THE ASIAN BULLETIN OF BIG DATA MANAGMENT
Vol. 3. Issue 1 (2023)
https://doi.org/10.62019/abbdm.v3i1.43

ASIAN BULLETIN OF BIG DATA MANAGEMENT
ISSN (Print): 2959-0795
http://abbdm.com/
ISSN (online): 2959-0809

Blockchain-Based Fintech Architecture for Enhanced Interoperability in Health Insurance

Zia Ahmed Shaikh*, Khalil-Ur-Rahmen Khoumbati, Shahzad Ahmed Memon, Lachhman Das Dhomeja, Kamran Dahri

Chronicle

Article history
Received: October 17, 2023
Received in the revised format: Sept 05, 2023
Accepted: Sept 6, 2023
Available online: Sept 11, 2023

Zia Ahmed Shaikh is currently affiliated with Dr. A. H. S. Bukhari Postgradute Centre of Information and Communication Technology, University of Sindh, Jamshoro, Pakistan.
Email: zia.shaikh@scholars.usindh.edu.pk

Khalil-Ur-Rahmen Khoumbati, Lachhman Das Dhomeja & Kamran Dahri are currently affiliated with Department of Information Technology, University of Sindh, Jamshoro, Pakistan.
Email: khalil.khoumbati@usindh.edu.pk
Email: lachhman@usindh.edu.pk
Email: kamran.dahri@usindh.edu.pk

Shahzad Ahmed Memon is currently affiliated with Department of Electronic Engineering, University of Sindh, Jamshoro, Pakistan.
Email: shahzad.memon@usindh.edu.pk

***Corresponding Author**

Abstract

Health Insurances play vital role in one's life to bear costly medical services and delays in payments from insurer to service providers causes chaotic to insureds seeking immediate treatment for their diseases. Almost every stakeholder in this ecosystem is equipped with his own significantly efficient independent information systems usually known as Management Information Systems (MIS) which most of the times remain sufficient for their internal business needs but apart from so much technical advancements, the inter-communication of these stakeholders for up-to-date status of insurer, insured, and health service provider is still missing in various scenarios which causes distress to all stakeholders and patients. In this paper, we have proposed a Blockchain based data sharing solution among all the stakeholders to fast up the processes and smoothness of network along with a concept of Insurance e-Wallet for insured entities where they can have summary of all their purchased Insurance plans, their processed or pending claims, remaining limits, and upcoming changes in their policies from insurance vendors. Apart from interoperability, the second most important aspect this architecture addresses the avoiding of redundant paper work that every stakeholder manages to maintain their day-to-day activity records, these are almost the same set of documents regarding an insurance claim that a service provider, insurer, and a patient maintains. To avoid this redundancy, we made use of IPFS as the decentralized repository for such documents which makes Blockchain solution cost effective and light weight as just the reference or the hash ID is put in Blockchain instead of whole document in binary format. A prototype is developed based on suggested architecture and two experiments are performed on implemented prototype, first one for measuring expected growth rate of Blockchain based on routine appendment of data and second for measuring document access time required to access files from IPFS server. Lastly the paper concludes with some prominent implementation challenges that stakeholders may face during Blockchain 's implementation to achieve transformation in this industry.

Keywords: Health Insurance; Blockchain; Smart Contract; Insurance e-Wallet; IPFS

INTRODUCTION

Health Insurance is a financial agreement for payments of health-related costs made between an individual, or group of individuals and an insurance company directly or on behalf of an employer or the government(Kuroki, 2022), and are available in various forms such as coverage for hospitalizations, maternity services, accidents, medical examinations, OPDs and a lot more (Imarc, 2021; Nyman, 1999). In health insurance, three types of stakeholders are involved: Insurer, Insured and Health Care Service Provider (HCSP). Insurance provider or an employer is the one who covers the risk of insured entities; insured is an entity who is covered or whose risk is transferred to insurer; Health Care Service Provider (HCSP) is the entity which provides health care services to insured persons, which may be a hospital, diagnostic lab, a doctor's clinic or any other health service providing institute. Entire health-insurance process revolves among these three entities. As it is commonly observed that companies tend to deliver medical assistance to their employees through health-insurance facilities. Health insurance is premium of upfront payment that insured entity pays on behalf of an insurance policy. This practice enables the employees to stay aligned with the firms for longer durations(Trude, Sally; Christianson, Jon B; Lesser, Cara S; Watts, Carolyn; Benoit, 2002). However, certain hindrances are present under this activity that affect the effectiveness of the insurance policy, for instance, trust issues, lack of transparency and most importantly, absence of the insurer. Subsequently, the payment of insurance amount becomes complex, and the insurer does not receive the expected amount of service. Hence, insurance companies receive negative ratings, and the entire cycle gets disturbed(Gary, 2019).

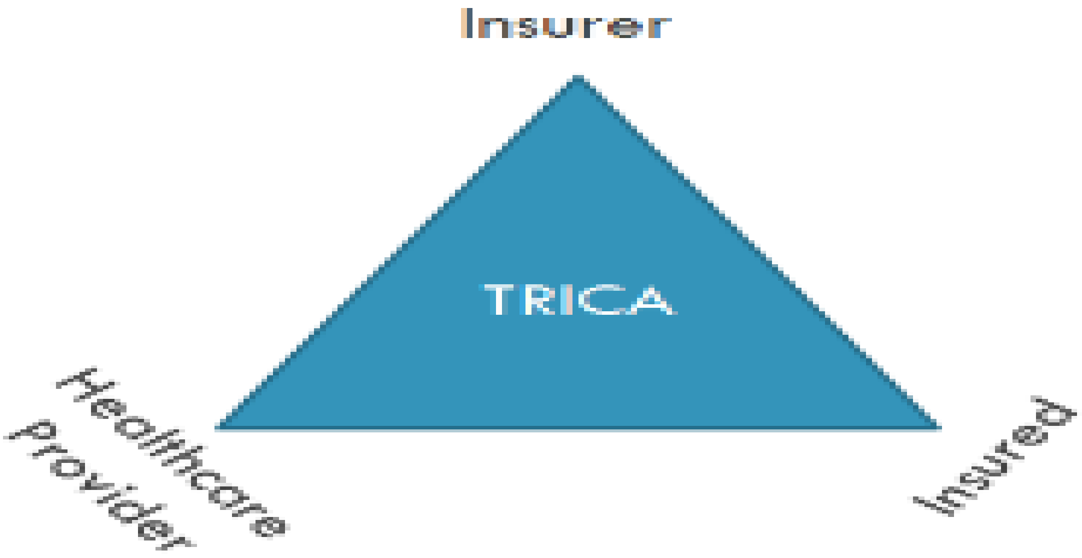


Figure 1.
Stakeholders of Health Insurance System

The rest of the paper is organized as follows. In section 2 we discuss three major issues which can be addressed through proposed technological reforms. Section 3 discusses issues faced by each of stakeholders particularly, insurer, insurance company and health care provider. In section 4, related work is illustrated to determine contemporary situation of the highlighted area and denotes gap that is addressed within this study. Section 5 presents the proposed architecture and provides description of each of architectural components. In section 6, we present implementation and testing. Section 7 demonstrates technical experiments for expected growth rate of Blockchain and expected time to access files through the IPFS network. Finally, we conclude the paper in Section 8.

PROBLEMS IN EXISTING SCENARIOS

Even though both Insurers and HCSPs have adopted various robust Information Systems (IS) (Albert Pang, Misho Markovski, 2020) which are very mature enough in their domains; however interoperability is still a major issue due to which various communicational processes between these stakeholders are operated manually, for example submission of medical bills from HCSPs to insurer, auditing of medical treatment bills from insurer, disbursement of payment from insurer to HCSPs etc. and due to all these delayed manual processes and because payments are delayed to healthcare providers ultimately patients are refused for medical treatments on behalf of insurers. Manual processes, which require extensive human interaction, are also error-prone and fraud chances are extremely high and difficult to investigate, Probable frauds may include billing of non-rendered services, billing for non-covered services, misrepresentation of service dates, misrepresentation of service locations, billing for unauthorized provider of services, waiving of co-payments, incorrect reporting of diagnosis, unbundling of services, over-utilization and false or un-necessary issuance of prescription drugs. Likewise, for Insureds there is no such centralized system from where they can view a summary of all their insurances. Though insureds can view statistics of their insurance policies from respective insurance companies provided online panels. But for different insurance plans purchased from different insurance vendors, the insureds have to sign into separate Online-Panels provided by respective insurance companies, and hence no provision of a single point allowing the insureds to view the statistics of their every insurance plan purchased from different vendors.

The three major problems that this study addresses are here as under.

Identity Management Across Organizations

People interact with various organizations for their needful services. These organization usually allows their users an online panel or a mobile app to interact with their services. It's a common phenomenon that each organization maintains its own database(Sedlmeir et al., 2021) of its users and their associated business data. For such online panels an individual may have one identity across multiple platforms or may want different identities supporting different 'personas' for himself, for his family members, and other associated persons. Due to which an end user has to memorize his or her login credentials for each separate login panel. Though this problem can be solved by using OpenID (Recordon & Reed, 2006) mechanisms but not all vendors are relaying on any third-party identity provider to manage login credentials for their secure data. As a result, the problem of an end user remains there. More complications occurs when a person moves across different organizations to avail different services(*6 Common Identity Challenges That Can Be Addressed In An IAM Strategy*, n.d.; *Top 9 Identity & Access Management Challenges with Your Hybrid IT Environment | Okta*, n.d.), there he creates different identities for every different organization and sometimes due to lack of verification and lose KYC policy a customer can create multiple identities for same organization depicting as different person behind different identity.

N x N Integration Problem

Interoperability (Hodapp & Hanelt, 2022) between heterogeneous systems has been a common issue in all fields and has been focused in research numerous times with different aspects. Health insurance is not an exception. Huge amount of work has already been done in industry and academics to overcome this area of research (Park et al., 2022) but still a lot needs to be done. Interoperability allows transferring information among various stakeholders in the business domain. Even though various organizations expose their APIs for other organizations to connect to their systems technologically. Still in that case N number of APIs need to connect N number of systems. As suppose Organization-A wants to connect to Organization-B a connection is made between A and B, at the same time Organization-A also wants to connect to Organization-C. Another connection is made between A and C. Such number of connections will be made between N number of organizations, which causes trouble for each organization to manage their system and incoming connections to their system. Figure 2 shows true picture of connections being made between heterogeneous systems (ehcos.com, n.d.).

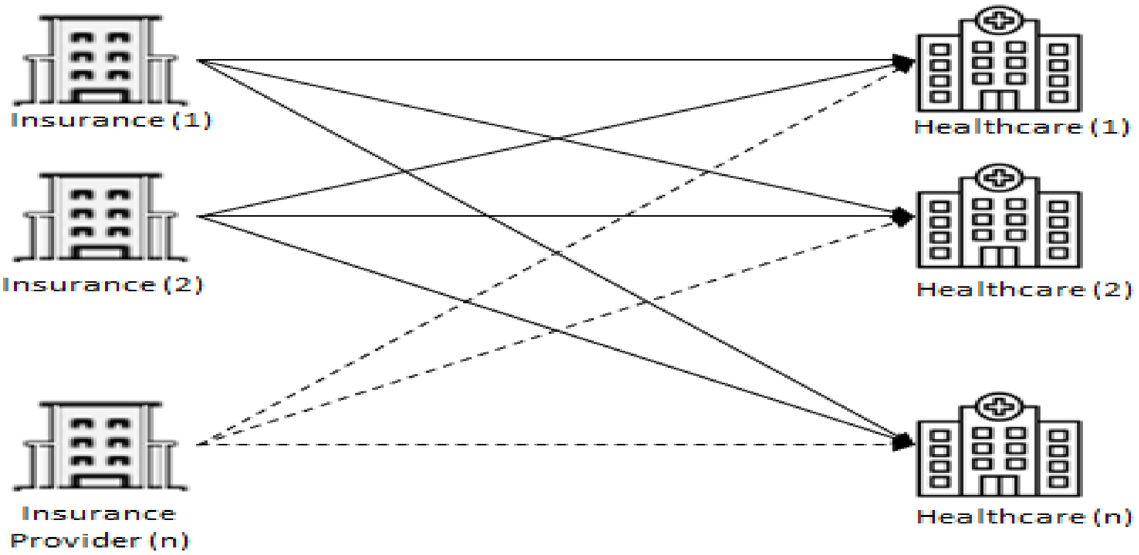


Figure 2.
N number of organizations connect to N number of systems

Redundancy of Insurance Documents.

All three stakeholders in this insurance industry manage records for every activity for each case. Patients may lose some of their documents after the case is processed as they seem to be less responsible in this regard, but Insurer and healthcare service provider always maintain historical records for each case even after several years. This tends to huge paperwork on both sides which is also required for auditing and other statistical purposes. Online file management tools make collaborative sharing and editing possible. However, standard online file management systems like Google Drive and OneDrive often only offer a small amount of storage space and a slow download speed for free users due to the high costs of communication and storage infrastructures. The fact that these file management systems rely on centralized architecture prone to single point failure and expose users to the danger of privacy leakage is another disadvantage. If a connected immutable record keeping network is established between insurers and health service providers along with the history of each record where a patient can also get information as and when required, we assume that paperwork burden from all stakeholders may reduce significantly.

PROBLEMS FACED BY EACH STAKEHOLDER

In this section, we point out and briefly discuss some common issues faced by Health-Insurance stakeholders in this business domain.

Insurer Issues: An insurer (Insurance Company, Government, or an Employer) needs to pay huge initial amount to Healthcare Service Providers to take them on its panel without which the Insurer will hardly be able to attract enough customers towards its insurance plans. This initial cost is a burden on Insurance business and that makes insurance plans even more expensive for patients. Apart from this, Frauds like altered situation such as fake billing, extra charging of room rentals for insured patients, fake health diagnosis, unnecessary medical exams and procedures, costs extremely high to insurers(Ismail & Zeadally, 2021) and chances for detection of such frauds are extremely low due to manual communications paper-work with HCSPs (Rawte & Anuradha, 2015). All these activities involve high human intervention for record keeping for each individual case which causes time and efforts at part of each stakeholder.

Health-Care Service Provider Issues: Payments on behalf of claims are often delayed from the respective insurance company, Government or employer which causes difficulties in continuation of good medical services to insured-patients. Likewise, huge paperwork and high human intervention are involved for each case's record keeping and auditing purposes.

Insured Issues: Insured (the patient) can only avail facilities from Healthcare Providers, which are on the network of the employer or insurance company that are usually know as On-PANEL, without depositing any amount but by submitting their Medical Insurance Card. If he / she visits a hospital or diagnostic lab other than one on the panel, then patient needs to pay bills from his pocket. Though afterwards he / she can submit the bills for reimbursement to his employer or Insurance company, it is usually a delayed process. Additionally, a regional limitation is also embedded within this area. Moreover, in some cases patients with insurance card are not taken seriously in the hospitals due to delay in payments by insurance companies. Another problem is that in most cases, the patient cannot avail facilities from more than one insurance companies at a time; mostly this restriction is from HCSPs to prevent fraud and audit complexities. Precisely, from the background information of the insurance companies and patient's experiences, the common problems faced by stakeholders include delay in payments, risk of frauds, territory limitation, lack of trust caused due to weak transparency among parties. Alongside, the practice of tiresome and lengthy paperwork and high human interventions subsidize the insurance procedure into more complex versions. In response, contemporary Insurance companies are obliged to develop their standard of service, health-care service providers must collaborate to deliver optimized health services to patients and insurers must maintain their updated health record to sustain the transparency standards.

LITERATURE REVIEW

In this section, we provide some related work on insurance sector using Blockchain technology. One of the related works is that of IBM's Insurance Blockchain project called Open Insurance Data Link (openIDL) (Bertrand Portier, 2018). IBM is reimagining the business of insurance by reshaping its processes and transformation of whole insurance industry by adopting new methodologies through this framework. The openIDL is built on top of the Linux Foundation's Hyperledger Fabric permissioned

Blockchain. In continuation, this Blockchain is designed using modern Design Thinking methodologies with American Association of Insurance Services (AAIS) member carriers, insurance regulators, service companies, and academics, along with AAIS and IBM executives. They claim to be the first Blockchain platform that enables the efficient, secure, and permissioned-based collection and sharing of statistical data. The openIDL is an open Blockchain network that streamlines regulatory reporting and provides new insights for insurers, while enhancing timeliness, accuracy, and value for regulators. AAIS members may participate in the openIDL Blockchain as part of their existing or new program affiliations. Hence, this fact has been induced in here so that design structure of Blockchain to bridge the gap of insurance companies can be done. Another Blockchain based insurance related work is from Black Insure (Norta et al., 2019). This Estonian group is working on a business-to-business Blockchain based digital ledger platform which can connect insurance brokers directly with capitalists by enabling them to launch their own virtual insurance companies by rethinking whole value-chain involved in this business domain with the removal of intermediary third parties.

They are claiming to reshape and redesign the whole insurance model from scratch to have the possibility to remove a lot of unnecessary steps and costs, thereby creating a truly decentralized insurance value chain from Agent to Investor on Blockchain in which local MGAs, brokers, and agents will design insurance products for market needs as a step towards making insurances more scalable and business decisions closer to end users. Some other studies in this area are BlockCIS(Lepoint et al., 2018), CioSy(Loukil et al., 2021) and SIFUBSM(Hassan et al., 2021). All systems discussed above so far are working to transform whole insurance processes starting from policy purchasing to claim processing till final disbursement of claimed amount. Secondly, both are very general enough trying to cope with all types of insurances, while we are focusing specifically on improvements in processes involved in Health Insurance Systems and the architecture proposed in this paper does not replace any existing scenario. Neither we are suggesting transforming all business processes nor businesses need to change their existing MIS. Rather we are proposing architecture to connect all stakeholders to remain up to date to medical-plan status as suggested in (K. Dahri, M.A. Memon, K. Khoumbati, 2019; Pawar et al., 2022).

PROPOSED ARCHITECTURE

To cope with the challenges, we propose a health insurance system which is based on Blockchain Technology. It is a decentralized peer-to-peer distributed ledger technology providing several features, including security, immutability, data sharing, data integrity, decentralization and mobility etc.(McGhin et al., 2019). The Blockchain Technology was initially used in Crypto-currencies and Bitcoin and the latter being the first noteworthy product using Blockchain Technology (Nakamoto, 2008). This technology has recently received much attention from the community and is being exploited in a number of domains (Aquib et al., 2020). We also propose a concept of Insurance e-Wallet which enables insureds to view statistics of all their insurance plans at one point. As a proof of concept, the proposed system has been designed, implemented, and tested. In this paper, we provide detailed description of the proposed architecture and its implementation. The high-level architecture of the proposed system is shown in figure 3, in which insurers, insureds and health-care service providers all are connected to a network of Blockchain. Insurer, which is basically an insurance company, is authorized to create new users on network by using Registrar contract from their Information-System connected to our Blockchain network or through our provided Dapp Web Application, which gives them a new generated crypto-graphical address for that new Insured-Person mapped to his National Identity Number. Upon the creation of any new user on the network a QR-Code is generated for this cryptographic-address printed on patient's insurance card for later identification from various other vendor systems. Once user is created on network a new medical insurance-plan or client's purchased plan is bound to that user's public address.

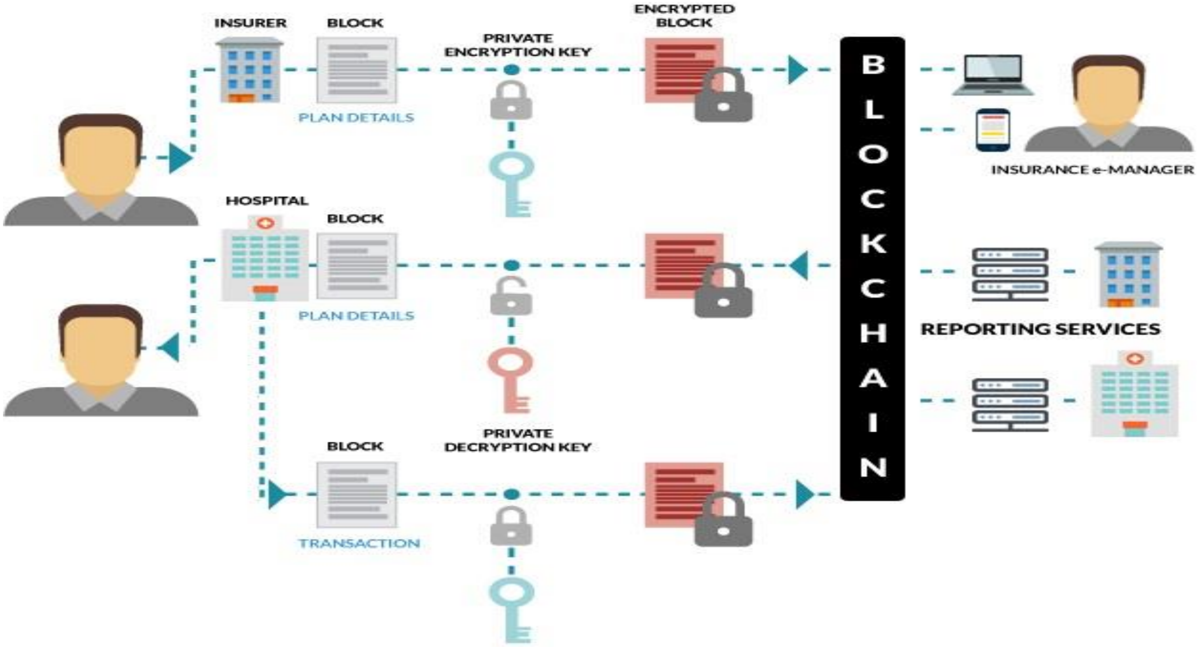


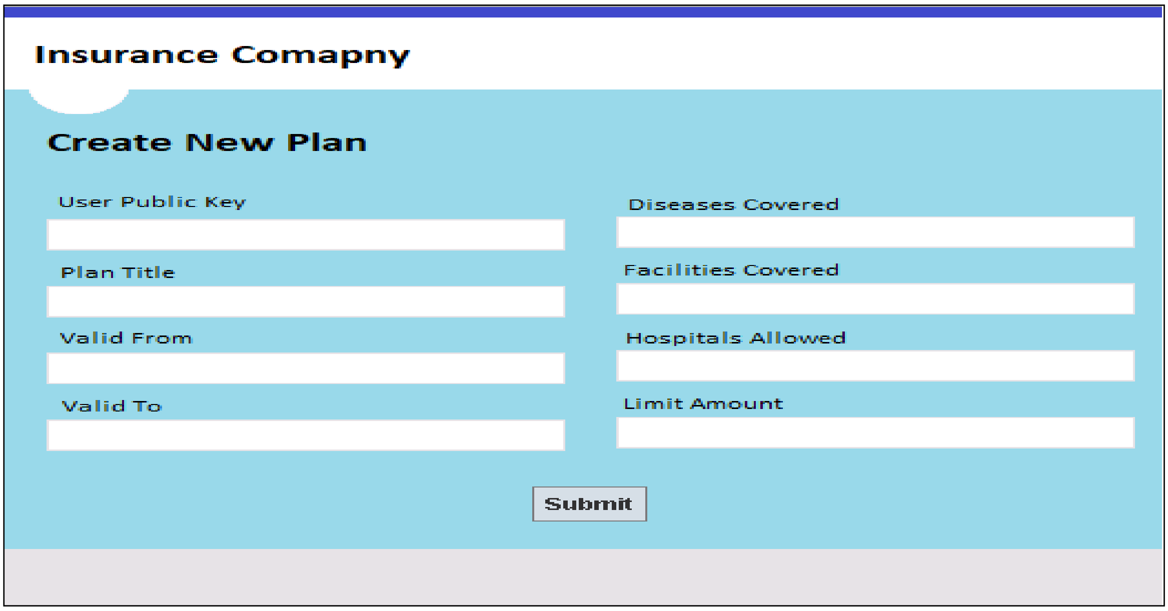
Figure 3.
High level architecture of proposed model

This new plan is added as a block on the network containing all required information including cryptographic addresses of the insurer and insured, hospitals allowed, diseases covered, valid-from date, valid-to date, spending limit and other related information. Upon this insured-person's reaching to any Health Care Service Provider unit for medical services they fetch user's plan data by providing his/her crypto-graphic address and medical services are provided within his plan's limits. And a transaction block is generated containing: references to cryptographic identity of plan, HCSP's cryptographic address, amount consumed, treatment details and any other related information. This transaction block needs approval from the concerned insurer (the creator of utilized plan) before publishing on Blockchain. Once validated, this block is added onto the network and all associated nodes are synchronized accordingly to update their local ledgers.

Before appending each block to the Blockchain network, it undergoes encryption using the insured person's private key. The encrypted block is subsequently added to the Blockchain. When a healthcare service provider requires access to an insured patient's record, the pertinent block is retrieved using the patient's public key and decrypted using the patient's private key. This meticulous process ensures the security of patients' data, allowing only authorized entities to access and read the records contained within the patient's data blocks.

IMPLEMENTATION AND TESTING

This section discusses the implementation details of the proposed system. To test the system, we created two separate prototypes for vendor systems one for posting data on behalf of Health Insurance Company as shown in figure 4.



Insurance Comapny

Create New Plan

User Public Key

Plan Title

Valid From

Valid To

Diseases Covered

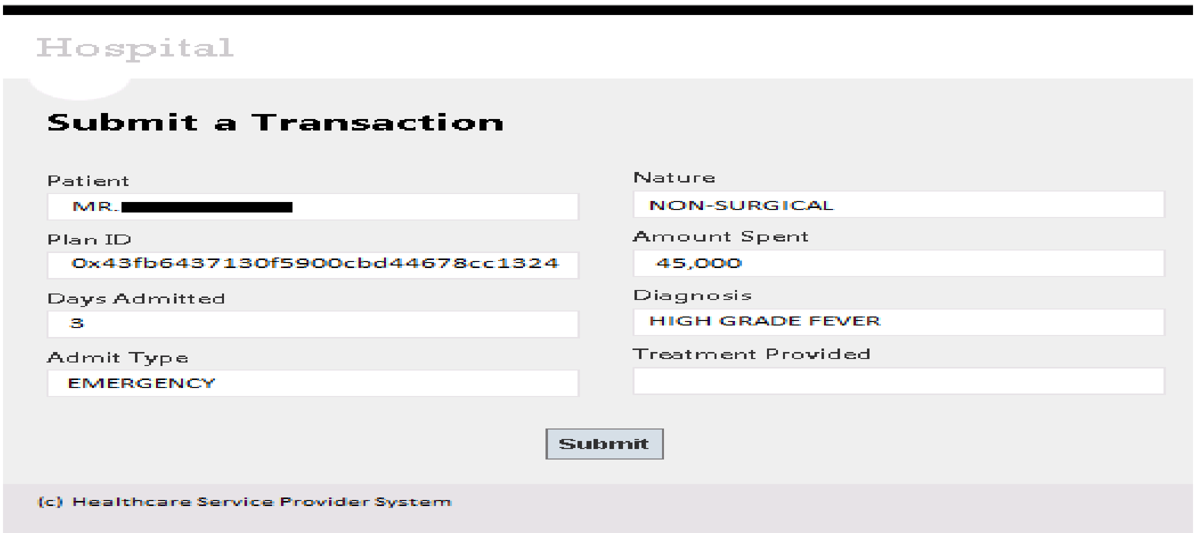
Facilities Covered

Hospitals Allowed

Limit Amount

Figure 3.
Insurer Form to Create Insurance-Plan

Another app was built for a hospital to throw data onto the Blockchain network as shown in figure 5.These sample forms were created using Asp.Net to connect to Blockchain using its services. Prior to that we deployed a Private Blockchain network using Ethereum (Buterin, 2014) and wrote smart contracts in Solidity (the programming language used to write smart-contracts on Ethereum framework) for registration of Insureds, Plan Creation, Claim Submission, Claim Validation, and the Summary-Contract for reporting purposes.



Hospital

Submit a Transaction

Patient: MR.[redacted]

Plan ID: 0x43fb6437130f5900cbd44678cc1324

Days Admitted: 3

Admit Type: EMERGENCY

Nature: NON-SURGICAL

Amount Spent: 45,000

Diagnosis: HIGH GRADE FEVER

Treatment Provided:

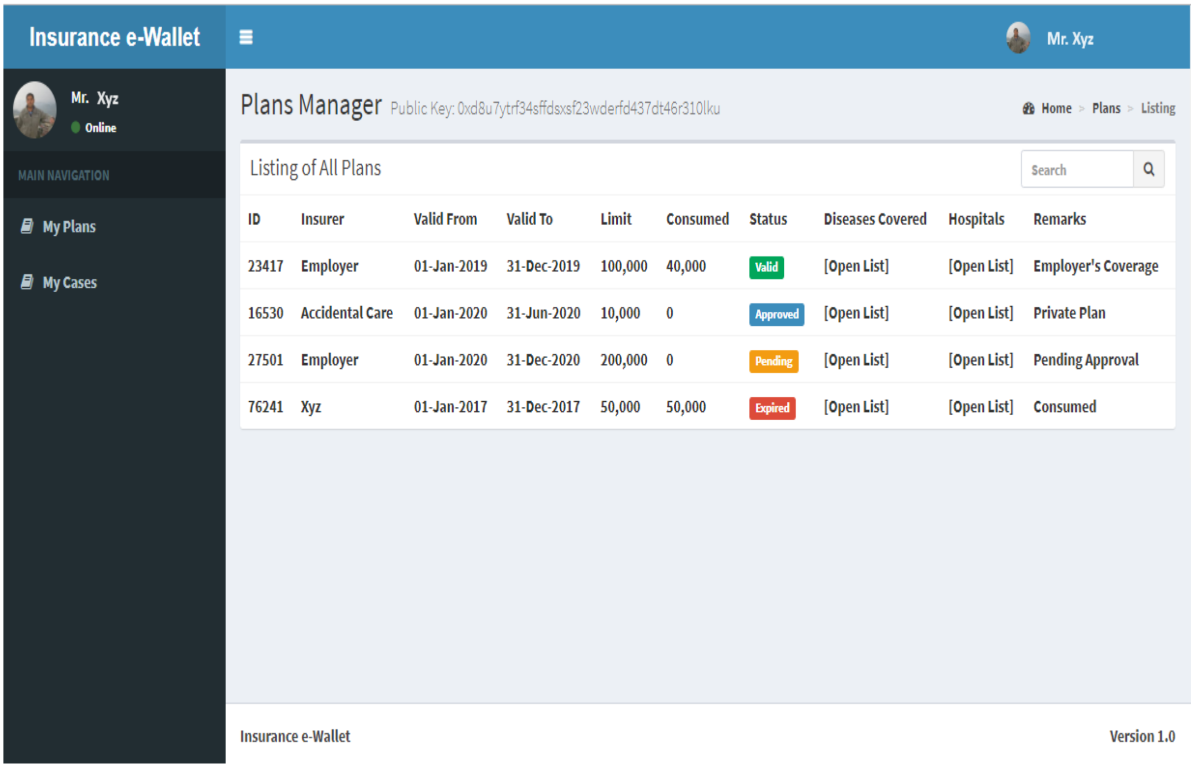
(c) Healthcare Service Provider System

Figure 4.
Healthcare Provider form to Consume Plan

Every new user (insured-person) gets their own account identified by a cryptographic address which is last 20 bytes of the hashed public-key. All persons on the network are identified by this unique hashed cryptographic address which needs to be synced with all connected nodes of stakeholders to synchronize updated status of insured patients. Apart from storing transactional details we also need to manage insurance-policy documents in scanned format, to achieve this task we made use of IPFS (Benet, 2014) as the storage hub for policy related files. IPFS – Inter-Planetary File System (Buterin, 2014) is basically a peer-to-peer distributed file storage system. Whenever the data is put on this file storage system an encrypted hash is generated (ipfs, n.d.) for the content using the public-key of content issuer which on the other hand is decrypted by receiver's private key. Usage of IPFS for content storage between different stakeholder also addresses the trust requirement between users of system.

All transactions on the network must follow the rules defined in smart contracts otherwise the transactions are put in the deceptive block for some time, and after a certain period that transaction will be deleted automatically. Major contribution of this research work is the development of an Insurance e-Wallet app, which is a separate module for Insured persons to track their updated status for their insurance policies and claims. This handy app fetches data from our Blockchain network based on logged-in user's identity. We have two major sections in this module named "My Plans" which displays user's insurance plans from any Insurance provider and another tab is for "My Cases" which displays the claims related to the logged-in person's insurance usage. Insured person is also able to view status of his insurance plan which may be either: Valid, Approved, Pending or Expired; along with the list of coverage details and provisioned hospitals from their respective links.

By the help of this app for the insured persons our aim is to make a central informative panel for patients to view all their policies conveniently and without hassle of asking for updates from each insurance company individually all a person needs is a connectivity with our Blockchain network to fetch the updated information associated with his login credentials.



Plans Manager Public Key: 0xd8u7ytrf34sffdsxsf23wderfd437dt46r310lku

Listing of All Plans

ID	Insurer	Valid From	Valid To	Limit	Consumed	Status	Diseases Covered	Hospitals	Remarks
23417	Employer	01-Jan-2019	31-Dec-2019	100,000	40,000	Valid	[Open List]	[Open List]	Employer's Coverage
16530	Accidental Care	01-Jan-2020	31-Jun-2020	10,000	0	Approved	[Open List]	[Open List]	Private Plan
27501	Employer	01-Jan-2020	31-Dec-2020	200,000	0	Pending	[Open List]	[Open List]	Pending Approval
76241	Xyz	01-Jan-2017	31-Dec-2017	50,000	50,000	Expired	[Open List]	[Open List]	Consumed

Figure 5.
Insured Individual's Interface of Insurance e-Walle

EVALUATION EXPERIMENTS

We performed two experiments to measure size and approximate growth rate of Blockchain network and the rate at which documents can be accessed over the network. Both experiments are discussed in detail below.

Size and Growth Rate of Blockchain Network

One of the major challenges that Blockchain networks face is growth in data-size. The block structure and transaction structure define how much a node's transaction library will enlarge on addition of any new block. As we know that blocks contain transaction and transaction contains data. Therefore, generally size of each transaction depends on size of data that is associated with each transaction. However, in our system we have made use of IPFS to contain BLOB data such as insurance-case documents in forms of PDFs, images, etc, and the transaction in Blockchain network will only stores the hashes of IPFS' blocks. Hence this way of handling transactions and by associating external IPFS based data storage container helps us to significantly reduce the block size. Which finally reflects to the size of each individual Node's data library.

Expected increment per day = (Number of Expected Blocks per day) x (Size of Block)

To determine the node ledger size and growth rate of the Blockchain network in this system, tests based on calculated assumptions derived from size of blocks per unit time have been simulated. For clarity, the transactions of existing vendor networks have been explained and the number of users on this system has been adopted to exaggerate the entire size of the Blockchain in our Blockchain -based data-sharing scheme for a given period. By carefully structuring the block size in our system, we adopt the use cases of user transactions per second to create an over-exaggerated value for users sending such requests per second. The importance is to prove the growth rate of the Blockchain network in our system in exaggerated conditions. The following formulas are used in the calculation for all vendor transactions per second and can be used for real case scenarios. As we have seen previously during creation of insurance plan that our average block size remains under 0.05 MB, for exaggerated values we take block size as 0.1 MB. Assuming the system consists of 500 users with a maximum of 5 users sending transactions each minute, the size of the Blockchain network would be: 0.5 mb/m, 30 MB/h, 720 MB/d, and 256.64 GB/year.

Table 1.
Growth rate of Blockchain based on transactions.

Transactions (Per Hour)	Per Hour	Per Day	Per Year	In 10 Years
100	10 MB	240 MB	85.54 GB	855.46 GB
1,500	150 MB	3.51 GB	1.25 TB	12.53 TB
5,000	500 MB	11.71 GB	4.177 TB	41.77 TB
30,000	2.92 GB	70.31 GB	25.06 TB	250.62 TB
100,000	9.7 GB	234.375 GB	83.54 TB	835.41 TB

Table 1 shows an estimated growth of Blockchain network for an exaggerated block size of 0.1 MB, along with an over-exaggerated number of transactions per hour. The total size in bytes of the results shown in the table above are outputs pertaining to blocks generated in our proposed system. Data sizes generated are represented in megabytes (MB), gigabytes (GB), and terabytes (TB). The transaction column illustrates the number of transactions per period. Data generated per period in relation to the block size represents the amount in size for the Blockchain network over a period.

Evaluating Document Access Time

For this experiment, we set up a conventional cloud-based virtual machine storage using Microsoft Azure(Microsoft, 2021). A virtual machine with windows 10 was established. We evaluated the efficiency of documents access time by comparing cloud-based storage system with the local configured node of IPFS based on two parameters: the number of submitted documents, and the size of documents. The measurement of the performance was based on the following metrics: upload and download time of document PDFs. We obtained anonymized sample documents containing A4 size scanned images of documents of range from 100kb to 3 MB to verify the file access time in Seconds. The experiment was performed on our local computer with an internet download speed of 25.35 MBps and an upload speed of 12.91 MBps. 80 PDF documents of size range from 100 KB to 3 MB were uploaded to our distributed IPFS network and conventional cloud network and then downloaded the files to the local computer. The download time is observed during the documents accessed from the IPFS system using document's hash identity stored in the Blockchain . Figure 7 shows the time taken to fetch the documents from our local IPFS node and cloud-based document storage. The graph shows that the proposed system takes less than 1s to download 10 files of 5 MB while from the cloud storage same size and same number of files took 3 seconds. Then from IPFS it took 2 seconds to download 25 files of 15 MB while for cloud storage it took 9s. The bar graph in Figure 7 shows that difference of access time increases as we increased number of files. Finally, within 6 seconds 80 files of 50MB were downloaded by the proposed system and cloud-based-storage took 32 seconds to download similar number of files. As evident from the figures, we can see that the PDF file access time of the IPFS storage network outperforms the conventional cloud storage. As expected, the proposed approach is faster due to its distributed operations running silently at the back end. The traditional storage system is a complex process due to the centralized server, queued transactions, and privacy issues. In general, the experiments show that the IPFS based storage solution is robust and possible to access all the documents faster and without interruptions.

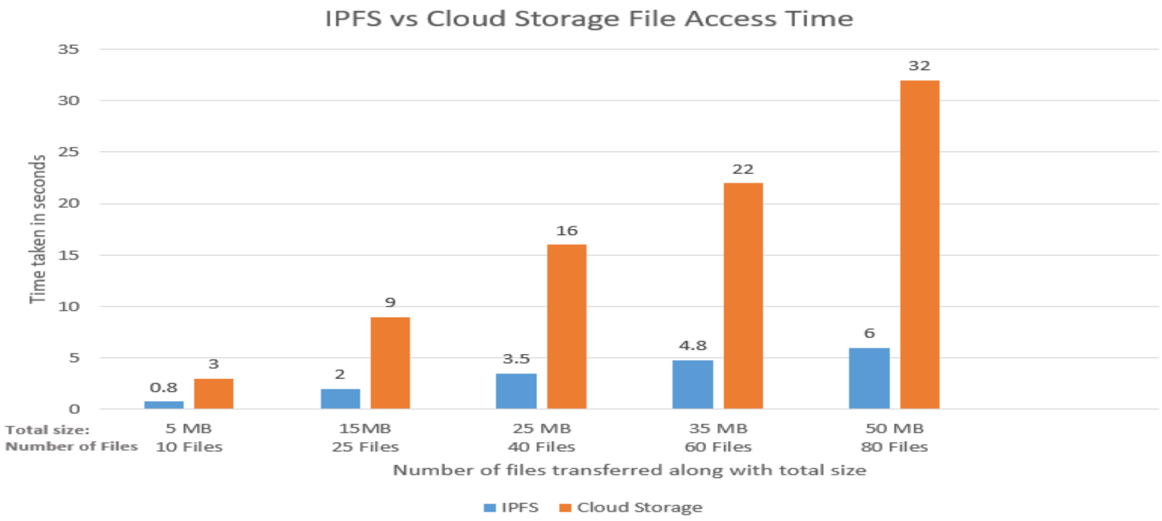


Figure 6.
IPFS vs Cloud Storage File Access Time

Based on our experiments, we have concluded that Blockchain handles large amounts of data efficiently through a combination of innovative strategies. By integrating technologies like the Inter-Planetary File System (IPFS), Blockchain networks can significantly reduce block sizes. Instead of storing extensive data within transactions, only cryptographic hashes of external data are recorded, minimizing the overall data footprint. Furthermore, the structure of each block and its associated transactions is designed to ensure scalability and efficient data management. This architecture, coupled with decentralized storage and consensus mechanisms, allows Blockchain networks to handle substantial volumes of data while maintaining data integrity, security, and immutability.

IMPLEMENTATION CHALLENGES

Transformation in any industry is always challenging, while Blockchain technology offers a promising solution to the long-standing data sharing and interoperability challenges in the health insurance sector, its may face following challenges in Blockchain 's implementations. (Dahri et al., 2020; Reegu et al., 2022)

Data Privacy and Security: Health insurance involves highly sensitive and personal information. Ensuring the privacy and security of this data is paramount.

Regulatory Compliance: The healthcare and insurance industries are heavily regulated. Adhering to these regulations while implementing a Blockchain solution can be complex. Compliance with standards like HIPAA is crucial and challenging.

Scalability: As the size of the Blockchain grows with more transactions, scalability becomes an issue. Though we are making use of IPFS to overcome this issue, but the size of IPFS may also grow based on number of documents with each claim/case.

Cost: Implementing and maintaining a Blockchain -based system can be costly initially costly as every organization will be required to adopt implementation infrastructure needs. The initial investment in technology, training, and ongoing maintenance may pose challenges for smaller insurance providers.

User Adoption: Getting healthcare providers, insurers, and patients to adopt Blockchain technology can be a hurdle. Training and education are often needed to ensure that all stakeholders are comfortable with the system.

Consensus Mechanism: Selecting the appropriate consensus mechanism for the Blockchain can be tricky. Public, private, or consortium Blockchain s each have their pros and cons, and the choice depends on the specific use case.

Data Standardization: Ensuring that data is standardized across the network is crucial for seamless data exchange. In healthcare, data is often siloed and comes in various formats, making standardization a challenge.

Legal and Liability Issues: Determining liability and dispute resolution in case of errors or disputes on the Blockchain can be legally complex. More futuristic Smart contracts can be designed to address these issues.

CONCLUSION

In this paper, a working model for Blockchain based decentralized Health Insurance System has been presented. The proposed model is capable to handle insurance policies, claim processing, validations of transactions, management of supporting documents with the physiognomies of transparency and data integrity and interoperability among various vendor systems. We made use of traditional development frameworks for the development of vendor-prototypes, Ethereum for Blockchain network, IPFS to sort out distributed file sharing mechanism and encapsulated our business rules inside smart contracts to maintain uniformity in health insurance ecosystem. As this study has proposed a health insurance system which is based on Blockchain 's versatile nature for data-sharing and synchronization capabilities. From this objective, our system can be used as reference for overall insurance management systems which deal to insure vehicles, businesses, cargo and other insurance areas as well as for other record management systems to keep data sync among various vendors. Eventually, this study serves as an initiating point for further research in the similar domains.

DECLARATIONS

Acknowledgement: We appreciate the generous support from all the supervisors and their different affiliations.

Funding: No funding body in the public, private, or nonprofit sectors provided a particular grant for this research.

Availability of data and material: In the approach, the data sources for the variables are stated.

Authors' contributions: Each author participated equally to the creation of this work.

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

Consent to Participate: Yes

Consent for publication and Ethical approval: Because this study does not include human or animal data, ethical approval is not required for publication. All authors have given their consent.

REFERENCES

6 Common Identity Challenges That Can Be Addressed In An IAM Strategy. (n.d.). Retrieved October 27, 2022, from https://www.idenhaus.com/6-common-identity-challenges-which-can-be-addressed-in-an-iam-strategy/

Albert Pang, Misho Markovski, M. T. (2020). *Top 10 Insurance Software Vendors and Market Forecast 2019-2024*. Vertical Market Reports. https://www.appsruntheworld.com/top-10-insurance-software-vendors-and-market-forecast/

Aquib, M., Dhomeja, L. Das, Dahri, K., & Malkani, Y. A. (2020, January). Blockchain -based Land Record Management in Pakistan. *2020 3rd International Conference on Computing, Mathematics and Engineering Technologies (ICoMET)*. https://doi.org/10.1109/iCoMET48670.2020.9073927

Benet, J. (2014). *IPFS - Content Addressed, Versioned, P2P File System*. *Draft 3*. http://arxiv.org/abs/1407.3561

Bertrand Portier. (2018). *Blockchain in insurance: Five reasons why openIDL will succeed*.

Buterin, V. (2014). A next-generation smart contract and decentralized application platform. *Etherum*, *January*, 1–36. http://buyxpr.com/build/pdfs/EthereumWhitePaper.pdf

Dahri, K., Memon, B., Aquib, M., & Shaikh, Z. A. (2020). Blockchain Implementation Challenges and Limitations: A Critical Review. *University of Sindh Journal of Information and Communication Technology*, *4*(4), 245–248.

ehcos.com. (n.d.). *Data Interoperability; A Key Component for Connected Health Systems*. Retrieved October 26, 2022, from https://www.ehcos.com/en/data-interoperability-a-key-component-for-connected-health-systems/

Gary. (2019). *Fundamental Health Insurance Problems and Solutions*.

Hassan, A., Ali, M. I., Ahammed, R., Khan, M. M., Alsufyani, N., & Alsufyani, A. (2021). Secured Insurance Framework Using Blockchain and Smart Contract. *Scientific Programming*, *2021*, 1–11. https://doi.org/10.1155/2021/6787406

Hodapp, D., & Hanelt, A. (2022). Interoperability in the era of digital innovation: An information systems research agenda. *Https://Doi.Org/10.1177/02683962211064304*. https://doi.org/10.1177/02683962211064304

Imarc. (2021). *volume of health insurance industry*. https://www.imarcgroup.com/health-insurance-market

ipfs. (n.d.). *Hashing | IPFS Docs*. Retrieved October 31, 2022, from https://docs.ipfs.tech/concepts/hashing/#important-hash-characteristics

Ismail, L., & Zeadally, S. (2021). Healthcare Insurance Frauds: Taxonomy and Blockchain -Based Detection Framework (Block-HI). *IT Professional*, *23*(4), 36–43. https://doi.org/10.1109/MITP.2021.3071534

K. Dahri, M.A. Memon, K. Khoumbati, I. A. I. (2019). Interoperable Health Care System Using Blockchain Technology. *SI NDH UNIVERSITY RESEARCHJOURNAL (SCIENCE SERIES)*, *51*(03), 437–440.

Kuroki, M. (2022). State minimum wages and health insurance coverage in the United States: 2008–2018. *International Journal of Health Economics and Management*, *22*(2), 163–180. https://doi.org/10.1007/S10754-021-09313-6/TABLES/7

Lepoint, T., Ciocarlie, G., & Eldefrawy, K. (2018). BlockCIS—A Blockchain -Based Cyber Insurance System. *2018 IEEE International Conference on Cloud Engineering (IC2E)*, 378–384. https://doi.org/10.1109/IC2E.2018.00072

Loukil, F., Boukadi, K., Hussain, R., & Abed, M. (2021). CioSy: A Collaborative Blockchain -Based Insurance System. *Electronics*, *10*(11), 1343. https://doi.org/10.3390/electronics10111343

McGhin, T., Choo, K. K. R., Liu, C. Z., & He, D. (2019). Blockchain in healthcare applications: Research challenges and opportunities. *Journal of Network and Computer Applications*, *135*, 62–75. https://doi.org/10.1016/J.JNCA.2019.02.027

Microsoft. (2021). *Microsoft Azure*. https://azure.microsoft.com/en-us/

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. *Www.Bitcoin.Org*, 9. https://doi.org/10.1007/s10838-008-9062-0

Norta, A., Rossar, R., Parve, M., & Laas-Billson, L. (2019). *Achieving a High Level of Open Market-Information Symmetry with Decentralised Insurance Marketplaces on Blockchain s*. 299–318. https://doi.org/10.1007/978-3-030-22871-2_22

Nyman, J. A. (1999). The value of health insurance: The access motive. *Journal of Health Economics*, *18*(2), 141–152. https://doi.org/10.1016/S0167-6296(98)00049-6

Park, A., Wilson, M., Robson, K., Demetis, D., & Kietzmann, J. (2022). Interoperability: Our exciting and terrifying Web3 future. *Business Horizons*. https://doi.org/10.1016/J.BUSHOR.2022.10.005

Pawar, P., Parolia, N., Shinde, S., Edoh, T. O., & Singh, M. (2022). eHealthChain—a Blockchain -based personal health information management system. *Annales Des Telecommunications/Annals of Telecommunications*, *77*(1–2), 33–45. https://doi.org/10.1007/S12243-021-00868-6/FIGURES/10

Rawte, V., & Anuradha, G. (2015). Fraud detection in health insurance using data mining techniques. *Proceedings - 2015 International Conference on Communication, Information and Computing Technology, ICCICT 2015*. https://doi.org/10.1109/ICCICT.2015.7045689

Recordon, D., & Reed, D. (2006). OpenID 2.0: A platform for user-centric identity management. *Proceedings of the Second ACM Workshop on Digital Identity Management, DIM 2006. Co-Located with the 13th ACM Conference on Computer and Communications Security, CCS'06*, 11–16. https://doi.org/10.1145/1179529.1179532

Reegu, F. A., Abas, H., Hakami, Z., Tiwari, S., Akmam, R., Muda, I., Almashqbeh, H. A., & Jain, R. (2022). Systematic assessment of the interoperability requirements and challenges of secure Blockchain -based electronic health records. *Security and Communication Networks*, *2022*.

Sedlmeir, J., Smethurst, R., Rieger, A., & Fridgen, G. (2021). Digital Identities and Verifiable Credentials. *Business and Information Systems Engineering*, *63*(5), 603–613. https://doi.org/10.1007/S12599-021-00722-Y/TABLES/3

Top 9 Identity & Access Management Challenges with Your Hybrid IT Environment | Okta. (n.d.). Retrieved October 27, 2022, from https://www.okta.com/resources/whitepaper/top-9-iam-challenges-with-your-hybrid-it-environment/

Trude, Sally; Christianson, Jon B; Lesser, Cara S; Watts, Carolyn; Benoit, A. M. (2002). Employer-sponsored health insurance: Pressing problems, incremental changes. *Health Affairs; Chevy Chase*, *21*(1). https://www.proquest.com/docview/71526572?pq-origsite=summon