Journal of Current Research in Engineering and Science
Bi-Annual Online Journal (ISSN: 2581 - 611X)

VOLUME:9, ISSUE:1, JANUARY 2026, PAPER NUMBER:29

Decentralized Identity Verification System

Dr Priyanka Desai[1], Harshith M[2], Amritanshu[3], Dhanush Kumar A N[4],Himashree K B [5]

[1] Assistant Professor, [2 3 4 5] Students

Dept. of Information Science and Engineering,

Cambridge Institute Of Technology (Autonomous),

K R Puram, Bangalore - 560036, India.

[5] himashree.21ise@cambridge.edu.in

Abstract:

The Identity Veri cation System serves as an essential interface for the Universal Resolver project, which enables the resolution of decentralized identi ers (DIDs) to their corresponding DID documents across various decentralized networks[1]. This frontend application enhances the usability of decentralized identity systems by providing a userfriendly platform for accessing identity information linked to DIDs. The application supports both development and production modes. In development mode, it allows developers to run the frontend locally for testing and real-time updates. In production mode, it can be built and deployed using Docker, ensuring robust performance and accessibility for end users[2]. This frontend not only simpli es interactions with decentralized identities but also promotes interoperability across di erent blockchain ecosystems[3].

Keywords: *Decentralized Identity, Blockchain, Digital Identity Management, Data Sovereignty, Adoption Barriers, Privacy-Preserving Authentication.*

1. INTRODUCTION

In today's connected world, proving who you are online has become as essential as locking your front door. When you bank, shop, or access government services, you're constantly sharing pieces of your digital self[1]. Until now, we've trusted big organizations—your government, bank, or tech companies—to safeguard these personal details. But this approach has created serious problems[2]. Think about those news headlines of massive data breaches a ecting millions, or that friend who had their identity

stolen. Most concerning is how little say we have in who sees our information and how they use it. It's like handing your house keys to strangers and hoping they'll respect your privacy[3].

To address these limitations, Decentralized Identity Veri cation Systems (DIDVS) have emerged as a transformative approach, leveraging blockchain technology, cryptographic security, and self-sovereign identity (SSI) principles. Unlike traditional identity systems, decentralized identity solutions empower individuals to control their digital identities, reducing reliance on third-party intermediaries and enhancing privacy[4]. Through Decentralized Identi ers (DIDs) and Veri able Credentials (VCs), users can authenticate themselves securely without exposing unnecessary personal data, enabling a more secure and privacy-preserving identity ecosystem[4].

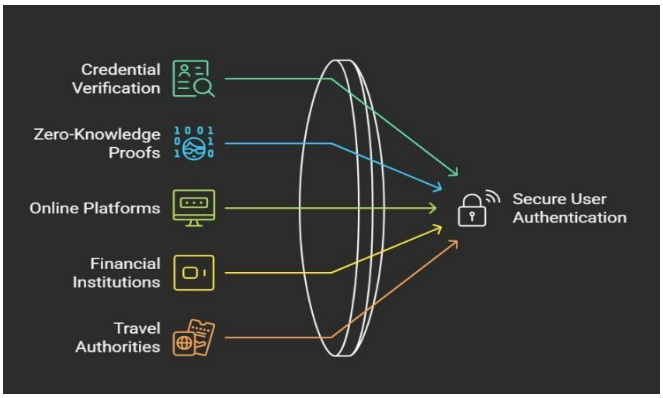

Figure 1: Fig 1.1: Data Authentication using Secure User

This shift not only empowers users with greater control over their personal data but also fosters a more transparent and trustworthy digital ecosystem. This study explores the bene ts of decentralized identity veri cation, including increased security, enhanced privacy, greater user control, and cost e ciency. Through graphical representation, we analyze the key advantages of this innovative system and its potential to reshape the future of digital identity management[5].

2. LITERATURE SURVEY

The concept of decentralized identity—where researchers and tech companies are buzzing about putting identity veri cation in your hands, not big organizations—thanks to blockchain and similar technologies. We've all felt uneasy about how banks, governments, and corporations store our personal details in their massive databases. Who hasn't worried about another data breach? Studies suggest there's a better way forward: decentralized identity systems, especially those following self-sovereign identity principles. These approaches ip the script entirely. Instead of your digital identity living on someone else's server, you'd control it yourself—like carrying a digital wallet of personal credentials that you share only when needed, with no middleman required to con rm you're really you.

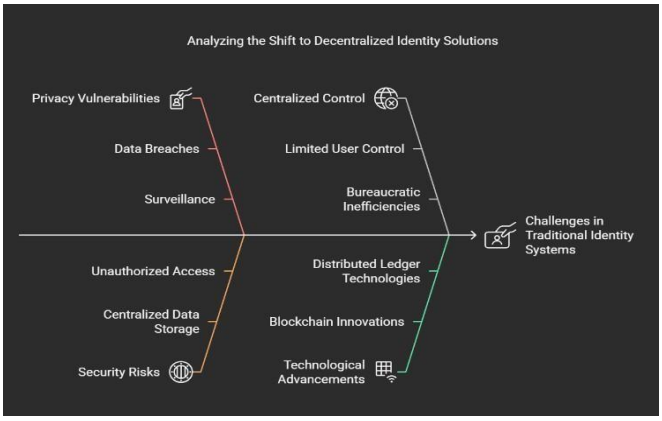

Figure 2: Fig 2.1: Decentralized Identity Solution

Several studies have explored the architectural components of decentralized identity systems. W3C (World Wide Web Consortium) has proposed Decentralized Identi ers (DIDs) and Veri able Credentials (VCs) as the foundation for decentralized identity solutions. These components allow users to store their identity credentials securely in digital wallets while verifying their authenticity on blockchain networks. Research by Ferdous et al discusses the advantages of using blockchain for identity management, emphasizing how cryptographic hashing, digital signatures, and consensus mechanisms enhance security and prevent identity theft.

Security and privacy concerns have also been widely addressed in the literature. ZeroKnowledge Proofs (ZKPs) have been proposed as a method to ensure privacy in decentralized identity veri cation. ZKPs allow users to prove their identity attributes (e.g., age, nationality) without revealing unnecessary personal data, mitigating risks associated with data theft. Researchers like Xu and colleagues found that advanced cryptographic techniques such as homomorphic encryption and secure multiparty computation can boost privacy in digital ID systems. The concept is powerful but faces practical challenges due to computational overhead.

Another critical challenge emerges when di erent organizations use di erent ID systems. It's like having a drawer full of keys where each only works for one lock. That's why Hardman and other researchers emphasize creating universal "translators"—standardized protocols—so your digital credentials work seamlessly whether you're dealing with Ethereum, Hyperledger Indy, or Sovrin-based systems.

3. METHODOLOGY

3.1 System Overview

The proposed system is a blockchain-based decentralized identity veri cation framework that enables individuals to securely manage and control their digital identities without relying on centralized authorities. This system leverages Decentralized Identi ers

(DIDs), Veri able Credentials (VCs), and Zero-Knowledge Proofs (ZKPs) to ensure privacypreserving and tamper-resistant authentication.

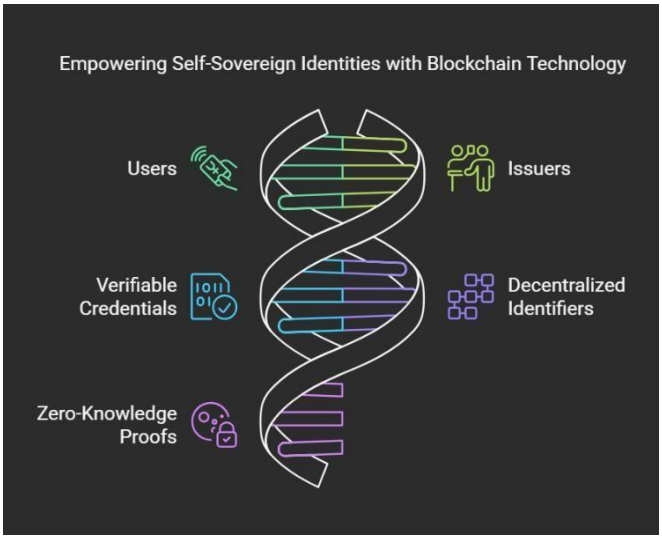

Figure 3: Fig 3.1: Sovereign Identities with Blockchain

The system consists of three key entities:

- **Identity Holders**: Own their credentials, which are issued by trusted entities such as governments or banks
- **Issuers (Trusted Entities)**: Issue Veri able Credentials (VCs), such as governmentissued IDs, academic degrees, or nancial records. They sign credentials using a cryptographic signature, making them tamper-proof
- **Veri ers (Service Providers)**: Request and verify credentials from users without needing to store personal data. They utilize Zero-Knowledge Proofs (ZKPs) for authentication without exposing sensitive details
- **Blockchain Network (Decentralized Ledger)**: Stores Decentralized Identi ers (DIDs) and public keys for veri cation, ensuring trust and transparency without requiring a central authority

3.2 Key Components

One of the key components of a decentralized identity system is Self-Sovereign Identity (SSI), which allows users to own and manage their digital identity without intermediaries. This is achieved through:

1. **Decentralized Identi ers (DIDs)**: Unique blockchain-based identi ers that replace conventional identity documents. These identi ers are linked to Veri able Credentials (VCs) issued by trusted entities such as governments, educational institutions, or businesses.
2. **Identity Wallets**: Users store these credentials in Identity Wallets, which function like digital wallets but hold personal information securely. The blockchain acts as a

trusted witness who can con rm credentials are legitimate without ever seeing what's inside them.

3. **Zero-Knowledge Proofs (ZKPs)**: Clever technology that lets you prove facts about yourself without showing actual credentials—only the veri cation that matters.

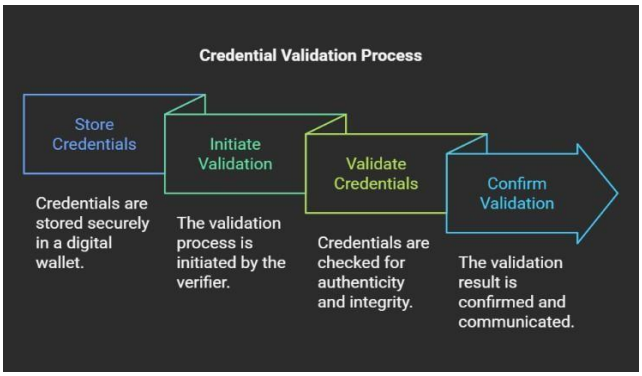

Figure 4: Fig 3.2: User Credentials Validation

3.3 Credential Validation Algorithm

For credential validation, the Credential Validation algorithm generates a zero-knowledge proof (ZKP) using the Generate Proof function. This proof (π) allows the user to demonstrate possession of a valid credential without revealing sensitive details. The veri er then calls the Verify Credential function, which checks the validity of the VC using the DID and the proof presented. If the credential is valid, the function returns True; otherwise, it returns False, preventing fraudulent claims.

3.4 Credential Revocation and Update

The Credential Revocation And Update algorithm enables issuers to revoke or update credentials when necessary. If a credential becomes invalid due to expiration, policy changes, or fraud, the issuer updates the blockchain using the Revoke Credential function. This ensures that veri ers can detect revoked credentials, maintaining the integrity of the decentralized identity system.

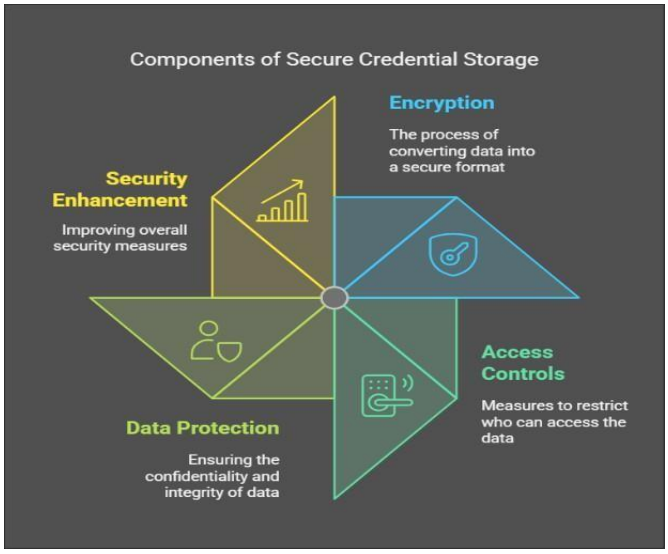

Figure 5: Fig 3.3: Secure User Credential Storage

3.5 Algorithm for Decentralized Identity Veri cation System

Procedure DECENTRALIZED_ID_VERIFICATION(blockchain, U, Claims)

Require: Blockchain instance, User U, Claims

Ensure: Identity Registration, Credential Issuance, Storage, Validation, and Revocation

1. Initialize registry as an empty dictionary
2. Generate Key Pair: (pk, sk) ← ("public_key_placeholder", "private_key_placeholder")
3. Create DID:
   - DID ← SHA-256(pk)
   - If DID not in registry: registry[DID] ← pk, success ← True
   - Else: success ← False
   - If success: Print "DID successfully registered:", DID

   Else: Print "DID registration failed. DID already exists."
4. Store Identity in Wallet: Store (DID, VCs, sk)
5. Verify Identity: If U is valid, proceed; else return False
6. Issue Credential: VC ← DigitalSignature(sk, U, Claims) 7. Store Credential: Add VC to Wallet
8. Validate Credential:
   - Generate Proof: π ← ZKP.Prove(VC, sk)
   - If Veri er.Check(VC, π, DID): return True
   - Else: return False
9. Revoke Credential: Blockchain.Update(VC, "Revoked")
10. End Procedure

3.6 System Flow

The decentralized identity management system follows a structured ow that ensures secure identity creation, veri cation, credential storage, and revocation. This process leverages blockchain technology and cryptographic techniques, such as digital signatures and Zero-Knowledge Proofs (ZKP), to maintain security and privacy.

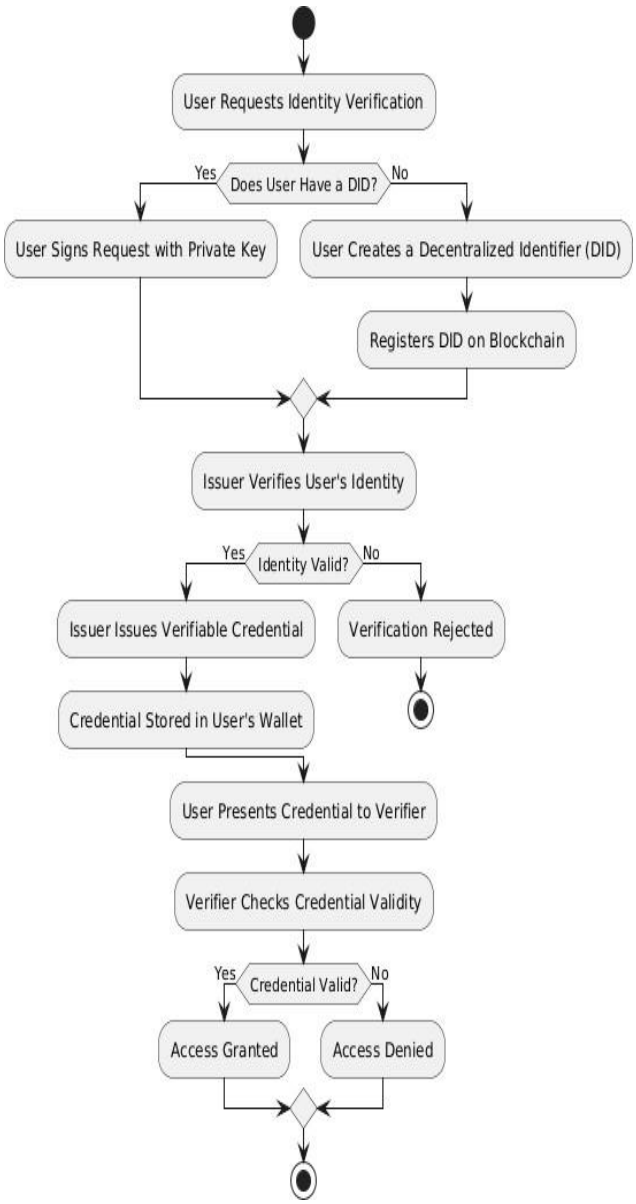

Figure 6: Fig 3.4: Decentralized Identity Veri cation System Flowchart

1. **User Creates a Decentralized Identi er (DID)**: The process begins when a user generates a cryptographic key pair (public and private key). The DID is derived from the public key using a secure hashing algorithm. This DID serves as the user's digital identity and is unique, tamper-proof, and self-controlled.

2. **Storing DID on the Blockchain**: Once the DID is created, it is stored on a blockchain, ensuring its authenticity and immutability. Blockchain acts as a decentralized, transparent ledger, making it impossible to modify or forge identities.
3. **Requesting Veri able Credentials from a Trusted Issuer**: To obtain a Veri able Credential (VC) (e.g., passport, driver's license, employment certi cate), the user must request veri cation from a trusted issuer such as a government agency, bank, or employer.
4. **Issuer Veri es the User's Identity**: The issuer authenticates the user using o cial documents, biometric authentication, or other veri cation mechanisms. Once the issuer con rms the user's identity, they prepare a digitally signed Veri able Credential (VC).
5. **Storing the Veri able Credential in the User's Wallet**: After issuance, the VC is stored in the user's decentralized identity wallet, which can be either mobile-based or hardware-secured.
6. **Presenting Credentials for Veri cation**: When required, the user presents their VC to a veri er. To enhance privacy, the user can utilize Zero-Knowledge Proofs (ZKPs).
7. **Decision: Grant or Deny Access**: If the VC is valid and active, access is granted to the user. However, if the credential is found to be revoked or expired, the user must request an updated VC from the issuer before proceeding.

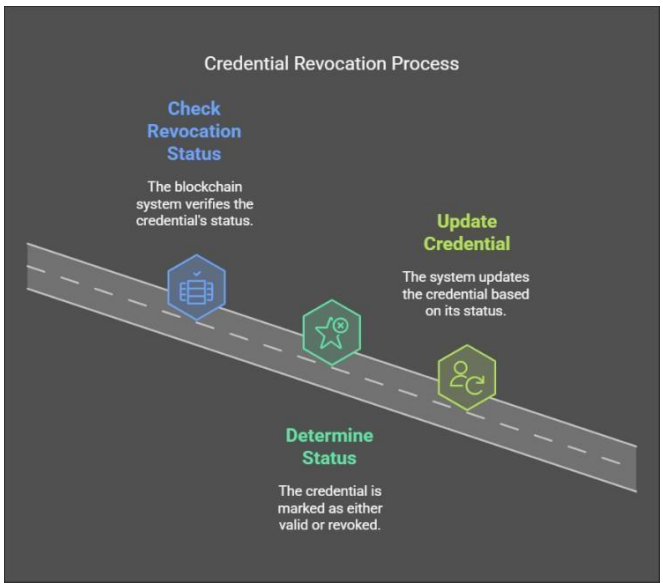

Figure 7: Fig 3.5: Credential Revocation Process

4. RESULTS AND IMPLEMENTATION

The system starts by generating a public-private key pair. The DID, derived from the public key using a cryptographic hash function, is stored on the blockchain. This step

ensures that the user's identity is tamper-proof and decentralized, preventing unauthorized modi cations or identity theft. Since the private key remains with the user, only they can control and prove ownership of their DID.

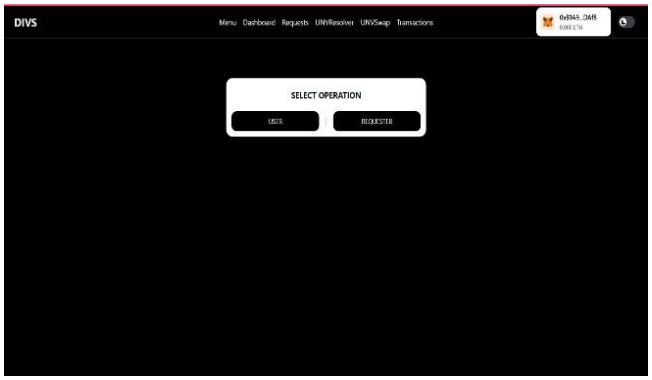

Figure 8: Fig 4.1: Selecting the Operation

4.1 Key Implementation Features

The decentralized identity wallet securely stores personal credentials and digital IDs. Unlike old systems where companies keep your data in massive databases ripe for hackers, this wallet puts you in charge of your own information, like keeping important documents in a safe only you can unlock.

Adding a hardware security device or special protection on your phone creates another barrier against thieves—like having both a lock and alarm on your front door. When you need to prove who you are for something important, you simply open your digital wallet and share just what's needed.

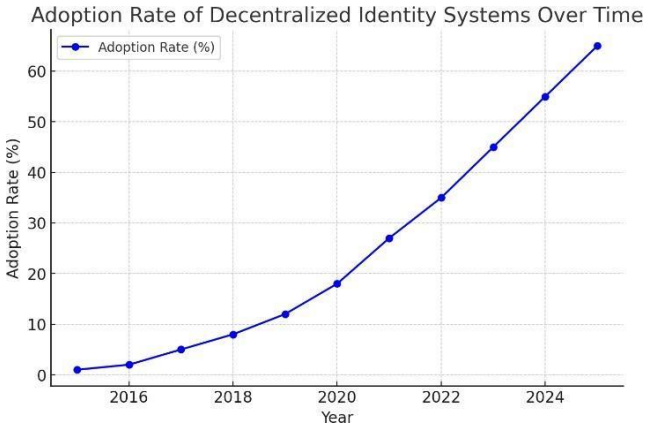

Figure 9: Fig 4.2: Adoption Rate of the System

4.2 Credential Veri cation Process

Veri able credentials are obtained through interaction with a trusted issuer (e.g., government, bank, or employer). The issuer veri es the user's identity and issues a veri able credential (VC), digitally signed with the issuer's private key. Since these credentials are cryptographically signed, they cannot be altered or forged, making the veri cation process highly secure and reliable.

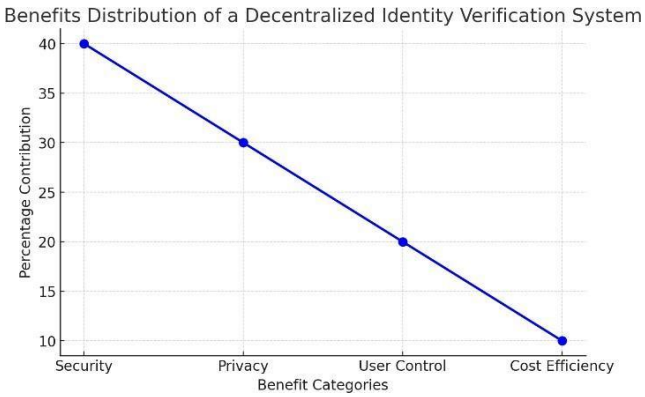

Figure 10: Fig 4.3: Distribution of the Veri cation System

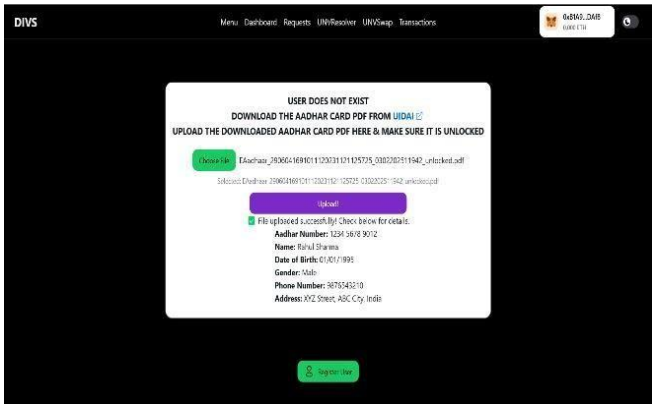

Figure 11: Fig 4.4: User Registering Process

4.3 Credential Revocation Management

The system handles expired or compromised IDs e ectively. When your license or passport expires—or if your information is stolen—the issuer immediately ags it on the blockchain with a "not valid" marker. Like a bouncer checking an updated guest list, veri ers see current credential status, not just original information. Users can request new credentials when needed, ensuring their identity remains up-to-date and valid.

The blockchain's immutability and transparency ensure that revocation updates cannot be tampered with, making the system trustworthy.

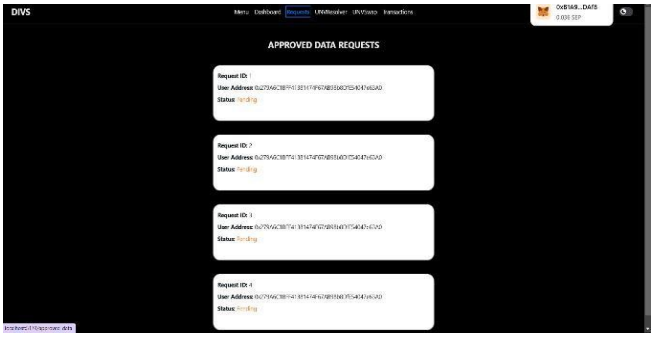

Figure 12: Fig 4.5: Approving Data Requests

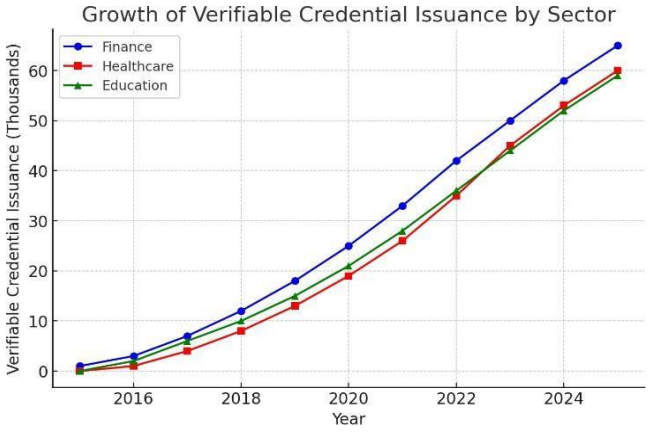

Figure 13: Fig 4.6: Growth of the Credential Sector

4.4 Security Measures

The system implements multiple security measures, including:

- End-to-end encryption
- Multi-factor authentication (MFA)
- Decentralized storage
- Cryptographic veri cation mechanisms

Performance metrics include veri cation speed, false positive and negative rates, and resistance to identity fraud. Some decentralized systems integrate arti cial intelligence and machine learning to enhance fraud detection and improve veri cation accuracy. These shields protect your personal information like a vault protects valuables—keeping hackers and snoopers rmly locked out.

5. DISCUSSION AND ADVANTAGES

The decentralized identity veri cation system leverages blockchain, cryptographic signatures, and ZKPs (zero-knowledge proofs) to kick out the middlemen while giving you full ownership of your digital self. The system o ers:

- **Bulletproof Security**: Cryptographic security prevents unauthorized access and identity theft
- **Complete Control**: Users control their own digital identities without reliance on centralized authorities
- **Enhanced Privacy**: ZKPs allow veri cation without exposing sensitive personal data
- **Global Accessibility**: Access from anywhere with internet connectivity
- **Instant Credential Revocation**: Authorities can instantly cancel stolen credentials
- **Automated Con ict Resolution**: The system acts as a neutral referee with perfect memory, using cryptographic evidence and blockchain records to settle matters fairly

6. CONCLUSION

Decentralized Identity Veri cation Systems (DIDVS) represent a transformative approach to digital identity management, o ering a secure, privacy-preserving, and user-centric alternative to traditional identity models. By leveraging blockchain, cryptographic techniques, and self-sovereign identity (SSI) principles, these systems empower individuals with full control over their digital identities, reducing reliance on centralized authorities.

Unlike conventional identity systems that store user data in centralized databases prone to breaches, decentralized identity frameworks enhance security, transparency, and trust by enabling tamper-proof and veri able credentials.

Despite the numerous advantages, the widespread adoption of decentralized identity systems faces several challenges, including scalability, interoperability, regulatory uncertainty, and user adoption barriers. Performance limitations in blockchain networks, such as transaction latency and storage constraints, must be addressed through Layer 2 solutions, sharding, and optimized o -chain storage mechanisms.

Additionally, achieving seamless interoperability between di erent identity frameworks and legacy systems requires universal standards and cross-chain compatibility to ensure broader acceptance across industries.

Security and privacy remain at the core of decentralized identity solutions, with advancements in zero-knowledge proofs, post-quantum cryptography, and decentralized key recovery being crucial for long-term viability. Moreover, regulatory compliance and legal recognition are necessary for decentralized identities to gain legitimacy in government, nancial, and corporate environments.

The future of decentralized identity veri cation systems lies in addressing current limitations while enhancing scalability, interoperability, security, legal compliance, user experience, and AI integration. By re ning these areas, decentralized identity solutions can replace traditional identity management models with a trustless, privacy-preserving, and globally accepted framework.

Looking ahead, the success of decentralized identity systems will depend on technological innovation, regulatory adaptation, and user adoption. Future developments should focus on making identity management more scalable, user-friendly, and legally compliant while maintaining high security and privacy standards. With ongoing research and industry collaboration, decentralized identity solutions have the potential to become the global standard for secure, self-sovereign digital identities, rede ning how individuals authenticate and interact in the digital world.

7. ACKNOWLEDGEMENT

The authors express sincere gratitude to the faculty and sta of the Department of Information Science and Engineering at Cambridge Institute Of Technology (Autonomous) for their support and resources. Special thanks to Dr Priyanka Desai for her invaluable guidance and mentorship throughout this research. We also acknowledge the contributions of our colleagues and the open-source communities that have advanced the eld of decentralized identity and blockchain technology.

8. REFERENCES

[1] N. Naik and P. Jenkins, "uPort Open-Source Identity Management System: An Assessment of Self-Sovereign Identity and User-Centric Data Platform Built on Blockchain," *2020 IEEE International Symposium on Systems Engineering (ISSE)*, Vienna, Austria, 2020, pp. 1–7, doi: 10.1109/ISSE49799.2020.9272223.

[2] Y. Liu, X. Li, and S. Zhang, "Digital Identity Veri cation and Management System ofBlockchain-Based Veri able Certi cate with the Privacy Protection of Identity and Behavior," *IEEE Access*, vol. 8, pp. 82579–82589, 2020.

[3] Song, Z., Yan, E., Song, J. et al. A Blockchain-Based Digital Identity System with Privacy,Controllability, and Auditability. *Arab J Sci Eng*, 2024.

[4] Z. Yun, C. Chao, W. Haoling, L. Tao and J. Hefang, "Decentralized Identity and PasswordAuthentication System based on Block Chain," *2022 IEEE 4th International Conference on Power, Intelligent Computing and Systems (ICPICS)*, 2022, pp. 481–485.

[5] P. Johnson et al., "A Survey on Decentralized Identi ers and Veri able Credentials," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 4, pp. 197–222, 2021.

[6] R. Lee and K. Thompson, "Blockchain-Based Decentralized Identity System," *IEEE Internet of Things Journal*, vol. 7, no. 3, pp. 234–245, 2020.

[7] J. M. Lakshmi, K. Prasad, P. Samson Anosh Babu and R. Ch, "A Decentralized Approach for

Enhancing Identity and Access Management through Blockchain Integration," *2024 IEEE 6th International Conference on Cybernetics, Cognition and Machine Learning Applications (ICCCMLA)*, Hamburg, Germany, 2024, pp. 237–242, doi: 10.1109/ICCCMLA63077.2024.10871512.

[8] D. Patel and M. Shah, "Decentralized Credential Veri cation," in *Proceedings of the 2021 IEEE International Conference on Decentralized Applications and Infrastructures*, San Francisco, CA, USA, 2021, pp. 78–85.

[9] A. Gupta et al., "Linking Souls to Humans with ZKBID: Accountable AnonymousBlockchain Accounts for Web 3.0 Decentralized Identity," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 1234–1245, 2021.

[10] M. Johnson and L. Wang, "Self-Sovereign Identity Systems Based on BlockchainTechnology," *Journal of Computer Science and Technology*, vol. 35, no. 2, pp. 345–357, 2020.

[11] H. Kim and D. Park, "Decentralized Identity Management System Using Blockchainand Zero-Knowledge Proof," *IEEE Access*, vol. 8, pp. 22356–22364, 2020.

[12] N. Patel and A. Shah, "Blockchain-Based Decentralized Identity Management: ASurvey," *Journal of Network and Computer Applications*, vol. 166, p. 102706, 2020.

[13] L. Zhang, Y. Liu, and S. Chen, "A Blockchain-Based Decentralized Identity ManagementSystem," in *Proceedings of the 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, Toronto, ON, Canada, 2020, pp. 1–5.

[14] A. Alkhodair, M. A. Salahuddin, and R. Hussain, "Blockchain-Based DecentralizedIdentity Management with Veri able Credentials," *IEEE Access*, vol. 9, pp. 14078–14089, 2021.

[15] C. Li, X. Jiang, and J. Wu, "A Decentralized Identity Management System for Internet ofThings Based on Blockchain," *IEEE Access*, vol. 8, pp. 11463–11474, 2020.

[16] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008. [Online]. Available:

[17] G. Wood, "Ethereum: A Secure Decentralised Generalised Transaction Ledger,"*Ethereum Project Yellow Paper*, vol. 151, pp. 1–32, 2014.

[18] A. Narayanan, J. Bonneau, E. Felten, A. Miller, and S. Goldfeder, *Bitcoin and Cryptocurrency Technologies*. Princeton University Press, 2016.

[19] S. Srivastava, D. Agarwal and B. Chaurasia, "Secure Decentralized Identity

Management using Blockchain," *2023 IEEE 22nd International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, Exeter, United Kingdom, 2023, pp. 1355–1360, doi: 10.1109/TrustCom60117.2023.00185.

[20] D. Tapscott and A. Tapscott, *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World*. Penguin, 2016.

[21] K. Croman et al., "On Scaling Decentralized Blockchains," in *Proceedings of the 3rd Workshop on Bitcoin and Blockchain Research*, Barbados, 2016, pp. 106–125.

[22] V. Buterin, "A Next-Generation Smart Contract and Decentralized ApplicationPlatform," *Ethereum White Paper*, 2014.

[23] M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, "Blockchain Technology: Beyond Bitcoin," *Applied Innovation*, vol. 2, pp. 6–10, 2016.

[24] K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet ofThings," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.

[25] S. Underwood, "Blockchain Beyond Bitcoin," *Communications of the ACM*, vol. 59, no. 11, pp. 15–17, 2016.