

EFFECTIVE LEDGER AND DECENTRALISATION IN HEALTHCARE USING BLOCKCHAIN

DEEPU C¹, KRISHNA P², DINESH K³, GOWRI V⁴

^{1,2,3} UG Scholar, Department of CSE, Kingston College, Vellore-59

⁴ Asst.Professor, Department of CSE, Kingston College, Vellore-59

Abstract - Healthcare block chains provide an innovative way to store healthcare information, execute healthcare transactions, and build trust for sharing health data in a decentralized open health network environment. Although the healthcare block chain technology has attracted broad interests and attention in industry, government and academia, the security and privacy concerns remain the focus of debate when deploying block chains for information sharing in the healthcare sector from business operation to research collaboration. This paper focuses on the security and privacy requirements for medical data sharing using block chain, and provides a comprehensive overview of security and privacy risks and requirements, along with technical solutions techniques. First, we discuss the security and privacy requirements and attributes required for electronic medical data sharing by deploying the healthcare block chain. Second, we categorize existing efforts into three benchmark block chain use cases for electronic medical information sharing and discuss the technologies to execute these security and privacy properties in the three categories of use cases for healthcare block chain, such as anonymous signatures, attribute-based encryption, zero-knowledge proofs, and verification techniques for smart contract. Finally, we discuss other potential block chain application scenarios in healthcare. We conjecture that this survey will help healthcare professionals, decision makers, and healthcare service developers to gain technical and intuitive insights into the security and privacy of healthcare block chains in terms of concepts, risks, requirements, development and deployment technologies and systems.

Key Words: Asymmetric-key algorithm and hash function, SHA-256 algorithm.

1. INTRODUCTION

Warehouse data is more important to deal with stored database; a warehouse can be defined functionally developed in which to store large products or materials (goods) for commercial purposes. The form of archiving developed over time depends on many contexts such as materials, information, sites, cultures, etc. it may have checked and store in a warehouse to prevent the security

problem. Commonly used data was an identifier for each data to easily rectify and retrieve the database record. This is one of the main sections to verify and manage the information needed for login and verify inventory details based on ID and its additional record updates. The scanned QR list may contain all the data about the product it contains all the details about it. It will prevent the attacks from other foreign agents that has been prevented by using this warehouse, the tedious process like data loss, data if there is any discrepancy, the information management will be retrieved when it has been verified with the QR ID, and it will be easy to extract the product counts for each. The purpose and methodologies which achieves the security prevention and easy retrieving of data from the database. Here, preprocess the data which will calculate the records from the database, this model may update the security enhancement and data handling will also become an efficient with the database.

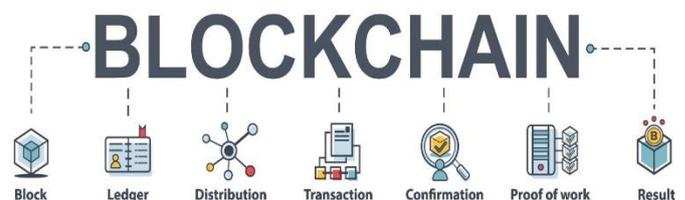


Figure 1: Overview of Block Chain

2. RELATED WORKS

[1] The work done by author, M. A. Engelhardt, "Hitching healthcare to the chain: An introduction to block chain technology in the healthcare sector," Technology Innovation Management Review, vol. 7, pp. 22–34, 10 2017.

Health services must balance patient care with information privacy, access, and completeness. The massive scale of the healthcare industry also amplifies the importance of cost control. The promise of block chain technology in health services, combined with application layers built atop it, is to be a mechanism that provides utmost

privacy while ensuring that appropriate users can easily add to and access a permanent record of information. Block chains, also called distributed ledgers, enable a combination of cost reduction and increased accessibility to information by connecting stakeholders directly without requirements for third-party brokers, potentially giving better results at lower costs. New ventures are looking to apply block chain technology to solve real-world problems, including efforts to track public health, centralize research data, monitor and fulfill prescriptions, lower administrative overheads, and organize patient data from an increasing number of inputs. Here, concrete examples of the application of block chain technology in the health sector are described, touching on near-term promise and challenges.

[2] The work done by author, S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," www.bitcoin.org, 9., 2008.

A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

[3] The work done by author, R. Zhang and L. Liu, "Security models and requirements for healthcare application clouds," in 2010 IEEE 3rd International Conference on Cloud Computing, July 2010, pp. 268–275.

Widespread use of electronic health record (EHR), building a secure EHR sharing environment has attracted a lot of attention in both healthcare industry and academic community. Cloud computing paradigm is one of the popular health IT infrastructure for facilitating EHR sharing and EHR integration. In this paper we discuss important concepts related to EHR sharing and integration in healthcare clouds and analyze the arising security and privacy issues in access and management of EHRs. We describe an EHR security reference model for managing security issues in healthcare clouds, which highlights three important core components in securing an EHR cloud. We illustrate the development of the EHR security reference model through a use-case scenario and describe the corresponding security countermeasures and state of art security techniques that can be applied as basic security guards.

3. PROPOSED SYSTEM

Consecutive case file. Since our patient records are in consecutive order, this provides our doctor with full clarity on the treatment and medications administered to particular cases. On the block chain, all of the patient's medical records, including outpatient, inpatient, and wearable device tests are also automatically updated chronologically ordered.

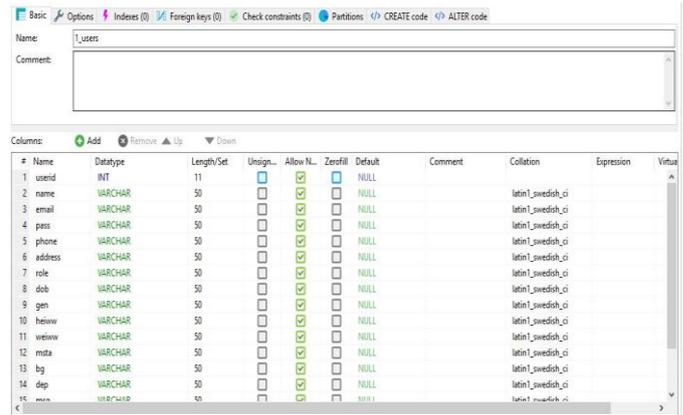
Block chain allows general validation statements where the network commits to implementing the consent and does not require any central authority to participate and manage the entire network. The block chain ensures that the updated information is secure enough that no one can tamper with the security information and our proposed model, ensure that the information verification process is carried out without the authority of the council.

3.1 MODULES DESCRIPTIONS

- 1) Hospital module
- 2) Patient module
- 3) Admin module
- 4) Doctor module

3.1.1 HOSPITAL MODULE

In this module register their details such as hospital name, mobile, email id, password, address for login to the page. If it has registered then the user will login to the module, then it has been redirected to the home page. It has a menu such as doctor, patient list, patient details. In this doctor menu the details of doctors have been updated. In the list of patient has been register in the OP with their details has been collected such as name, date of birth, gender, height, weight, marital status, blood group, department, remarks. Then view the details of patients records.



#	Name	Datatype	Length/Set	Unsign...	Allow N...	Zerofill	Default	Comment	Collation	Expression	Virtual
1	userid	INT	11				NULL		latin1_swedish_ci		
2	name	VARCHAR	50				NULL		latin1_swedish_ci		
3	email	VARCHAR	50				NULL		latin1_swedish_ci		
4	pass	VARCHAR	50				NULL		latin1_swedish_ci		
5	phone	VARCHAR	50				NULL		latin1_swedish_ci		
6	address	VARCHAR	50				NULL		latin1_swedish_ci		
7	role	VARCHAR	50				NULL		latin1_swedish_ci		
8	dob	VARCHAR	50				NULL		latin1_swedish_ci		
9	gen	VARCHAR	50				NULL		latin1_swedish_ci		
10	height	VARCHAR	50				NULL		latin1_swedish_ci		
11	weight	VARCHAR	50				NULL		latin1_swedish_ci		
12	msta	VARCHAR	50				NULL		latin1_swedish_ci		
13	bg	VARCHAR	50				NULL		latin1_swedish_ci		
14	dep	VARCHAR	50				NULL		latin1_swedish_ci		
15		latin1_swedish_ci		

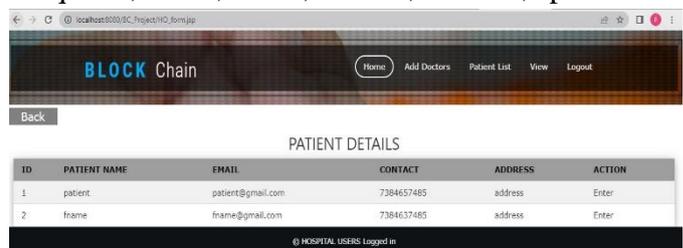
Figure 3: Patients Login Details



Figure 2: Patient Login Form

3.1.2 PATIENT MODULE

In this module patient has register their details such as name, mobile, email id, password, address for login to the page. If it has done successful then they will register their name, date-of-birth, height, gender, weight, blood group, marital status, specialist, description. Once it has registered then they will book the related hospital for their treatment. After that if the registration is done then they will login with valid email and password to make transaction for the required amount of their consultant and they will log out from their page. Those all the details have been stored in the database for the other references.



ID	PATIENT NAME	EMAIL	CONTACT	ADDRESS	ACTION
1	patient	patient@gmail.com	7384657485	address	Enter
2	frame	frame@gmail.com	7384657485	address	Enter

Figure 4: Overview of Patients Details

3.1.4 DOCTOR MODULE

In this module doctor will register their details such as name, mobile, email id, password, address for login to the page. If it has done successful, then it has been redirected to the home page. It contains the booked patients list from the patient module with its patient's unique id, doctor will view the list and add their report with them, by verifying the patient's id, name, and they will select the particular patient report of doctor, if it has been done then the doctor will set the next appointment

date. If the patient is not paid or they will get cured, then admin will able to delete their records from the database.

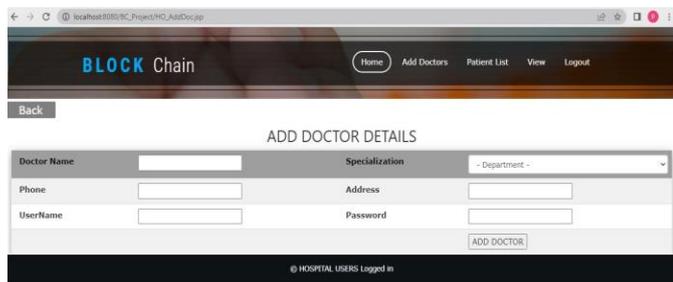


Figure 5: Doctor Details Form

4. ARCHITECTURAL AND DATAFLOW DIGRAM

4.1 SYSTEM ARCHITECTURE

The healthcare zone is one of the maximum crucial domain names that influences the whole international populace and is carefully connected to the improvement of any country. It additionally performs a vital position in how a rustic is perceived in retaining financial stability. The healthcare zone is one of the maximum crucial domain names that influences the whole international populace and is carefully connected to the improvement of any country. It additionally performs a vital position in how a rustic is perceived in retaining financial stability. There have been greater records generated with inside the closing years than for the duration of the entire of human history. It wishes to be processed, stored, and analyzed for use. That is the motive of records collection. It targets to investigate a specific subject matter or vicinity and examine it for making accurate decisions. Updated and correct records can substantially enhance the results, whether or not used for personal, public, or governmental matters. So, block chain powered fitness records change should release the authentic cost of interoperability. Block chain-primarily based totally structures have the ability to lessen or dispose of the friction and prices of present day intermediaries.

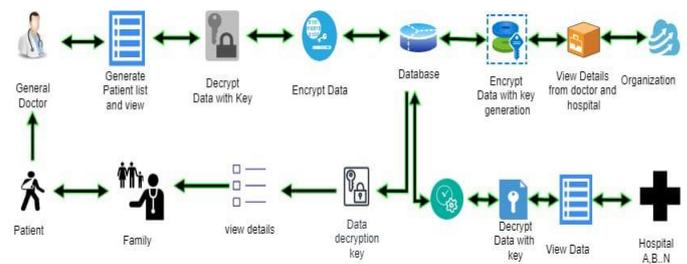


Figure 6: System Architecture

4.2 DATAFLOW DIAGRAM

A statistics go with the drift diagram is a graphical device used to explain and examine the motion of statistics thru a device. These are the significant device and the idea from which the alternative additives are advanced. The transformation of statistics from enter to output thru processing, can be defined logically and independently of bodily additives related to the device. These are called the logical statistics go with the drift diagrams. The bodily statistics go with the drift diagrams display the real implements and motion of statistics among people, departments and workstations. A complete description of a device genuinely includes a hard and fast of statistics go with the drift diagrams. Using acquainted notations Yourdon, Gane and Sarson notation develops the statistics go with the drift diagrams. Each issue in a DFD is categorized with a descriptive name. The method is similarly recognized with a variety of in order to be used for identity reason. The improvement of DFD'S is completed on numerous levels. Each method in decrease stage diagrams may be damaged down right into a greater particular DFD with inside the subsequent stage. The lop-stage diagram is frequently known as context diagram. It consists a unmarried method bit, which performs a important function in reading the present day device. The method with inside the context stage diagram is exploded into every other method at the primary stage DFD. The concept at the back of the explosion of a method into greater method is that know-how at one stage of element is exploded into more element at the following stage. This is

completed till similarly explosion is essential and a good enough quantity of element is defined for analysts to apprehend the method. Larry Constantine first advanced the DFD as a manner of expressing device necessities in a graphical form, this cause the modular layout. A DFD is likewise called a “bubble Chart” has the reason of clarifying device necessities and figuring out fundamental alterations that becomes programmed in device layout. So it's far the place to begin of the layout to the bottom stage of element. A DFD includes a chain of bubbles joined through statistics flows with inside the device.

4.2.1 LEVEL 0

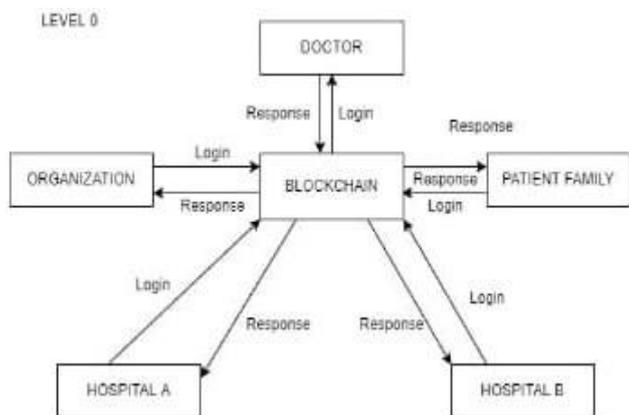


Figure 7: Level 0 Dataflow Diagram

4.2.2 LEVEL 1

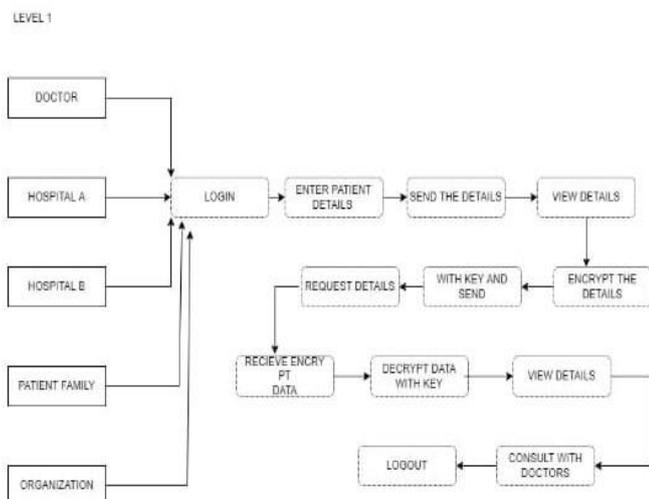


Figure 8: Level 1 Dataflow Diagram

4.2.3 LEVEL 2

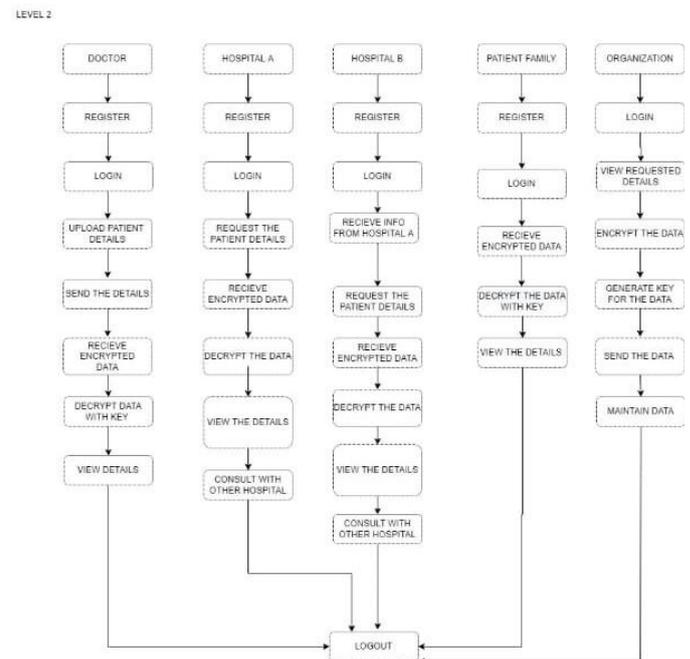


Figure 9: Level 2 Dataflow Diagram

5. OUTPUT SCREENS

5.1 HOME PAGE

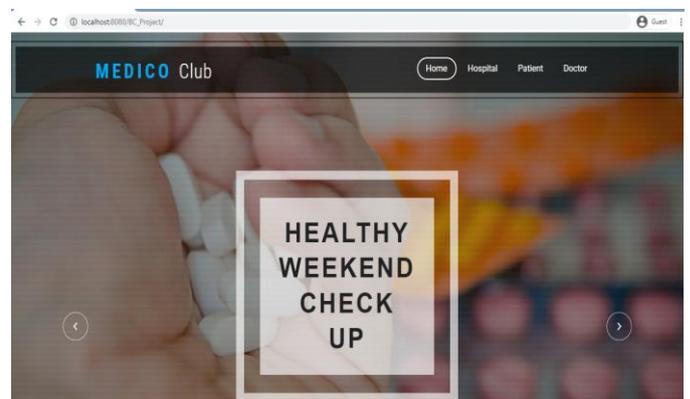


Figure 10: Home screen

5.2 LOGIN PAGE

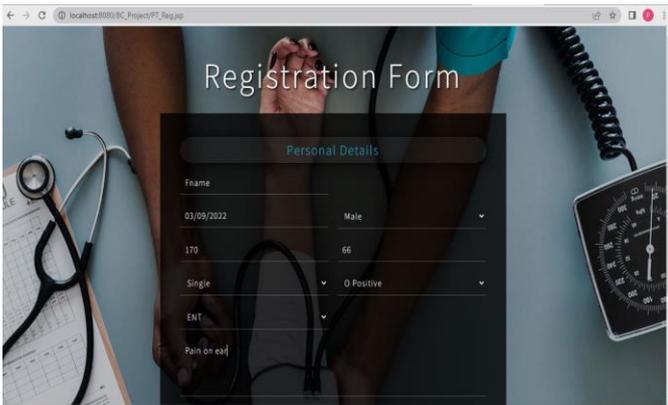


Figure 11: LOGIN PAGE

5.3 DOCTOR DETAILS



Figure 12: DOCTOR INFO. SCREEN

5.4 PATIENT LOGIN



Figure 13: PATIENT LOGIN SCREEN

5.5 PATIENTS DETAILS

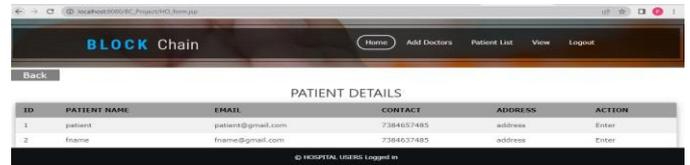


Figure 14: PATIENT DETAILS SCREEN

5.6 DATABASE MANAGEMENT

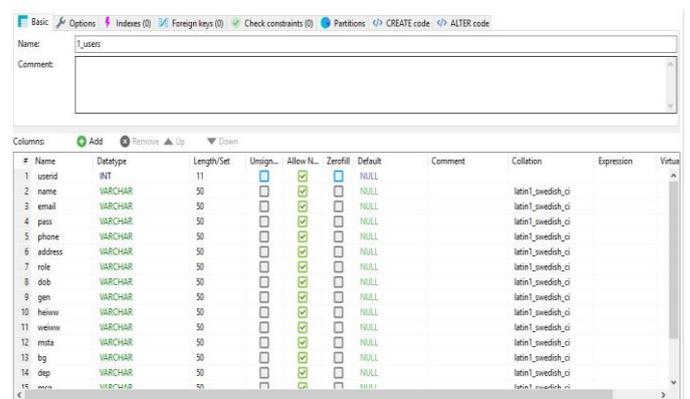


Figure 15: DBMS SCREEN

5.7 HOSPITAL GALLERY

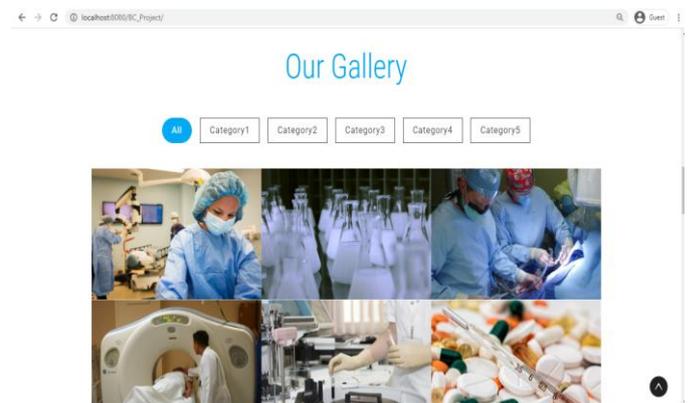


Figure 16: HOSPITAL GALLERY SCREEN

5.8 CARD PAYMENT



Figure 17: PAYMENT SCREEN

6. CONCLUSION

The proposed model combines the advantages of DL and a self-growing shape such that it can extract more effective capabilities in a green manner. Its miles absolutely really well worth noting that the changing method of form length is finished in a developing manner. It has no extra operation of deleting neurons in a learning method, it reduces computational complexity. As a give up result, the mixture and rolling optimization can accumulate higher monitoring manage performances. There isn't any get away from the reality that the want and call for finite and prone water will preserve to increase and so will opposition for it. More uncertainty in water availability, better frequency of severe climate events, and greater speedy go back flows of water to the ecosystem are anticipated with inside the destiny. The functionality of the technique in assessing little volumes inner allowable country areas in facts pushed manner and the simple desired role of without version set evaluation is proven exactly. We moreover constitute how one may want to make use of this method to pick out solvers for no convex development problems through dividing the practicable vicinity of the solvers. In destiny it's been more suitable and implemented with experimented for a powerful wanted situations.

ACKNOWLEDGEMENT

The authors would like to thank Mrs. V. Gowri for his suggestions and excellent guidance throughout the project period

REFERENCES

- [1] M. A. Engelhardt, "Hitching healthcare to the chain: An introduction to block chain technology in the healthcare sector," *Technology Innovation Management Review*, vol. 7, pp. 22–34, 10 2017.
- [2] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *www.bitcoin.org*, 9., 2008.
- [3] R. Zhang and L. Liu, "Security models and requirements for healthcare application clouds," in *2010 IEEE 3rd International Conference on Cloud Computing*, July 2010, pp. 268–275.
- [4] ANSI, "Iso/ts 18308 health informatics-requirements for an electronic health record architecture."
- [5] "Ethereum." [Online]. Available: <https://www.ethereum.org/>
- [6] M. Meingast, T. Roosta, and S. Sastry, "Security and privacy issues with health care information technology," in *2006 International Conference of the IEEE Engineering in Medicine and Biology Society*, Aug 2006, pp. 5453–5458.
- [7] A. Demers, "Epidemic algorithms for replicated database maintenance," *PODC 1987*, 1987.
- [8] D. Johnson, A. Menezes, and S. Vanstone, "The elliptic curve digital signature algorithm (ecdsa)," *International Journal of Information Security*, vol. 1, no. 1, pp. 36–63, Aug 2001.
- [9] A. Narayanan, J. Bonneau, E. Felten, A. Miller, and S. Goldfeder, *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*, 2016.
- [10] M. Bellare, R. Canetti, and H. Krawczyk, "Keying hash functions for message authentication," in *CRYPTO '96*, N. Koblitz, Ed., 1996, pp. 1–15.