International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 08 Issue: 02 | February - 2024 SJIF Rating: 8.176 ISSN: 2582-3930

# Securing Birth Certifications using Block Chain

Khushi Agrawal
*Electronics and Telecommunications Department*
*Sardar Patel Institute of Technology*
Mumbai, India
khushikagrawal@gmail.com

Manan Arora
*Electronics and Telecommunications Department*
*Sardar Patel Institute of Technology*
Mumbai, India
arora.m2611@gmail.com

***Abstract*—In today's digital age, the secure and immutable storage of vital records, such as birth certificates, is of paramount importance. Traditional systems for recording and managing such documents often suffer from vulnerabilities and lack transparency. To address these challenges, we present a web application that leverages blockchain technology to record and manage birth certificates. By utilizing a decentralized and distributed ledger, our application ensures data integrity, transparency, and increased security. This paper outlines the design, implementation, and evaluation of our birth certificate recording system, highlighting its benefits for hospitals, registrars, and individuals.**

***Index Terms*—blockchain, birth certificates, decentralized, smart contract**

## I. Introduction

The recording and verification of birth certificates play a crucial role in establishing legal identities and facilitating various administrative processes. However, the existing paper-based or centralized digital systems for managing birth records present numerous challenges. These include potential data tampering, lack of transparency, and reliance on trust in centralized authorities.

To address these challenges, we propose a novel approach that utilizes blockchain technology to record and manage birth certificates in a decentralized and secure manner. Blockchain, the underlying technology behind cryptocurrencies, offers a distributed and immutable ledger that can provide transparency, data integrity, and tamper-resistance. By leveraging this technology, we aim to revolutionize the process of birth certificate management, introducing a more efficient, secure, and transparent solution.

Our web application employs a smart contract written in Solidity, the programming language for Ethereum, to store and manage birth certificate data. The smart contract is designed to facilitate interactions between different stakeholders involved in the process, including hospitals and registrars. The birth certificate details are collected by the hospital account, which then sends the recorded data to the registrar account for verification. Once the registrar verifies the information, the details are uploaded onto the blockchain, ensuring immutability and accessibility to authorized parties.

In this paper, we present the architecture, design choices, and implementation details of our birth certificate recording application. We discuss the advantages and challenges of employing blockchain technology in this domain and provide an evaluation of our system's performance and security. Furthermore, we discuss the potential impact of our application on enhancing data integrity, privacy, and efficiency in the management of birth certificates.

The remainder of this paper is organized as follows: Sec- tion 2 provides an overview of related work in the field of blockchain-based identity management systems. Section 3 presents the system architecture and design of our birth certificate recording application. Section 4 outlines the implementation details and the technologies employed. Section 5 presents the evaluation of our system, discussing performance metrics and security considerations. Finally, Section 6 concludes the paper with a summary of our contributions and directions for future work.

## II. Related Work

Wide-ranging successful occurrences connected to the misbehavior of certificate authorities have been discovered during the past few decades. A certificate authority (hereby referred to as CA) is a company that verifies identities and uses digital certificates to link them to cryptographic key pairs. Some CAs that were compromised earlier were Comodo and DigiNo-tar. They provided fake certificates to well-known websites like Microsoft and Google in 2011 and 2012 respectively[3][9][10].

This project requires the study of different methods of certificate generation, storage, and authorization. The first method proposed is a tamper-proof birth certificate system that utilizes blockchain technology, cryptography algorithms, and the Inter Planetary File System (IPFS) protocol. This system aims to secure birth records, enable access and sharing with user permission, and provide quick validation and authentication of records.

The second method introduced is the Blockchain-Based Public Key Infrastructure (BB-PKI) certificate management system. It leverages blockchain technology to address vulnerabilities caused by CA misbehavior and impersonation attacks against Registration Authorities (RAs). BB-PKI ensures secure certificate issuance, updates, and revocations while monitoring and preventing misbehavior by RAs and eliminating the single point of failure (SPoF) inherent in traditional PKI systems[3].

The third method is the Notary Based PKI (NBPKI), which presents a new PKI model closer to the real world of handwritten signatures[5]. In NBPKI, end users utilize self-signed

X.509 certificates certified by trusted parties called Notarial Authorities (NAs) to create and verify document signatures. NAs certify the trustworthiness of the user's certificate for specific signatures at particular times.

Additionally, the paper discusses the deployment challenges associated with log-based PKI enhancements and explores the concept of certificate transparency. Certificate transparency aims to reduce incorrectly issued certificates by publicly logging their existence, allowing interested parties to verify their accuracy and detect misissuance[7].

While these methods offer various advantages, they also have disadvantages to consider. For example, the tamper- proof birth certificate system may require user registration, potentially leading to fraud and duplication of certificates. The NBPKI model introduces an additional stage in the verification process, relying on trust between users and NAs. Deployment challenges and the security and data consistency of log servers are concerns with certificate transparency.

By studying these different methods and their implications, this paper contributes to the understanding of certificate generation, storage, and authorization techniques and provides insights into potential solutions for enhancing the security and integrity of certificate management systems.

## III. Proposed System Architecture

In the current system of birth registration, there are two entities that are involved in the process, these are the Hospital and the Registrars. The proposed system aims to build the current infrastructure on blockchain while maintaining the functions and responsibilities of both authorities as they are. The proposed system thus comprises of three types of entities in the blockchain, these are: The Root Certificate Authority, The Registrar, and the Hospital.

### *A. Root Certificate Authority*

The Root CA is responsible for deploying the contract and identifying and assigning Certificate Authorities on the blockchain. The Root CA creates a directory of CAs that are whitelisted by it and maintains a record of the details of the CA. In the case of this project, the Certificate authority isthe Registrar at the Gram Panchayat or any local government body.

### *B. Registrar*

The registrar creates a database of recognized hospitals and PHCs on the blockchain. The registrar will record the details of the hospital and its physical address. Only the recognised hospitals will be allowed to create birth certificates on the blockchain. The parents of the child send a request to registrar to verify the birth details and thus issue the certificate to the child. The details of the child are open to view to the registrar using the birth certificate ID which was generated by the hospital. The registrar, being the Certificate Authority (CA) in the blockchain infrastructure, approves the certificate and signs it with her account address. In case a registrar deems a certificate to be invalid or falsified, it is given the authority to revoke a certificate using the unique ID of the birth certificate.

### *C. Hospital/Primary Health Center*

The recognized hospitals and PHCs are allowed to create birth certificates on the blockchain. The details of the birth are first noted by a registrar-recognized hospital or a PHC. They take the details of the parents' name, address, and baby name. The hospitals then input these details which are then stored on the blockchain and a unique certificate ID is generated. This certificate ID is issued to the parents who then send a request to the registrar to approve the birth certificate of the child.

## IV. Implementation

The programme utilizes a combination of technologies to achieve its functionality. The primary components include the smart contract written in Solidity, the Metamask wallet for account management, PHP for deploying the application on the front end, and HTML and JavaScript for creating web pages and integrating the front end with the smart contract.

The smart contract, written in Solidity, forms the backbone of the application. It defines the data structure and logic for recording and managing birth certificate details on the blockchain. The Solidity smart contract includes functions for collecting and verifying birth certificate data, as well as securely storing the information on the blockchain.

Metamask is employed to provide wallet accounts for the application. It enables users to securely interact with the blockchain and sign transactions. Metamask integrates seamlessly with the web browser, allowing users to manage their accounts, sign transactions, and authorize interactions with the smart contract.

PHP is used for deploying the application on the front end. It facilitates the communication between the user interface and the smart contract. PHP scripts handle user inputs, process data, and interact with the blockchain through the smart contract's functions. This integration enables seamless user experience and efficient data handling.

To create the user interface, HTML and JavaScript are utilized. HTML is used to structure the web pages, while JavaScript provides interactivity and dynamic behavior to enhance the user experience. JavaScript code is responsible for capturing user inputs, triggering transactions, and updating the user interface based on the smart contract's response.

Overall, this combination of technologies creates a comprehensive and user-friendly birth certificate recording application. The Solidity smart contract ensures the secure storage and management of birth certificate data on the blockchain. Metamask enables users to interact with the application securely, while PHP, HTML, and JavaScript provide a seamless front-end experience, allowing users to easily record and verify birth certificate details.

### *A. Structure of the Birth Certificate*

The certificate includes the following:

1) Father Name
2) Mother Name
3) Baby Name
4) Birth Date

5) Birth Time
6) Sex
7) Permanent Address
8) Doctor Name
9) Unique Certificate ID
10) Hospital Address
11) Registrar Verification Check
12) Registrar Address

The last four fields are not user editable and are added to the certificate by the smart contract itself. Therefore a complete digital signature of the birth certificate is produced. Only the Hospitals can add the details given in Figure 2 and the registrar cannot change these details unless there is an exceptional case where the name of the child was not provided at birth. In this case, the registrar can input the name of the child and thereby complete the certificate details.

### *B. Registrar Whitelisting*

The root CA is the authority that will whitelist registrar accounts and thereby give the registrar the privilege to whitelist hospitals, receive data from hospitals, verify said details and upload them on blockchain and create certificates.

### *C. Hospital Whitelisting*

The registrar whitelists hospitals and Public Healthcare Centres that will send the birth details of births taking place at their facilities. In this way, a system is created where the registrar defines its jurisdiction over a certain geographical area or the type of healthcare centres that they choose to verifybirths in. Example: a registrar can choose to either validate certificates from a specific geographical area or the registrar can choose to validate births from only government hospitals and another registrar may choose to validate births from only private hospitals.

The hospital accounts thus whitelisted are responsible for noting the birth details and transferring the same to the assigned registrar.

## V. Result Analysis

This section is based on running the created Decentralised Web-Application through a sample of 10 deployments and creation and verification of a sample size of 100 certificates.

Accordingly, the cost associated with the operation of the Decentralised Web-Application is: Cost of deploying the Decentralised Web-Application is 197,742 wei, registering a hospital and registering a registrar is roughly 276,770 wei each and creating a certificate costs 253,620 wei, and verification of the certificate requires another 257,076 wei.

The total cost for deploying the Decentralised Web-Application, registering a hospital, registering a registrar, creating a certificate, and verifying a certificate is 1,262,978 wei. In terms of Ether, this amounts to 1.21e-12 Ether which equals 0.00000025 INR.

As of the price of Ether at the time of writing, the average cost per certificate, thus, is INR 0.00000010. In 2023, there occurred an estimated 25 million births in India. The cost to issue certificates for all these births is INR 6.25.

The performance of the Decentralised Web-Application has been tested using Remix and Solhint and no security breaches or excessive gas usage has been detected.

## VI. Future Work

For the future enhancement of the Blockchain-based Birth Certificate Application, several key areas have been identified:

1) Implementing Parallel Computing: To increase the throughput and scalability of the application, integrating parallel computing techniques will be explored. This will involve optimizing the blockchain network to process multiple transactions simultaneously, reducing transaction confirmation times, and enhancing the system's ability to serve a larger user base effectively.
2) Storage Optimization using IPFS: To improve data storage efficiency and reduce costs, the application will investigate the use of the InterPlanetary File System (IPFS) for storing birth certificates. IPFS offers a distributed storage solution that could enhance data availability and integrity while ensuring that the system remains scalable and resilient to data loss.
3) Enhanced Security Protocols: Continued research into advanced encryption methods and security protocols will be undertaken to ensure the highest levels of data security and privacy. This includes exploring quantum- resistant encryption techniques to future-proof the sys- tem against emerging threats.
4) User Interface and Experience Improvements: Based on user feedback and usability testing, the application will undergo iterative design improvements to make it more intuitive and accessible for all stakeholders, including parents, hospital staff, and government officials.

These enhancements aim to solidify the Decentralised Web-Application's position as a cutting-edge solution for birth certificate management, addressing current limitations and preparing the system for future challenges and opportunities.

## Acknowledgment

We would like to express our deepest gratitude to Professor Dayanand Ambawade and Professor Bhalchandra Chaudhari for their invaluable guidance, support, and expertise throughout the development of this research project. Their extensive knowledge and insights have been instrumental in shaping our understanding and providing valuable direction.

Professor Dayanand Ambawade's expertise in the field of certificate management systems and blockchain technologyhas been immensely valuable. His mentorship and insightful discussions have greatly contributed to the development of our ideas and the overall quality of this work.

We would also like to extend our heartfelt appreciation to Professor Bhalchandra Chaudhari for their continuous support and encouragement.

We are truly grateful for the time and effort both professors have dedicated to reviewing our work, offering constructive

feedback, and providing guidance at every stage of this project. Their commitment to excellence and their passion for thesubject matter has been truly inspiring.

Finally, we would like to express our sincere appreciationto all individuals who have contributed to this project in any way, whether through discussions, feedback, or support. Your contributions have been invaluable.

## REFERENCES

[1] Zhao, Xiongfei, and Yain-Whar Si. "NFTCert: NFT-based certificates with online payment gateway." In 2021 IEEE International Conference on Blockchain (Blockchain), pp. 538-543. IEEE, 2021.
[2] E. Rescorla, "The Transport Layer Security (TLS) protocol ver- sion 1.3," RFC, vol. 8446, pp. 1–160, 2018. [Online]. Available: https://doi.org/10.17487/RFC8446
[3] A. Garba, Q. Hu, Z. Chen, and M. R. Asghar, "BB-PKI: Blockchain- based public key infrastructure certificate management," in Proc. IEEE 22nd Int. Conf. High Perform. Comput. Commun., IEEE 18th Int. Conf.Smart City, IEEE 6th Int. Conf. Data Sci.Syst. (HPCC/SmartCity/DSS), Dec. 2020, pp. 824–829
[4] M. Hasan, A. Rahman and M. J. Islam, "DistB-CVS: A Distributed Secure Blockchain based Online Certificate Verification System from Bangladesh Perspective," 2020 2nd International Conference on Ad- vanced Information and Communication Technology (ICAICT), 2020, pp. 460-465, doi: 10.1109/ICAICT51780.2020.9333523.
[5] Vigil, M.A.G., Moecke, C.T., Cust´odio, R.F., Volkamer, M. (2013). "The Notary Based PKI" In: De Capitani di Vimercati, S., Mitchell, C. (eds) Public Key Infrastructures, Services, and Applications. EuroPKI 2012. Lecture Notes in Computer Science, vol 7868. Springer, Berlin, Heidelberg.
[6] Okabe, Jun-ichi & Surjit, V., 2012. "Village-Level Birth Records: A Case Study," Review of Agrarian Studies, Foundation for Agrarian Studies, vol. 2(1), July.
[7] A. Langley, E. Kasper, and B. Laurie, "Certificate transparency," IETF, 2013.
[8] G. Wood, "Ethereum: A secure decentralized generalized transaction ledger, Berlin Version," Ethereum Found., Tech. Rep. 61f6d40, 2018.
[9] Comodo fraud incident 2011-03-23. https://www.comodo.com/Comodo-Fraud-Incident-2011-03-23.html, March 2011, last accessed: December 5, 2022.
[10] D. Fisher, "Final report on DigiNotar hack shows total compromise of CA servers," https://threatpost.com/ final-report-diginotar-hack-shows- total-compromise-ca-servers-103112/77170, 2012, last accessed: De- cember 5, 2022.
[11] Google, "What is certificate transparency?" http://www.certificate-transparency.org/what-is-ct, 2013, last accessed: November 25, 2022.
[12] M. Y. Kubilay, M. S. Kiraz, and H. A. Mantar, "CertLedger: A new PKI model with certificate transparency based on blockchain," Computers & Security, 2019.
[13] J. Chen, S. Yao, Q. Yuan, K. He, S. Ji, and R. Du, "Certchain: Public and efficient certificate audit based on blockchain for tls connections,"in IEEE INFOCOM 2018-IEEE Conference on Computer Communica- tions. IEEE, 2018, pp. 2060–2068.