VALIDEX: A Decentralized Platform for Tamper-Proof Academic and Employment Credential Verification

Gaurav Gundre[1], Viraj Khot[2], Prof. Dr. Hari Palani[3]
[1]*Gaurav Gundre, MIT ADT University, Pune-412201*
[2]*Viraj Khot, MIT ADT University, Pune-412201*
[3]*Prof. Dr. Hari Palani, MIT ADT University, Pune-412201*

***Abstract*—This paper presents VALIDEX, an innovative decentralized platform for verifying credentials that aims to tackle the inefficiencies and vulnerabilities found in today's academic and employment verification processes. VALIDEX utilizes blockchain technology, including Hyperledger Indy, Fabric, and IPFS, to build a secure, tamper-proof environment that allows for instant, globally verifiable, and user-controlled management of credentials. Our method removes manual bottlenecks, gives users complete ownership, and uses cryptographic techniques to maintain authenticity and privacy throughout the entire credential lifecycle. We also explore key technical decisions, integration strategies, and the advantages of our solution compared to existing options.**

***Index Terms*—Blockchain, Credential Verification, Decentralized Identity, Hyperledger Indy, Hyperledger Fabric, IPFS**

I. INTRODUCTION

Credential verification is still a tricky and often error-filled process that depends heavily on manual checks and centralized authorities, leading to delays and unnecessary costs. As global mobility increases and digital transformation accelerates, the shortcomings of current systems like DigiLocker, ABC ID, and various paper-based methods are becoming more apparent. These systems struggle with issues like lack of interoperability, security risks, and trust deficits.

VALIDEX steps in with a solid solution that utilizes decentralized identities (DIDs), verifiable credentials (VCs), and blockchain technology to provide a reliable, user-focused approach to verifying academic and employment credentials. With VALIDEX, users can take charge of their credentials, while institutions and employers can verify them quickly and securely, all without needing intermediaries.

II. LITERATURE REVIEW

A. Blockchain and Credential Verification

Numerous studies have confirmed the significant role of blockchain in the realm of digital credentialing. Rustemi et al. conducted a thorough review of various blockchain-based certificate verification systems, emphasizing the advantages of decentralized trust and auditability. Most existing platforms rely on Ethereum smart contracts or Hyperledger frameworks to tackle issues of transparency and integrity, but many overlook the crucial aspects of global interoperability and user privacy.

A number of academic prototypes are using permissioned blockchains like Hyperledger Fabric to create efficient, permission-controlled registries, often paired with distributed file storage solutions like IPFS for scalable and encrypted credentials. Hyperledger Indy has emerged as a leading ledger focused on self-sovereign identity (SSI), offering robust native support for decentralized identifiers (DIDs) and zero-knowledge proofs that enhance credential privacy.

B. Existing Solutions and Limitations

Government portals such as DigiLocker in India provide centralized repositories that help reduce fraud, but they come with geographical restrictions and lack adequate privacy controls. ABC ID is at the forefront of decentralized user ownership, yet it grapples with challenges related to scalability and standardization.

The VALIDEX platform takes these insights to heart, offering:

A global platform that complies with open standards for cross-border verifications.

Peer-to-peer sharing capabilities with selective disclosure options.

On-chain registries designed for credential revocation and auditing.

III. VALIDEX PLATFORM ARCHITECTURE

VALIDEX adopts a multi-layer technical stack:

1. Identity Layer: Hyperledger Indy for decentralized identifiers (DIDs) and verifiable credentials.
2. Ledger Layer: Hyperledger Fabric for issuer registry and event logs in a permissioned setup.
3. Storage Layer: IPFS for permanent, encrypted off-chain credential files.
4. User Interface: Mobile wallets (Flutter) and web portals for holders, issuers, and verifiers.
5. Public Anchor (optional): Polygon anchors hashes for global auditability.

IV. WORKFLOW AND LIFECYCLE

Credential Issuance: Institutions generate verifiable, cryptographically-signed credentials.

Secure Storage: Credentials encrypted and stored on IPFS, with hashes anchored to Fabric.

Instant Verification: Verifiers check authenticity instantly via blockchain records.

User Control: Holders manage sharing via mobile wallets and dashboards.

Tamper Detection: Any modification triggers a hash mismatch and invalidation.

V. COMPARISON: VALIDEX VS. EXISTING SYSTEMS

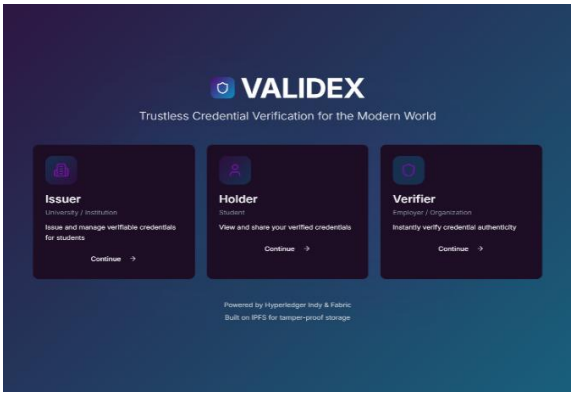
Feature	DigiLocker	ABC ID	VALIDEX
Data Control	Centralized	User-owned, decentralized	User-owned, decentralized
Global Verification	India only	Limited	Global portability
Tamper Detection	Basic digital signatures	Advanced	Cryptographic immutability
Revocation	No standard	On-chain registry	On-chain registry
Trust Model	Government-managed	Consortium	Consortium/Public hybrid
Privacy	Limited	Some	Zero-knowledge proofs

VI. DEVELOPMENT AND RESULTS

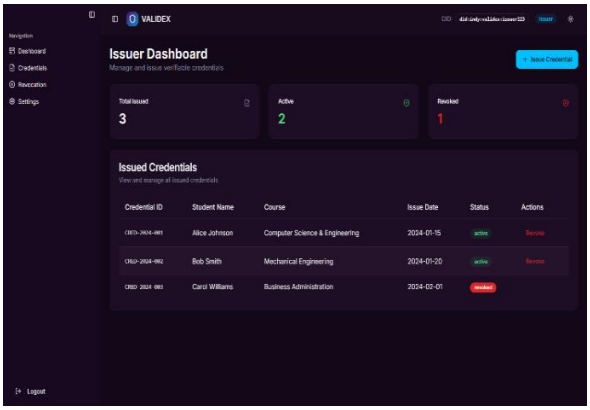
A. Milestones Completed

1. We completed a thorough review and validation of the entire architecture.
2. We successfully deployed the Hyperledger Fabric network.
3. We set up the Hyperledger Indy agent to manage decentralized identifiers (DIDs) and credentials.
4. We integrated IPFS for secure, encrypted storage solutions.
5. We developed a mobile wallet prototype using Flutter.
6. We worked on API development tailored for institutions.
7. We formed a partnership with a blockchain consultancy to enhance our development and validation efforts.

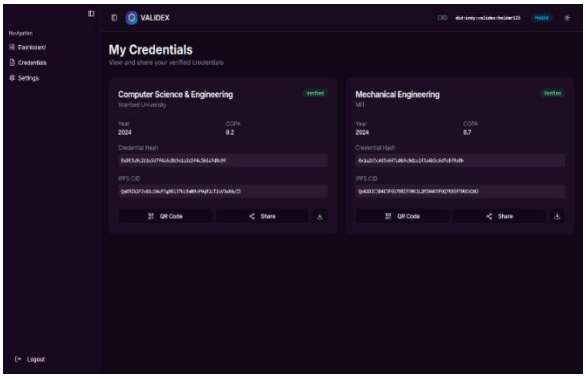
B. Sample Screenshots (Implementation Snaps)



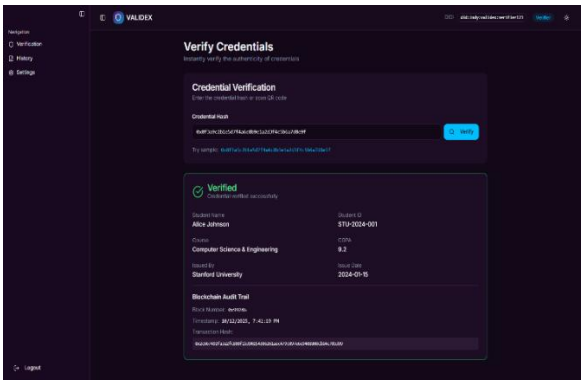
i. Login / onboarding



ii. Issuer Dashboard



iii. Credential dashboard



iv. Verifier admin dashboard

VII. DISCUSSION AND FUTURE WORK

VALIDEX is all about harnessing decentralization and cutting-edge cryptographic techniques to tackle the ongoing challenges faced by credential verification systems. Its design puts user ownership, privacy, and instant trust front and center, making it a significant leap forward from the traditional centralized and semi-digital platforms we're used to.

That said, rolling out a scalable production deployment comes with its own set of important technical and operational hurdles. To scale effectively, we need to optimize transaction throughput and storage while ensuring low-latency verification for a potentially huge user base that includes educational institutions, employers, and regulatory bodies around the world. This means fine-tuning consensus mechanisms and efficiently integrating off-chain solutions like IPFS.

It's also crucial to integrate with various national frameworks and comply with regulatory requirements, including data protection laws like GDPR and India's data privacy regulations. Developing interoperability protocols to align with existing digital identity ecosystems, certificate authorities, and legacy systems will be a key focus to encourage widespread adoption.

Privacy enhancement is another major goal. While current zero-knowledge proof (ZKP) implementations allow for selective disclosure of credential information, future plans include incorporating more advanced ZKP schemes and revocation mechanisms that maintain privacy even during credential revocation and querying processes.

Further research will aim to improve usability for both end users and administrators, featuring richer mobile wallet capabilities, smoother verification workflows, and fraud detection analytics. Strengthening production-grade security measures, such as multi-factor authentication, role-based access control, and robust cryptographic key management, will help build trust.

Ultimately, VALIDEX aspires to become a universally accepted layer of trust that supports lifelong credential ownership and cross-border verifiability. To make this vision a reality, the project will focus on extensive pilot deployments.

VIII. CONCLUSION

VALIDEX provides a secure and efficient way to verify credentials by harnessing the power of blockchain technology. This ensures that credentials are not only tamper-proof but also instantly verifiable from anywhere in the world. By cutting out the middlemen, it slashes verification times from weeks down to mere seconds, giving users complete control over their credentials while keeping their privacy intact through selective disclosure. The decentralized nature of the system boosts trust, transparency, and portability for both academic and employment credentials, setting a new benchmark for digital verification. This groundbreaking platform significantly lowers the risks of fraud, cuts operational costs, and simplifies workflows for institutions and employers around the globe.

ACKNOWLEDGMENT

The authors would like to extend their heartfelt thanks to the faculty and mentors at MIT ADT School of Computing, Pune for their invaluable support and guidance. A special shoutout goes to *Hypermine Ltd.* for their technical know-how and insightful

contributions during the development and validation of the VALIDEX platform. We're also grateful to the educational institutions and industry partners who took part in the pilot testing and provided us with their feedback. Last but not least, we truly appreciate every member of the development team whose hard work and dedication made this research a reality.

REFERENCES

[1] A. Mathew, S. Goel, and R. Ravindran, "Blockchain-based credential verification system for academic records," IEEE Trans. Learning Technologies, vol. 15, no. 3, pp. 482–492, Jul.–Sep. 2022.

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

[3] A. Tobin and D. Reed, "The inevitable rise of self-sovereign identity," Sovrin Foundation, White Paper, 2016.

[4] D. Tapscott and A. Tapscott, Blockchain Revolution: How the Technology Behind Bitcoin and Other Cryptocurrencies is Changing the World, 1st ed. New York, NY: Portfolio, 2016.

[5] M. Swan, Blockchain: Blueprint for a New Economy, 1st ed. Sebastopol, CA: O'Reilly Media, 2015.

[6] M. Arruda and K. Park, "Decentralized identity: Concepts and use cases," in Emerging Technologies for Identity Management, R. Young, Ed. London, UK: Springer, 2020, pp. 55–74.

[7] C. Allen, "The Path to Self-Sovereign Identity," in Self-Sovereign Identity, J. G. Finney and K. Herold, Eds. Boston, MA: MIT Press, 2021, pp. 87–108.

[8] M. Swan, Blockchain: Blueprint for a New Economy, 1st ed. Sebastopol, CA: O'Reilly Media, 2015.

[9] M. R. Sir Deshmukh and M. V. Memprekar, "Securing Academic Credentials," *International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)*, vol. 5, 2021.

[10] T. Hardjono, A. Maler, and D. Reed, "Introduction to Self-Sovereign Identity," *IEEE Communications Standards Magazine*, vol. 3, no. 4, pp. 64–68, 2019.

[11] N. Atzei, M. Bartoletti, and T. Cimoli, "A survey of attacks on Ethereum smart contracts (SoK)," in *Proc. Int. Conf. Principles of Security and Trust*, Springer, 2017, pp. 164–186.

[12] Hyperledger Foundation, *Anon Creds Specification: Anonymous Credentials for Hyperledger Indy*, 2023. [Online]. Available: https://hyperledger.github.io/anoncreds-spec/

[13] Hyperledger Foundation, *Hyperledger Indy Documentation*. [Online]. Available: https://hyperledger-indy.readthedocs.io/

[14] D. Reed *et al.*, *Decentralized Identifiers (DIDs) v1.0*, W3C Recommendation, 2023. [Online]. Available: https://www.w3.org/TR/did-core/

[15] M. Sporny, D. Longley, and D. Chadwick, *Verifiable Credentials Data Model 1.1*, W3C Recommendation, 2024. [Online]. Available: https://www.w3.org/TR/vc-data-model/

[16] Hyperledger Foundation, *Hyperledger Aries Framework Overview*, 2024. [Online]. Available: https://www.hyperledger.org/use/aries

[17] Vercel Inc., *Vite: Next Generation Frontend Tooling*, 2024. [Online]. Available: https://vitejs.dev/

[18] "IEEE Standard 3209-2023: IEEE Standard for Blockchain Identity Key Management," IEEE Computer Society, Feb. 8 2024.