Towards distributed data, security and IoT integration in healthcare through blockchain

Dr. Alan Tominey
contact@gorki.dev

February 5, 2024
v1.0

Abstract

Many medical institutions have historically depended on local infrastructure to store patient records, and a significant number do not have robust backup systems, creating a "single point of failure". In addition, many institutions have moved towards minimising data transfer and sharing in an effort to protect data and privacy[1]. This shift towards silos and ring-fencing, driven by inadequate technology, is in opposition to the benefits and insight that data availability is bringing to healthcare[2, 3]. Conversely, as a number of other institutions shift towards cloud-based storage, they face threats from another vector. For instance, during the COVID-19 crisis, healthcare systems were notably targeted by ransomware and distributed denial-of-service attacks[4]. These digital attacks hampered critical emergency services, rendering numerous patients without medical care. Simultaneously, there's been a surge in the development of compact health sensors, wearable health sensors and IoT devices, that monitor patients' vital statistics. This progression has bolstered the overall quality of the healthcare ecosystem[5]. They serve dual purposes: for the everyday user, they offer advanced health and fitness monitoring; for healthcare practitioners, they present a richer dataset. This wealth of information can potentially speed up diagnoses and shape treatment modalities[6], however with the increased frequency of reporting this has brought an equal increase in the volume of the data that is required to be distributed and stored. In the quest for more secure storage, there's growing interest in technologies like distributed file systems (e.g. IPFS) and Blockchain[7]. However, it's crucial to note that utilizing IPFS merely transfers the data ownership to another system that demands its own management[8]. This approach was chosen partly because the underlying blockchain structure isn't equipped to handle data directly on-chain and opens vulnerabilities in the integration of these technologies, through two-way communication systems (oracles). This article delves into IPFS and Blockchain-based healthcare storage solutions, examining the architectures and effectiveness of existing systems and previously proposed solutions. The paper will present a specific solution to the problems described. This holistic approach integrates smart contracts, facilitating multi-party access to data, and prioritizes security, transparency, and efficiency in healthcare data management.

1 Introduction

1.1 Data in healthcare

The healthcare industry has long recognized the significance of data in improving patient care, enhancing medical research, and optimizing operational processes[9, 10, 11]. Even before the advent of transformative technologies such as the Internet of Things (IoT), blockchain, and big data analytics, healthcare practitioners and researchers acknowledged the value of collecting and analysing large quantities of data[12]. This historical perspective underscores the enduring importance of data in healthcare and lays the foundation for understanding how emerging technologies can further revolutionize the field. Today, the healthcare sector is increasingly recognizing the importance of the collection, dissemination, and use of this data in improving patient outcomes, enhancing the efficiency of care delivery, and driving medical research. The inclusion of Big Data and the Internet of Things (IoT) has revolutionized the way healthcare data is collected, analysed, and utilized, offering enormous potential for the sector[13, 14]. IoT devices, ranging from wearable devices to implantable surgical devices, are increasingly being used to collect health-related data. These devices can measure various health parameters and connect to the internet, enabling remote monitoring and data collection[15, 13]. This Internet of Medical Things (IoMT) supports the digital revolution in healthcare, particularly in the development of products such as wearable devices that allow patients, elderly people, or people with chronic diseases to remotely monitor their health status. It's important to note that not all IoT devices are clinically tested or proven to be safe or effective[13], however the advances in available data and the proper facilities to consume it are an important step towards an energy-efficient and resource-optimized healthcare system[16]. The growing volume of data and the evolution of data driven techniques for diagnosis presents a keen challenge on the security and availability of stored data. A decentralised approach to storage of data is often brought forward as an option to avoid attacks (like DDOS), or loss/degradation of data, and ensure high availability[7]. Blockchain-based solutions are often described as a solution to address the decentralisation of systems, however it is often noted that blockchain solutions are unable to handle the volume of data required, and therefore adjunct systems are often integrated to alleviate this issue[17, 18, 8, 19, 20, 21], however it is important to note that any point of integration in a system, or additional component can represent a potential attach vector[22, 23, 24, 25] – it is therefore incumbent on any system design for sensitive data to minimise the number of integrations. Leading architects to prefer systems that have the native capability to achieve as many of the stated goals as possible.

1.2 Blockchain and healthcare

There is growing attention and investment in the importance of blockchain technology in improving patient outcomes, enhancing the efficiency of care delivery, and driving medical research, from large multi-national companies and government organisations[26]. The advent of blockchain technology has the potential to revolutionize the way healthcare data is collected, analysed, and utilized, offering enormous potential for the sector[17, 27, 28]. For example, Estonia has been recognised as leading the way secure patient data is stored and controlled in-country using blockchain technology[29]. Blockchain technology is often incorporated into the security of Internet of Things (IoT) based Remote Patient Monitoring (RPM) systems. The secure and efficient transmission of medical data is a primary concern in RPM systems, and the inability to delete or change information from blocks makes blockchain technology an ideal solution for healthcare systems. However, the original form of blockchain technology has limitations when connected to IoT scenarios. Scalability is often discussed, however there are also issues with latency, bandwidth and transaction rates[30]. There have been numerous attempts to tackle these challenges with limited success, primarily due to the need to apply scaling solutions, or limit the interaction of the system with the blockchain to avoid bottlenecks in the system[31, 19, 20]. Blockchain technology is being used to manage the exchange of health records, which is crucial for diagnosis and treatment. The technology allows patients to keep personal data and determine with whom this can be shared, thus resolving current data ownership, and sharing issues[32]. Blockchain's ability to connect disparate systems, while maintaining self-sovereignty of the data, and increase the accuracy of electronic health records has tremendous potential in healthcare[33]. Despite the potential benefits of data sharing, hospitals often face challenges in sharing their data. This reluctance is often due to concerns about privacy and data security, interoperability problems, and a lack of resources for secure transfer[34]. Blockchain technology presents unique opportunities to reduce complexity, enable trust-less collaboration, and create secure and immutable information. However, several technical, organizational, behavioural and economic challenges must be addressed before a healthcare blockchain can be adopted by organizations globally[35, 28].

1.3 Communication in a decentralised healthcare setting

Decentralization is a moniker for a vast array of alterations that modern technology can make to the way traditional industries have operated. In healthcare it can refer to the process of distributing the data and diagnostic resources, or authority, responsibility, and accountability of healthcare services across multiple entities rather than a single centralized authority. This approach has also been increasingly recognized for its potential to improve the efficiency of resource allocation and overall healthcare outcomes[36]. However the growing scale and scope of a decentralised system causes a need for systems to be even more tightly integrated, allowing for seamless collaboration between the disparate entities, a robust communication protocol is therefore required to facilitate decentralization[37, 38].

1.4 Existing blockchain and healthcare architectures

A recurring theme in the literature surrounding blockchain implementations in healthcare is that of the blockchain, being present as an adjunct to the system. This kind of implementation is a symptom of the 'trilemma' that is often talked about in blockchain context. The trilemma is the extension of the CAP theory, presented by brewer, expressed in terms of modern distributed networks[40]. Essentially, that systems must choose between decentralisation, scalability, and security. In many cases, this leads developers to choose which of the three aspects are the least important to their particular use case and move that part of the system off-chain onto an ancillary system[41, 42, 43]. Due to the nature of most modern blockchains, being payment networks, focusing on transactions, or simple addition/subtraction of wallet balances. Scalability and security are often the focus. Due to the relatively low volume of data that is required, data on-chain and the decentralisation challenges that data bring, are often sacrificed[44]. A characteristic example of this can be seen in Figure 1, the blockchain system is orchestrated by the "system administrator", its primary use in the system can be thought of as a verification network. Whilst the verification of the data is, valuable, it is pertinent to the discussion of this paper that the architecture seeks to limit the systems exposure to the limitations of the blockchain by merely referring to the network once the data is managed. It is essentially building a second layer of the system, and "rolling up" data for verification of state on the blockchain layer. Similarly figure 2 demonstrates the integration of mul-

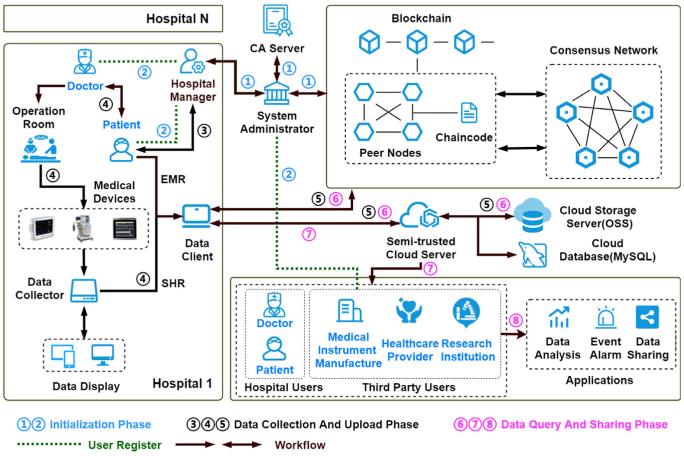

Figure 1: example of limited, complex system architecture, blockchain implemented as validation component only, very little participation shown in system[39]

tiple integrated components, in the same manner as above, leading to complex communication between the system, leading to multiple attack vectors[25], and only leveraging the blockchain features as a ledger of activities, which in turn will be hashed and potentially lost to the state of the network presenting only breadcrumbs of the data trail that generated it. It should be recognized that considerably more of the blockchain applications discussed in academic circles involves a range of system integrations aimed at addressing the fundamental constraints associated with the underlying blockchain technology. Such integrative measures have led certain scholars to question the efficacy of blockchains as a remedy for decentralizing healthcare systems. For instance, there is a faction of the academic community that dismisses the proposition of utilizing blockchain technology for the specific purpose of allocating unique identifiers to patients[45], and some that cast doubt, on how appropriate the use of blockchain is for large-scale processing due to the disadvantages described above[46]. Similarly, while many advocate for the use of blockchain purely to enhance security, there are authors that have historically highlighted possible issues associated with blockchain-based systems, designed utilizing Proof of Work (PoW) and Proof of Stake (PoS) consensus techniques[47]. This has led to a great deal of attention and work in the area of information security at the highest levels of industry and government[48]. These factors establish that it is imperative, in the design and construction of these systems, that information security and data sovereignty are implicit in the underlying technologies and not just part of the system architecture.

2 Purpose of the paper

In this paper we set forward a novel blockchain framework for healthcare. Using a lightning-fast, linearly scalable, leaderless, decentralised data network and blockchain with a powerful smart-contract language and interoperability features directly from the virtual machine we aim to address the limitations keeping adoption of blockchain technology from the global healthcare industry. We present the following features as being central to this implementation:

- **Data on-chain:** allowing decentralised storage of data directly on the blockchain. Eliminating the need for a secondary file system integration, while maintaining the economic feasibility through a high-volume data network and blockchain.

- **Interoperability:** eliminating the need for integration of oracles, or secondary systems required to orchestrate governance of the system. The blockchain, establishes itself as the core part of the system. A communication and orchestration layer, rather than a verification layer as an adjunct.

- **Scalability:** a linearly scalable model for blockchain, able to handle the computational burden of the system through concurrent block execution.

- **Security:** a fine-grained security model, able to provide the data sovereignty and management required for highly sensitive data.

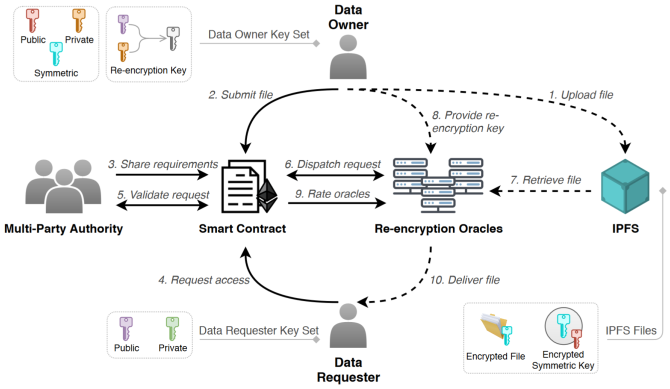

Figure 2: example of limited blockchain architecture, IPFS integration and oracle encryption implemented with blockchain as adjunct validation engine only [18]

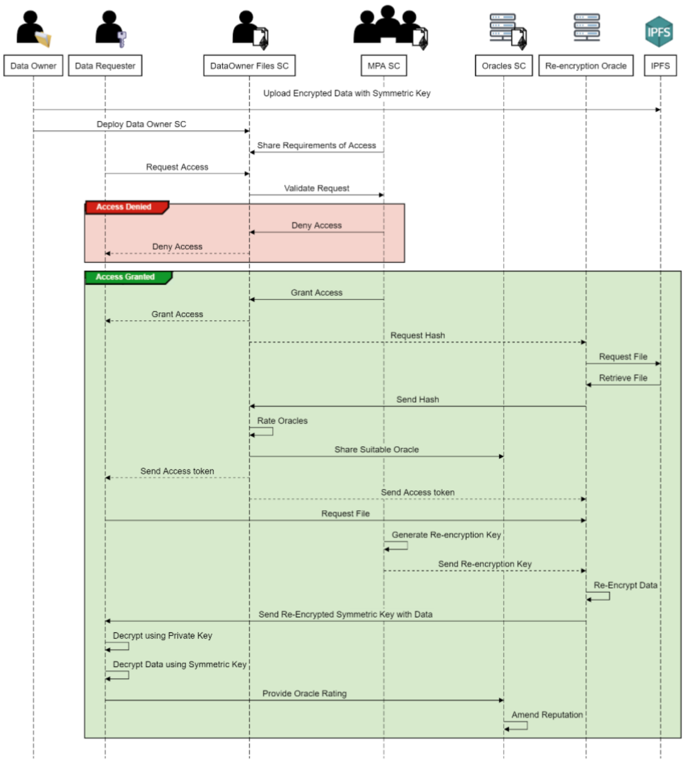

Figure 3: example of limited blockchain architecture, sequence diagram that can be drastically simplified by removing several components, each external call is a vector for attack [18]

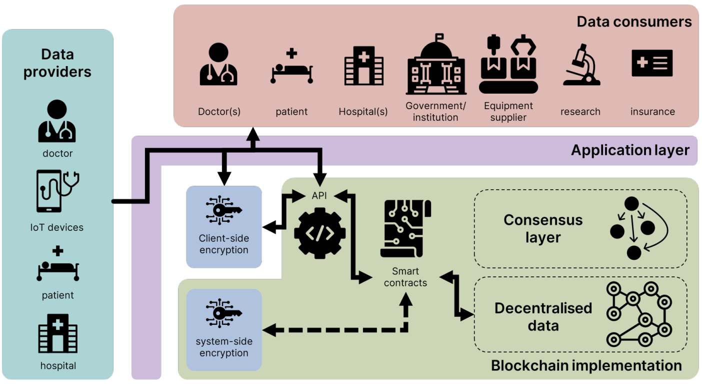

Figure 4: Proposed blockchain-centric architecture

3 Proposed blockchain framework

Figure 4 details a high-level overview of a blockchain-based healthcare data system/application through a communication API, capable of integrating with healthcare ‘data providers. Creating a novel architecture that leverages the blockchain’s unique features to create a self-contained, highly secure, and efficient data management ecosystem.

3.1 Self-contained data storage

In this innovative system, all healthcare data, whether generated by IoT devices, medical equipment, or patient records, is stored on the blockchain. This approach ensures that every piece of information is accounted for and accessible within the blockchain, eliminating the need for disparate databases and reducing the risk of unintended data fragmentation.

3.2 Data management

Data security is paramount in healthcare. This system employs a dual-layer approach to data encryption:

1. Client-Side Encryption: Patient data is encrypted on the client side before being uploaded to the blockchain, ensuring that sensitive information remains confidential even before reaching the blockchain.

2. On-Chain Encryption via Smart Contracts: Additionally, the system offers the option to encrypt data directly on the blockchain through smart contract interfaces, providing an extra layer of security for data at rest.

Data management can be considered as part of a three-tiered system, (Fig. 5) integrity, access, and privacy. The schematic shown above is a simplification of the original description[31], this simplification omits the integrations that were made necessary by the limitations of the blockchain technologies that were discussed in the paper. Notably, third party systems and equivalence checking, made necessary by the limited capabilities of traditional blockchains when handling data. Similarly, a lower compute power, in simpler turing-complete blockchains, requires them to communicate with external systems through an orchestration layer, meaning that IoT integration, and legacy system integration is not direct.

- **Encryption:** possible at the point of data generation and loaded on-chain as a self-contained encrypted piece of data. This, theoretically, provides the highest level of encryption security however may limit other integrated functionality. The powerful virtual machine of the blockchain can also be utilised to encrypt data, a concurrent execution engine also ensures that compute functions do not impede other participants in the network.

- **Architecture:** Optimised node architectures for different levels of compute and data handling also enable systems that are directly connected to IoT devices to cope with high throughput, whilst data-heavy, lower throughput nodes can handle data transactions. Sharding can also be leveraged to enable more privacy and security of internal data.

- **Smart-contract:** smart contracts capable of complex calculations and direct integration with legacy systems, hardware and software enable a full suite of data integrations, communication, and orchestration.

- **Language features:** The smart contract language provides an elegant solution to enable ’object capabilities’ (OCAPs). The OCAP security model is a superior model to ’access control lists’ (ACL). ACL is now almost ubiquitous, and used almost all blockchains, despite its weakness to hacks. An implementation of the principle of unforgeable names as first-class citizens in the blockchain, means users can generate an unforgeable name and use it as a capability (in this example the OCAP becomes like a key to a secure room,

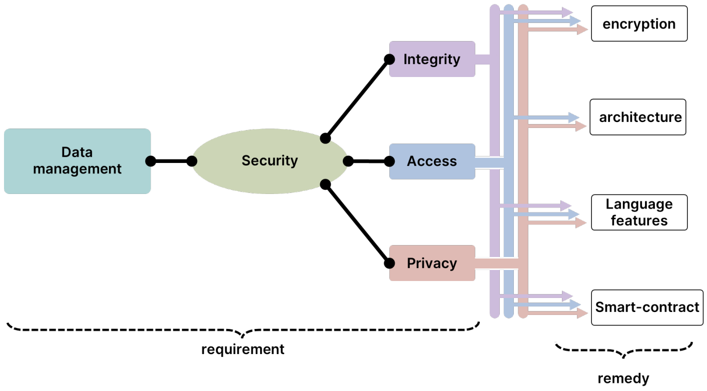

Figure 5: data management features addressed as system capabilities, modified version from Adere et. al[31]

or their medical data) – it is then possible to pass this capability to anyone, or restrict further sharing of this capability, creating fine-grained security models to be to manage and secure decentralised data.

- **Query language:** the powerful smart-contract programming language, also operates like a query language for the blockchain. Allowing pattern matching in the smart-contract which enables on-chain search to take place. This enables researchers to access data, if the participants of the network allow them.

3.3 Data verification and storage

The blockchain manages the verification and storage of healthcare data seamlessly. As data is generated, it undergoes cryptographic verification and is then permanently stored on the blockchain. This ensures data integrity and immutability, making it tamper-proof and resistant to unauthorized alterations.

3.4 Integration with medical equipment

The system includes an integrated API layer that facilitates seamless communication between various healthcare equipment, IoT devices, and the blockchain. This allows for real-time data streaming from medical instruments, enabling timely and accurate monitoring of patient health.

3.5 Ownership and access control

Ownership and access to healthcare data are governed by smart contracts, unforgeable names and object-capabilities, providing fine-grained control over who can view, utilize, or modify the data. Patients, healthcare providers, and authorized stakeholders can define access permissions, ensuring data privacy and compliance with regulations like HIPAA.

3.6 Data removal and wiping

A unique feature of this blockchain-based system is the ability to remove data from the blockchain effectively, if permitted to. Data can be consumed in a channel, eliminating it from the blockchain's state. This can be implemented once garbage-collection and the last finalised state have been found, steps can be taken to irradicate data from view. This feature is particularly useful for adhering to data retention policies, allowing for the responsible handling of patient information.

In summary, this blockchain-based healthcare data system represents a groundbreaking advancement in healthcare data management. Its self-contained architecture, data encryption options, data verification, and access control through smart contracts provide a secure, transparent, and flexible solution for managing and safeguarding healthcare data. The integrated API ensures seamless communication with medical equipment, enhancing real-time monitoring and diagnostics. Additionally, the ability to remove data from the blockchain when necessary, and query on-chain resources for search capabilities, adds a layer of data lifecycle management and research capabilities, ensuring compliance with regulatory requirements, data privacy standards whilst enabling the next generation or frontier medical research and development with IoT.

4 Features and capabilities of the new blockchain enabling this system

The Gorki protocol is being designed to minimise the amount of synchronisation required to avoid the infamous blockchain trilemma (liveness, safety, and fault-tolerance) to ruin user experience. Four major innovations and principles have been implemented in a blockchain model. The mathematical model backing the state of a computer is derived from process calculus, which uses process ”names” as the fundamental element of that computer's state, and computation is described through the process of exchanging data between "names". To give concurrent access to this state, names are stored inside a tuple space[49], inherited from coordination language Linda. For practical reasons, this can be seen as a map that stores the content of the channels (the data passed between the names), which allows Gorki to easily compute the proof of state by maintaining this map in the form of a Merkle tree. Another benefit of this model is that it allows easy access to sharding through namespaces. Since each name can belong to one or more namespace, transferring a value from one shard into another is a matter of transferring records through the states. Rholang, the programming language of the platform, is an exact description of the state of the computer. In essence, it is the WYSIWYG principle. Rholang supports an object-capability security model that unlocks an enormous amount of value when deployed to a shared execution environment like a blockchain. Rholang is the API to a powerful concurrent state machine which prevents the user from making mistakes, restricts access and manages resources. Since process calculus has a history of usage proving concurrent programs (CCS)[50], this opens a path towards a proof system for on-chain smart-contracts. This allows formal verification of processes that are running concurrently, creating a method that allows the user to ensure their programs, smart-contracts and applications are running as intended. It is well known that systems that rely on a leader for consensus are prone to attacks, but also, there are no systems to date presented that are entirely asynchronous. One breakthrough is the Nakamoto consensus used in PoW systems, which employs economic incentives to make finality probabilistic and make attacking unprofitable. Gorki is developing a consensus algorithm inspired by the Casper CBC research branch to enable a genuinely leaderless PoS consensus. Gorki employs programming principles inherited from Rholang, building composable modules under concurrent settings. Essentially, all software manipulates data in memory, but finding the right compromise between simplicity and efficiency is crucial. Concurrency and composability are the main requirements that software should match in the upcoming decade to fully utilise hardware resources and reach the levels of performance required to facilitate the next generation of decentralised applications. Each of these components and the innovations they unlock are designed to meet specific market needs.

5 Conclusion

The proposed blockchain architecture envisioned for the healthcare sector (fig. 4) aims to be an all-encompassing orchestration layer, crucial for the functioning of a distributed healthcare application. Its capabilities extend to managing extensive data on-chain, ensuring the data's high availability and secure transmission, a critical feature in the context of increasing data volumes from various sources such as the Internet of Medical Things (IoMT). The scalability of this platform is of paramount importance, as it must handle not only large data sets but also provide real computational power. This would be essential for analysing and processing healthcare data in a timely and efficient manner, which is vital for improving patient outcomes and operational processes within healthcare systems. Security is a focal point in this design (fig. 5), featuring fine-grained security models that protect sensitive data while allowing for controlled access as needed. This is particularly important given the sensitive nature of healthcare data and the consequent privacy and security concerns. Interoperability is a cornerstone of this blockchain solution, enabling seamless integration into any existing system without the need for numerous adjunct systems or complex integrations. This minimizes potential attack vectors and creates a more streamlined, efficient, and secure data handling process. By addressing the limitations of traditional blockchain applications in healthcare, such as scalability and the need for additional integrations, this architecture seeks to provide a robust, secure, and efficient platform for decentralized healthcare, facilitating better resource allocation, communication, and ultimately, healthcare outcomes.

References

[1] Odai Enaizan, A. A. Zaidan, N. H. M Alwi, B. B. Zaidan, M. A. Alsalem, O. S. Albahri, and A. S. Albahri. Electronic medical record systems: decision support examination framework for individual, security and privacy concerns using multi-perspective analysis. Health and Technology, 10(3):795–822, May 2020.

[2] Sohail Imran, Tariq Mahmood, Ahsan Morshed, and Timos Sellis. Big data analytics in healthcare A systematic literature review and roadmap for practical implementation. IEEE/CAA Journal of Automatica Sinica, 8(1):1–22, January 2021.

[3] Arjun Panesar. Data. In Arjun Panesar, editor, Machine Learning and AI for Healthcare : Big Data for Improved Health Outcomes, pages 19–62. Apress, Berkeley, CA, 2021.

[4] HealthITSecurity. The Threat of Distributed Denial-Of-Service Attacks in Healthcare, November 2021.

[5] Faisal Jamil, Shabir Ahmad, Naeem Iqbal, and Do-Hyeun Kim. Towards a Remote Monitoring of Patient Vital Signs Based on IoT-Based Blockchain Integrity Management Platforms in Smart Hospitals. Sensors, 20(8):2195, January 2020. Number: 8 Publisher: Multidisciplinary Digital Publishing Institute.

[6] Adusumalli Sai Manoj, Mohammed Ali Hussain, Paleti Surya Teja, Adusumalli Sai Manoj, Mohammed Ali Hussain, and Paleti Surya Teja. Patient

Health Monitoring Using IoT, January 2019. Archive Location: patient-health-monitoring-using-iot ISBN: 9781522580218 Publisher: IGI Global.

[7] Shivansh Kumar, Aman Kumar Bharti, and Ruhul Amin. Decentralized secure storage of medical records using Blockchain and <span style="font-variant:small-caps;">IPFS</span> : A comparative analysis with future directions. SECURITY AND PRIVACY, 4(5):e162, September 2021.

[8] Jayapriya Jayabalan and N. Jeyanthi. Scalable blockchain model using off-chain IPFS storage for healthcare data security and privacy. Journal of Parallel and Distributed Computing, 164:152–167, June 2022.

[9] P. Coorevits, M. Sundgren, G. O. Klein, A. Bahr, B. Claerhout, C. Daniel, M. Dugas, D. Dupont, A. Schmidt, P. Singleton, G. De Moor, and D. Kalra. Electronic health records: new opportunities for clinical research. Journal of internal medicine, 274(6):547–560, 2013. Place: HOBOKEN Publisher: Wiley.

[10] K Hayrinen, K Saranto, and P Nykanen. Definition, structure, content, use and impacts of electronic health records: A review of the research literature. International Journal of Medical Informatics, 77(5):291–304, May 2008.

[11] Ligang Luo, Liping Li, Jiajia Hu, Xiaozhe Wang, Boulin Hou, Tianze Zhang, and Lue Ping Zhao. A hybrid solution for extracting structured medical information from unstructured data in medical records via a double-reading/entry system. BMC medical informatics and decision making, 16(1):114–114, 2016. Place: LONDON Publisher: Springer Nature.

[12] Lacey Colligan, Henry WW Potts, Chelsea T. Finn, and Robert A. Sinkin. Cognitive workload changes for nurses transitioning from a legacy system with paper documentation to a commercial electronic health record. International journal of medical informatics (Shannon, Ireland), 84(7):469–476, 2015. Place: CLARE Publisher: Elsevier Ireland Ltd.

[13] Jaimon T. Kelly, Katrina L. Campbell, Enying Gong, and Paul Scuffham. The Internet of Things: Impact and Implications for Health Care Delivery. Journal of Medical Internet Research, 22(11):e20135, November 2020. Company: Journal of Medical Internet Research Distributor: Journal of Medical Internet Research Institution: Journal of Medical Internet Research Label: Journal of Medical Internet Research Publisher: JMIR Publications Inc., Toronto, Canada.

[14] Roberta Pastorino, Corrado De Vito, Giuseppe Migliara, Katrin Glocker, Ilona Binenbaum, Walter Ricciardi, and Stefania Boccia. Benefits and challenges of Big Data in healthcare: an overview of the European initiatives. The European Journal of Public Health, 29(Suppl 3):23–27, October 2019.

[15] Manal Al-rawashdeh, Pantea Keikhosrokiani, Bahari Belaton, Moatsum Alawida, and Abdalwhab Zwiri. IoT Adoption and Application for Smart Healthcare: A Systematic Review. Sensors (Basel, Switzerland), 22(14):5377, July 2022.

[16] Mohit Kumar, Ashwani Kumar, Sahil Verma, Pronaya Bhattacharya, Deepak Ghimire, Seong-heum Kim, and A. S. M. Sanwar Hosen. Healthcare Internet of Things (H-IoT): Current Trends, Future Prospects, Applications, Challenges, and Security Issues. Electronics, 12(9):2050, January 2023. Number: 9 Publisher: Multidisciplinary Digital Publishing Institute.

[17] Kebira Azbeg, Ouail Ouchetto, and Said Jai Andaloussi. BlockMedCare: A healthcare system based on IoT, Blockchain and IPFS for data management security. Egyptian Informatics Journal, 23(2):329–343, July 2022.

[18] Ammar Battah, Mohammad Madine, Hamad Alzaabi, Ibrar Yaqoob, Khaled Salah, and Raja Jayaraman. Blockchain-based Multi-Party Authorization for Accessing IPFS Encrypted Data. preprint, August 2020.

[19] Rahul Johari, Vivek Kumar, Kalpana Gupta, and Deo Prakash Vidyarthi. BLOSOM: BLOckchain technology for Security Of Medical records. ICT Express, 8(1):56–60, March 2022.

[20] Gautam Srivastava, Jorge Crichigno, and Shalini Dhar. A Light and Secure Healthcare Blockchain for IoT Medical Devices. In 2019 IEEE Canadian Conference of Electrical and Computer Engineering (CCECE), pages 1–5, Edmonton, AB, Canada, May 2019. IEEE.

[21] Hyoeun Ye and Sejin Park. Reliable vehicle data storage using blockchain and ipfs. Electronics (Basel), 10(10):1130–, 2021. Place: Basel Publisher: MDPI AG.

[22] Justice Adeenze-Kangah and Yuting Chen. Detecting Proper SSL/TLS Implementation with Usage Patterns. Journal of Physics: Conference Series, 1176(2):22045–, 2019. Place: Bristol Publisher: IOP Publishing.

[23] S. De Capitani di Vimercati, S. Foresti, S. Jajodia, and P. Samarati. Access Control Policies and Languages in Open Environments. In Ting Yu and Sushil Jajodia, editors, Secure Data Management in Decentralized Systems, Advances in Information Security, pages 21–58. Springer US, Boston, MA, 2007.

[24] Hugo Krawczyk, Kenneth G. Paterson, and Hoeteck Wee. On the Security of the TLS Protocol: A Systematic Analysis. In Advances in Cryptology – CRYPTO 2013, volume 8042 of Lecture Notes in Computer

Science, pages 429–448. Springer Berlin Heidelberg, Berlin, Heidelberg, 2013. ISSN: 0302-9743 Issue: 1.

[25] Adam J. Lee, Kent E. Seamons, Marianne Winslett, and Ting Yu. Automated Trust Negotiation in Open Systems. In Ting Yu and Sushil Jajodia, editors, Secure Data Management in Decentralized Systems, Advances in Information Security, pages 217–258. Springer US, Boston, MA, 2007.

[26] Gary Leeming, John Ainsworth, and David A Clifton. Blockchain in health care: hype, trust, and digital health. The Lancet, 393(10190):2476–2477, June 2019.

[27] Abid Haleem, Mohd Javaid, Ravi Pratap Singh, Rajiv Suman, and Shanay Rab. Blockchain technology applications in healthcare: An overview. International Journal of Intelligent Networks, 2:130–139, January 2021.

[28] Hamed Taherdoost. The Role of Blockchain in Medical Data Sharing. Cryptography, 7(3):36, September 2023. Number: 3 Publisher: Multidisciplinary Digital Publishing Institute.

[29] Deepak Saxena and Jitendra Kumar Verma. Blockchain for public health: Technology, applications, and a case study. In Computational Intelligence and Its Applications in Healthcare, pages 53–61. Elsevier, 2020.

[30] Kithmini Godewatte Arachchige, Philip Branch, and Jason But. Evaluation of Blockchain Networks' Scalability Limitations in Low-Powered Internet of Things (IoT) Sensor Networks. Future Internet, 15(9):317, September 2023.

[31] Endale Mitiku Adere. Blockchain in healthcare and IoT: A systematic literature review. Array, 14:100139, July 2022.

[32] Huma Saeed, Hassaan Malik, Umair Bashir, Aiesha Ahmad, Shafia Riaz, Maheen Ilyas, Wajahat Anwaar Bukhari, and Muhammad Imran Ali Khan. Blockchain technology in healthcare: A systematic review. PLoS ONE, 17(4):e0266462, April 2022.

[33] Deepa Elangovan, Chiau Soon Long, Faizah Safina Bakrin, Ching Siang Tan, Khang Wen Goh, Siang Fei Yeoh, Mei Jun Loy, Zahid Hussain, Kah Seng Lee, Azam Che Idris, and Long Chiau Ming. The Use of Blockchain Technology in the Health Care Sector: Systematic Review. JMIR Medical Informatics, 10(1):e17278, January 2022.

[34] Tim Hulsen. Sharing Is Caring—Data Sharing Initiatives in Healthcare. International Journal of Environmental Research and Public Health, 17(9):3046, May 2020.

[35] Luis B. Elvas, Carlos Serrão, and Joao C. Ferreira. Sharing Health Information Using a Blockchain. Healthcare, 11(2):170, January 2023.

[36] Adenantera Dwicaksono and Ashley M. Fox. Does Decentralization Improve Health System Performance and Outcomes in Low- and Middle-Income Countries? A Systematic Review of Evidence From Quantitative Studies. The Milbank Quarterly, 96(2):323–368, June 2018.

[37] Pranab Bardhan. Decentralization of Governance and Development. Journal of Economic Perspectives, 16(4):185–205, November 2002.

[38] Samuel H. Christie, Lalana Kagal, Alessandro Ricci, and Munindar P. Singh. Decentralized Systems. IEEE internet computing, 26(6):5–6, 2022.

[39] Zeng Chen, Weidong Xu, Bingtao Wang, and Hua Yu. A blockchain-based preserving and sharing system for medical data privacy. Future Generation Computer Systems, 124:338–350, November 2021.

[40] Eric Brewer. CAP twelve years later: How the "rules" have changed. Computer, 45(2):23–29, February 2012.

[41] Gianmaria Del Monte, Diego Pennino, and Maurizio Pizzonia. Scaling Blockchains Without Giving up Decentralization and Security, June 2020. arXiv:2005.06665 [cs].

[42] Damiano Di Francesco Maesa and Paolo Mori. Blockchain 3.0 applications survey. Journal of Parallel and Distributed Computing, 138:99–114, April 2020.

[43] Saha Reno and Md. Mokammel Haque. Solving blockchain trilemma using off-chain storage protocol. IET Information Security, 17(4):681–702, 2023. _eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1049/ise2.12124.

[44] Qiheng Zhou, Huawei Huang, Zibin Zheng, and Jing Bian. Solutions to Scalability of Blockchain: A Survey. IEEE Access, 8:16440–16455, 2020. Conference Name: IEEE Access.

[45] Jia Zhou Edward C. Cheng, Ying Le and Yang Lu. Healthcare services across China – on implementing an extensible universally unique patient identifier system. International Journal of Healthcare Management, 11(3):210–216, 2018. Publisher: Taylor & Francis _eprint: https://doi.org/10.1080/20479700.2017.1398388.

[46] Tien Tuan Anh Dinh, Rui Liu, Meihui Zhang, Gang Chen, Beng Chin Ooi, and Ji Wang. Untangling Blockchain: A Data Processing View of Blockchain Systems. IEEE Transactions on Knowledge and Data Engineering, 30(7):1366–1385, July 2018.

[47] Thomas P. Keenan. Alice in Blockchains: Surprising Security Pitfalls in PoW and PoS Blockchain Systems. In 2017 15th Annual Conference on Privacy, Security and Trust (PST), pages 400–4002, August 2017.

[48] European Union Agency for Network and Information Security. Distributed ledger technology & cybersecurity: improving information security in the financial sector. Publications Office, LU, 2016.

[49] Enrico Denti and Andrea Omicini. An architecture for tuple-based coordination of multi-agent systems. Software, practice & experience, 29(12):1103–1121, 1999. Place: Chichester, UK Publisher: John Wiley & Sons, Ltd.

[50] Howard Bowman. Concurrency Theory Calculi an Automata for Modelling Untimed and Timed Concurrent Systems / by Howard Bowman, Rodolfo Gomez. Springer London, London, 1st ed. 2006. edition, 2006.