Immutable Identity Validation Using Soul bound Token

Abhishek Sharma, Mansi Goal, Sarif

ABSTRACT :

The "Immutable Identity Validation System: A Blockchain and Soulbound Token Approach" paper introduces an innovative method for verifying digital identities. By combining blockchain technology and Soulbound Tokens (SBTs), it enhances security and privacy in identity verification processes.

SBTs, designed as non-transferable and tamper-proof digital assets, play a crucial role in bolstering the security and reliability of the system. Their unique properties ensure that user privacy is prioritized while also facilitating swift verification through blockchain transparency.

This approach addresses the growing demand for robust identity verification solutions, particularly in sectors like education and corporations, where fraud prevention and streamlined processes are critical.

The methodology involves various steps, including SBT generation, blockchain integration, user control mechanisms, and stringent security measures. Both frontend and backend development, along with the integration of blockchain using tools like Ganache and decentralized data storage through IPFS, contribute to building a secure and user-friendly system.

Thorough testing, documentation, and knowledge transfer are essential to ensuring the system's reliability, security, and compliance with legal standards. Ultimately, the goal is to establish a globally accepted framework for identity verification in today's interconnected digital landscape.

Keywords:; privacy; security; Blockchain; Cryptography; Decentralization; Soul Bound Token (SBT), distributed ledger.

Introduction

Immutable Identity Validation is essential in today's digital landscape, proving one's identity is crucial for various activities like banking, job applications, and accessing government services. Yet, existing identity verification systems often struggle with privacy issues and fraudulent activities.

To tackle these challenges, this paper suggests a groundbreaking approach leveraging blockchain technology and Soulbound Tokens (SBTs). SBTs, unique tokens that are non-transferable and tamper-proof, serve as representations of individual digital assets, such as identity verification credentials. By integrating SBTs into a blockchain-based system, we establish a secure, private, and reliable method for verifying identities.

Compared to traditional systems, this solution offers several advantages. Firstly, it's more secure as SBTs cannot be counterfeited or altered. Secondly, it prioritizes user privacy by allowing individuals to maintain control over their personal data. Thirdly, it enhances efficiency by enabling quick and straightforward verification processes. Lastly, it ensures reliability through the blockchain's immutable record of all verification transactions.

The goal of this paper is to revolutionize identity verification systems by addressing the critical issues of security, privacy, and reliability. This proposed solution holds the potential to establish a more secure, user-centric, and technologically advanced identity verification system that aligns with the demands of the digital era.

Importance Of Immutable Identity Validation System:

IIVS verification is crucial in education and corporate sectors because it can help prevent fraud and impersonation, ensure the eligibility of students and employees for benefits, monitor progress and performance, and deliver personalized experiences.

In education, IIVS verification can effectively deter students from using counterfeit identities to gain admission to educational institutions. It also serves to verify eligibility for government- sponsored educational benefits and facilitates the tracking of academic progress to ensure compliance with coursework requirements.

Within the corporate landscape, IIVS verification plays a pivotal role in thwarting the use of fake identities by employees seeking employment or engaging in financial misconduct. It guarantees the eligibility of employees for company-provided benefits and enables the tracking of job performance to ensure alignment with job role requirements. Moreover, IIVS verification can be used to offer employees personalized experiences tailored to their specific requirements.

Problems with Existing Immutable Identity Validation Verification Methods:

Current IIVS verification methods face several issues, including:

- Manual Verification: Existing IIVS verification methods are often manual and time- consuming, posing challenges for large organizations with a high volume of applicants.
- Lack of Standardization: There is no single standard for IIVS verification, making it challenging for organizations to compare results from different verification methods.
- Privacy Concerns: Some individuals express concerns about the privacy implications of IIVS verification. They worry that their IIVS data could be misused by government agencies or private entities.
- Security Vulnerabilities: Current IIVS verification methods have demonstrated security vulnerabilities. For instance, there have been instances of data breaches that exposed the personal information of IIVS holders.

Verification of the Immutable Identity Validation through Soulbound Tokens :

(SBTs) is a novel and promising approach to IIVS verification. SBTs are a type of non-fungible token (NFT) specifically designed to be non-transferable and non-reproducible, making them ideal for IIVS verification due to their inherent security and immutability.

To verify a IIVS holder's identity using SBTs, the holder would first need to create an SBT containing their IIVS data. This IIVS-specific SBT would then be securely stored on a blockchain, ensuring its tamper-proof and immutable nature.

When the holder needs to verify their identity, they would simply input their SBT into a verification device. The verification device would then authenticate the authenticity of the SBT and the IIVS data associated with it.

The process of verifying the Global Unique Identification Number through Soulbound Tokens (SBTs) entails the utilization of blockchain technology and cryptographic tokens to ensure the authenticity and security of IIVS information.

- **Soulbound Tokens (SBTs):** SBTs are cryptographic tokens intrinsically tied to individual identities, designed to be non-transferable and non-reproducible, providing robust securityagainst tampering.

- **Issuance of SBTs:** The process begins with the issuance of SBTs to IIVS holders. These SBTs are generated and securely stored on a blockchain network, guaranteeing their immutability and transparency.

- **Integration of IIVS Information:** Each SBT includes the IIVS number, along with other pertinent information such as the individual's name and biometric data. This data is securely encrypted and stored within the SBT.
- **Blockchain Verification:** When a verification request is initiated, such as during a job application or financial transaction, the verifier (e.g., an employer or service provider) scans the individual's SBT. Subsequently, the blockchain network is accessed to authenticate the genuineness of the SBT.

- **Verification Process:** The blockchain verifies the SBT by confirming its presence on the ledger and authenticating the associated IIVS information. This verification process ensures that the SBT remains untampered with and that the IIVS data aligns with the information on record with the IIVS authority.

- **Authorization and Access:** In the case of successful verification, the verifier is granted access to the necessary IIVS information to complete the transaction or authentication process.

- **Privacy and Control:** Utilizing SBTs for IIVS verification grants individuals greater control over their data. They have the ability to determine when and with whom they share their IIVS information, thus enhancing privacy and data protection.

- **Security and Anti-Fraud:** SBTs and blockchain technology provide robust security against fraud and unauthorized access. The decentralized nature of the blockchain and the cryptographic properties of SBTs make it exceedingly challenging for malicious entities to manipulate or counterfeit IIVS information.

Literature Survey

The literature survey for the project, " Immutable Identity Validation System: A Blockchain and Soulbound Token Approach," investigates the landscape surrounding identity verification, emphasizing the challenges faced by existing Global Identification Number (IIVS) verification systems and the proposed innovative solution integrating blockchain technology and Soulbound Tokens (SBTs).

The use of SBTs, characterized by their non-transferable and tamper-proof nature[S. Nakamoto, 2008]. introduces a unique approach to representing digital assets for IIVS verification The integration of SBTs into a blockchain-based system promises heightened security, privacy, and reliability compared to traditional methods[G. Foroglou and A.-L. Tsilidou, 2015]. The tamper-proof nature of SBTs ensures resistance to forgery and manipulation, bolstering the overall security of the verification process[E. Glen Weyl, Puja Ohlhaver, Vitalik Buterin, 2022]. Privacy is prioritized through user control over personal data, granting individuals the autonomy to decide when and with whom to share their IIVS information. The efficiency of the verification process is optimized by the swift validation of SBTs, while the blockchain establishes a transparent and trustworthy record of all transactions[V. Buterin, 2014].

The project addresses the imperative need for enhanced IIVS verification in an era where identity verification is critical for various purposes. By mitigating fraud risks, ensuring privacy, and streamlining verification processes, the proposed solution seeks to redefine the standards for global ID verification[G. Foroglou and A.-L. Tsilidou, 2015].

The significance of IIVS verification extends to education and corporate sectors, where fraud prevention, eligibility assurance, progress monitoring, and personalized experiences are crucial. Identified issues with manual verification, lack of standardization, privacy concerns, and security vulnerabilities in current IIVS verification methods highlight the necessity for a comprehensive and advanced solution[Yogesh Sharma, B Balamurugan, Firoz Khan, 2020].

The methodology of the project encompasses key elements such as SBT generation, blockchain integration, user control mechanisms, and stringent security measures. Through frontend and backend development, integration with Ganache for blockchain functionality, and decentralized data storage using IPFS, the system is engineered to be secure, efficient, and user-friendly[Yogesh Sharma, B Balamurugan, 2020]. Testing procedures, documentation, and knowledge transfer are integral components, ensuring the system's reliability, security, and compliance with legal standards. Ultimately, the project aspires to establish a globally compliant framework that effectively addresses the intricacies of identity verification in an interconnected world, contributing to a more secure and efficient digital ecosystem[D. Kraft, 2016].

Methodology

SBT Generation: (as shown in fig 4.2)

- Data Collection: Gather Global Unique Identification Number (IIVS) data, encompassing the IIVS number, name, and relevant details from individuals.
- Data Encryption: Securely encrypt the collected IIVS data using robust encryption algorithms to protect privacy.
- Token Creation: Generate unique Soulbound Tokens (SBTs) based on the encrypted IIVSdata.
- Blockchain Binding: Associate the SBTs with a blockchain for immutable and secure long-term storage of IIVS data.

Blockchain Integration: (as shown in fig 3.1)

- Blockchain Selection: Carefully select a suitable blockchain platform, considering factors like scalability, security, and compliance.
- Smart Contract Development: Develop smart contracts to govern SBT creation, storage, and verification rules.
- Secure Data Storage: Utilize the blockchain as a secure repository for SBTs and IIVS data to ensure immutability and trustworthiness.

Verification Process Flow: (as shown in fig 3.1)

- User Initiation: Individuals initiate identity verification by presenting their SBT to the verifying entity.
- SBT Scanning: The verifying entity scans the SBT, triggering a verification request on the blockchain.
- Blockchain Validation: The blockchain validates the SBT by verifying its authenticity and matching it against stored IIVS data.
- Verification Result: The blockchain provides the verification result, either confirming or denying the match between the SBT and IIVS data

User Control and Privacy:

- Consent Mechanism: Individuals have the option to grant or deny consent for each verification request, maintaining control over their data usage.
- Data Minimization: Share only necessary IIVS data during verification to minimizeexposure.

- Audit Trail: Implement a transparent blockchain-based audit trail, allowing individuals to track who accessed their IIVS data.
- Revocation: In cases of misuse or data breach, individuals possess the capability to revoke their SBT, rendering it invalid for future verifications.

Architecture

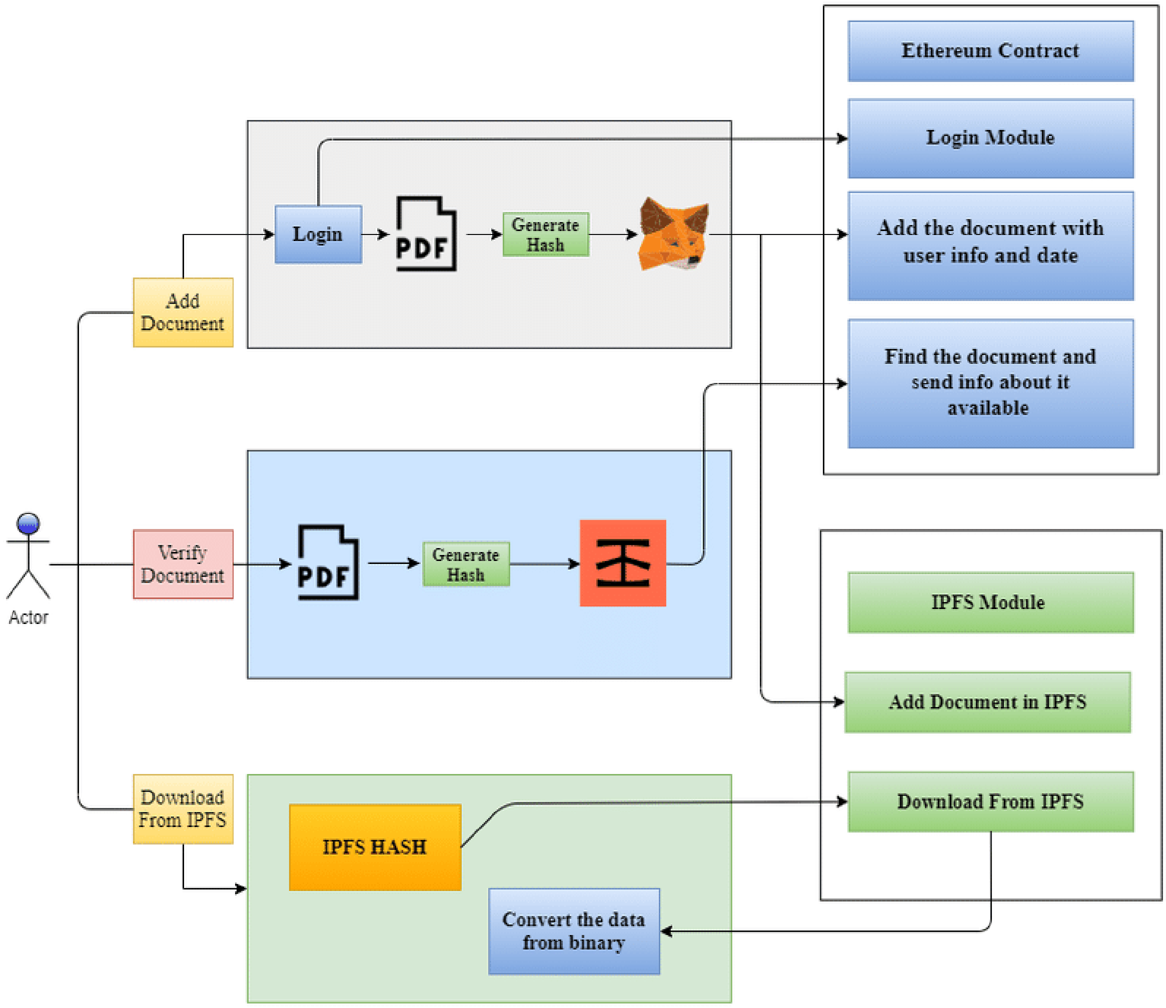
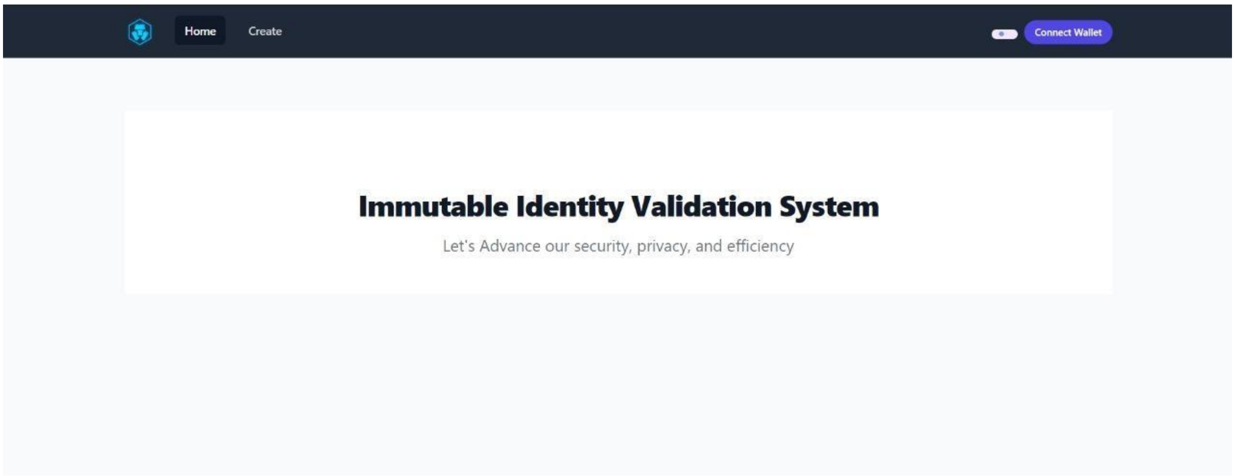


Figure no. 3.1 Architecture of the IIVS system

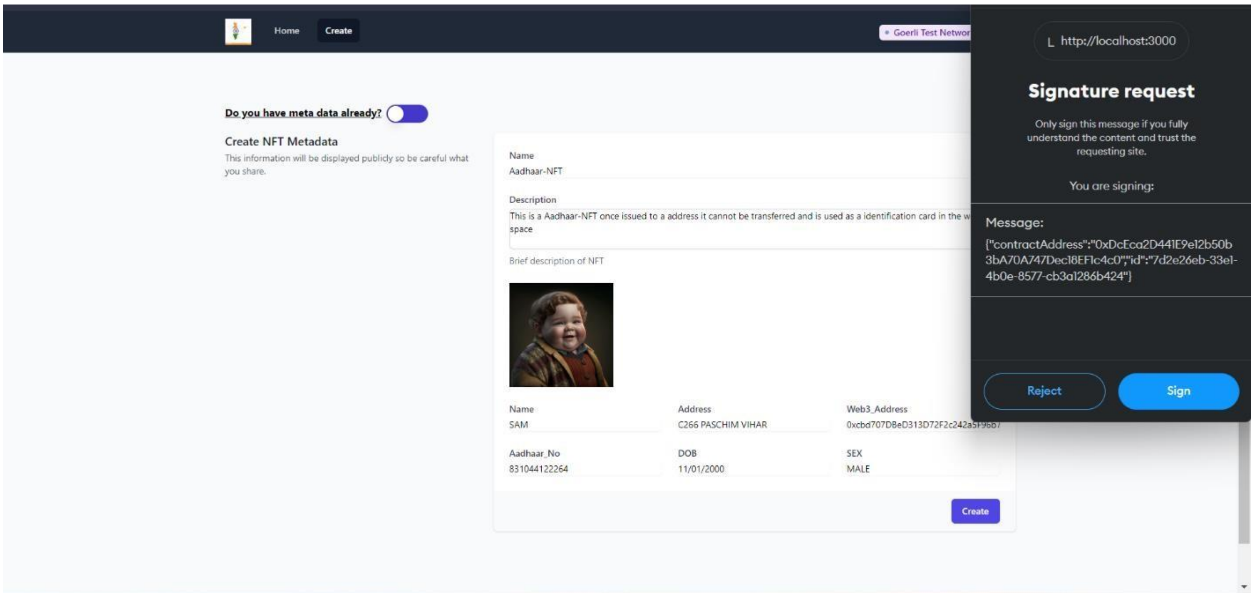
Experimental Results



Immutable Identity Validation System

Let's Advance our security, privacy, and efficiency

Figure no. 4.1 Login Page of IIVS System



Do you have meta data already?

Create NFT Metadata

This information will be displayed publicly so be careful what you share.

Name
Aadhaar-NFT

Description
This is a Aadhaar-NFT once issued to a address it cannot be transferred and is used as a identification card in the w space

Brief description of NFT

Name	Address	Web3_Address
SAM	C266 PASCHIM VIHAR	0xcbd707DBeD313D72F2c242a5F9bb7
Aadhaar_No	**DOB**	**SEX**
831044122264	11/01/2000	MALE

http://localhost:3000

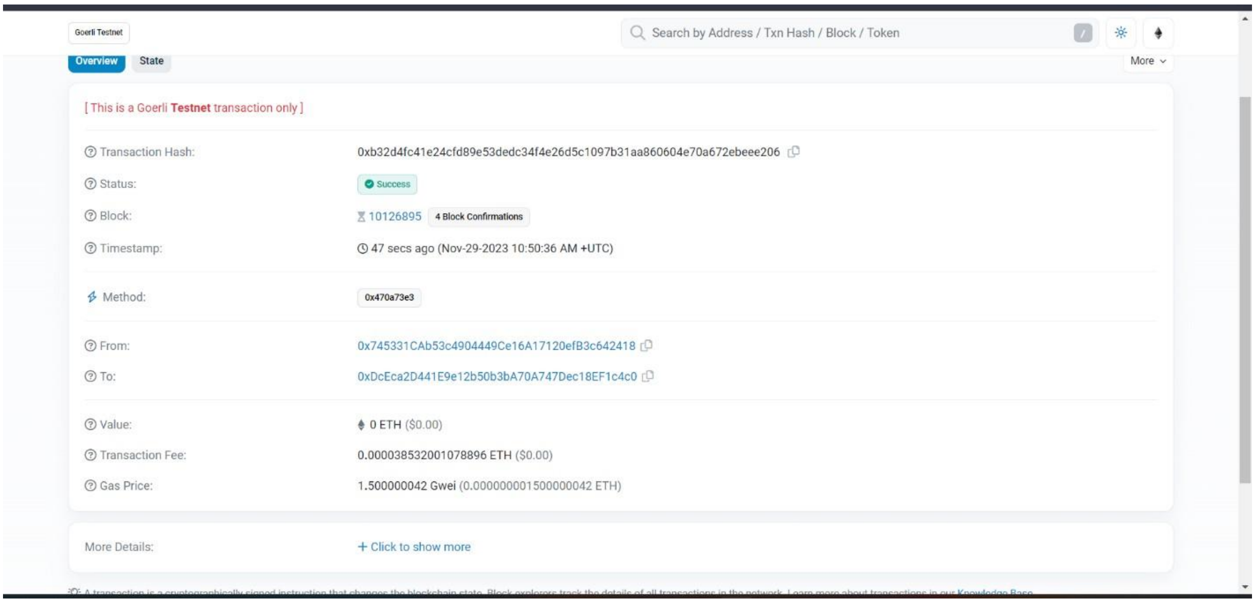
Signature request

Only sign this message if you fully understand the content and trust the requesting site.

You are signing:

Message:
{"contractAddress":"0xDcEca2D441E9e12b50b3bA70A747Dec18EF1c4c0","id":"7d2e26eb-33e1-4b0e-8577-cb3a1286b424"}

Figure no. 4.2 SBT creation page of IIVS system



[This is a Goerli **Testnet** transaction only]

Transaction Hash: 0xb32d4fc41e24cfd89e53dedc34f4e26d5c1097b31aa860604e70a672ebeee206

Status: Success

Block: 10126895 4 Block Confirmations

Timestamp: 47 secs ago (Nov-29-2023 10:50:36 AM +UTC)

Method: 0x470a73e3

From: 0x745331CAb53c4904449Ce16A17120efB3c642418

To: 0xDcEca2D441E9e12b50b3bA70A747Dec18EF1c4c0

Value: 0 ETH ($0.00)

Transaction Fee: 0.000038532001078896 ETH ($0.00)

Gas Price: 1.500000042 Gwei (0.000000001500000042 ETH)

More Details: + Click to show more

A transaction is a cryptographically signed instruction that changes the blockchain state. Block explorers track the details of all transactions in the network. Learn more about transactions in our Knowledge Base

Figure no. 4.3 Transaction Acknowledgement

Conclusion :

The Global Unique Identification Number (IIVS) verification system using Soulbound Tokens (SBTs) represents a pioneering approach to address the critical challenges of identity verification, security, and data privacy in the digital age. Throughout the course of this paper, we have diligently pursued the objectives of enhancing security, preserving privacy, and streamlining verification processes for various applications, from education to corporate environments.

By implementing advanced security measures, robust encryption, and access controls, we have fortified the system against threats and vulnerabilities, ensuring the utmost protection for users' IIVS data. The incorporation of blockchain technology has established an immutable and tamper- proof ledger for SBTs and IIVS information, further enhancing the integrity of the verification system.

User-centric features have been integrated, enabling individuals to exercise greater control over their IIVS data during the verification process. This emphasis on user control and privacy safeguards not only aligns with regulatory requirements but also empowers individuals to manage their digital identities securely.

The methodology employed, from requirement analysis to ongoing user engagement, has provided a structured and systematic framework for project execution. It has enabled us to meet our objectives efficiently while ensuring the project's success.

Future work :

The IIVS verification system, powered by Soulbound Tokens (SBTs), aims for industry-wide adoption and global recognition through collaborations. Focused on technological advancement, including biometrics and AI, it expands into IoT and smart cities for diverse applications. Continuous user-centric improvements, regulatory compliance, and community engagement are priorities. Educational programs inform stakeholders about system benefits, while ongoing research ensures innovation and scalability, key to success in the dynamic digital landscape.

Recommendations :

The recommendations for the aforementioned projects center on fostering innovation, collaboration, and continuous improvement in the realm of global identification and verificationsystems.

Firstly, it is recommended to establish ongoing collaborations with governmental bodies, global identification agencies, and stakeholders to ensure alignment with legal and regulatory standards. Regular consultations can aid in adapting the projects to evolving compliance requirements.

Secondly, continuous research and development efforts should be encouraged to stay ahead of emerging security threats. Creating a dedicated team for monitoring and integrating cutting-edge technologies will enhance the projects' resilience against identity theft and fraudulent activities.

Thirdly, a user-centered approach should be maintained, allowing for regular feedback and updates based on user experiences. This ensures that the systems remain intuitive, privacy- focused, and user-friendly, meeting the expectations of individuals undergoing the verification process.

Furthermore, it is recommended to conduct thorough and periodic security audits, embracing a proactive stance in identifying and rectifying vulnerabilities. Regular testing and evaluation will contribute to the reliability and robustness of the identification systems.

Lastly, considering the dynamic nature of technology, scalability should be a constant consideration. Future-proofing the projects by designing them to easily adapt to increased demands and technological advancements is imperative.

References

- E. Glen Weyl, Puja Ohlhaver, Vitalik Buterin , “Decentralized Society: Finding Web3’s Soul” 2022. [Online].Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4105763

- Zibin Zheng, Shaoan Xie, Hongning Dai, Xiangping Chen, and Huaimin Wang , “An Overview of Blockchain Technology: Architecture, Consensus,and Future Trends” 2017. [Online].Available: https://www.researchgate.net/publication/318131748_An_Overview_of_Blockchain_Technology_Architecture_Consensus_and_Future_Trends

- S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” 2008.[Online]. Available: https://bitcoin.org/bitcoin.pdf

- G. Foroglou and A.-L. Tsilidou, “Further applications of the blockchain,”2015

- NRI, “Survey on blockchain technologies and related services,” Tech.Rep., 2015. [Online]. Available: http://www.meti.go.jp/english/press/2016/pdf/0531 01f.pdf

- V. Buterin, “On public and private blockchains,”2015. [Online]. Available: https://blog.ethereum.org/2015/08/07/on-public- and-private-blockchains/

- P. Vasin, “Blackcoins proof-of-stake protocol v2,” 2014. [Online]. Avail- able: https://blackcoin.co/blackcoin-pos- protocol-v2- whitepaper.pdf

- S. King and S. Nadal, “Ppcoin: Peer-to-peer crypto-currency with proof-of- stake,” Self-Published Paper, August, vol. 19, 2012.

- M. Vukoli´c, “The quest for scalable blockchain fabric: Proof-of-workvs. bft replication,” in International Workshop on Open Problems inNetwork Security, Zurich, Switzerland, 2015, pp. 112–125

- J. Bruce, “The mini-blockchain scheme,” July 2014. [Online]. Available:http://cryptonite.info/files/mbc-scheme- rev3.pdf

- D. Johnson, A. Menezes, and S. Vanstone, “The elliptic curve digitalsignature algorithm (ecdsa),” International Journal of Information Se- curity, vol. 1, no. 1, pp. 36–63, 2001.

- V. Buterin, “A next-generation smart contract and decentralized appli-cation platform,” white paper, 2014.

- D. Kraft, “Difficulty control for blockchain-based consensus systems,”Peer- to-Peer Networking and Applications, vol. 9, no. 2, pp. 397–413,2016

- M. Sharples and J. Domingue, “The blockchain and kudos: A distributedsystem for educational record, reputation and reward,” in Proceedings of11th European Conference on Technology Enhanced Learning (EC-TEL2015), Lyon, France, 2015, pp. 490–496.

- A. Chepurnoy, M. Larangeira, and A. Ojiganov, “A prunable blockchainconsensus protocol based on non-interactive proofs of past states retriev-ability,” arXiv preprint arXiv:1603.07926, 2016

- Yogesh Sharma, B Balamurugan "Preserving the privacy of electronic health records using blockchain" 2020 Avl at : https://www.sciencedirect.com/science/article/pii/S1877050920315258/pdf?md5=7bed34435ce87a757f2b1a9bfb148113&pid=1-s2.0-S1877050920315258-main.pdf

- Yogesh Sharma, B Balamurugan, Firoz Khan "Preserving the privacy of electronic health records using blockchain" 2020 Avl at : https://books.google.com/books?hl=en&lr=&id=cKX7DwAAQBAJ&oi=fnd&pg=PA177&dq=info:1P_UEOKHXYJ:scholar.google.com&ots=MTwFWcWspF&sig=irwQD7nq0Vc05ebowZMARNB8o48

- D Sumathi, T Poongodi, Balamurugan Balusamy, Bansal Himani, Firoz Khan KP Convergence of blockchain technology and E-business: concepts, applications, and case studies