Blockchain-based Incident Reporting System for Patient Safety and Quality in Healthcare

Dounia Marbouh, Mecit Can Emre Simsekler, Khaled Salah, Raja Jayaraman, Samer Ellahham

Abstract Adverse events pose significant threats to patient safety and quality in healthcare worldwide. To understand how and why such events occur, incident reporting and investigation gained an imperative role in healthcare operations. Therefore, healthcare organizations and national health services have implemented local and national level Incident Reporting Systems (IRSs) to enhance the quality of reporting. However, the literature indicates that reporting practice is insufficient due to underreporting, incomplete incident data, privacy issues, unreliable classifications, the delay from the time of reporting to the investigation, and lack of feedback to reporters. The situation can be potentially improved, however, by exploiting the Blockchain Technology (BCT) that has inherent and unique features, such as security, data integrity and privacy, and provenance. To shed light on this, we first develop a blockchain-based reporting system showing how incidents data can be reported and shared through a secure and trusted distributed ledger. Further, we present algorithms that depict the various interactions among the stakeholders in the reporting network. Through the cost and security analysis, we finally demonstrate the feasibility of the

Dounia Marbouh
Department of Industrial and Systems Engineering, Khalifa University of Science and Technology, Abu Dhabi, 127788, UAE e-mail: 100050079@ku.ac.ae

Mecit Can Emre Simsekler
Department of Industrial and Systems Engineering, Khalifa University of Science and Technology, Abu Dhabi, 127788, UAE e-mail: emre.simsekler@ku.ac.ae

Khaled Salah
Department of Electrical Engineering and Computer Science, Khalifa University of Science and Technology, Abu Dhabi, 127788, UAE e-mail: khaled.salah@ku.ac.ae

Raja Jayaraman
Department of Industrial and Systems Engineering, Khalifa University of Science and Technology, Abu Dhabi, 127788, UAE e-mail: raja.jayaraman@ku.ac.ae

Samer Ellahham
Heart and Vascular Institute and Quality and Patient Safety Institute, Cleveland Clinic Abu Dhabi, Abu Dhabi, United Arab Emirates. e-mail: ellahas@clevelandclinicabudhabi.ae

proposed solution while ensuring security, integrity, transparency, and traceability amongst stakeholders. This study also discusses potential challenges and suggests future research to provide significant insights into the implementation of the incident reporting system.

1 Introduction

In the last two decades, healthcare organizations have devoted substantial efforts to improve patient safety because of the high rate of incidents harming thousands of people globally (Makary and Daniel, 2016). To prevent the occurrences of patient safety incidents and deliver high-quality services, hospitals and national healthcare services have started implementing incident reporting systems (IRSs). These systems can lead to identifying failures, risks and hazards that led to the incident and result in applying improvements to avoid future incident reports (Wang et al., 2017). Although various tools and methods are used for risk identification (Simsekler et al., 2019), incident reporting systems have a unique position with the opportunity of providing narratives for practitioners to learn from their mistakes and experiences (Shojania and Thomas, 2013), and for policy-makers to implement safer care policies (Ramírez et al., 2018). However, despite their distinct features, earlier studies identified a range of obstacles that potentially prevent these reporting systems from contributing to the safety efforts (Levtzion-Korach et al., 2010; Macrae, 2016; Stavropoulou et al., 2015).

Underreporting is among the significant concerns that create a reservoir of information (Noble and Pronovost, 2010). Further, incomplete incident data, hindsight bias, unreliable classifications, confidentiality, blame culture, the time delay between reporting and investigation, fear of possible consequences, and lack of feedback are other frequent barriers encountered in incident reporting (Anderson et al., 2013; Armitage et al., 2018; Tariq et al., 2012). Further, incident reporting systems have not been successfully connected across hospitals, even though each may identify different yet complementary patient safety issues to learn systematically (Ramírez et al., 2018). As a result, current reporting systems are limited to collect comprehensive information on safety events, as incident data is scattered and fragmented across the system (Stavropoulou et al., 2015).

To address the limitations mentioned above in current reporting systems, blockchain Technology (BCT) may provide opportunities with its unique features, such as transparency, immutability, privacy, etc. (Ray et al., 2020). As an emerging technology, blockchain is expected to leverage the exchange of data among stakeholders in different domains and industries, including healthcare (Omar et al., 2020, 2019). Blockchain technology has the potential to transform healthcare by placing the patient at the center of the health system and increasing the security, privacy, and interoperability of health data. This technology could provide a new model for health information exchange (HIE) by making electronic health records (EHRs) more efficient and secure.

In this particular patient safety context, healthcare providers in health services may benefit from the use of blockchain to report and investigate incidents in a secure, faster, and reliable manner. To explore this, we propose a blockchain-based solution that builds a reliable incident reporting system. The fundamental contributions of this paper are as follows: - We present a review of the current incident reporting systems as applied to patient safety in healthcare. - We develop a blockchain-based solution for reporting incidents using smart contracts. - We propose a framework along with algorithms that outline the mechanisms of the proposed solution and provide a detailed sequence diagram of the blockchain-based reporting system. - We present a cost and security analysis of the proposed solution to show the feasibility of the implementation in healthcare.

The remainder of the paper is organized as follows: the relevant literature on incident reporting and blockchain are presented in Section 2, followed by a description of the proposed blockchain-based solution in Section 3. Section 4 presents the implementation steps, along with testing scenarios. Discussion of the proposed approach, cost and security analysis, challenges, and future research directions are presented in Section 5. Finally, summarizing remarks are presented in Section 6.

2 Related Work

In this section, we provide background information related to the incident reporting systems. Further, we give an example of a sophisticated reporting system and explain the potential benefit of adopting blockchain technology.

2.1 Incident Reporting System (IRS)

Incident reporting systems are among the most common tools used for risk identification within the scope of risk management for patient safety efforts worldwide (Stavropoulou et al., 2015). A patient safety incident is defined as any unexpected or unintended event that could lead to the harm of one or more patients receiving any form of care (Wang et al., 2017). The primary purpose of incident reporting is to help in enhancing patient safety by building knowledge from past experiences and errors. Many countries, such as UK, Sweden, Norway, and Australia, have developed electronic reporting systems for confidential and voluntary reporting for safety improvement (Gong et al., 2017). An incident reporting system is also established to detect, absorb, and avoid errors in addition to identifying patterns and trends related to patients' safety risks (Hagley et al., 2019). Further, they provide valuable insights into why patients and how patients could get harmed due to various contributory factors and hazards (Levtzion-Korach et al., 2010).

An ideal IRS is a multi-stage process; its main steps are illustrated in Figure1.

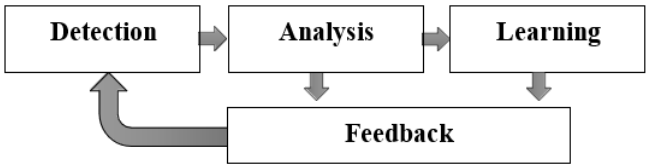

Fig. 1 Main Stages in Incident Reporting Systems

In general, incident data is reported in an incident reporting system at the detection stage. It is followed by the analysis stage, where the reports are investigated to feed the learning stage where learning from the incident is presented. The learning stage may potentially lead to some changes in practice or policies with the proper feedback mechanism. To create an effective reporting system, the World Health Organization (WHO) emphasizes on the importance of both detection and feedback as key features (WHO, 2005). As discussed earlier, even though incident reporting is the tool to learn from past experiences, underreporting is still the main challenge. Further, hindsight bias, recall bias, incomplete data, inaccurate classifications, and the delay between reporting and giving feedback to reporters, have also been identified as limitations (Shojania, 2010). Moreover, the followings are significant concerns in incident reporting systems that have been identified in recent studies (Ramírez et al., 2018):

-Change: The ability to measure changes and trends over time is limited.

-Feedback: The reporter may fail to track the status of the event and a timely feedback is not provided.

-Complementary: Incident reporting systems identify different but complementary patient safety issues for several hospitals. Yet, these systems are not well connected.

-Timely feedback: Incident reporting systems fail to communicate identified events with stakeholders in a timely manner.

While individual hospitals may have their internal incident reporting systems, called Local Reporting Management System (LMRS), some countries have also implemented national-level centralized reporting systems to share learning with all possible stakeholders. To understand the role of such aspects in incident reporting systems, one example can be given from the British National Health Service (NHS): the National Reporting and Learning System (NRLS). Established in late 2003, the NRLS provides resources and guidance for users and healthcare stakeholders to understand the reporting and learning process better. The primary function of the NRLS is to enable healthcare providers to learn from past experiences and reflect their built knowledge in the policy and practice for safer delivery of care. The NHS entity, called NHS Improvement, operates and manages the NRLS. It also uses information from the NRLS to develop guidance for the national hospitals to reduce risks to patients (NHS Improvement, 2018).

To foster reporting and encourage openness, reporting to NRLS is voluntary except for serious incidents (NHS Improvement, 2018). As a result, the NRLS data

does not present the absolute number of national patient safety incidents occurring. However, severe patient safety incidents that resulted in death or severe injury are reviewed individually by NHS Improvement clinicians at a national level to maximize learning. The NRLS is not the only database for patients' incidents in the UK. Yet, it is the single national database to encapsulate the several types of patient safety incidents. Another incident reporting systems include the CQC notification database, Strategic Executive Information System (StEIS), severe hazards of transfusion (SHOT) scheme, (MHRA), yellow card scheme, PHE notifications database, and NHS safety thermometer (NHS Improvement, 2019). All these different entities and system layers show that many stakeholders and organizations are part of the system. Therefore, if such a system is fragmented and if organizations' incident databases do not communicate with each other, this may hinder the collection and analysis of incidents in a systematic manner.

2.2 Blockchain Technology and Potential Benefits

A blockchain is a distributed ledger that captures transactions amongst multiple stakeholders in a manner that is verifiable and efficient (Iansiti and Lakhani, 2017). Developed in 2008 by Satoshi Nakamoto, the unknown person or people behind the bitcoin white paper, it is a data structure that links data records (Cole et al., 2019). This technology guarantees immutability thanks to the distributed network without the need for any centralized authority (Atzori, 2017). A blockchain entails having ordered transactions placed in a block structure. Each block contains a hash (unique identifier), a hash of the previous block, and timestamped batches of recent transactions (Yoon, 2019). As a result, this design ensures that the blocks are connected chronologically, therefore, they build what is called a blockchain. The blockchain platforms are, primarily, (i) permission-less: a public blockchain network, (ii) permissioned, a private network and access can be restricted and given to pre-defined participants, and (iii) consortium, a mix of permission-less and permissioned (Chaer et al., 2019). In public blockchain platforms, records and transactions are verified and validated by thousands of nodes. The latter described mechanism ensures the immutability of data in a blockchain.

The evolution of blockchain technology and its application in diverse contexts has occurred in various phases. The first phase of blockchain evolution was related to cryptocurrency and the second pertained to the application of smart contracts in areas such as real estate and finance (Swan, 2015). The third generation of evolution was focused on the applications of blockchain in non-financial domains such as government, healthcare (Miau Yang, 2018), and culture. Additionally, driven by innovative technological features such as data immutability, blockchain is now considered to be in its fourth stage of evolution with the incorporation of artificial intelligence (AI). Blockchain's asserted diversity in its scope of applications may be attributed to its potential for creating decentralized and trust-less transaction environments (Zhang et al., 2018). The healthcare industry is a prime candidate for blockchain technology;

as blockchain has the potential to address critical concerns, such as automated claim validation and public health management (Mettler, 2016). Concurrently, it enables data records to be unified, updated, securely exchanged, and accessed in a timely by appropriate authorities with the use of consensus protocols. This is a major advantage afforded by the application of blockchain technology within the healthcare space because current practices require data to be stored with third parties (Hölbl et al., 2018). Finally, blockchain can potentially bring transparency to data management processes (Ito et al., 2018) while also reducing the chances of data mishandling or misuse because of possible human error (Alla et al., 2018).

Unlike traditional database systems, blockchain utilizes its inherent properties to ensure transparency, immutability, and accuracy during data collection and data management transactions . Further, in a traditional centralized database, it is impossible to reward a user for reporting an incident. However, a blockchain platform can make the incentivizing process easy. Thanks to the cryptocurrency properties of blockchain, reporters can now get a reward for reporting an incident to encourage reporting and enhance the culture. Overall, distinct advantages are available in the blockchain-based incident reporting system compared to the traditional IR database, such as the NRLS. The comparison and features are summarized in Table 1 (Khan and Salah, 2018; Khezr et al., 2019).

Moreover, blockchain enables two or more parties to interact easily with one another in a digital environment and permits them to exchange data in the absence of a central authority. In many aspects, blockchain has started transforming many industries and domains, such as energy, law, tourism, supply chain, and banking, by enabling value exchange, openness, and trust across business ecosystems (Yi, 2019). Further, It has proved to be beneficial in the healthcare sector, as it promises to enhance healthcare data privacy and secure data management (Gökalp et al., 2018). The following section will, therefore, discuss the potential benefits of blockchain in incident reporting in further detail.

Blockchain has several features that can help in addressing the challenges experienced by the current incident reporting systems. Current gaps in the IRS can be summarized as follows: lack of information dissemination in real-time, absence of incentives, lack of security and privacy, fragmentation of adverse-events data across different organizations and the inability to have constructive feedback on whether the incident report had led to an action (Macrae, 2016). To respond to the current needs of these reporting systems, the blockchain features can be exploited. In fact, the blockchain's key aspects, such as time sequence, data security and privacy, decentralization, transparency, incentives, and traceability, can be useful for ensuring better reporting systems.

For instance, by exploiting the decentralization feature, healthcare providers can access, update, and get feedback about incidents they reported, and incidents that occurred in their healthcare settings. Giving feedback to healthcare practitioners would educate them about risks in their environment. They would also gain ideas on how to reduce risks further and inform them about actions taken in response to similar situations. With blockchain, staff would also feel safe when reporting incidents since this technology provides a balance of security and privacy. This feature may establish

Table 1 Comparison between Using a Centralized Database and a Blockchain Platform

Feature	Traditional Centralized Database	Blockchain Platform
Authority	Controlled by a central authority (administrator)	Authority is shared among stakeholders and is decentralized
Data Integrity	Data can be altered	Data is auditable and immutable
Data handling	Can support only four primary operations: read, create, update, and delete	Only read and write options are available
Data Privacy	High chances of malicious cyber-attacks	Transaction data is stored in blocks using cryptography technology
Data Provenance	Databases cannot ensure that data has not been altered, forged, reproduced, or stolen	Users can trace and verify the provenance of all the previous transactions by accessing any node in the network
Transparency	Databases are not as transparent as in BC	Transaction data is stored in a distributed network
Quality assurance	Administrators are needed to authenticate data	Data can be traced from its origin using cryptography technology
Fault tolerance	Considerable threat of single point of failure (SPF)	The ledger is fault-tolerant
Incentive	There is no incentives mechanism in databases	Health professionals and patients can be incentivized for reporting promptly and accurately
Consensus	Databases do not have a consensus mechanism as they are centralized	The validation mechanism ensures the integrity of the data as much as possible
Cost	Easy implementation and maintenance as it is a conventional technology	Limited certainty in operation and maintenance costs
Performance	Fast (more transactions processed per second) and offer high scalability	Can handle minimal transactions per second and has as scalability since the technology is at its developing phase

a strong blame-free culture of incident reporting that values sharing and continuous learning.

Performing data analytics in healthcare is possible when blockchain is combined with machine learning and artificial intelligence technologies (Mamoshina et al., 2018). By doing so, the data analysis process would be carried out automatically without the intervention of statisticians. Data analytics tools would be used to generate statistical reports which would be uploaded on the blockchain network of all parties to view. This feature would allow the national health services to check reports on any adverse events in real-time. Blockchain would automate the analysis process by having an analytics node in the network, which would oversee data cleaning and anonymization. The latter is made possible because raw data would be fed into this analytics node, and data integrity would be ensured by blockchain (Wehbe et al., 2018).

While blockchain has merits to provide a secure incident reporting and sharing platform, its potential has not been explored for a particular incident reporting platform yet. Therefore, we aim to build upon this research to leverage the benefits of the blockchain by adding a unique application area of incident reporting in healthcare safety context. With the proposed blockchain-based solution below, we aim to exploit

the essential blockchain technology features that may help accelerate patient safety enhancement.

3 Proposed Blockchain-based Solution

3.1 System Overview

The existing national incident reporting systems like the NRLS have several gaps, as discussed before. Blockchain technology, however, has the potential to fill in these gaps and to improve the current process. According to a study by Naome and colleagues (2020), more than 59 percent of healthcare providers confirmed that knowing what, how and who to report incidents to may improve adherence. Further, almost half of the respondents supported that offering rewards could encourage reporting, 55.7 percent confirmed that providing feedback and corrective action plans of the reported incidents increased reporting. Also, 55.7 percent claimed that providing training to health practitioners to detect incidents inspired incident reporting (Naome et al., 2020). Therefore, barriers to incidents reporting can be summarized as: lack of knowledge and instructions, absence of reward and incentive, and absence of feedback and corrective actions. By removing these barriers, we can ensure better adherence to incident reporting.

Figure 2 shows our proposed system overview and how the stakeholders would interact with the blockchain platform to remove the barriers discussed. As a natural process in incident reporting, the patient or health practitioner would report an incident to the blockchain. Our system contains different stakeholders such as the ministry of health, FDA, pharmacies, healthcare practitioners and patients. The party reporting the incident (patient or healthcare practitioner) would be able to upload the details of an incident which can be stored in the IPFS. For serious incidents FDA and ministry of health would be required to develop an action plan to be shared among other stakeholders and that can be stored in the IPFS as well. One unique feature about our system is the ability to distribute some coins as a reward for the incident reporters. Adding a reward mechanism in our proposed solution would ensure healthcare providers and patients participation in incidents sharing. According to Kingston and colleagues, senior medical staff agreed on the lack of motivation to report an incident. They added that incident reporting is of little value and time waste, and advised that financial incentives for generated reports might be a greater motivation for reporting (Kingston et al., 2004).

In addition to adding a reward mechanism, having a feedback mechanism is crucial. Effective feedback on incident reporting systems is vital to learn from failures of the delivery of care. Feedback from incident reports should also include corrective actions to improve safety and address specific vulnerabilities in care systems, if recurrent failures are to be prevented and the feedback loop closed (Benn et al., 2009). Figure 3 depicts the main functional stages of the learning process of incident reporting, drawing upon existing safety systems from the literature review,

in combination with our proposed solution. Our proposed incident reporting system operates on three distinct levels. The first level is operational, and this is where the reporter (health practitioner or patient) reports the incident. The following level is organizational, in which the responsible party (health practitioner) is required to provide detailed information about the incident into the LRMS or blockchain directly. In the case of any serious incident, a safety issue analysis should be run by the organization to identify the contributory factors and immediately improve the system. The last level is regulatory and involves parties such as ministry of health and FDA. In this level, the incidents data are consolidated, aggregated, and analyzed for potential feedback. After the analysis of the aggregated data, corrective actions, results and feedback is disseminated across the system and stored in the IPFS to correct vulnerabilities and finally, the reporter gets awarded.

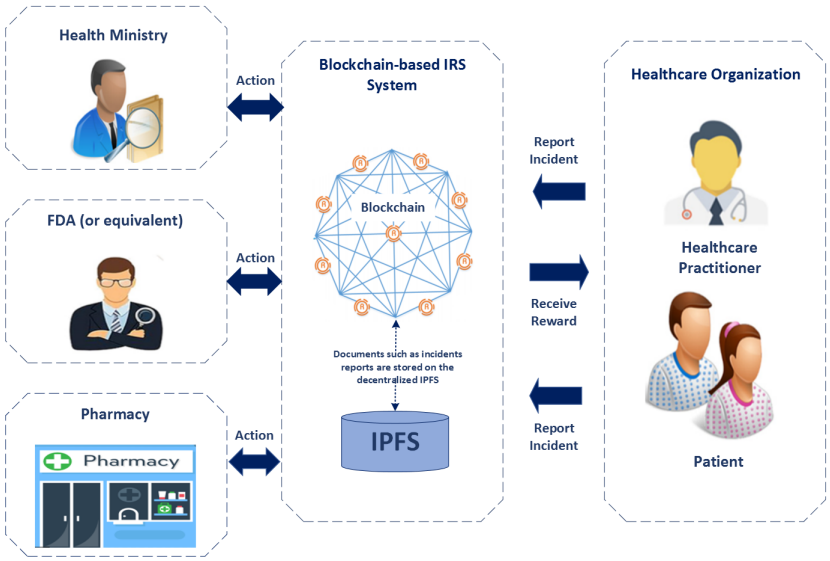

Fig. 2 System Overview of Proposed Solution

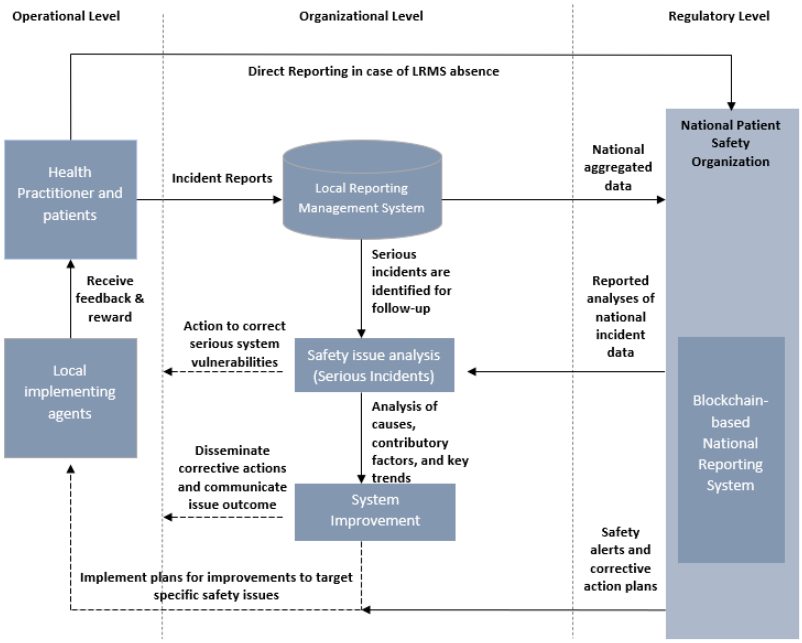

Fig. 3 Framework of Incident Reporting System

While Figure 2 and 3 show the system overview and give the proposed feedback framework, the following section will highlight the roles and responsibilities of stakeholders in the proposed solution.

3.2 Stakeholders Roles and Responsibilities

Various stakeholders play a role in a typical incident reporting system, as discussed earlier. Our proposed blockchain-based incident reporting system will have a particular focus on medication incidents, as one of the leading incident types in healthcare (Cohen and Smetzer, 2013). A medication incident is any event where the expected course of events in the support and administration of medications is not followed, or both. Medication incidents may include the following particular examples: medicines given to the incorrect patient, incorrect medicine/ dose/ route being given, out of date medicine, incorrect storage/ labeling/ packaging/ naming of medicine, etc. (Tariq et al., 2012). The stakeholders involved in a medication incident reporting and sharing process are mainly the Food and Drug Administration (FDA) (or equivalent), pharmacies, health ministry, healthcare practitioners, and patients. Table 2 encapsulates the roles and key responsibilities of these stakeholders.

Table 2 Stakeholders Roles and Responsibilities

Stakeholders	Roles	Responsibilities
Patient	An individual who receives care in a healthcare setting	- Notify, communicate, and provide the necessary incident-related information. - Submit incident report.
Hospital practitioner	An individual who delivers care to a patient and who may witness, at any stage, an incident or near misses.	- Notify, communicate, and provide the necessary incident-related information. - Submit the incident report to the hospital's local risk management system. - Submit directly to the blockchain platform in case the hospital does not have a local risk management system. - Follow the corrective action plan once provided.
Pharmacy	Prepares medications by reviewing and interpreting physician orders.	- Adhere to the corrective action plan. - Adjust the storage conditions, if applicable. - Withdraw the medication, if needed.
Health Ministry	It reviews incidents, generates action plans, and develop advice and guidance.	- Share learning nationally to reduce the risk to patients. - Use data from the blockchain platform to develop guidance to minimize risks to patients.
FDA (and equivalent)	It monitors and prevents medication errors of regulated drugs and therapeutic biological products.	- Analyze and monitor medication error reports. - Guide manufacturers in regard to designing and naming the drug products. - Take regulatory actions such as issuing a safety communication and revising the labeling.

4 Implementation

In this section, we present and discuss the system architecture, message sequence diagram, and algorithms for implementing the proposed blockchain-based IRS. The smart contract is written in Solidity, the used language for Ethereum smart contracts. The contract is then executed with Remix IDE, a browser-based compiler with an embedded debugger used for alerting and alarming the user with error notifications and warnings accordingly.

4.1 System Architecture

In this section, we propose an Ethereum blockchain-based solution. In the proposed solution, blockchain is used to share the incident reports with stakeholders. Further, in our proposed solution, the shared incident data can be traded, and the encrypted transaction information is existing among the stakeholders to ensure its reliability and security.

The system architecture in Figure 4 integrates the IPFS technology into the system to store a collection of hashed files that could be retrieved anytime when incorporated

within the blockchain. Incident reports stored on the IPFS network are assigned a unique cryptographic hash, which is later used to track the corresponding report. Therefore, this makes the IPFS an ideal environment to store data, as reports are immutable, traceable, and timestamped via blockchain. Examples of certain vital documents that could be stored in the IPFS include but not limited to: healthcare professionals e-forms, patients e-forms, FDA and ministry of health action plans, standard operating procedure (SOP) (detailed instructions on how to report an event), incident reporting protocol, injured patients data and their medical history, etc. The system architecture would compromise four layers, as follows:

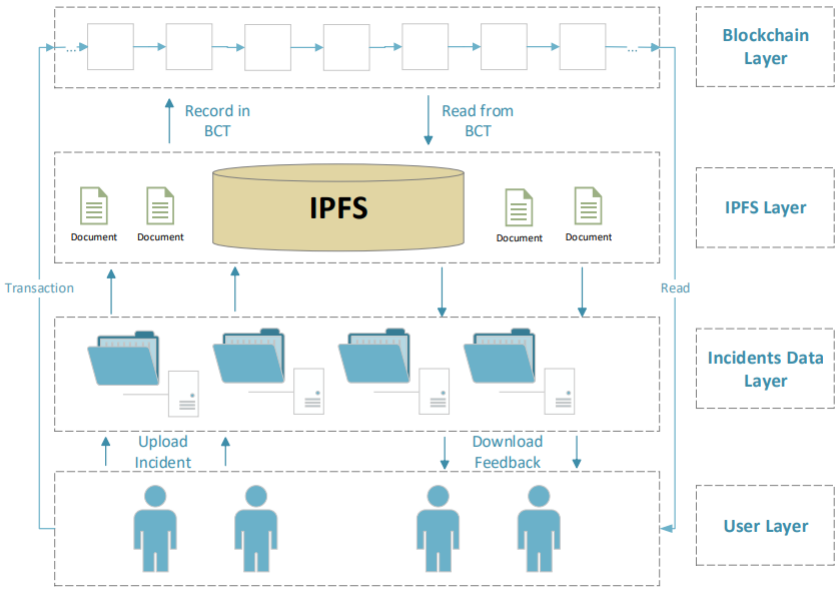

Fig. 4 System Architecture of Incidents Reporting among Stakeholders

User Layer. Stakeholders of the blockchain in the user layer have access to the same kind of information. Stakeholders can also use the blockchain to fulfill transactions that can be tracked and can further use it to inhibit the shared incident reports from being tampered.

Data Layer. Data represents the incident reports and action plans that stakeholders, such as patients or healthcare practitioners want to share and protect. Stakeholders in the data layer can collectively maintain the data. For the privacy of the uploaded data, the data is encrypted using the cryptographic mechanisms. Afterward, the data of the encrypted incident is uploaded onto the IPFS for sharing.

IPFS Layer. Interplanetary File System is a peer-to-peer protocol and network. The IPFS is a decentralized storage network in which each file is identified through its hashing function. The data owner uploads the data encrypted with a symmetric key that is further encrypted with the data owner's public key. Once the database

is requested for the data (based on the hash of the file), it provides the proxy. As explained before, the IPFS would contain important files such as the incident reports, FDA and MoH action plans.

Blockchain Layer. Blockchain technology layer can permanently record all movements, modifications, restorations, and ownership details of incidents data on the distributed transparent and tamper-proof ledger. Furthermore, transparency of transaction records increases the trust of patients and healthcare organizations. Using immutable transaction records, blockchain technology also assists in providing feedback to reporter and history of the incident.

4.2 Entity Relationship Diagram

The entity-relationship diagram in Figure 5 illustrates the attributes of the smart contracts along with its functions. It also shows the relationship between different stakeholders and smart contracts. These relations and metadata are vital in implementing smart contracts. Furthermore, the relationship between any entity and the contract is one-to-one as the stakeholders were assumed to be single entities. That is the FDA, pharmacies, health ministry, patients, and healthcare practitioners.

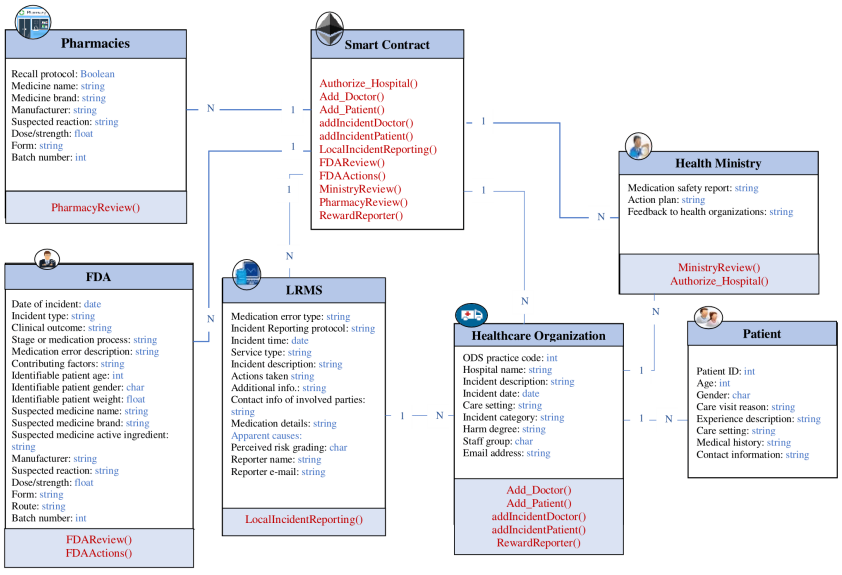

Fig. 5 Entity-relationship diagram between different stakeholders and smart contract

4.3 Message Sequence Diagram

A message sequence diagram shows the interactions between different stakeholders, while simultaneously showing various events that are triggered in the sequence of functions within the smart contract. Further, each participant in the network holds an Ethereum Address that enables them to interact with each other by calling functions within the smart contract. Figure 6 illustrates the sequence flow between different stakeholders from uploading an incident report to getting feedback. Initially, the

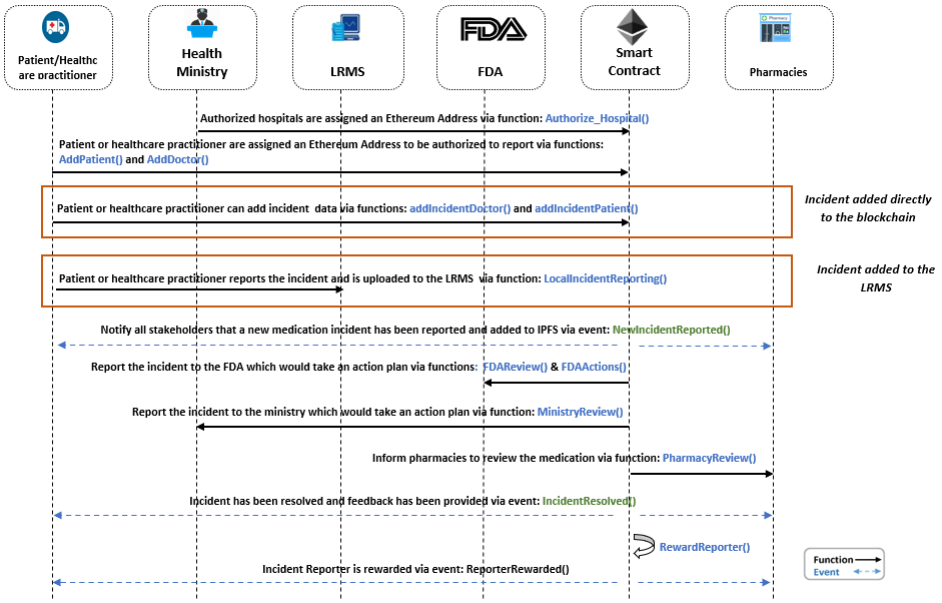

Fig. 6 Message Sequence Diagram between different stakeholders and smart contract

Ministry of Health would register authorized hospitals in the system via a function called *AuthorizeHospital*( ). Then, healthcare practitioners and patients would be registered and assigned an Ethereum Address by executing the functions *AddDoctor*( ) and *AddPatient*( ). By being registered in the system, the reporting party would be able to upload information of an incident. This incident claim is either reported in the local reporting management system (LRMS), if the hospital has one, or is reported directly to the blockchain. This occurs by executing the function called *LocalIncidentReporting*( ). If the authorized hospital does not have a LRMS, the reporting party can report directly into the blockchain platform by executing the following functions, *addIncidentDoctor*( ) and *addIncidentPatient*( ). After the successful reporting of the incident, the event is broadcasted among all stakeholders by *NewIncidentReported*( ). In the case of a serious incident, the stakeholders are

requested to act. The ministry of health will have to review the incident and generate an action plan via function *MinistryReview*( ).

Additionally, the FDA may need to review the incident *FDAReview*( ) and act if required by *FDAActions*( ). If the ministry of health and the FDA confirms and approve the danger of the medication involved in the incident, the pharmacies are informed to withdraw the latter via function *PharmacyReview*( ). At the end of the process, the reporter is rewarded by executing *RewardReporter*( ) for reporting the incident and encouraged to report on future occasions.

4.4 Implementation Framework

We now describe the algorithms that highlight the working principles of our proposed blockchain solution for incident reporting system. The proposed solution was deployed and tested on a virtual test Ethereum network using Remix IDE. The smart contract code was implemented and debugged. All function calls can be viewed in the console to verify the methods' functionality, the output, and the cost of execution.

Algorithm 1 below describes the initial steps that would be taken to register the incident reporting party (patient or doctor). First, incidents reporters are assigned Ethereum addresses to be able to interact with the smart contracts. Algorithm 1 describes how only incident reporters are registered under the function AddDoctor() and addPatient() to check whether the address is registered or not. If the reporter is not registered, then these functions are responsible for registering the latter by appending its Ethereum Address to the list of the incident reporters (doctors, patients, etc.).

Algorithm 1 Reporting Patient Registration

Input: *PatientAddress*

1 Patient*Address* is the Ethereum Address of the patient that would upload data into the smart contract.
2 Verify if reporter exists already.
3 **if** reporter already exists then
4 | Allow incident reporting.
5 **else**
6 | Initialize reporter information.
7 | Append the reporter to the list of allowed incident reporters.
8 **end**

Algorithm 2 shows that doctors with a valid address are allowed to interact with the smart contract and are able to report. It also shows the variables that are needed from the doctor when deciding to report an incident. These variables include Doctor ID, incident description, Incident date, incident category, harm degree. . . etc. If the address of the patient is unauthorized or unregistered, the patient would not be able

to successfully report the details of the incident as the smart contract would reject all other unauthorized Ethereum addresses.

Algorithm 2 Submit new incident report (Doctor)

```
Input: DoctorID, IncidentDescription, IncidentDate,
IncidentCategory, CareSetting, staffgroup, emailaddress
if Caller == Doctor then
    if Doctor== True
    Add new incident report
    Update IPFS incident details.
    Emit an event to inform stakeholders
    end
else
    Doctor is not registered.
end
```

Algorithm 3 demonstrates that only patients allowed to interact with the smart contract at this stage are able to report. Allowed patients are those with a authorized Ethereum address. It also shows the variables that are needed from the patient when deciding to report an incident. These variables include ID, age, primary care visit reason, experience description. . . etc. If the address of the patient is authorized and recognized, the patient would be able to successfully report the details of the incident.

Algorithm 3 Submit new incident report (Patient)

```
Input: Patient ID, Age; Care Visit Reason, Experience
Description, Care Setting, Medical History, Contact Information
if Caller == Patient then
    if Patient== True
    Add new incident report
    Update IPFS incident details.
    Emit an event to inform stakeholders
    end
else
    Patient is not registered.
end
```

Algorithm 4 illustrates the actions undertaken by the ministry of health if the incident reported is a serious incident (leading to a serious injury or death). In our proposed solution, we are focusing on the case of medication incidents and errors. Thereby, in the case of a serious incident, the ministry would review the latter and develop and action plan to be added to the IPFS. This action plan can be accessed

by the different stakeholders (FDA, pharmacies...etc). Furthermore, the ministry of health would classify the incident and send any feedback when applicable as explained in Figure 3.

Algorithm 4 Ministry of Health Incident Review & Action Plan

```
Input: IPFS_IncidentDetails, HarmDegree
if HarmDegree == High
then
    Allow ministry action plan to be added to IPFS.
    Emit an event to add an action plan addressing the incident.
    Emit another event to contact relevant stakeholders.
else
    Emit an event to review the incident, classify it, and send
feedback to reporter.
end
```

Algorithm 5 describes the steps taken by the FDA when a serious incident is reported. The FDA would review the incident classify it to determine the cause and type of error. The FDA would then identify and revise information that may contribute to medication error and contact the medication manufacturer to either revise the labels, labeling, packaging, product design or proprietary name and/or stop manufacturing the medication by developing an action plan.

Algorithm 5 FDA Incident Review & Action Plan

```
Input: IPFS_IncidentDetails, HarmDegree, IncidentCategory
if Incident Category is Medication
    if HarmDegree == High
    then
        Allow FDA action plan to be added to IPFS.
        Emit an event to contact medicine manufacturer.
        Emit an event to develop an action plan.
    end
else
    Emit an event to review the incident.
end
```

Algorithm 6 demonstrates the process undertaken by pharmacies once they receive a medication-related incident. The pharmacy would review the action plan developed by both the FDA and/or the Ministry of Health. The pharmacy would

then update the status of the medication according to the action plan. If necessary, pharmacies would withdraw the medication.

Algorithm 6 Pharmacy Incident Review

```
Input: IPFS_IncidentDetails, HarmDegree, IncidentCategory
if Incident Category is Medication
   if HarmDegree == High
   then
      Update medication status.
      Emit an event to withdraw medication
   end
else
    Emit an event to review the action plans.
end
```

Algorithm 7 explains how a stakeholder can be rewarded for reporting an incident. Rewarding is an essential component of our proposed solution as it would give stakeholders more reasons to report. The receiver can be either the reporting patient or healthcare practitioner. If the Ethereum address does not correspond to an entity with a valid address and who recently reported a true incident event, the system would preview an error.

Algorithm 7 Reward for Reporting an Incident

```
Input: address Receiver, amount
   if Receiver == Patient or Receiver == Doctor then
   Allow payment of patient by transferring the amount.
   Emit an event to notify the reporter of the reward.
   end
   else
    Preview an error and return the contract to the previous state.
end
```

5 Discussion

The aim of incident reporting is to report incidents and share information about adverse events to ensure lessons are learned, and previous tragedies are not repeated. Since their inception, the reporting systems have used the patient safety incidents reported to identify risks and how they might be avoided. Annually, up to nine

thousand people die in the United States alone as a result of a medication error. Moreover, hundreds of thousands of other patients can experience a complication related to a medication or adverse reaction, but it is often not reported. It has also been reported that looking after patients that suffer from medication-associated errors exceed 40 billion dollars each year. A medication error does not only involve a financial cost, but also includes the physical and psychological pain and distress resulting from the error to the patients (Tariq et al., 2020). Therefore, our proposed platform can contribute into mitigating these errors, while presenting a financially feasible solution that has few challenges as the sections below describe.

5.1 Cost Analysis

Our proposed blockchain-based solution to incident reporting captures the primary operations required to take place in the reporting process. In this section, we present the cost analysis of the proposed system. For transactions to get executed successfully, a gas fee is required to be paid by stakeholders in the network. The Ethereum gas is the unit used to measure the computational effort required for transaction executions. Ethereum transactions incur two types of costs of their execution. While execution cost is related to the costs of changing states in the contract and internal storage, transaction cost is the execution cost along with the cost of sending data, such as contract deployment and transaction input cost (Chaer et al., 2019).

Moreover, it should be noted that as the gas price increases, the rate of adding verified transactions to each block increases. Accordingly, this price is expected to increase during high network traffic as miners compete to add transactions in the blocks to receive transaction fees. Table 3 shows the transaction and execution gases along with the corresponding transaction fees for deploying the contract and executing the major functions.

The average gas price equal to 4 Gwei was obtained on the 15th of October 2020, according to the ETH Gas Station. This transaction fee was converted to US Dollars at an Ether exchange rate of 1 ETH = 369 USD (ETH Gas Station, 2020). We notice that the cost incurred by the stakeholders is slightly over 7 USD. This analysis shows that implementing the presented solution is feasible and encourages cost-savings to all stakeholders in the network.

5.2 Security Analysis

In this section, we discuss the security properties of the proposed blockchain-based incident reporting system to address core security concerns related to integrity, availability, accountability, authorization, nonrepudiation, and resistance to cyberattacks such as Distributed Denial of Service (DDoS) attack (Hasan and Salah, 2019).

Table 3 Transaction Cost Incurred at an average Gas Price of 4 Gwei at an Exchange Rate of 1 ETH = 369 USD

Function Name	Transaction Gas	Execution Gas	Average Transaction Fee (USD)
Deployment	1442069	1046869	4.86
AuthorizeHospital()	36578	5438	0.078
AddPatient()	45673	3792	0.077
AddDoctor()	45677	3740	0.076
addIncidentDoctor()	109824	10769	0.18
addIncidentPatient()	10146	10394	0.17
LocalIncidentReporting()	106828	28780	0.21
FDAReview()	376876	84995	0.71
MinistryReview()	356879	28770	0.59
PharmacyReview()	244860	23076	0.41
RewardReporter()	249576	14736	0.35

The code of this implementation is made publicly available on GitHub and has been validated using the security tool, called SmartCheck. This tool enables the evaluation and eradication of weaknesses in the code. The most common bugs that can occur in a code include malicious libraries, timestamp dependence, locked money, and reentrancy. In addition to the possible existing weaknesses, errors, and exploits pose severe threats to data security and cause significant losses. Consequently, we verified that the code is free from the common threats. Further, our proposed smart contract would be less vulnerable compared to other smart contracts as it has no fallback loops or functions. Moreover, blockchain has, by design, built-in security features that enable building a secure, resilient, and trusted networks and services. For example, security requirements such as authorization, nonrepudiation, integrity, privacy, and availability can be achieved easily through the use of blockchain.

Integrity. The participating stakeholders in the incident reporting can sign the transactions digitally to guarantee that the integrity of incident data will be well preserved. Moreover, once information about an incident is added to the blockchain network, then it becomes challenging to tamper with it due to the immutability and its decentralized structure and combination of cryptography and sequential hashing, unlike a traditional standard database.

Availability. The transaction logs of stakeholders involved in incident reporting are always available that can assist in tracing the provenance of an incident. Moreover, duplicated incident records are stored on the blockchain nodes. As a result, the system becomes resilient and robust against a single point of failure.

Authorization. The role of different stakeholders in incident reporting is altered as per Table 2. Through the authorization feature, only authorized stakeholders can perform a specific task. Securing data access in blockchain networks is essential for ensuring that only users with authorized access can participate and add appropriate data accordingly. Moreover, the blockchain infrastructure ensures that each data block is fully encrypted before it gets added to the chain of existing blocks. Thus, if an attacker could gain access to the blockchain data and network, then this does not,

certainly, mean that the attacker would be able to retrieve and read the information due to the use of end-to-end encryption methods. Only authorized users can decrypt and see this information via their private keys.

Nonrepudiation. All transactions of incident reporting are digitally and cryptographically signed by their actors. This feature indicates that users or organizations can trace back a particular incident report at a specific time and accordingly identify the user behind that transaction using their public address. This security property reassures users since no one can duplicate their signature on a transaction that has not been created by them. This feature enhances the system reliability as it becomes easier to detect fraudulent transactions because every transaction stored in the ledger is cryptographically connected to its user.

Resistance to cyberattacks. Cyberattacks have become progressively more complex due to the increasing use of sophisticated malware and threat from professional cyber organizations. Users and organizations may attempt to steal valuable data, such as financial data, personally identifiable information, intellectual property, health records, etc. Several strategies, such as monetizing data access by advanced ransomware techniques or disrupting business operations through DDoS attacks, have been attempted.

5.3 Challenges

Blockchain technology carries a unique set of challenges with it that have greatly contributed to its slow-moving adoption, including:

Scalability. The blockchain network traffic becomes bulky as the number of transactions increases every day. Every node on the blockchain must store all validated transactions, and this becomes an obstacle as there is a restriction on the block size and time interval used to create a new block. Current blockchain platforms process only a few transactions per second, which becomes problematic as millions of transactions are needed to be processed in real-time. Since the block size is limited, this causes small transactions to be delayed as miners prefer to validate transactions with high transaction fees (Onik et al., 2019; Zhang et al., 2018).

Selfish Mining. The blockchain network that depends on a consensus of the majority to validate transactions is prone to attackers if they could compromise a significantly large group of nodes. For example, malign actors can compromise a public blockchain network if they could manipulate at least 51 percent of the consensus and mining power. The same problem can also occur if several miners secretly join forces to create a majority and control the blockchain. The strategy used by selfish miners is that they create a private branch by mining blocks without broadcasting, and they publish the private chain only when it is longer than the current public chain. They mine this chain without competitors; meanwhile, honest miners waste their resources on mining a useless branch. As a result, by doing so, selfish miners earn more revenue (Khan and Salah, 2018).

Legal Challenges. Until this date, smart contracts and blockchain, in general, are highly de-regulated and non-standardized at the national and international levels. Due to having many stakeholders, data ownership, and existing medical law of the traditional healthcare system are essential issues to be considered. Further, new regulations on health policy, data sharing, digital health-service related policy, and digital inequality and digital connectivity should be addressed (Gökalp et al., 2018).

Privacy Concerns. Blockchain technology is susceptible to privacy leakage as balances and details of all public keys are made transparent to all network members. However, there have been two proposed solutions that are divided into mixing solution and anonymous solution to achieve anonymity in blockchains. Mixing service provides anonymity by using multiple input addresses to transfer funds to various output addresses while anonymous is a service that prevents transaction graph analysis by unlinking the payment origins for a transaction (Dubovitskaya et al., 2017) (Onik et al., 2019).

6 Conclusion

In this paper, we proposed a novel blockchain-based framework for incidents reporting using Ethereum smart contracts. Our proposed blockchain-based solution promotes transparency, traceability, and streamlines communication between stakeholders in the process. Moreover, it ensures data immutability and security while simultaneously encourages the collection of incidents from various stakeholders. The smart contract code was used to capture interactions, and share the process flows in the appropriate order. Further, we integrated the IPFS technology in our framework to store various files such as incident reports, corrective action plans, etc. The proposed solution can also ensure the reliability of reporting while maintaining high efficiency in the non-fully trusted environment. Also, the proposed blockchain-based reporting system encourages both healthcare practitioners and patients to actively participate in sharing and reporting incidents thanks to the incentivizing mechanism.

The system architecture, sequence diagram, and algorithms are not limited to medication errors but can be extended to reporting several other types of errors and incidents. The functions developed were tested in the Remix environment to demonstrate the validity and operational aspects of the smart contract, as stated in the algorithms. Also, we performed a cost analysis to compute the transaction costs incurred when interacting with the smart contract. It revealed that a minimal cost of less than 1 USD is incurred when executing transactions, while the cost of deploying the contract was less than 5 USD. This shows that the proposed solution is feasible as the stakeholders pay 7.6 USD when compared to traditional incident reporting systems, which require a partial payment to be made to third-party service providers. Future research can be extended to include the development of front-end DApps, that patients and healthcare practitioners can easily use to report any incident. The smart contract can also be developed to capture further areas of incidents and can be connected to the electronic health records (EHR) for better learning results.

7 Acknowledgement

This publication is based upon work supported by the Khalifa University of Science and Technology under Award No. CIRA-2019-001.

8 References

1. Anderson, J.E., Kodate, N., Walters, R., Dodds, A., 2013. Can incident reporting improve safety? Healthcare practitioners' views of the effectiveness of incident reporting. Int J Qual Health Care 25, 141–150. https://doi.org/10.1093/intqhc/mzs081
2. Armitage, G., Moore, S., Reynolds, C., Laloë, P.-A., Coulson, C., McEachan, R., Lawton, R., Watt, I., Wright, J., O'Hara, J., 2018. Patient-reported safety incidents as a new source of patient safety data: an exploratory comparative study in an acute hospital in England. J. Health Serv. Res. Policy 23, 36–43. https://doi.org/10.1177/1355819617727563
3. Atzori, M., 2017. Blockchain technology and decentralized governance: Is the state still necessary? J. Gov. Regul. 6, 45–62. https://doi.org/10.22495/jgrv6i1p5
4. Benn, J., Koutantji, M., Wallace, L., Spurgeon, P., Rejman, M., Healey, A., Vincent, C., 2009. Feedback from incident reporting: information and action to improve patient safety. Qual. Saf. Health Care 18, 11–21.
5. Chaer, K. Salah, C. Lima, P. P. Ray and T. Sheltami, "Blockchain for 5G: Opportunities and Challenges," 2019 IEEE Globecom Workshops (GC Wkshps), Waikoloa, HI, USA, 2019, pp. 1-6, doi:10.1109/GCWkshps45667.2019.9024627.
6. Cohen, M.R., Smetzer, J.L., 2013. ISMP Medication Error Report Analysis - Preventing Mix-Ups Between Various Formulations of Amphotericin B; Arixtra Is Not a Hemostat; Measurement Mix-Up; Drug Names Too Close for Comfort; New Vaccine Errors Reporting Program. Hosp. Pharm. 48, 95.
7. Cole, R., Stevenson, M., Aitken, J., 2019. Blockchain technology: implications for operations and supply chain management. Supply Chain Manag. Int. J. 24, 469–483. https://doi.org/10.1108/SCM-09-2018-0309
8. Dubovitskaya, A., Xu, Z., Ryu, S., Schumacher, M., Wang, F., 2017. Secure and Trustable Electronic Medical Records Sharing using Blockchain. AMIA Annu. Symp. Proc. AMIA Symp. 2017, 650–659. ETH Gas Station, 2020.
9. Gökalp, E., Gökalp, M.O., Çoban, S., Eren, P.E., 2018. Analysing Opportunities and Challenges of Integrated Blockchain Technologies in Healthcare, in: Wrycza, S., Maślankowski, J. (Eds.), Information Systems: Research, Development, Applications, Education. Springer International Publishing, Cham, pp. 174–183. https://doi.org/10.1007/978-3-030-00060-813
10. Gong, Y., Kang, H., Wu, X., Hua, L., 2017. Enhancing Patient Safety Event Reporting: A Systematic Review of System Design Features. Appl. Clin. Inform. 08, 893–909. https://doi.org/10.4338/ACI-2016-02-R-0023

11. Hagley, G., Mills, P.D., Watts, B.V., Wu, A.W., 2019. Review of alternatives to root cause analysis: developing a robust system for incident report analysis. BMJ Open Qual. 8, e000646. https://doi.org/10.1136/bmjoq-2019-000646
12. Hasan, H.R., Salah, K., 2019. Combating Deepfake Videos Using Blockchain and Smart Contracts. IEEE Access 7, 41596–41606.
13. Iansiti, M., Lakhani, K., 2017. The Truth About Blockchain. Harv. Bus. Rev.
14. Khan, M.A., Salah, K., 2018. IoT security: Review, blockchain solutions, and open challenges. Future Gener. Comput. Syst. 82, 395–411.
15. Khezr, S., Moniruzzaman, M., Yassine, A., Benlamri, R., 2019. Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research. Appl. Sci. 9, 1736. https://doi.org/10.3390/app9091736
16. Kingston, M.J., Evans, S.M., Smith, B.J., Berry, J.G., 2004. Attitudes of doctors and nurses towards incident reporting: a qualitative analysis. Med. J. Aust. 181, 36–39.
17. Levtzion-Korach, O., Frankel, A., Alcalai, H., Keohane, C., Orav, J., Graydon-Baker, E., Barnes, J., Gordon, K., Puopolo, A.L., Tomov, E.I., Sato, L., Bates, D.W., 2010. Integrating Incident Data from Five Reporting Systems to Assess Patient Safety: Making Sense of the Elephant. Jt. Comm. J. Qual. Patient Saf. 36, 402-AP18. https://doi.org/10.1016/S1553-7250(10)36059-4
18. Macrae, C., 2016. The problem with incident reporting: Table 1. BMJ Qual. Saf. 25, 71–75. https://doi.org/10.1136/bmjqs-2015-004732
19. Makary, M.A., Daniel, M., 2016. Medical error—the third leading cause of death in the US. BMJ 353, i2139. https://doi.org/10.1136/bmj.i2139
20. Mamoshina, P., Ojomoko, L., Yanovich, Y., Ostrovski, A., Botezatu, A., Prikhodko, P., Izumchenko, E., Aliper, A., Romantsov, K., Zhebrak, A., Ogu, I.O., Zhavoronkov, A., 2018. Converging blockchain and next-generation artificial intelligence technologies to decentralize and accelerate biomedical research and healthcare. Oncotarget 9, 5665–5690. https://doi.org/10.18632/oncotarget.22345
21. Mayer, A.H., da Costa, C.A., Righi, R. da R., 2020. Electronic health records in a Blockchain: A systematic review. Health Informatics J. 26, 1273–1288. https://doi.org/10.1177/1460458219866350
22. Naome, T., James, M., Christine, A., Mugisha, T.I., 2020. Practice, perceived barriers and motivating factors to medical-incident reporting: a cross-section survey of health care providers at Mbarara regional referral hospital, southwestern Uganda. BMC Health Serv. Res. 20. https://doi.org/10.1186/s12913-020-05155-z
23. NHS Improvement, 2019. National patient safety incident reports.
24. NHS Improvement, 2018. Learning from patient safety incidents.
25. Noble, D.J., Pronovost, P.J., 2010. Underreporting of Patient Safety Incidents Reduces Health Care's Ability to Quantify and Accurately Measure Harm Reduction. J. Patient Saf. 6, 247–250. https://doi.org/10.1097/PTS.0b013e3181fd1697
26. Omar, I.A., Jayaraman, R., Salah, K. et al. Ensuring protocol compliance and data transparency in clinical trials using Blockchain smart contracts. BMC Medical Research Methodology 20, 224 (2020). https://doi.org/10.1186/s12874-020-01109-5
27. Omar, I.A., Jayaraman, R., Salah, K. and Simsekler, M. C. E. "Exploiting Ethereum Smart Contracts for Clinical Trial Management," 2019 IEEE/ACS 16th

International Conference on Computer Systems and Applications (AICCSA), Abu Dhabi, United Arab Emirates, 2019, pp. 1-6/ doi: 10.1109/AICCSA47632.2019.9035341.
28. Onik, Md.M.H., Aich, S., Yang, J., Kim, C.-S., Kim, H.-C., 2019. Blockchain in Healthcare: Challenges and Solutions, in: Big Data Analytics for Intelligent Healthcare Management. Elsevier, pp. 197–226. https://doi.org/10.1016/B978-0-12-818146-1.00008-8
29. Ramírez, E., Martín, A., Villán, Y., Lorente, M., Ojeda, J., Moro, M., Vara, C., Avenza, M., Domingo, M.J., Alonso, P., Asensio, M.J., Blázquez, J.A., Hernández, R., Frías, J., Frank, A., 2018. Effectiveness and limitations of an incident-reporting system analyzed by local clinical safety leaders in a tertiary hospital: Prospective evaluation through real-time observations of patient safety incidents. Medicine (Baltimore) 97, e12509. https://doi.org/10.1097/MD.0000000000012509
30. Ray, P.P., Dash, D., Salah, K., Kumar, N., 2020. Blockchain for IoT-Based Healthcare: Background, Consensus, Platforms, and Use Cases. IEEE Syst. J. 1–10. https://doi.org/10.1109/JSYST.2020.2963840
31. Shojania, K.G., 2010. The elephant of patient safety: what you see depends on how you look. Jt. Comm. J. Qual. Patient Saf. Jt. Comm. Resour. 36, 399–401.
32. Shojania, K.G., Thomas, E.J., 2013. Trends in adverse events over time: why are we not improving? BMJ Qual. Saf. 22, 273–277. https://doi.org/10.1136/bmjqs-2013-001935
33. Simsekler, M.C.E., Gurses, A.P., Smith, B.E., Ozonoff, A., 2019. Integration of multiple methods in identifying patient safety risks. Saf. Sci. 118, 530–537. https://doi.org/10.1016/j.ssci.2019.05.057
34. Stavropoulou, C., Doherty, C., Tosey, P., 2015. How Effective Are Incident-Reporting Systems for Improving Patient Safety? A Systematic Literature Review: Incident-Reporting Systems for Improving Patients' Safety. Milbank Q. 93, 826–866. https://doi.org/10.1111/1468-0009.12166
35. Sujan, M.A., Habli, I., Kelly, T.P., Pozzi, S., Johnson, C.W., 2016. Should healthcare providers do safety cases? Lessons from a cross-industry review of safety case practices. Saf. Sci. 84, 181–189. https://doi.org/10.1016/j.ssci.2015.12.021
36. Tandon, A., Dhir, A., Islam, N. and Mäntymäki, M., 2020. Blockchain in healthcare: A systematic literature review, synthesizing framework and future research agenda. Computers in Industry, 122, p.103290.
https://doi.org/10.1016/j.compind.2020.103290
37. Tariq, A., Georgiou, A., Westbrook, J., 2012. Medication incident reporting in residential aged care facilities: Limitations and risks to residents' safety. BMC Geriatr. 12. https://doi.org/10.1186/1471-2318-12-67
38. Tariq, R.A., Vashisht, R., Scherbak, Y., 2020. Medication Errors, in: StatPearls. StatPearls Publishing, Treasure Island (FL).
39. Wang, Y., Coiera, E., Runciman, W., Magrabi, F., 2017. Using multiclass classification to automate the identification of patient safety incident reports by type and severity. BMC Med. Inform.
40. Decis. Mak. 17, 84. https://doi.org/10.1186/s12911-017-0483-8 WHO, 2005. WHO Draft Guidelines for Adverse Event Reporting: From Information to Action. World Health Organization.

41. Yi, H., 2019. Securing instant messaging based on blockchain with machine learning. Saf. Sci. 120, 6–13. https://doi.org/10.1016/j.ssci.2019.06.025
42. Yoon, H.-J., 2019. Blockchain Technology and Healthcare. Healthc. Inform. Res. https://doi.org/10.4258/hir.2019.25.2.59
43. Zhang, P., Schmidt, D.C., White, J., Lenz, G., 2018. Blockchain Technology Use Cases in Healthcare, in: Advances in Computers. Elsevier, pp. 1–41. https://doi.org/10.1016/bs.adcom.2018.03.006