Non-Changeable Document using Blockchain

Rohan Gaikwad[1], Adesh Bhor[2], Yash Bhor[3], Prof. Shubham shelke[4]

Student, Dept. of Computer Engg., Samarth Group of Institutions College of Engineering, Belhe, Maharashtra, India[1-3] Lecturer, Dept. of Computer Engg., Samarth Group of Institutions College of Engineering, Belhe, Maharashtra, India[4]

Abstract - The concept of Non-Changeable Documents (NCDs) using blockchain technology is a pivotal development in ensuring data integrity and security. This paper explores the innovative approach of employing blockchain to create immutable records, guaranteeing the authenticity and integrity of documents. NCDs leverage the decentralization and cryptographic features of blockchain, rendering documents unalterable. Their application spans across various industries, including legal, healthcare, and finance, promising significant advantages in terms of fraud prevention, transparency, and compliance.

This research paper also delves into the technical underpinnings of NCDs, elucidating the cryptographic mechanisms and consensus protocols that safeguard their reliability. By harnessing the decentralized and tamper-proof nature of blockchain, NCDs provide a formidable solution for organizations seeking to safeguard critical data against unauthorized alterations. This transformative potential of Non-Changeable Documents underscores their ability to elevate document security and establish trust in an increasingly interconnected digital landscape. In an era marked by data breaches and concerns over document authenticity, NCDs offer a promising avenue to ensure the integrity and security of sensitive information, reinforcing trust in digital records.

Key Words: Blockchain, Documents, Fraud, Smart Contract, Ethereum Blockchain, Security .

1.INTRODUCTION

In our contemporary digital landscape, the importance of securing and preserving the integrity of critical documents has reached a paramount level. Documents, spanning legal contracts, medical records, financial statements, and a multitude of sensitive data, serve as the bedrock of our interconnected society. Yet, maintaining the authenticity and safeguarding these documents against tampering presents an ongoing challenge, particularly in an environment riddled with cyber threats and data breaches.

Blockchain technology, initially conceived as the foundational framework for cryptocurrencies like Bitcoin, has evolved to present a pioneering solution to this predicament: Non-Changeable Documents (NCDs). These NCDs leverage the disruptive potential of blockchain, ensuring that documents remain impervious to unauthorized alterations and verifiable by any party granted access to the blockchain network.

This paper embarks on an exploration of the NCD concept, aiming to redefine the landscape of sensitive data management and protection. We delve into how blockchain's decentralized and cryptographic characteristics can be effectively employed to engender truly non-changeable documents. By delving into the technical underpinnings and practical applications of NCDs, our objective is to elucidate the transformative capabilities of this technology in fortifying document security and instilling trust in a digital-centric world where the reliance on electronic record-keeping is on a perpetual rise.

2. RELATED WORK

When our system produces data, it goes through a robust process to ensure security and accuracy. This document has been assigned a persistent data (NCD) token, which is a 15-character identifier designed to record sensitive data. The composition of the NCD token has been carefully designed: the first 6 characters represent the original organization or company, the next 2 characters represent the type, and the last 7 characters represent the paper unique identification number. This systematic tokenization is necessary to create a security and authentication mechanism for all data in the system.

Once tokenized, the file and the associated NCD token will start moving to the appropriate and secure location. The system uses smart contracts, which are self-executing contracts where the contract terms are written directly into the program code. This smart contract acts as the guardian of data integrity and is an integral part of the blockchain network. Data files feature encryption technology that uses cryptography to increase the confidentiality and immutability of data. This encrypted data and the NCD token are then immutably stored on the blockchain. Blockchain is known for its distribution and tamper-proofing, ensuring that data maintains its integrity throughout its lifecycle.

To facilitate access or authentication, external entities seeking access to specific information initiate requests via smart contracts. Smart contracts act as gatekeepers and then trigger confirmation requests from data subjects, usually via email communication. This authorization model adds an additional layer of security, ensuring that data access is only allowed when authorized by the data owner. Once permission is granted, the smart contract dynamically creates a one-time access policy for the requesting organization. This single sign-on increases data security by limiting exposure and misuse. Additionally, to promote transparency and accountability, NCD carefully collects information about organizations accessing or analyzing data. This historical access data is an important tool for analysis and analysis, allowing the system to detect and prevent illegal or suspicious activity.

NCD Main Content:

Code 15 Code Code: Each document is assigned a u nique code, making identification and tracking easi er.
Secure Blockchain Storage: Use the security feature s of Blockchain to protect data.
Temporary Access Rights: Increase information sec urity by temporarily authorizing and controlling acc ess to the organization's requests.
Access History: Collect and store detailed informati on about an organization accessing or analyzing inf ormation for security purposes.
Crime Fighting Data Generation: Use unique NCD token and blockchain transfer to prevent fraud**.**

3. CONCLUSIONS

The introduction of Non-Changeable Documents (NCDs) through the integration of blockchain technology represents a significant breakthrough in the pursuit of data integrity and document security within our digital era. In an environment where information and records are increasingly digitized, the vulnerabilities associated with data tampering and fraudulent activities have become more pronounced than ever. NCDs, as elucidated in this paper, present an effective solution to these pressing challenges.

Through the utilization of blockchain's decentralized and cryptographic features, NCDs ensure the preservation of documents in an immutable and trustworthy state. The potential applications of NCDs extend across various sectors, encompassing fields such as law, healthcare, finance, and many more, where the assurance of document authenticity and non-alteration is paramount.

By dissecting the technical aspects of NCDs, we have unveiled the inner workings of this technology, shedding light on the cryptographic mechanisms and consensus protocols that form the foundation of its reliability. This research substantiates that NCDs can serve as a robust and dependable system for safeguarding critical data against unauthorized modifications, thereby reinforcing confidence in the realm of digital record-keeping.

As we navigate an era characterized by digital transformation and an increasing dependence on electronic records, NCDs offer a promising avenue to protect the integrity and security of sensitive information. With NCDs, we possess a transformative tool that not only secures data but also instills trust in the authenticity and immutability of digital documents, addressing the paramount needs of our contemporary digital landscape.

ACKNOWLEDGEMENT

The culmination of this research paper, titled "Non-Changeable Document using Blockchain," has been a collaborative effort that relied on the support and contributions of numerous individuals and resources. We express our sincere gratitude to those who have played a role, both direct and indirect, in the development of this work.

Foremost, we extend our appreciation to our academic mentors, for their unwavering guidance, valuable insights, and constant encouragement during the course of this research. Their expertise and mentorship have been instrumental in shaping the direction and quality of this study.

We are also indebted to the individuals who generously participated and shared their expertise, providing critical perspectives and data through interviews, surveys, and discussions, enriching the real-world dimension of this research.

We acknowledge the extensive resources and support offered by [University/Institution Name], as well as the diligent assistance provided by its library staff. Their contributions facilitated access to the essential literature and data sources integral to this research.

Our heartfelt gratitude goes to our friends and family, whose unwavering support and understanding have been a source of motivation throughout this journey.

Lastly, we acknowledge the wider academic and scientific community for their collective efforts in advancing the field of blockchain technology and document security, upon which this research builds.

It is important to note that any errors or omissions within this paper are the sole responsibility of the authors.

We extend our thanks to all those who have contributed to the successful completion of this research endeavor.

REFERENCES

[1] Daniel Benalcazar , Synthetic ID Card Image Generation for Improving Presentation Attack Detection, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL.18,2023, pp.1814-1824,
DOI: https://doi.org/10.1109/TIFS.2023.3255585

[2] TAHMID HASAN PRANTO, KAZI TAMZID AKHTER MD. HASIB1, TAHSINUR RAHMAN , AKM BAHALUL HAQUE , A. K. M. NAJMUL ISLAM AND RASHEDUR M. RAHMAN , Blockchain and Machine Learning for Fraud Detection: A Privacy-Preserving and Adaptive Incentive-Based Approach,IEEE RESEARCH 2022, pp,87115-87134,
DOI:10.1109/ACCESS.2022.3198956

[3] HAGER SALEH, ABDULLAH ALHARBI AND SAEED HAMOOD ALSAMHI , Optimized Convolutional Neural Network for Fake News Detection,IEEE 2021,pp.129471-129489,
DOI:10.1109/ACCESS.2021.3112806 .

[4] PENG KANG, WENZHONG YANG , AND TIANTIAN DING, Blockchain Document Forwarding and Proof Method Based on NDN Network.

IEEE Research 2022, pp. 75312-75322,
DOI: 10.1109/ACCESS.2022.3178992 .

[5] SHINYA HAGA AND KAZUMASA OMOTE, Blockchain-Based Autonomous Notarization System Using National eID Card, IEEE Research 2022,pp.87477-87489,
DOI: 10.1109/ACCESS.2022.3199744.