being used in healthcare data management and connected vehicles. Section 4 describes in detail the proposed system architecture. Finally, Section 5 wraps up this paper and offers some suggestions for future research. Table 1 summarizes a list of abbreviations and acronyms used in this paper.

Table 1. List of abbreviations and acronyms used in this paper.

Abbreviation	Full Form
WHO	World Health Organization
BC	Blockchain
IoT	Internet of Things
IoMT	Internet of Medical Things
ITS	Intelligent Transportation System
IoV	Internet of Vehicles
VANET	Vehicular Ad Hoc Networks
V2V	Vehicle to Vehicle
M2M	Machine to Machine
EMR	Electronic Medical Record
DLT	Distributed Ledger Technology
P2P	Peer to Peer
PoW	Proof of work
PoS	Proof of Stake
DPoS	Delegated Proof of Stake
PBFT	Practical Byzantine Fault Tolerance
HIS	health information system
MAS	Multi-agent system

2. Background

2.1. Internet of Vehicles and Road Accident

Yang et al. [13] proposed the IoV concept. It is, in fact, an improvement of VANET. In this network, people, vehicles, and their surroundings are grouped together or integrated to ensure better and safer operation of road services. In IoV, communication is not limited to vehicles (V2V), but we also find vehicle-to-everything communication [14], which leads to several applications. These applications include road safety applications such as collision, road speed and spot warning information. It moreover enables vehicles to exchange data on traffic and road conditions with their neighbors [15]. Vehicular communication involves the problem of exchanged data security. Security concerns can occur during any point in the IoV network's life cycle. Because massive amounts of data are created at any time and continue to grow, ensuring data security becomes increasingly difficult. So, it is necessary to guarantee data confidentiality against attacks or illegal use of crucial personal data. In this case, only authorized nodes can access the information. Furthermore, data integrity must be verified, so that end users receive the exchanged data without modification.

2.2. Internet of Medical Things

The IoMT integrates the digital and physical worlds to enhance patient health through faster, more accurate diagnosis and treatment as well as real-time changes in patient behavior and health condition [16]. The connectedness of medical equipment will have a significant impact on patients and doctors. IoMT plays a leading role in improving the efficiency, responsiveness, and remote monitoring of medical devices. The IoMT is

processed by connecting and communicating M2M using Wi-Fi-equipped medical devices. The received data are stored in the cloud server database and analyzed.

EMR is a filing system for information relevant to treatment. It contains elements from the computerized medical record. The process of opening a file should be easy and secure, since it involves sensitive medical information made available by physicians on a decentralized archiving system [17].

Since they are recorded in multiple health care organizations and manipulated in a centralized way, data decomposition, counterfeiting, and destruction are all major threats to today's health record frameworks. As such, many hospitals store their patients' data in a database via an agent. Regardless of the situation, each person is required to bring his report, if he switches doctors or hospitals. This is an untrustworthy method of overseeing such sensitive information [18].

2.3. Blockchain Technology

Satoshi Nakamoto's Bitcoin application, introduced in 2008, supported BC. BC is built on the idea of a distributed blockchain that allows for more secure transactions. Between the years 2009 and 2013, digital currency transactions were the basis of blockchain 1.0. Subsequently, BC 2.0 appeared following the use of smart contracts. These last ones offer a greater level of security and a tamper-proof transaction process. BC 3.0 and the concept of DApps were introduced by the Ethereum platform. BC 4.0 is gaining traction in business and industry.

Because of its powerful capabilities not only regarding distributed storage, but also for confidentiality, data protection, efficiency, automation, and lower processing cost, BC technology has recently emerged as a secure distributed process used in a variety of industrial application fields. The primary benefits that a BC technology can offer have motivated many industries and researchers to integrate it into a wide range of fields. These characteristics include decentralization, immutability, security and privacy, transparency, automation, and traceability [19].

2.3.1. Blockchains as Distributed Ledgers

A sort of distributed ledger technology called a blockchain enables numerous parties to share a single view of data without the need for a central authority. A distributed ledger is essentially a database that is shared among a group of computers, with a copy of the ledger being kept on each member of the network. Blockchains are intended to be tamper-proof, transparent, and secure. To do this, they employ encryption to make sure that once data is put to the blockchain, it cannot be changed or removed without the network's other users' consent. Blocks of data are connected in a chronological chain to form blockchains. Each block consists of a group of transactions, and each transaction denotes the transfer of data or digital assets. As a new block is added to the chain, the other network users verify it; if they find it to be genuine, the block is added to the chain and becomes a permanent part of the ledger. The potential of blockchains to build trust between parties who may not already have it is one of their main advantages. It is challenging for one party to falsify the data or game the system because the ledger is shared and can be read by anybody on the network [20–23].

Ledger databases are most associated with cryptocurrency transactions, as they provide the underlying infrastructure for cryptocurrencies such as Bitcoin and Ethereum. However, ledger databases have a wide range of potential applications, including supply chain management, voting systems, and digital identity management, among others.

Ledger databases are a type of database that is designed to maintain a continuously growing list of transactions or records, known as a ledger. The ledger database provides a tamper-proof, transparent, and auditable history of all transactions that have occurred. These databases are commonly used in finance, banking, and accounting.

There are several ledger databases technologies that are designed to support blockchain-based applications. Among them, we find Oracle blockchain table, Alibaba LedgerDB, and

Microsoft SQL Ledger [24–27]. Oracle blockchain table is a feature of the Oracle Database that allows developers to create blockchain applications using familiar SQL commands. It provides a secure and scalable infrastructure for storing blockchain data and executing smart contracts. With the Oracle blockchain table, developers can create blockchain applications without having to learn new programming languages or tools. Alibaba LedgerDB is a distributed database technology that is designed to support blockchain applications. It provides a highly scalable and reliable infrastructure for storing and processing large amounts of data. Alibaba LedgerDB is built on top of the Alibaba Cloud platform, and it is designed to be easy to use and deploy. Microsoft SQL Ledger is a blockchain-based ledger that is built on top of the Microsoft SQL Server database. It provides a secure and scalable infrastructure for storing and processing blockchain data, and it supports the development of smart contracts using familiar programming languages such as C# and NET. Microsoft SQL Ledger is designed to be easy to use and integrate with existing Microsoft technologies.

Overall, these technologies provide developers with powerful tools for building blockchain applications, and they offer a range of features and capabilities that make it easier to create secure, scalable, and reliable blockchain-based systems.

2.3.2. Smart Contracts

In 1995, Nick Szabo defines the smart contract as “a computerized transaction protocol that executes the terms of a contract. The general objectives of smart contract design are to satisfy common contractual conditions (such as payment terms, liens, confidentiality, and even enforcement), minimize exceptions both malicious and accidental, and minimize the need for trusted intermediaries. Related economic goals include lowering fraud loss, arbitration and enforcement costs, and other transaction costs” [28].

2.3.3. Consensus Mechanism

BC consensus protocols are “the agreement of a common value among a group of nodes in BC systems.” Indeed, their primary role is to instill trust in an untrustworthy atmosphere, as well as to validate the authenticity and reliability of data records linked to the new block [29]. In the PoW mechanism, a mathematical challenge or puzzle represents an amount of work that must be completed by a miner. This amount is easy to check but depends on the time needed to validate a block. A PoW guarantees the integrity of the blocks and transactions, but when overseeing the work, the PoW consumes a large amount of energy, not to mention the decrease in the number of miners. Most BC systems use this block validation mechanism. The PoS has the same goal as the PoW. Its basic principle is to randomly choose the validator of the block. This mechanism is more energy efficient because there is no mining where a lot of resources are consumed. Block validation is based on the amount of money in the node. A variant that has the same principle of proof of stake is named Delegated Proof of Stake. In the first one, the block validation is performed by any node of the network with a minimum number of crypto currencies. On the other hand, in DPoS, BC users use the voting principle to choose representatives. These representatives have the role of validating the blocks in place of the voters. It is a form of participatory democracy that brings speed and precision to the validation of transactions. The Practical Byzantine Fault Tolerance (PBFT) consensus algorithm is based on the same voting principle. It allows the main nodes in the distributed network to choose the transaction to be executed first. It uses the authentication of the request and response of nodes that allows avoiding system failures. PBFT guarantees a high performance by reducing the execution time seen in the PoW consensus, but with a delay in the data transfer.

3. Related Works

BC technology provides benefits such as decentralization, immutability, confidentiality, and data security exchange. As a result, BC could be a powerful tool for transforming

the IoV and IoMT systems into ones that are trustworthy, dependable, and private [30,31]. Tables 2 and 3 outline various works discussed in this section.

3.1. BC and IoV Shared Data

Yang et al. [32] propose a decentralized trust management approach in vehicle networks based on BC. Vehicles in this framework use the Bayesian inference method to validate data transmitted from surrounding vehicles. They employ a hybrid consensus technique that incorporates PoW and PoS. Through this fusion, all Roadside Units (RSUs) collaborate to keep the confidence BC up to date, credible, and coherent.

In [31], the authors suggested a trust management mechanism for the IoV system. The researched framework is to use BC technology to solve the scalability problem. Smart contracts and PoW as a consensus protocol verify the decentralized feature. The authors use the Ethereum BC platform for validation, which allows them to examine the system's performance in terms of average throughput and execution time.

In [33], the authors suggested security rules for fatal crash detection and alerting in an Intelligent Transportation System (ITS) atmosphere that used an identity verification technique named BCAS-VADN (Blockchain-enabled Certificate-based Authentication Scheme for Vehicle Accident Detection and Notification). They store the information generated by this method using BC technology. Moreover, the platform's safety and truthfulness are affirmed with a Practical Byzantine Fault Tolerance consensus mechanism and the encryption of interactions via a cryptographic hash signature.

A model for the exchange of information between system actors based on smart contracts and multi-agent systems (MAS) is proposed by Mhamdi et al. [34]. Here, the distributed information flow among both multiple stakeholders is the primary essential characteristic. The envisaged system is made up of many agents. Every agent has their own BC address. The BC keeps track of the actors' transactions as well as its own information. The smart contract guarantees these transactions, which are endorsed by consensus protocol, automatically. The suggested model is built around three key ideas: smart contracts, access control, and MAS.

Blockchain IoV solution for payment (PSEV) [35] is a BC-based framework that enables the establishment of reimbursements and secure data transmission between IoV involved parties. Using smart contracts, this approach guarantees the automation of data transfer operations. To verify their solution, the author developed a decentralized real-time parking booking and billing application on the Ethereum BC. When compared to current systems, the proposed framework has a lower cost and shorter execution time. It also ensures the integrity, immutability, and confidentiality of the data.

Table 2. IoV-BC summarized Literature Review.

Ref	Contribution	Blockchain			Performance			
		1	2	3	4	5	6	7
[31]	Focus on providing protected automation of data transfer operations between the various IoV involved parties.	*			*		*	*
[32]	Guarantee that received interactions between vehicles and their neighbors are trusted and decentralized.		*				*	
[33]	suggested a security rules for fatal crash detection and alerting in an ITS atmosphere		*	*		*		

Table 2. Cont.

Ref.	Contribution	Blockchain			Performance			
		1	2	3	4	5	6	7
[34]	Maintain the safety and confidence of the system's agents by constructing automatically generated interaction via smart contracts.	*	*	*		*	*	*
[35]	Secure message transmission between automobiles in the IoV subnet.		*				*	

1: Smart contract, 2: consensus mechanism, 3: Access control, 4: confidentiality, 5: Integrity, 6: privacy, 7: Authentication, *: Covered.

3.2. Monitoring Patient Data with Blockchain

To study the impact and integration of this technology in the healthcare sector, we compiled statistics about the numbers of articles published in this context. This is based on a simple query “BC and healthcare”. This study included the scientific articles published between 2018 and 2021 from the IEEE, Springer, and Science Direct databases.

Figure 1 represents the number of articles published during the last 4 years. It is noticeable that the exploitation of BC technology in the healthcare field is growing. It has attracted increased attention from several researchers, exceeding 1260 in 2022 for just the three mentioned publishers.

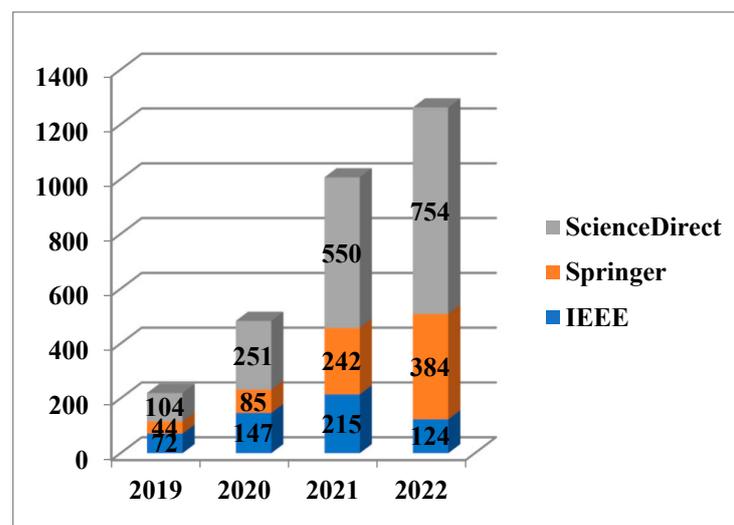
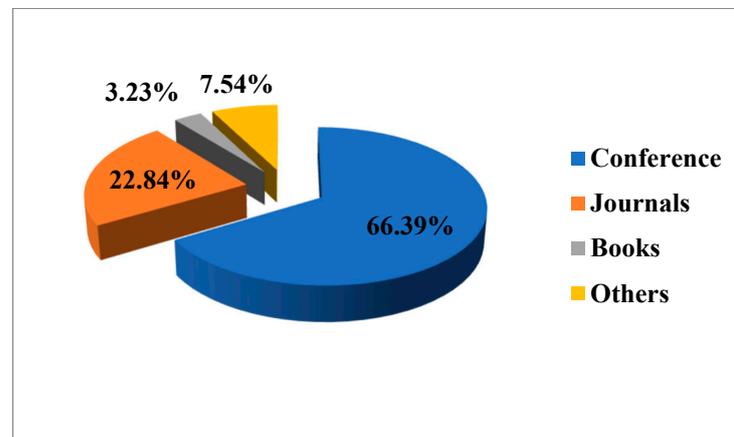


Figure 1. Number of articles in BC and healthcare with respect to publisher and years.

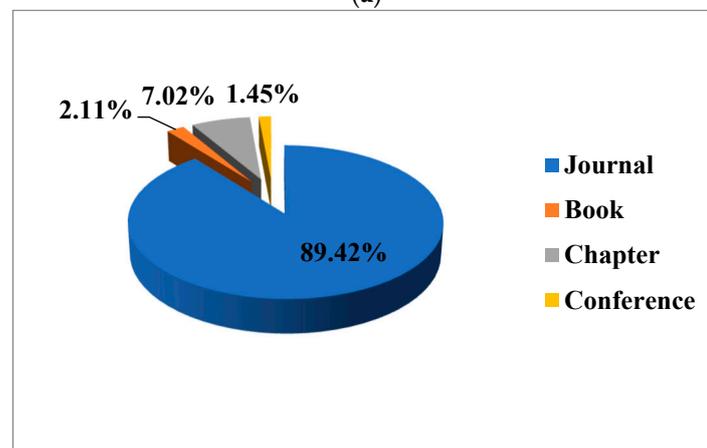
Analyzing the type of publications in IEEE as shown in Figure 2a, conference papers occupy a percentage of about 66% to almost 23% of the articles in journals. On the other hand, the latter represent 89% in Springer and 60% in Science Direct (Figure 2b,c).

Through developing a method for remote patient monitoring, Ref. [36] tackles the problem of patient data privacy and transparency. The Hyperledger Fabric BC and smart contracts serve as the basis for this platform. The suggested systems gather and distribute data from medical sensors via the BC network. These data are then monitored and managed by smart hospital stakeholders using a data-accessible web application built with HTML5 and JavaScript. The patient's vital parameters are traceable and secure, ensuring good performance. The presented prototype performs well due to its low response time, simple interface, and greater transaction. It does, however, have security flaws because of a gap

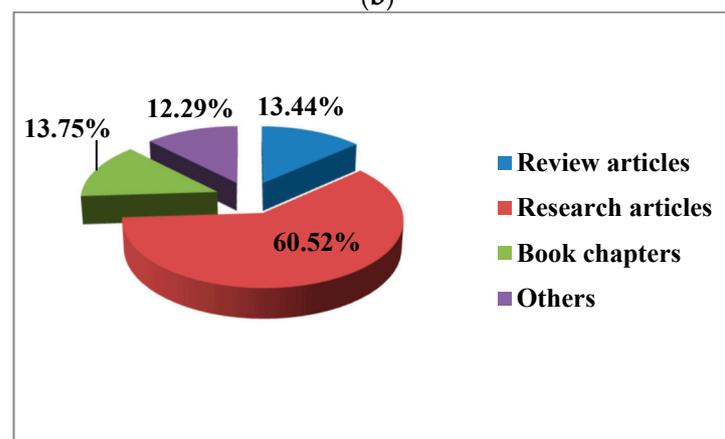
in identity verification between network elements, specifically between the server and IoT sensors.



(a)



(b)



(c)

Figure 2. The statistics of works in BC and healthcare according to article type. (a) The statistics of articles in IEEE. (b) The statistics of articles in Springer. (c) The statistics of articles in Science Direct.

The authors of [37] designed a system for patient surveillance and that notifies health providers about an emergency case using smart contracts. This telemonitoring system ensures the patient's security and privacy by implementing BC. Data from IoT sensors will be processed before being stored in the BC by smart contracts for patient monitoring. This step enables doctors to instantaneously check on their patients. The final role focuses

on the firm and its diagnostic implants. A smart contract is formed between both the financial institution and the patient when a device is purchased that allows the device to be registered in his name. Thus, the information retrieved by the IoT tool is recorded in healthcare center.

In their study, Saini et al. [38] used the Ethereum private BC. To manage EMR, it employs the smart contract concept. The EMR includes private patient information. When overseeing them, security should be considered. To that end, the authors developed a framework for medical data sharing among patients, hospitals, and any other agency involved in the project. Incorporating cryptographic and access control features, the smart contracts used ensure EMR privacy, while the cloud allows health records to be stored to minimize bottlenecks. The proposed framework ensures decentralized and patient-centric real-time EMR monitoring.

The authors of [39] recommended a system called BiiMed. Within the proposed method, so many actors will share the patient's EMR. The DLT guarantees system integration and data protection. The proposed scheme consists of two parts. The health information system (HIS) collects, saves, and transmits health records, whereas the BiiMed framework manages data files. It is based on smart contracts and the Ethereum BC. Seamless integration and reliability are critical components of EMR interaction. These characteristics are affirmed by the technology founded using a decentralized, trustworthy network.

Table 3. IoMT-BC summarized Literature Review.

Ref	Contribution	Blockchain			Performance			
		1	2	3	4	5	6	7
[36]	Create a platform which thus enables you to track the patient's vital indicators.	*		*			*	
[37]	create a system for remote surveillance of patients and alerting health professionals in the event of an emergency	*			*		*	*
[38]	Create a model for spreading health records among patients, hospitals, and other entities who are involved.	*		*				
[39]	To suggest the BiiMed framework. The goal of this remedy is to allow different involved parties to access the patient's electronic medical record.	*				*		

1: Smart contract, 2: consensus mechanism, 3: access control, 4: confidentiality, 5: integrity, 6: privacy, 7: authentication, *: Covered.

4. Proposed Framework

The proposed system is composed of three main stakeholders: connected vehicles, emergency vehicles and hospital emergency services.

The idea, as illustrated in Figure 3, is to broadcast the information in case of a road accident to the neighboring vehicles to give way or change the traffic voice. In a second step,

emergency vehicles are sought in the surroundings and the exact location of the accident is transmitted. After arriving at the indicated location, these vehicles collect information about the injured person through sensors that measure vital signals to the emergency service. These services in turn process the data in advance. The prompt treatment of the data and the timely arrival of the emergency service increase the likelihood of saving the life of a human being. To reach our goal, we divide our system into three sub-systems that will be detailed in the next section. Based on BC technology, we process all data automatically via smart contracts.

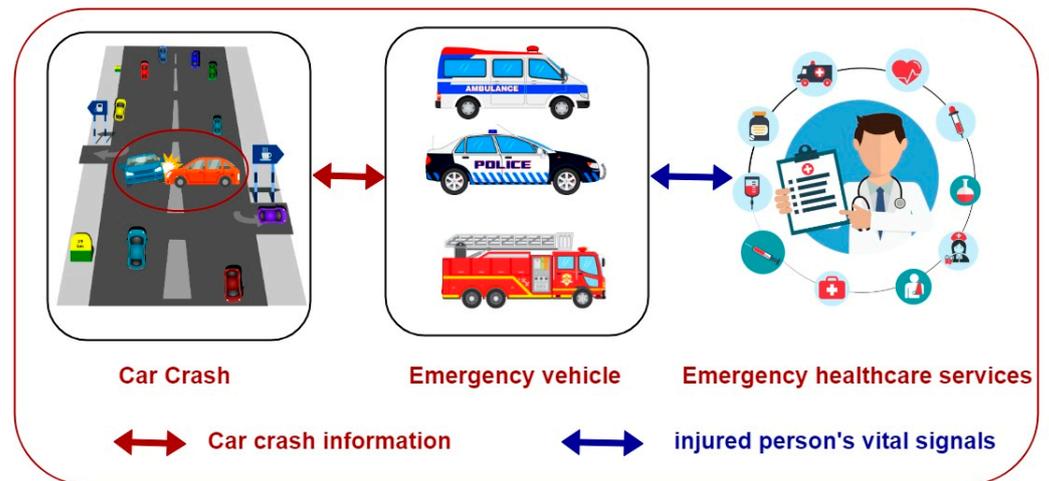


Figure 3. Proposed system.

4.1. V2V Communication Sub-System

In the case of vehicular communication, each smart vehicle can transfer information either to neighboring vehicles or to the nearest emergency services. The distributed information must be decentralized. Indeed, the list of services and the vehicles are registered on the BC. In case of an accident, a request is automatically launched to search for a nearby medical center, which in turn informs the ambulance to travel to the scene of the accident. As a result of these requests, data about the parties involved are automatically recorded via a smart contract.

In such a case, priority on the road is given to the emergency vehicles. Figure 4 illustrates the communication process between the vehicles. After receiving an accident alert, the emergency vehicles proceed as follows:

1. Automatically generate an itinerary by indicating its position and destination.
2. Use GPS to locate the other vehicles on the route.
3. Send a message to the located vehicles to give way.

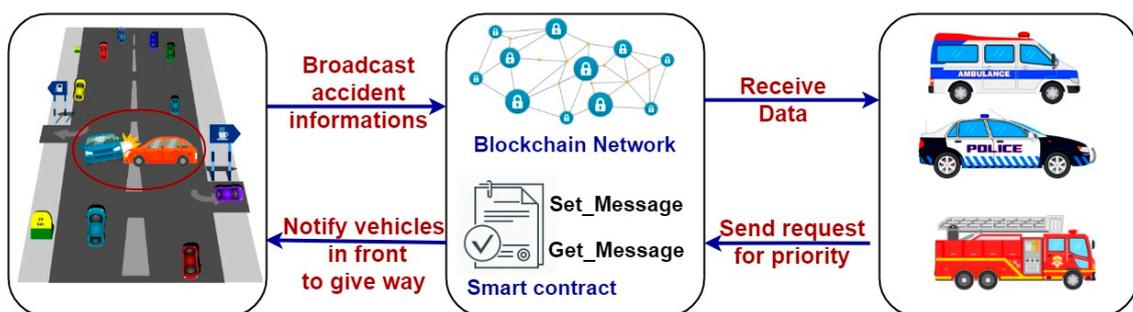


Figure 4. V2V communication sub-system.

The Blockchain network allows the management of communication between cars. Vehicles access a public blockchain network to send the data collected on the location of an accident. This whole process runs automatically via smart contracts. The smart contract has two main roles: sending messages or publishing a new message on the blockchain network, and reading messages, which allows the device connected to the blockchain network to read the existing data.

4.2. Emergency Vehicles and Healthcare Communication Sub-System

This sub-system allows communication between the emergency vehicles and the emergency service center (Figure 5). Each injured person in an emergency vehicle must be equipped with sensors to measure vital signals such as temperature, respiration rate, oxygen level, etc. The collected information is transmitted to the appropriate emergency service to be processed in advance by medical staff. In this case a smart contract is established between the sources of the medical data and the existing system in the hospitals. So, in this way, an EMR containing the medical data of the person in question is handled in a decentralized and secure way.

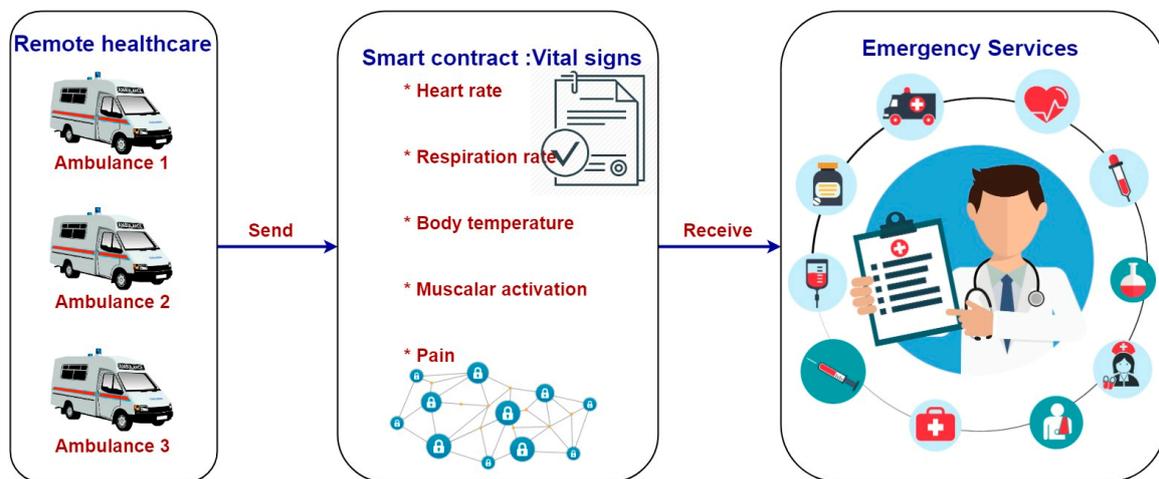


Figure 5. Emergency vehicles and healthcare communication sub-system, *: details of Smart contract.

4.3. Remote Healthcare Sub-System

This part consists of tracking the patient by different stakeholders, namely the doctor, the analysis laboratory and the pharmacist. For the management of EMR of the patient, each stakeholder must authenticate with his identifier and his role. The manipulated information is gathered and saved on the BC. A smart contract is responsible for their update.

4.4. System Requirements

The data manipulated in our system are sensitive and requires confidentiality and security during transmission. So, we need two types of BC: public and consortium.

- Public BC: Everyone with Internet connectivity can connect to a BC platform to become an authorized node, making the public BC open and unconstrained. This person has access to both recent and old data, and they can also do mining operations—complex calculations necessary to confirm transactions and add them to the ledger. On the network, no valid entries or transactions can be altered. This kind of BC is used to hold information about vehicles and other emergency services.
- A consortium BC: this type of BC operates in a restrictive environment as a closed network. The members of this network collaborate on a decentralized network. However, access is limited to a particular group. The controlling organization defines permission levels, security, permissions, and accessibility. We need to identify all the medical staff

so that it can manage the data of the injured person in full confidentiality and security, so we resort to the use of this type of BC.

For the transmission of vital signs of an injured person, sensors are needed to collect the information and transmit it in real time to the appropriate service. These devices are integrated into computer networks via the web. This process takes place as illustrated in Figure 6.

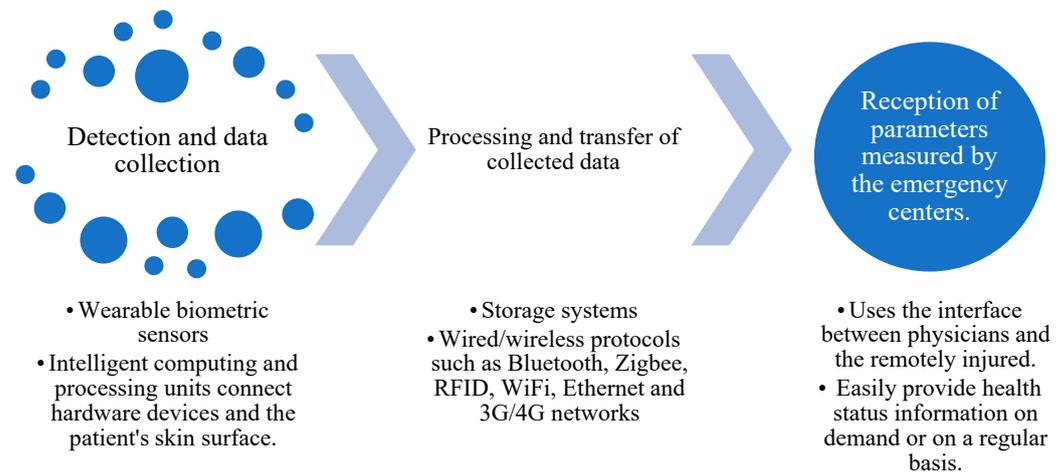


Figure 6. Vital Signs Collection Process.

In this article, we are just interested in the simulation of the part of the proposed system that involves the processing of data manipulated via BC technology. The study of sensors used as well as the communication protocols in IoMT network architecture are the subject of another paper.

5. System Implementation and Results

In our system, several actors share a large amount of information. The crucial aspect of the manipulated information requires a fast transfer in a secure way and in real time. Therefore, these requirements must be considered. To ensure this, smart contracts are used to automate the distribution of data. Authentication and access control ensure confidentiality. Table 4 describes the concepts used.

5.1. Fundamental Framework and Software Required

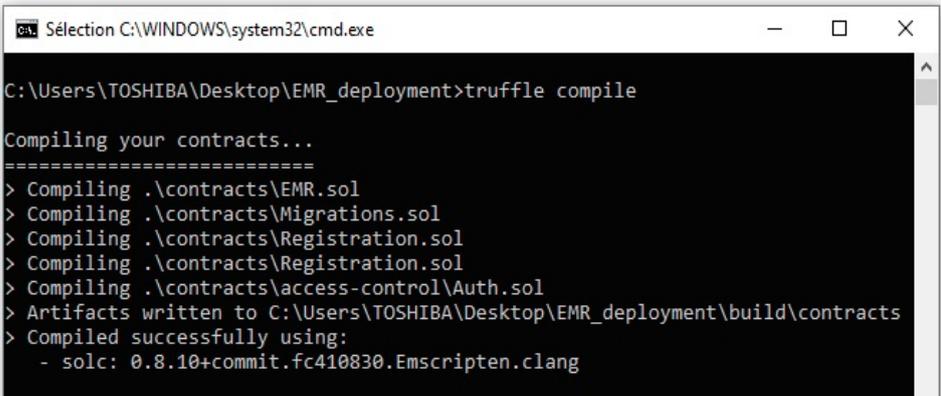
All simulations are executed on an Intel Core i5, CPU 2.60 GHz, 8 GB RAM, and Windows 10 to verify our framework. Ethereum BC is based on BC technology. It aims to create a platform based on smart contracts. This technology is also distributed via a P2P network. The smart contracts in Ethereum are written by the programming language Solidity; via this language, one manipulates transactions. An Ethereum transaction consists of several elements, such as the sender and the receiver as well as a fee that the sender must pay. Both the sender and the receiver have an account or an Ethereum address which consists of twenty bytes. We utilize the web3.js framework to access this account over an HTTP connection in JSON RPC style. To compile and move smart contracts to the neighborhood BC Ganache, one must use the Truffle development environment.

Table 4. Used concepts.

Concept	Description
Smart contract	Because they perform basic functions, smart contracts are among the most critical features of any BC schema. The implementation of various smart contracts, whether for the system, interested parties' enrolment, or for access control to manipulate and monitor exchanged data, is the first step in designing our conceptual model.
Access control	A method of restricting user access to resources. It specifies the actions that each user must take and prevents unauthorized access to information. The access control model is built on authentication, identification, and authorization. Based on role-based access control (RBAC) and attribute-based access control (ABAC), each user is assigned a role that defines their access to a resource.
Authentication	User authentication mostly through Ethereum addresses is required for each agent's entry into the system. Following authentication, medical personnel can consult and communicate with one another.

5.2. Smart Contracts Deployment

We use a personal blockchain, Ganache, to implement our smart contracts. It enables the deployment of smart contracts, the development of Dapp, and the execution of tests. Ganache offers ten Ethereum accounts, each with a balance of 100 ether, as well as a graphical interface for examining everything that happens on this network. The creation and transfer of smart contracts to the blockchain Ganache are shown in Figures 7 and 8.



```

C:\Users\TOSHIBA\Desktop\EMR_deployment>truffle compile

Compiling your contracts...
=====
> Compiling .\contracts\EMR.sol
> Compiling .\contracts\Migrations.sol
> Compiling .\contracts\Registration.sol
> Compiling .\contracts\Registration.sol
> Compiling .\contracts\access-control\Auth.sol
> Artifacts written to C:\Users\TOSHIBA\Desktop\EMR_deployment\build\contracts
> Compiled successfully using:
  - solc: 0.8.10+commit.fc410830.Emscripten.clang

```

Figure 7. Truffle smart contract compilation.

Several smart contracts have been developed to meet the requirement of our system. Among them we find a Registration contract (Figure 9) which allows us to assign to each user a predefined role linked to his Ethereum account. The hospital contract, as shown in Figure 10, allows us to add information related to each emergency service. Figure 11 illustrates the basic functions of the doctor contract. These functions include the consultation of the patient's vital signs as well as the addition of prescriptions or treatments to be performed for a patient.

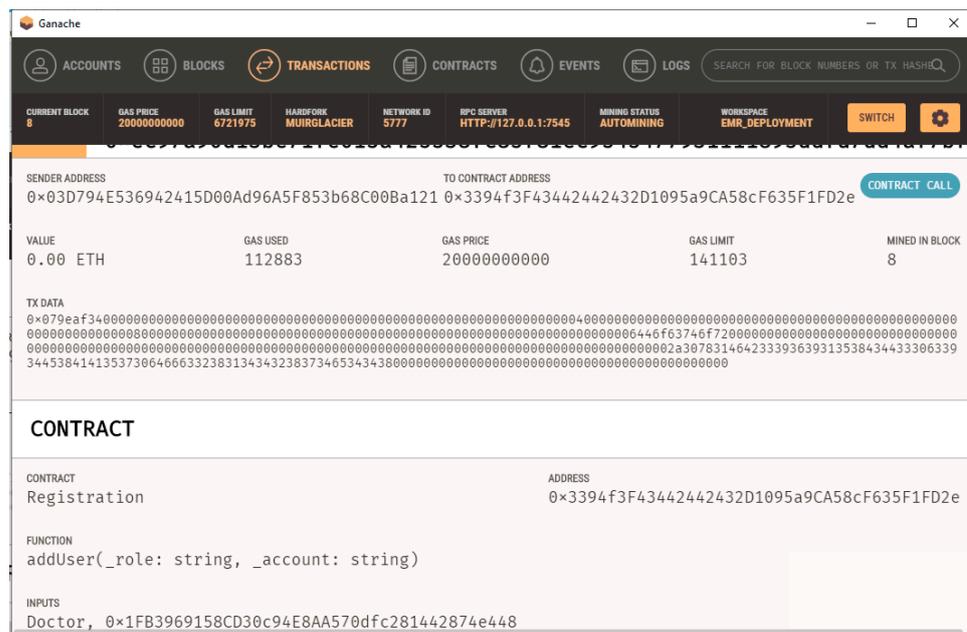


Figure 8. Registration smart contract deployed in Ganache.

```

Registration.sol
1 // SPDX-License-Identifier: MIT
2 pragma solidity >=0.4.22 <0.9.0;
3 contract Registration {
4     //constructor() public {
5     //}
6     struct User {
7         string Role;
8         string account;
9     }
10    User[] private usersList;
11    function addUser (string memory _role, string memory _account) public {
12        User memory newUser = User(_role, _account);
13        usersList.push(newUser);
14    }
15    ....
16 }
    
```

Figure 9. Registration contract.

```

Hospital.sol
1 // SPDX-License-Identifier: MIT
2 pragma solidity >=0.4.22 <0.9.0;
3 contract Hospital {
4     address [] public associated Hospitallist;
5     string public HospitalName;
6     string public HospitalAddress;
7     ...
8     constructor() public {}
9     modifier OnlyOwner {}
10    function registerPatient (address_patient) public{}
11    function executeTreatment (address_patient) public view return (uint){}
12    ....
13 }
    
```

Figure 10. Hospital contract.



```

Hospital.sol | doctor.sol
1 // SPDX-License-Identifier: MIT
2 pragma solidity >=0.4.22 <0.9.0;
3 contract doctor {
4   ...
5   constructor() public {}
6   function operation (address_patient) public {}
7   function putPatientMedication (address_patient) public {}
8   function verifyReport() public {}
9   ....
10  }

```

Figure 11. Doctor contract.

5.3. Smart Contracts Cost

The Ethereum BC assesses presented systems according to the costs incurred by smart contracts. These are the fundamental units for the execution of transactions and smart contract operations. Alternatively, both the transaction and execution costs would be incurred. The price of migrating the smart contract script to the Ethereum BC is referred to as the transaction cost. The size of the smart contract is a constraint. The underlying transactions that a smart contract performs determine its size. The data needed to store global variables and smart contract approach calls is their execution cost. The arithmetic activities performed during execution also have an impact on it.

The total smart contracts cost of the proposed system is approximately 0.02723253 Eth. The cost of each sub-system is detailed in Table 5. It can be noticed that the highest cost is occupied by the sub-system of monitoring vital signs of injured persons, followed by the sub-system of exchanging them between the emergency services. The large amount and types of data exchanged are the cause of this prohibitive cost.

Table 5. System deployment cost.

System	Transaction Cost (Eth)	Price (\$)
Vehicle-to-vehicle communication sub-system	0.003796388	13.21
Emergency vehicles-to-healthcare communication sub-system	0.005920182	20.6
Remote healthcare sub-system	0.01751596	58.85

Figure 12 depicts the execution costs of some smart contracts in our system. The results obtained are in Ether. The execution cost for the VitalSigns_contract is 0.0088114 Eth while the cost for the registration contract is 0.00823677 Eth; 0.0083497 is the cost of V2E_contract and, for the V2V_contract, it is 0.0082886 Eth. Since VitalSigns_contract oversees the data of injured people by several intervening or different medical staff, it occupies the highest energy amount. It also holds access control to the managed information. The registration contract consumes less energy. The V2V_contract contract deals with communication between vehicles by exchanging information about an accident. Finally, the V2E_contract allows sending vital signs of the patient to the emergency centers.

It should be taken into consideration that these energy values are only test values as we use the test Ethereum network and PoW consensus. For a real system, there are consensus that consume much less computing power, such as PoS or DPoS.

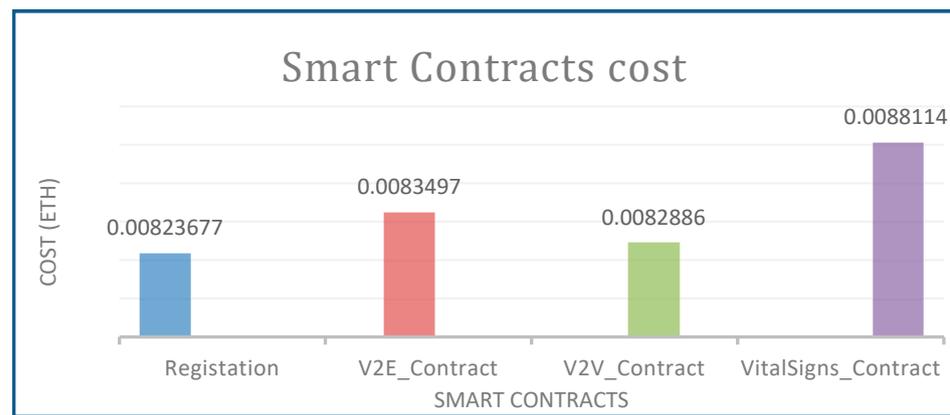


Figure 12. Smart contracts cost.

5.4. Comparative Analysis of the Proposed System and Related Work

In Table 6, we compare our work with some studies previously summarized in Section 3. BC technology, IoV, IoMT, access control and security are particularly important criteria on which we focus our comparison. All references satisfied the first criterion. In [25–27], the authors took into consideration the second Cr criterion. The authors in [28,30,31] satisfied Cr 3 criterion. Moreover, the access control-based criterion is satisfied in [26,28,30]. On the other hand, criterion 5 is found in the work of Halima et al., Jabbar et al. and Faisal et al. [26–28]. Finally, based on this analysis, it is clear that only our research considered all these evaluation criteria.

Table 6. Comparison of proposed system with related work.

Criterium ID	Reference	[25]	[26]	[27]	[28]	[30]	[31]	Our System
Cr 1		✓	✓	✓	✓	✓	✓	✓
Cr 2		✓	✓	✓	X	X	X	✓
Cr 3		X	X	X	✓	✓	✓	✓
Cr 4		✓	✓	X	✓	✓	X	✓
Cr 5		X	✓	✓	✓	X	X	✓
Cr 6		✓	✓	X	X	X	✓	✓

Cr 1: BC; Cr 2: IoV; Cr 3: IoMT-based; Cr 4: Access Control-based; Cr 5: Security; Cr 6: Integrity; X: Not supported; ✓: supported.

In the proposed system, very important and sensitive data are handled. For this, our system satisfies security requirements that include data security and communication security.

- **Confidentiality:** The remote healthcare sub-system contains patient vital signs. To ensure the confidentiality of these data, unauthorized manipulation by third parties must be avoided. The use of smart contracts, by rejecting access to the system by any untrusted third party, ensures patient privacy, trust, and accuracy. The information saved in the system is immutable and cannot be modified by third parties thanks to the use of blockchain technology. This guarantees the confidentiality of the data handled.
- **Integrity** is a further basic feature of systems that exchange sensitive data among users. As a result, the data integrity property of the proposed software solution must be evaluated. Data integrity is the accuracy and dependability of data throughout their entire life cycle. It is crucially related to the concept of data security and remains constant in its entirety. It is critical for data security to maintain consistency throughout its life cycle. In our system, Merkle Trees and cryptographic Hashing are responsible for maintaining the data integrity on public and private Blockchains.

- **Security:** The security of our suggested framework is guaranteed by the usage of the RBAC and ABAC techniques. Hence, no outsider is permitted to use the system. Do not forget that protocols and methods are used to secure the blockchain. As a result, agent data can be handled securely and privately. This information is only accessible to reliable individuals. Any untrusted outsider trying to access the system is denied access by the system.
- **Availability** means that a system is online and ready to be accessed at any time. The availability is ensured by the decentralized notion of the blockchain which fights against different attacks as well as the single point of failure.

6. Conclusions

This paper proposes a BC-based system allowing emergency vehicles to arrive as soon as possible at the scene of an accident. They first receive the location of the injured person. Then, with vehicular communication, they obtain road priority. In a second step and through the IoMT concept, our system allows us to collect the vital signs of the patient and transmit it to the emergency center, that, in turn prepares their treatment in advance. To achieve our goal, several smart contracts are deployed in Ethereum BC. To ensure safety, security, and trust surrounding the manipulated data, two types of access control were used, namely RBAC and ABAC.

BC technology, IoV and IoMT help to speed up the intervention in emergency cases. However, in such cases a large amount of data is manipulated. Since the data are stored in blocks, there is a problem of data storage. We will evaluate this attempt to promote the mixed hosting of blocks in the cloud and through distributed storage systems as future studies.

Author Contributions: Conceptualization, methodology, writing—original draft, results analysis, M.A.; data collection, data analysis, writing—review and editing, results analysis, H.M.; methodology, writing—review and editing, design and presentation, references, A.K.; methodology, writing—review and editing, L.A.; methodology, writing—review and editing, M.S.A.; methodology, writing—review and editing, M.D.A.; methodology, writing—review and editing, A.S.; methodology, writing—review and editing, S.H. All authors have read and agreed to the published version of the manuscript.

Funding: The authors extend their appreciation to the Deanship of Scientific Research at King Khalid University (KKU) for funding this research through the Research Group Program Under the Grant Number:(R.G.P2/451/44). This work was supported by Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2023R349), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The datasets used during the current study are available from the corresponding author on reasonable request.

Acknowledgments: The authors extend their appreciation to the Deanship of Scientific Research at King Khalid University (KKU) for funding this research through the Research Group Program Under the Grant Number:(R.G.P2/451/44). This work was supported by Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2023R349), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Fadhil, J.A.; Sarhan, Q.I. Internet of Vehicles (IoV): A Survey of Challenges and Solutions. In Proceedings of the 2020 21st International Arab Conference on Information Technology (ACIT), Giza, Egypt, 28–30 November 2020; pp. 1–10. [[CrossRef](#)]
2. Goyal, S.; Sharma, N.; Bhushan, B.; Shankar, A.; Sagayam, M. IoT Enabled Technology in Secured Healthcare: Applications, Challenges and Future Directions. In *Cognitive Internet of Medical Things for Smart Healthcare. Studies in Systems, Decision and Control*; Hassaniien, A.E., Khamparia, A., Gupta, D., Shankar, K., Slowik, A., Eds.; Springer: Cham, Switzerland, 2021; Volume 311. [[CrossRef](#)]

3. Kashyap, V.; Kumar, A.; Kumar, A.; Hu, Y.-C. A Systematic Survey on Fog and IoT Driven Healthcare: Open Challenges and Research Issues. *Electronics* **2022**, *11*, 2668. [CrossRef]
4. Onesimu, J.A.; Karthikeyan, J.; Sei, Y. An efficient clustering-based anonymization scheme for privacy-preserving data collection in IoT based healthcare services. *Peer-to-Peer Netw. Appl.* **2021**, *14*, 1629–1649. [CrossRef]
5. Kumar, M.; Chand, S. A Secure and Efficient Cloud-Centric Internet-of-Medical-Things-Enabled Smart Healthcare System with Public Verifiability. *IEEE Internet Things J.* **2020**, *7*, 10650–10659. [CrossRef]
6. Huang, J.M. Research on Internet of Vehicles and its Application in Intelligent Transportation. *Appl. Mech. Mater.* **2013**, 321–324, 2818–2821. [CrossRef]
7. Aubert, J.; de la Raudière, L.; Mis, J.-M. Report of the Joint Information Mission on Blockchain and Its Uses: An Issue of Governance. Available online: https://www.assemblee-nationale.fr/dyn/15/rapports/micblocs/l15b1501_rapport-information.pdf (accessed on 31 July 2022).
8. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. Available online: <https://bitcoin.org/bitcoin.pdf> (accessed on 25 August 2022).
9. Tasca, P.; Tessone, C.J. A Taxonomy of Blockchain Technologies: Principles of Identification and Classification. *Ledger* **2019**, *4*. [CrossRef]
10. Kaur, M.; Khan, M.Z.; Gupta, S.; Noorwali, A.; Chakraborty, C.; Pani, S.K. MBCP: Performance Analysis of Large Scale Mainstream Blockchain Consensus Protocols. *IEEE Access* **2021**, *9*, 80931–80944. [CrossRef]
11. Mhamdi, H.; Zouinkhi, A.; Sakli, H. Smart contracts for decentralized vehicle services. In Proceedings of the 2021 International Wireless Communications and Mobile Computing (IWCMC), Harbin, China, 28 June–2 July 2021; pp. 1846–1851. [CrossRef]
12. Javed, L.; Anjum, A.; Yakubu, B.M.; Iqbal, M.; Moqurrab, S.A.; Srivastava, G. ShareChain: Blockchain-enabled model for sharing patient data using federated learning and differential privacy. *Expert Syst.* **2022**, e13131. [CrossRef]
13. Yang, F.; Wang, S.; Li, J.; Liu, Z.; Sun, Q. An overview of Internet of Vehicles. *China Commun.* **2014**, *11*, 1–15. [CrossRef]
14. Karagiannis, G.; Altintas, O.; Ekici, E.; Heijenk, G.; Jarupan, B.; Lin, K.; Weil, T. Vehicular Networking: A Survey and Tutorial on Requirements, Architectures, Challenges, Standards and Solutions. *IEEE Commun. Surv. Tutor.* **2011**, *13*, 584–616. [CrossRef]
15. Maglaras, L.A.; Al-Bayatti, A.H.; He, Y.; Wagner, I.; Janicke, H. Social Internet of Vehicles for Smart Cities. *J. Sens. Actuator Netw.* **2016**, *5*, 3. [CrossRef]
16. Ben Othman, S.; Almalki, F.A.; Sakli, H. Internet of Things in the Healthcare Applications: Overview of Security and Privacy Issues. In *Intelligent Healthcare*; Chakraborty, C., Khosravi, M.R., Eds.; Springer: Singapore, 2022. [CrossRef]
17. Recommendation on a European Electronic Health Record Exchange Format. Available online: <https://digital-strategy.ec.europa.eu/fr/node/2138> (accessed on 20 September 2022).
18. Nishi, F.K.; Shams-E-Mofiz, M.; Khan, M.M.; Alsufyani, A.; Bourouis, S.; Gupta, P.; Saini, D.K. Electronic Healthcare Data Record Security Using Blockchain and Smart Contract. *J. Sens.* **2022**, *2022*, 7299185. [CrossRef]
19. Mhamdi, H.; Ayadi, M.; Ksibi, A.; Al-Rasheed, A.; Soufiene, B.O.; Hedi, S. SEMRachain: A Secure Electronic Medical Record Based on Blockchain Technology. *Electronics* **2022**, *11*, 3617. [CrossRef]
20. Fekete, D.; Kiss, A. A Survey of Ledger Technology-Based Databases. *Futur. Internet* **2021**, *13*, 197. [CrossRef]
21. Kuo, T.-T.; Kim, H.-E.; Ohno-Machado, L. Blockchain distributed ledger technologies for biomedical and health care applications. *J. Am. Med. Inform. Assoc.* **2017**, *24*, 1211–1220. [CrossRef]
22. Tseng, L.; Yao, X.; Otoum, S.; Aloqaily, M.; Jararweh, Y. Blockchain-based database in an IoT environment: Challenges, opportunities, and analysis. *Clust. Comput.* **2020**, *23*, 2151–2165. [CrossRef]
23. Yang, X.; Zhang, Y.; Wang, S.; Yu, B.; Li, F.; Li, Y.; Yan, W. LedgerDB: A centralized ledger database for universal audit and verification. *Proc. VLDB Endow.* **2020**, *13*, 3138–3151.
24. Liao, D.; Dong, X.; Xu, Z.; Han, H.; Yan, Z.; Sun, Q.; Li, Q. An Efficient Storage Architecture Based on Blockchain and Distributed Database for Public Security Big Data. In *Advances in Computer Science for Engineering and Education; ICCSEEA 2022. Lecture Notes on Data Engineering and Communications Technologies*; Hu, Z., Dychka, I., Petoukhov, S., He, M., Eds.; Springer: Cham, Switzerland, 2022; Volume 134. [CrossRef]
25. Ge, Z.; Loghin, D.; Ooi, B.C.; Ruan, P.; Wang, T. Hybrid blockchain database systems: Design and performance. *Proc. VLDB Endow.* **2022**, *15*, 1092–1104.
26. Loghin, D. The Anatomy of Blockchain Database Systems. *Data Eng.* **2022**, *48*.
27. Yang, X.; Wang, S.; Li, F.; Zhang, Y.; Yan, W.; Gai, F.; Yu, B.; Feng, L.; Gao, Q.; Li, Y. Ubiquitous Verification in Centralized Ledger Database. In Proceedings of the 2022 IEEE 38th International Conference on Data Engineering (ICDE), Kuala Lumpur, Malaysia, 9–12 May 2022; pp. 1808–1821. [CrossRef]
28. Szabo, N. Smart contracts: Formalizing and securing relationships on public networks. *First Monday* **1997**, *2*, 9. [CrossRef]
29. Viriyasitavat, W.; Hoonsopon, D. Blockchain characteristics and consensus in modern business processes. *J. Ind. Inf. Integr.* **2019**, *13*, 32–39. [CrossRef]
30. Mhamdi, H.; Ben Othman, S.; Zouinkhi, A.; Sakli, H. Blockchain Technology in Healthcare: Use Cases Study. In *Intelligent Healthcare*; Chakraborty, C., Khosravi, M.R., Eds.; Springer: Singapore, 2022. [CrossRef]
31. Singh, P.K.; Singh, R.; Nandi, S.K.; Ghafoor, K.Z.; Rawat, D.B.; Nandi, S. Blockchain-Based Adaptive Trust Management in Internet of Vehicles Using Smart Contract. *IEEE Trans. Intell. Transp. Syst.* **2020**, *22*, 3616–3630. [CrossRef]

32. Yang, Z.; Yang, K.; Lei, L.; Zheng, K.; Leung, V.C.M. Blockchain-Based Decentralized Trust Management in Vehicular Networks. *IEEE Internet Things J.* **2018**, *6*, 1495–1505. [[CrossRef](#)]
33. Vangala, A.; Bera, B.; Saha, S.; Das, A.K.; Kumar, N.; Park, Y.H. Blockchain-Enabled Certificate-Based Authentication for Vehicle Accident Detection and Notification in Intelligent Transportation Systems. *IEEE Sens. J.* **2020**, *21*, 15824–15838. [[CrossRef](#)]
34. Mhamdi, H.; Soufiene, B.O.; Zouinkhi, A.; Ali, O.; Sakli, H. Trust-Based Smart Contract for Automated Agent to Agent Communication. *Comput. Intell. Neurosci.* **2022**, *2022*, 5136865. [[CrossRef](#)] [[PubMed](#)]
35. Jabbar, R.; Fetais, N.; Kharbeche, M.; Krichen, M.; Barkaoui, K.; Shinoy, M. Blockchain for the Internet of vehicles: How to use blockchain to secure vehicle-to-everything (V2X) communication and payment? *IEEE Sens. J.* **2021**, *21*, 15807.
36. Jamil, F.; Ahmad, S.; Iqbal, N.; Kim, D.-H. Towards a remote monitoring of patient vital signs based on iot-based blockchain integrity management platforms in smart hospitals. *Sensors* **2020**, *20*, 2195. [[PubMed](#)]
37. Kazmi, H.S.Z.; Nazeer, F.; Mubarak, S.; Hameed, S.; Basharat, A.; Javaid, N. Trusted Remote Patient Monitoring Using Blockchain-Based Smart Contracts. In *Advances on Broad-Band Wireless Computing, Communication and Applications, BWCCA 2019, LNNS*; Springer Nature: Cham, Switzerland, 2020; Volume 97, pp. 765–776.
38. Saini, A.; Zhu, Q.; Singh, N.; Xiang, Y.; Gao, L.; Zhang, Y. A Smart-Contract-Based Access Control Framework for Cloud Smart Healthcare System. *IEEE Internet Things J.* **2020**, *8*, 5914–5925. [[CrossRef](#)]
39. Jabbar, R.; Fetais, N.; Krichen, M.; Barkaoui, K. Blockchain technology for healthcare: Enhancing shared electronic health record interoperability and integrity. In *Proceedings of the 2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT)*, Doha, Qatar, 2–5 February 2020; pp. 310–317.

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.