

Blockchain-based Decentralised Management of Digital Passports of Health (DPoH) for Vaccination Records

Abdulrahman Alreshidi

College of Computer Science and Engineering, University of Ha'il, Saudi Arabia

Abstract—With the recent impact of viral infections and pandemics – akin to a recent global healthcare emergency due to COVID-19 - there is an urgent need for mass-scale testing and vaccination initiatives for tackling the health and economic crises. However, the centralized storage of patient information has given rise to significant concerns regarding privacy, transparency, and efficient transmission of vaccination records. This paper exploits a blockchain-based solution that presents a novel approach by seamlessly integrating identity verification, encryption protocols, and decentralized storage via IPFS (InterPlanetary File System) which gives rise to the concept of Digital Passport of Health (DPoH). The proposed solution in this paper introduces the concept of DPoH, specifically designed for test certification, and leverages the power of smart contracts on Ethereum-based blockchain technology for securely creating, managing and transmitting data in the form of DPoH. The proposed solution is being evaluated in three dimensions including (i) *gas cost* (i.e. energy efficiency), (ii) *data storage* (i.e. storage efficiency), and (iii) *data access* (i.e. response time) for creation and transmission of DHoPs. The developed solution and its criteria-based validation are complemented with algorithmic implementations that can progress existing research and development on blockchain-based management of health-critical systems.

Keywords—Smart healthcare; blockchain; software architecture; digital passport of health; software engineering

I. INTRODUCTION

In recent years, the world has witnessed the relentless spread of viral infections resulting into epidemics (Ebola) and pandemics (COVID-19), prompting a need for innovative approaches to manage and mitigate their socio-economic impact on public health. The ongoing viral infections and pandemic, as highlighted by Chamola et al. [1], has underscored the importance of harnessing emerging technologies that include but are not limited to the sensor-driven Internet of Things (IoT), pervasive drones, artificial intelligence (AI), and secure blockchain to enhance healthcare systems' capabilities. Blockchain as a concept and its underlying technology has emerged as a promising tool to address various challenges related to healthcare as outlined by Hassija et al. in [2]. The potential of blockchain in healthcare has garnered significant attention, with various stakeholders recognizing its ability to transform data management, security, and transparency within the industry [3]. The central characteristics of blockchain technology which include decentralization and immutability, hold promise for addressing critical issues related to data privacy and trust [4]. Blockchain systems' application in healthcare has been explored in various contexts, from patient data management to the creation of open data platforms to

support healthcare responses [5], [6]. However, with the rising challenges posed by viral outbreaks, there remains a dire need to investigate how blockchain systems can effectively manage the health data and the certification of health-related documents such as test results and vaccination records [12]. More specifically, the spread of the most recent COVID-19 pandemic has already prompted discussions on leveraging blockchain for health-related purposes [7].

A. Research Context

Considering the context of connected and smart healthcare, our research focuses on leveraging blockchain technology to enable the effective management of health data in the age of viral outbreaks, be it epidemics or full-scale pandemics. Based on the foundations of existing research within the blockchain healthcare domain [2], [6], our proposed solution, as illustrated in Fig. 1 takes the form of a blockchain-based solution designed to offer a comprehensive remedy for the challenges that hinder healthcare data management during health crises. The primary feature of this proposed solution is the integration of state-of-the-art technology, including decentralized storage facilitated using the InterPlanetary File System (IPFS) [9], which manages digital identity, and robust encryption mechanisms as highlighted in Fig. 1. As part of the proposed solution, we focus on addressing the issues central to health-critical data such as insecurity, lack of privacy, and opaqueness. Moreover, the proposed solution aims to manage the digital certification of healthcare documents that can otherwise be manual, time-consuming, and error-prone. This can ensure security of sensitive health-critical data and ultimately enhance the trust, efficiency, and transparency that is quintessential for healthcare systems to operate seamlessly, even in the face of the most challenging of healthcare crises [11], [15].

B. Solution Overview

By leveraging the work of Eisenstadt et al. [9], who emphasized the role of mobile applications in COVID-19 test and vaccination certification [13], we introduce the concept of a Digital Passport of Health (DPoH) as a certification mechanism. Fig. 1 provides a high-level illustration of proposed solution where a (1) patient (vaccinated individual) has a vaccination record that is (2) stored and managed as a (3) DPoH (smart contract an blockchain based implementation) to be (4) retrieved as health records that be shared for examination by the medics that enables (5) secure and efficient medical examination of vaccination records in the form of DPoH.

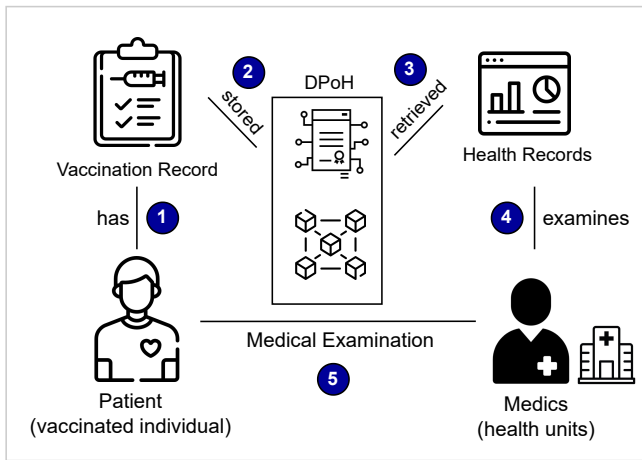


Fig. 1. An Illustrative view of the proposed solution.

We explore the use of Ethereum-based smart contracts [10] to facilitate the issuance and verification of DPoH, ensuring a prompt and reliable response from the relevant healthcare authorities [14]. More specifically, we present a detailed system model, the development of our proposed blockchain-based solution, and the evaluation of its feasibility and security. To validate the feasibility of our framework, we deploy a prototype smart contract on the Ethereum TESTNET network. This research aims to contribute to the ongoing discourse on employing blockchain technology to address the challenges posed by viral outbreaks. By exploring the integration of blockchain, decentralized storage, digital identity, and encryption, we seek to provide a solution that can enhance the management of health data certification processes.

C. Objectives and Primary Contributions

In this research, we aim to exploit the potential of blockchain technology to develop DPoH that serve as comprehensive records of individuals' vaccination and immunity certifications. The primary objective of this research is 'to leverage DPoHs as a decentralized and secure (block-chain based) approach to store, manage and transmit health-critical data using a decentralized identity management system'. Users are granted controlled access to their respective DPoH, ensuring data security, transparency, and user autonomy. The DPoH, which encompasses information regarding immunity and immunization status, are securely stored and managed through blockchain technology. This decentralized approach not only enhances data security but also ensures that individuals can validate and upload their immunity and vaccination records to decentralized storage platforms. By employing a blockchain-based solution, the solution empowers users' autonomy, giving them control over their health information along with the reliability and transparency of the certification process. The primary contributions of this research include:

- **Blockchain-based decentralized architecture:** Our research centers on the development of a blockchain-based decentralized architecture, specifically designed to create, manage, and secure critical health data, including vaccination records. This architecture is instrumental in the form of Digital Passports of Health

(DPoH), introducing a groundbreaking approach to the management of sensitive health information.

- **Security of DPoH via algorithmic solutions:** Ensuring the security and integrity of DPoH is paramount. To achieve this, our approach incorporates algorithmic solutions that provide a multifaceted security framework. These algorithms not only automate key security processes but also offer the flexibility of parameterized customization, tailoring security measures to the unique needs of the healthcare environment. Central to this security infrastructure are cutting-edge encryption techniques, enhanced via the robust and decentralized storage capabilities of InterPlanetary File System (IPFS for short). This combination ensures the protection of medical and identification data, mitigating the risks of data breaches and ensuring the utmost privacy.
- **Experimental validation and analysis:** To validate the applicability and reliability of our solution, we conducted several trail-based experiments. These experiments were conducted on a prototype deployed on the Ethereum test network, providing a controlled environment for thorough testing. Our performance evaluation encompassed critical aspects of system functionality, including gas consumption, data storage efficiency, and data access performance. Through these evaluations, we were able to affirm the system's readiness for real-world deployment and its capacity to meet the evolving demands of healthcare data management. This empirical validation serves as a testament to the practicality and dependability of our proposed solution, underpinning its potential to address critical healthcare challenges.

1) *Paper organization:* Section II discusses the related research. Section III details the research method and context. Section IV provides an architectural representation of the solution. Section V details algorithmic implementations. Section VI provides details on solution validations. Section VII presents the conclusion and envisions future research.

II. RELATED WORK

We now overview the most relevant existing research that can be broadly classified into two dimensions, namely, (a) managing digital certificates of immunization [Section VI(A)] and (b) documenting digital management of healthcare documents [(Section VI(B))]. Table 1 provides a comparative summary of the most relevant existing research.

A. Managing Digital Certificates of Immunization

Bansal et al. [16] presented a groundbreaking approach to the creation of immunity certificates utilizing blockchain technology, providing a viable resolution to the problems caused by the COVID-19 epidemic [3]. In their research, they identified the importance of blockchain's immutability in order to counteract the spread of misleading information and inaccurate claims. Additionally, their suggested method included the crucial elements of data confidentiality and test-taker privacy. However, a notable limitation of their research was the lack of a detailed design blueprint and a method for efficiently achieving the desired outcomes [5]. There is

a lack of consensus in the scientific and academic community on the effectiveness of blockchain systems in the context of healthcare technologies. In contrast, this study aims to consolidate the concept of blockchained healthcare systems based on published research that could conclusively confirm or indicate during the crucial period from April to July 2020. There was a noticeable absence of published studies that could definitively document or demonstrate immunity from secondary SARS-CoV-2 infections [15], [16].

Since the introduction of intelligence - machine learning (ML) and artificial intelligence (AI) - the healthcare industry has undergone a significant transition (ML). These technologies, especially in the area of medical imaging, have shown to be extremely useful for diagnosing diseases. Healthcare practitioners can make precise diagnoses by using AI-driven algorithms that can evaluate complex medical pictures, such as CT scans and X-rays. Their role has been especially noteworthy in the early identification of illnesses like COVID-19 [17]. Moreover, predictive analytics uses machine learning models to help medical professionals anticipate illness outbreaks. During pandemics, this predictive capacity is crucial because it allows resources to be allocated effectively to stop the spread of infections [18].






B. Digital Healthcare Documentation

Some recent studies have shown promising findings about mounting proof that clinical immunity exists and protects against SARS-CoV-2 re-infection(s) [8].

Though the exact length of this immunity is still being actively researched, recent research can be seen as a step forward in the fight against the epidemic [12]. A flexible framework in to manage this uncertainty, which can be modified in response to notifications and changes about immunity certificates and the parameters that go along with them [13]. Data security is one of the most important considerations in the creation of immunity certificate systems. A centralized database, while convenient, poses a significant risk of security breaches that could lead to the compromise of sensitive personal information [10]. An illustrative example of such a breach is the Equifax data hack, which impacted approximately 140 million individuals, highlighting the vulnerability of centralized data repositories to malicious actors. Hence, our proposed solution places a strong emphasis on data security and employs decentralized blockchain technology to minimize such risks and ensure the protection of individuals' health information [15].

Telehealth solutions have witnessed a surge in adoption, especially in the wake of the COVID-19 pandemic. These innovative technologies facilitate remote access to healthcare services, providing patients with the means to consult with healthcare professionals from the comfort and safety of their homes. Beyond the convenience it offers, telehealth solutions play a critical role in mitigating the risk of disease transmission, ensuring both patient and healthcare provider safety. Moreover, these solutions enhance patient care and monitoring, revolutionizing the healthcare landscape [19]. Genomic sequencing technologies have ushered in a new era of understanding disease pathogens at the genetic level. These tools are instrumental in unraveling the genetic makeup of various disease-causing agents. Notably, genome sequencing has been

TABLE 1. OVERVIEW OF CENTRALIZED VS DECENTRALIZED (BLOCKCHAIN-BASED) DIGITAL IDENTITY MANAGEMENT

Feature	Central Identity Management (relevant existing research)	Blockchain based Distributed Identity Management (feature of the proposed solution)
Governance Mechanism [5, 15] 	Central Governance	Decentral Governance
Identity Change [8, 10, 12] 	Change Management on Central Server	Change Management with Individual Consent
Key Management [23] 	Reset the password to recover lost identity/key	Digital assets is vanished if key is lost.
Storage [19, 24] 	Server is Central	Distributed Nodes.
Freedom [25] 	Risk of stolen Identity	User to reclaim stolen/lost Identities

essential in tracing the virus's mutations and variations in the instance of COVID-19. Understanding the behavior of the disease and developing a vaccine depend heavily on this information [20].

C. Conclusive Summary and Comparison of the Solution

The combination of Internet of Things (IoT) devices and wearable health technologies has made it possible to continuously and in real-time monitor symptoms and vital signs. These pervasive tools and technologies are now essential instruments for monitoring and treating a variety of illnesses, from COVID-19 to long-term ailments. By offering insightful information on their well-being, they enable people to take control of their health [21]. The emergence of digital vaccination passports represents a significant development in the post-COVID-19 world. These digital credentials serve as a means of verifying individuals' vaccination status, granting them access to travel and public spaces safely. They have rapidly become an essential component of health records, ensuring safe mobility and access [22]. These technological advancements collectively illustrate the dynamic and evolving landscape of healthcare, where innovation plays a pivotal role in enhancing disease diagnosis, prevention, and management. The integration of AI, telehealth, genomics, wearables, and digital credentials has redefined healthcare practices and empowered individuals to take control of their well-being.

In the dominion of healthcare, advanced data analytics techniques have emerged as a transformative force, facilitating real-time tracking of disease spread, efficient resource allocation, and the evaluation of treatment outcomes. Particularly in the context of pandemics, these insights become paramount for informed decision-making [23].

Simultaneously, the integration of robotics in healthcare settings has revolutionized healthcare service delivery. Robots are adeptly deployed for a spectrum of critical tasks, including disinfecting healthcare facilities, ensuring the secure and timely delivery of medications, and providing essential patient care, thereby significantly reducing the risk of disease transmission and bolstering the overall safety of healthcare

environments [24]. Furthermore, the deployment of computational models and simulations is indispensable in predicting the trajectory of disease spread and assessing the impact of diverse interventions. These tools play a vital role in shaping decision-making processes during outbreaks, allowing healthcare authorities to explore multiple scenarios, optimize resource allocation, and devise effective strategies for disease control and patient care, thus playing a pivotal role in mitigating the effects of pandemics [25].

Blockchain technology provides a decentralized, immutable platform to preserve sensitive medical data, acting as a strong defense for the confidentiality and privacy of patient health records. Its promise goes beyond data security; it can improve contact tracing effectiveness, which is an important component in infectious disease management and control. Blockchain expedites the procedure by offering a visible and tamper-proof ledger, guaranteeing patient data security and aiding in the prompt and precise tracing of illnesses and infections [26].

III. RESEARCH METHOD AND CONTEXT

In this section, we offer a comprehensive overview of our research methodology [Section II(1)] and contextually define and elaborate on the core concepts [Section II(2)] that serve as the foundational pillars of our research. The research methodology overview outlines the strategic framework guiding our study as a step-by-step approach to design, conduct, and validate the research process as per the illustrations in Fig. 2. To contextualise the research, we explore the key concepts, terminologies, and tool support the successful realization of our research, focusing on the tools and frameworks strategically chosen to streamline the tasks undertaken by software and system engineers, ultimately enhancing efficiency, accuracy, and overall feasibility throughout our research endeavor. This collective insight into the methodological, conceptual, and technological dimensions of our study ensures a comprehensive understanding of the proposed research and its methodology.

A. Research Method

An illustrative view of the overall research method is provided in Fig. 2 that shows a phase-wise decomposition of the overall method to conduct this research, as detailed below. To attain the research objectives, we employed both the quantitative and qualitative methods to conduct this research. Quantitative methods were used for data collection and analysis, enabling us to gather insights related to our study (Phase I, Fig. 2). Qualitative methods, on the other hand, facilitated the exploration of design and empirical evaluations (Phase II-III, Fig. 2).

Phase I – This initial phase serves as the bedrock of our research, where we delve into the existing body of knowledge to understand tstate-of-the-art in the field. With a rigorous analysis of relevant literature, we draw comparative analyses between the established solutions and our innovative proposal. The insights gained from this step inform and guide the subsequent phases of our research. A dedicated Section VI is exclusively devoted to offering an extensive discussion of the literature review, shedding light on the insights and findings gathered during this crucial step.

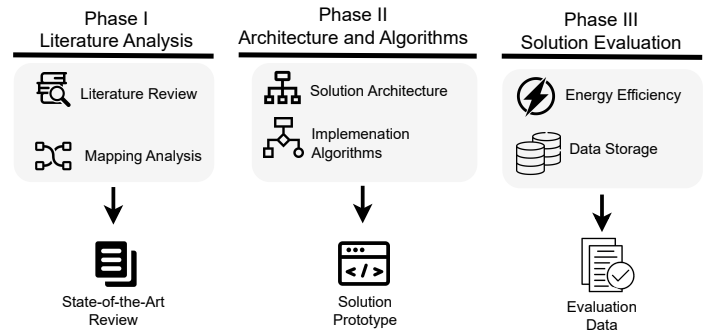


Fig. 2. Overview of the steps in research method.

Phase II – Building upon the insights garnered from the literature review, this phase involves the creation of a detailed blueprint for our proposed solution. It encompasses the architectural design that outlines the structural framework of our system, presented in Section III. modularized algorithms are meticulously crafted to operationalize our solution, with an intricate portrayal of these implementations provided in Section IV. This step is where our innovative approach takes shape, combining both conceptual and practical elements to lay the foundation for the solution.

Phase III – The final phase of our research methodology is dedicated to the rigorous evaluation of our proposed solution. Here, we seek to validate the efficiency and suitability of our approach in real-world scenarios. Section IV presents a comprehensive account of the solution evaluation, highlighting the empirical findings and results obtained during this pivotal step. A systematic testing and analysis evaluates the performance and effectiveness of proposed solution for its applicability and viability.

B. Context: Algorithms, Tools, Blockchain Technologies

The context of the research presented here mainly focuses on key concepts and terminologies underpinning blockchain-based algorithms along with tools and technologies that are fundamental to architect, implement, and validate the proposed solution. Both of these are elaborated below with a dedicated discussion of the algorithms in Section IV and technologies elaborated in Section V.

1) *Algorithms*: Our research heavily relied on several core algorithms tailored to specific aspects of our solution. These algorithms encompassed data encryption and decryption techniques to ensure the security of medical records and personal information within the blockchain-based DPoH. Additionally, algorithms were developed for efficient data retrieval and validation processes, optimizing the functionality and performance of the DPoHs, as overviewed in Fig. 3.

2) *Tools and blockchain technologies*: The successful implementation of our proposed solution requires the utilization of blockchain related technologies including:

- **Blockchain-based DPoH**: At the heart of our system, blockchain technology was used to create the immutable and transparent ledger for storing DPoH data. Ethereum, a popular blockchain platform, served as

the foundation for smart contracts and DPoH management.

- **Inter-Planetary File System (IPFS):** In order to ensure a safe and secure storage of medical records, IPFS was selected as the decentralized storage mechanism. The content-addressable structure and distributed architecture can guarantee the availability and integrity of the data that is stored.
- **Smart Contracts:** The issuance, verification, and management of DPoH can be automated by utilizing Ethereum's smart contract capabilities. In the certification process, these self-executing contracts can guarantee dependability and confidence.
- **Encryption Mechanisms:** To safeguard sensitive information, advanced encryption mechanisms such as AES (Advanced Encryption Standard) were employed for data at rest and during transmission. These mechanisms ensured the security and integrity of stored data within the DPoH.
- **Programming Frameworks:** Development and testing of the system were carried out using programming frameworks like Solidity for smart contract development, NodeJS for algorithm implementation, and Truffle for Ethereum contract testing.

By implementing these technologies, we aimed to simplify the implementation process for software and system engineers while ensuring that the DPoH system meets the highest standards of security, reliability, and functionality. In subsequent sections, we will elaborate on the architecture, algorithmic implementations, and evaluation of the proposed solution.

IV. ARCHITECTURAL VIEW OF THE PROPOSED SOLUTION

In the software and systems engineering context, architecture of the software-driven systems, services, and applications provide a blue-print to sketch the overall solution for the implementation [16]. The architecture-centric view, as a blue-print of the solution is illustrated in Fig. 3 that illustrates the overall design of the proposed solution. As per the architectural view in Fig. 3, the proposed system leverages Ethereum smart contracts, ensuring the immutability of records and trustworthy event management. Fig. 3 illustrates how our system segregates the handling of test reports and DPoH while maintaining data security and integrity. Test reports are promptly anchored in the blockchain, while DPoH data is securely stored on IPFS and linked to the blockchain, ensuring a comprehensive and reliable health data management process. Fig. 3 demonstrated a step-wise process for archiving DPoH and results of the medical test within system.

- **Submission of Test Report:** The process begins when a test report, which could be any medical document such as the blood test report or report of the lipid test, is generated by a lab assistant. To ensure the authenticity and immutability of this report, it is instantly deposited into the blockchain execution of smart contract.
- **DPoH Storage on IPFS:** Simultaneously, the DPoH, which represents an individual's health and vaccination status, is stored on the (IPFS). This decentral-

ized storage solution provides a secure and accessible repository within health centers section.

- **DPoH Uploading to IPFS:** Health facilities responsible for generating and maintaining DPoH data initiate the DPoH uploading process. During this phase, accessible DPoH data is uploaded to IPFS and a unique hash key is created as a result. This hash key serves as a reference point for the stored DPoH.
- **Incorporating Data in Blockchain:** The data recorded in the blockchain consists of two distinct components: the test report and the DPoH. Each component is handled separately within the system. The test report is directly integrated into the blockchain to ensure its immutability and transparency. In contrast, the DPoH, which is securely stored on IPFS, is linked with other essential details and then recorded within the blockchain. This mapping process ensures that the DPoH data is associated with the necessary context and can be readily accessed when needed.

In the realm of blockchain development and decentralized applications, several essential tools and technologies play a crucial role. Visual Studio Code, an open-source IDE, serves as a versatile platform to develop, test, and deploy smart contracts and blockchain applications. Ganache, a development blockchain emulator, enables blockchain developers to deploy a local Ethereum network to test and debug their decentralized solutions. Metamask, a browser extension, simplifies Ethereum-based application interaction with a user-friendly wallet and identity management system. Lastly, IPFS (Inter-Planetary File System) offers decentralized and secure storage, including medical records and DPoH, in a distributed, tamper-resistant manner.

V. ALGORITHMIC IMPLEMENTATION OF THE SOLUTION

After presenting the architecture, we now discuss the two algorithms that (i) generate the DPoH [Section IV(A)] and (ii) creating a web layer [Section V(A)] for secure and efficient transmission of the DPoH.

A. Algorithm 1: Digital Passport of Health

This algorithm is the essence of this process lies in the secure and immutable storage of medical data, including critical elements like blood test reports. This is achieved through the deployment of smart contract as a mapping mechanism designed to accommodate specific attributes.

Algorithm 1 Digital Health Passport

```
1: Input:  $\cup, \rho, \gamma$ 
2: Output:  $\mathcal{R}$ 
3: procedure DPoH
4:   if User( $\rho$ ) then
5:      $FS \leftarrow \text{File}(\gamma)$ 
6:      $FB \leftarrow \text{Buffer.form}(FS)$ 
7:      $ENCRYPTED \leftarrow \text{AES}(KEY, FB)$ 
8:      $FH \leftarrow IPFS.ADD(ENCRYPTED)$ 
9:      $\mathcal{R} \leftarrow ADD(\cup, \rho, FH)$ 
10:   end if
11: end procedure
```

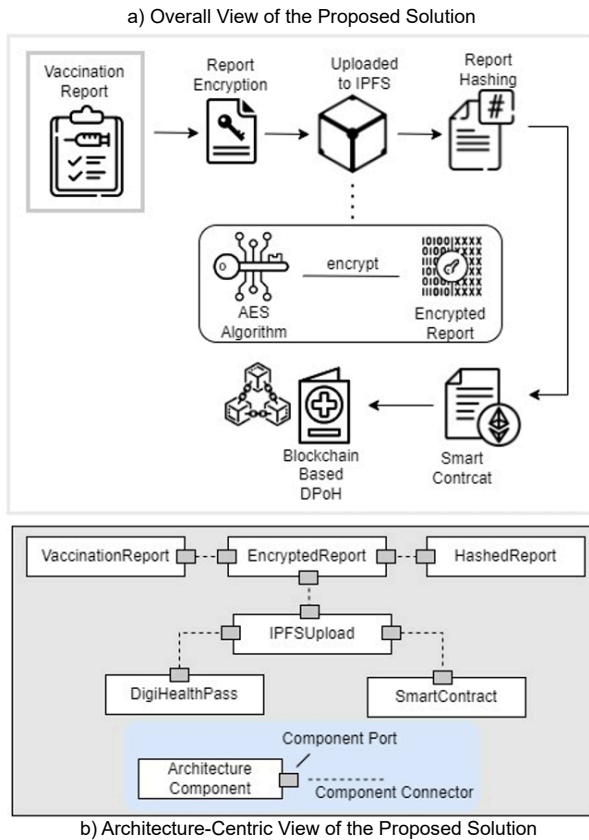


Fig. 3. Solution view (a) Overall view. (b) Architecture view.

1) *Input(s)*: Among the crucial parameters woven into this blockchain are the User ID of the patient, the Digital Passport ID and the Hash of the digital certificate (Line 1).

2) *Processing*: The processing includes mapping the input parameters to their corresponding identities that include the user id and user appointment id (Line 3 - 4). The mapping allows the addition of medical data reports to the blockchain ledger. In order to maintain the data integrity in the blockchain's secure vault, an additional layer of security is added, specifically to connect the identities that include user id and user appointment id in an encrypted way (Line 5 - 7). After mapping the ids, patient IDs and the DPoH sequence numbers are mapped and stored in a smart contract for its persistence in the blockchain (Line 8 - 10).

3) *Output(s)*: These security layers act as the foundation for anonymously and securely maintaining the record in the blockchain ledger, preserving the confidentiality and availability of medical data for both patients and stakeholders (Line 2).

B. Algorithm 2: Web Layer

This algorithm is fundamental for confirming and demonstrating data access in a blockchain, detailed below.

1) *Input(s)*: This algorithm provides a central mechanism to extract the records from blockchain and enable public access via a secure key (Line 1).

Algorithm 2 Web Layer

```

1: Input:  $\rho, \gamma$ 
2: Output:  $\mathcal{R}$ 
3: procedure ACCESSDPOH
4:   if  $\rho == \mathcal{EXIST}$  then
5:      $\mathcal{FH} \leftarrow \text{HealthCertificate}(\rho)$ 
6:      $\mathcal{ENCRYPTED} \leftarrow \text{IPFS}(\mathcal{FH})$ 
7:      $\mathcal{DECRYPTED} \leftarrow \text{AES}(\mathcal{ENCRYPTED})$ 
8:      $\mathcal{R} \leftarrow \text{DOWNLOAD}(\mathcal{DECRYPTED})$ 
9:   end if
10:  UpdateDashboard( $\mathcal{R}$ )
11: end procedure

```

2) *Processing*: Users have the ability to retrieve data from blockchains according to their predefined user preferences and settings, offering customisation and human-decision support (Line 3 - 4). To give a customized approach to data access, users can extract data, for example, by mapping their DPoH number to their patient ID (Line 5 - 7). Furthermore, stakeholders have the option to acquire a copy of the Digital Passport of Health (DPoH) certificate by providing the identity number of the user (Line 8 -10).

3) *Output(s)*: The output produces mapped data that is accessible by the stakeholders, improving data accessibility and transparency within the blockchain-based DPoH system (Line 2).

VI. RESULTS AND EVALUATIONS

The evaluation section presents the outcomes stemming from the implementation of our proposed approach.

A. Evaluation Environment

Our evaluation covered both hardware and software aspects. Hardware-wise, we employed a Windows Platform (core i7, 16 GB RAM) for radiologist to submit the lab test results and medical images to IPFS. On the software side, we automated testing with NodeJS and ReactJS in Visual Studio Code, utilizing libraries such as React, web3, and ipfs.http. A JavaScript performance script monitored CPU usage during tasks like uploading images to IPFS and blockchain storage. For local Ethereum simulation, we used the Ganache suite, integrating the Metamask extension for browser-based interactions. Fuel consumption, measured in Gwei (Ether's smallest unit), was assessed for smart contract execution, compared to planned data uploads. Our approach's cost analysis, detailed in Table 2, included gas and Ether cost.

- Evaluation of the smart contract functionality, emphasizing gas consumption as a critical metric (Fig. 4).
- Quantify the efficiency and effectiveness of data uploading and storage processes within the blockchain, shedding light on the system's capacity for handling these crucial operations (Fig. 5).
- Evaluation extends to query response time, which reflect the system's overall performance (Fig. 6). Throughout these assessments, we maintain a keen focus on algorithmic execution, ensuring that our approach operates with optimum efficiency.

TABLE 2. ENERGY AND EXECUTION ANALYSIS OF SMART CONTRACTS

Execution Classification	Energy (Gas Consumption)	Execution (Ether Cost)
Creation (DPoH)	556046	0.01112092
Migration (DPoH)	22695	0.0065473
Creation Cost	246574	0.0446789
Migration Cost	45378	0.0078965
Cumulative Data		0.06849198

B. Evaluation Energy (Gas Consumption) and Data Retrieval Efficiency

In Fig. 4, the item under evaluation focused on assessing the time required by the system users to upload and persist the data onto both IPFS and the blockchain ledger. As illustrated in Fig. 4, which showcases the outcomes of tests conducted with typical data sizes, interesting patterns emerge. Notably, when uploading data exceeding 1150 bytes in size, the average fuel consumption registers at approximately 1,194,052 Gas. Conversely, for data storage of approximately 300 bytes, the average fuel consumption hovers around 157,683 Gas. In Fig. 4, once the lab test results are ready for retrieval, the execution of the "AddDigitalHealthPassport" function is initiated. This pivotal event incorporates essential information, including the Ethereum addresses of the test and smart contract, the timestamp of the event publication, and the IPFS hash encapsulating the test results. The logs and event details are thoughtfully illustrated in the diagram provided. The Digital Passport of Health (DPoH) certificate is seamlessly uploaded to IPFS storage, which in turn generates a unique hash that becomes an integral part of the blockchain ledger, harmonizing with other patient information. Empowering patients with the ability to access their DPoH from any location, this system operates efficiently through the utilization of their passport number. Moreover, the patient's data can be instantaneously verified by other interconnected nations, further enhancing the DPoH's utility and global applicability.

Effective data management is a crucial component of our system, as seen in Fig. 5, where test reports and certificates are stored in IPFS and records are kept in the blockchain. One important parameter to assess the efficacy of data storage and retrieval is query response time. We ran two tests: one to see how quickly test reports, health certificates, and DPoH certificates could be stored, and another to see how quickly files with hashes could be added to the blockchain. The query response times are plotted in milliseconds on the vertical axis of Fig. 5.

The "Complete function" takes care of the entire procedure, from hashing medical data files to recording test results and certificates on IPFS and storing record data in the blockchain. Besides, the "Smart Contract Function" shows the time lag that Metamask's Smart Contract execution call.

C. Evaluating the Execution Efficiency (CPU Utilization)

Fig. 6 offers a comprehensive view of the execution times associated with data access within our system. There are two different parts for this data access, each with their own special features. The first category includes test report and

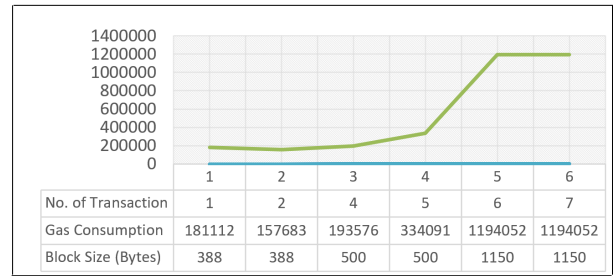


Fig. 4. Gas usage vs. block size and transactions.

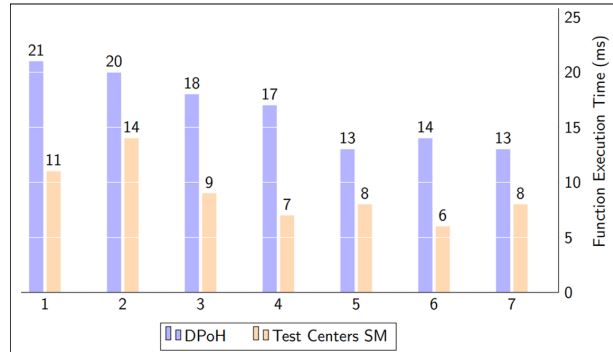


Fig. 5. Data storage time in IPFS and blockchain.

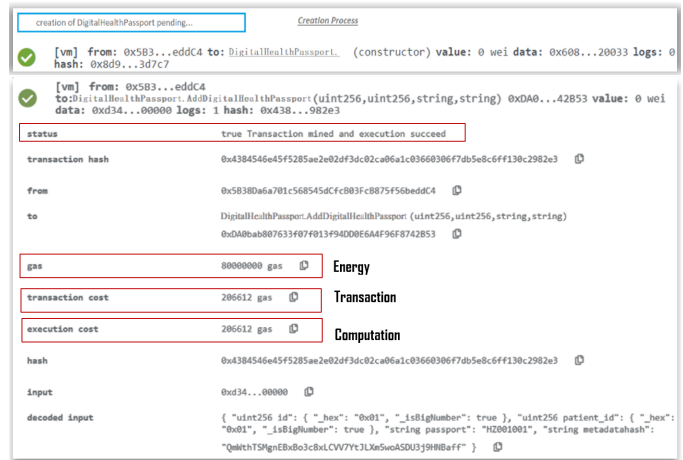


Fig. 6. Uploading DPoH report/certificate to blockchain.

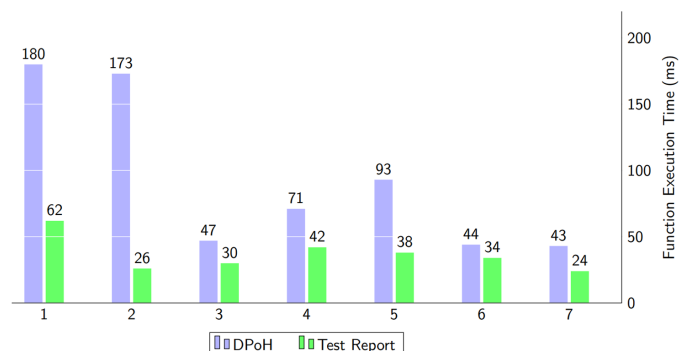


Fig. 7. Data access time via IPFS and blockchain.

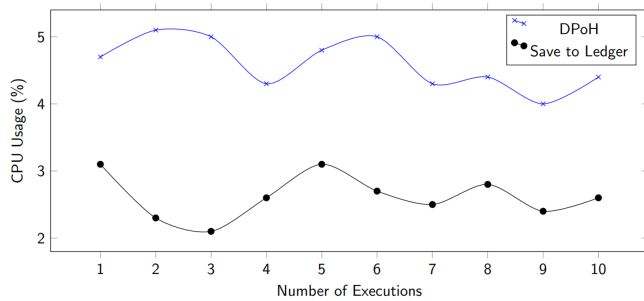


Fig. 8. CPU utilization (DPoH vs save to ledger).

health certificate retrieval from the Inter-Planetary File System (IPFS), made possible by the file hashes associated with them. This subsection focuses on access and execution performance of smart contract-based DPoH. The function execution time, i.e., access to the DPoH and medical test reports are illustrated in Fig. 7. A thorough depiction of CPU use when smart contract functions are being executed can be found in Fig. 8.

These features cover a variety of fundamental tasks, including data encryption, IPFS storage, and blockchain ledger recording. The execution of these tasks occurs within a single cycle, allowing for the precise measurement of CPU usage. One noteworthy observation is that the decryption technique is notably light on CPU resources. This figure not only presents the consumption of CPU resources but also sheds light on the efficiency and resource management within the system. The ability to execute these functions within a single cycle not only optimizes performance but also contributes to the overall effectiveness of the proposed solution. The minimal CPU usage during decryption highlights the efficiency and resource-conscious nature of this particular operation. Such insights are invaluable in assessing the performance and resource allocation within the system, underscoring the meticulous design and thoughtful execution of these functions.

VII. CONCLUSIONS AND FUTURE WORK

This article introduces a decentralized system architecture for the storage and distribution of DPoH certificates based on Ethereum and IPFS. The system's development, implementation, and testing for DPoHs and immunity certificates are discussed, emphasizing their role in preventing infectious diseases. Smart contracts detailed in the article leverage on-chain storage and on-chain events. The system employs self-sovereign identification, re-encryption, and relevant information to ensure accuracy and timeliness. Cost analysis evaluates algorithmic efficiency and practicality.

Future Research involves enhancing the decentralized solution with role customization for secure IPFS data access via re-encryption techniques. Patients can request certificate downloads through a secure channel, employing RSA-based keys for data decryption, thereby enhancing data provenance, efficiency, and audit effectiveness, all achieved without the need for third-party intermediaries or administrative entities. Moreover, more empirical data and case studies is required to provide a rigorous validation of the proposed solution. We also aim to extend to the solution and validate its applicability in the context of health management information systems.

REFERENCES

- [1] M.CHAMOLA, V. HASSIJA, V. GUPTA, AND M. GUIZANI, *A comprehensive review of the COVID-19 pandemic and the role of IoT, drones, AI, blockchain, and 5G in managing its impact*, IEEE Access, vol. 8, pp. 90225-90265, 2020.
- [2] ALJEDAANI, BAKHEET, ET AL. *An empirical study on secure usage of mobile health apps: The attack simulation approach.*, Information and Software Technology 163 (2023): 107285.
- [3] BLOCKCHAIN: OPPORTUNITIES FOR HEALTH CARE. AVAILABLE ONLINE: [HTTPS://WWW2.DELOITTE.COM/US/EN/PAGES/PUBLIC-SECTOR/ARTICLES/BLOCKCHAIN-OPPORTUNITIES-FOR-HEALTH-CARE.HTML](https://www2.deloitte.com/us/en/pages/public-sector/articles/blockchain-opportunities-for-health-care.html), (accessed on 29 May 2021).
- [4] OPEN DATA PLATFORM TO SUPPORT COVID-19 RESPONSE. AVAILABLE ONLINE: [HTTPS://WWW.IBM.COM/BLOGS/BLOCKCHAIN/2020/03/MIPASA-PROJECT-AND-IBM-BLOCKCHAIN-TEAM-ON-OPEN-DATA-PLATFORM-TO-SUPPORT-COVID-19-RESPONSE/](https://www.ibm.com/blogs/blockchain/2020/03/mipasa-project-and-ibm-blockchain-team-on-open-data-platform-to-support-covid-19-response/),(accessed on 29 May 2021).
- [5] M. C. CHANG AND D. PARK, *How can blockchain help people in the event of pandemics such as the COVID-19?*, J. Med. Syst., vol. 44, no. 5, pp. 1-2, May 2020.
- [6] K. M. KHAN, J. ARSHAD, AND M. M. KHAN, *Simulation of transaction malleability attack for blockchain-based e-voting*, Comput. Electr. Eng., vol. 83, May 2020, Art. no. 106583.
- [7] RAZZAQ, ABDUL, ET AL. *IoT Data Sharing Platform in Web 3.0 Using Blockchain Technology.*, Electronics 12.5 (2023): 1233.
- [8] M. EISENSTADT, M. RAMACHANDRAN, N. CHOWDHURY, A. THIRD AND J. DOMINGUE, *COVID-19 Antibody Test/Vaccination Certification: There's an App for That*, IEEE open journal of engineering and biology, 2020
- [9] D. RESIERE, AND H. KALLEL, *Implementation of medical and scientific cooperation in the caribbean using blockchain technology in coronavirus (COVID-19) pandemics*, J. Med. Syst., vol. 44, no. 7, pp. 1-2, Jul. 2020.
- [10] IMMUNITY PASSPORTS' IN THE CONTEXT OF COVID-19. Accessed: Jan 2021. [Online]. Available: <https://www.who.int/news-room/commentaries/detail/immunity-passports-in-the-context-of-covid-19>
- [11] RAZZAQ, ABDUL, AAKASH AHMAD, ASAD WAQAR MALIK, MAHDI FAHMIDEH, AND RABIE A. RAMADAN. *Software engineering for internet of underwater things to analyze oceanic data*. Internet of Things 24 (2023): 100893.
- [12] FAHMIDEH, MAHDI, ET AL. *Engineering Blockchain-based Software Systems: Foundations, Survey, and Future Directions*. ACM Computing Surveys 55.6 (2022): 1-44.
- [13] RAZZAQ, A.; MOHSAN, S.A.H.; GHAYYUR, S.A.K.; AL-KAHTANI, N.; ALKAHTANI, H.K.; MOSTAFA, S.M. *Blockchain in Healthcare: A Decentralized Platform for Digital Health Passport of COVID-19 Based on Vaccination and Immunity Certificates*. Healthcare 2022, 10, 2453. <https://doi.org/10.3390/healthcare10122453>
- [14] ALJALLOUD A, RAZZAQ A. *Modernizing the Legacy Healthcare System to Decentralize Platform Using Blockchain Technology*. Technologies. 2023; 11(4):84. <https://doi.org/10.3390/technologies11040084>
- [15] RAZZAQ, A. (2023) *A Web3 secure platform for assessments and educational resources based on Blockchain*, Computer Applications in Engineering Education, 2023. doi:10.1002/cae.22677.
- [16] AHMAD, A., WASEEM, M., LIANG, P., FAHMIDEH, M., AKTAR, M. S., MIKKONEN, T. (2023, JUNE). *Towards human-bot collaborative software architecting with chatgpt*. In Proceedings of the 27th International Conference on Evaluation and Assessment in Software Engineering.
- [17] WYNANTS, L., ET AL. *Prediction models for diagnosis and prognosis of covid-19: systematic review and critical appraisal*. The BMJ, 369, m1328. 2020
- [18] SUN, S., ET AL. (2020). *A machine learning-based model for survival prediction in patients with severe COVID-19 infection*. Frontiers in Cellular and Infection Microbiology, 10, 299.

- [19] SMITH, A. C., ET AL., *Telehealth for global emergencies: Implications for coronavirus disease 2019 (COVID-19)*. Journal of Telemedicine and Telecare, 1357633X20916567.
- [20] HADFIELD, J., ET AL.(2018), *Nextstrain: real-time tracking of pathogen evolution*. Bioinformatics, 34(23), 4121-4123.
- [21] MENA, L. J., ET AL. (2020). *A systematic review of wearable devices for health-related outcomes used in randomized controlled trials*. Journal of Telemedicine and Telecare, 1357633X20926952.
- [22] KOFLER, N., BAYLIS, F.,*Ten reasons why immunity passports are a bad idea*. Nature, 591(7849), 202-205. 2021
- [23] DAVENPORT, D., ET AL. (2020). *COVID-19 planning and response tools: Resources and promising practices for healthcare decision makers*. Applied Clinical Informatics, 11(04), 623-633.
- [24] SHAH, S. G. S., ET AL. (2020). *Use of robotic technology in the COVID-19 pandemic response*. Journal of Medical Systems, 44(8), 140.
- [25] LIPPI, G., MATTIUZZI, C., *Modeling the risk of SARS-CoV-2 transmission in hares for diagnostic purposes*. Journal of Medical Virology, 92(9), 1861-1862. 2020.
- [26] MENSE, A. (2021). *An exploratory analysis of blockchain-based solutions for health information management: Conceptual framework*. JMIR Medical Informatics, 9(7), e25563.