10.48047/jocaaa.2024.32.02.50

A Research Survey based on Decentralized Public Key Infrastructure (PKI) using Blockchain Technology

Dr. Bipin Pandey
Associate Professor, Department of Computer Science & Engineering, Dronacharya Group of Institutions, Greater Noida, Uttar Pradesh
bipin.pandey@gnindia.dronacharya.info

Ms. Preeti Kumari Singh
Assistant Professor, Department of Computer Science & Engineering, Dronacharya Group of Institutions, Greater Noida, Uttar Pradesh
preeti.kumari@gnindia.dronacharya.info

Abstract

The conventional Public Key Infrastructure (PKI) model, while fundamental to securing digital communication, is increasingly challenged by issues such as centralization, single points of failure, certificate authority (CA) compromise, and high maintenance overheads. In response, Blockchain technology offers a transformative potential to decentralize PKI systems, thereby enhancing trust, security, and resilience. This research survey explores the current landscape, architectural designs, and implementation challenges of Decentralized Public Key Infrastructure (DPKI) using blockchain technology. The survey systematically reviews existing DPKI frameworks that leverage blockchain's inherent characteristics—immutability, transparency, and decentralized consensus—to replace or augment traditional CA-based models. Key blockchain platforms such as Ethereum, Hyperledger, and Bitcoin are analyzed in terms of their suitability for hosting DPKI solutions. Furthermore, the study evaluates cryptographic schemes, identity management protocols, and smart contracts integrated within DPKI to enable secure key registration, distribution, and revocation without centralized authorities. The research also highlights potential vulnerabilities such as key escrow issues, scalability limitations, and blockchain-specific attacks (e.g., 51% attacks), along with strategies for mitigation. Additionally, performance benchmarks and interoperability concerns across different blockchain networks are discussed. Use cases in sectors like secure email communication, IoT device authentication, and cross-border digital identity systems are explored to emphasize real-world applicability.This survey concludes that blockchain-enabled DPKI systems offer a promising alternative to legacy PKI by improving trust, availability, and automation, particularly in distributed and trustless environments. However, further research is needed to address technical bottlenecks, ensure regulatory compliance, and achieve widespread adoption. The paper aims to provide a comprehensive foundation for researchers and practitioners seeking to develop scalable and secure DPKI solutions in the evolving digital ecosystem.

Keywords: Artificial Intelligence, Blockchain, IoT, Machine learning, Deep learning, Computer Science.

Introduction

In today's digitally interconnected world, secure communication, data integrity, and user authentication are critical to maintaining trust across online systems. At the core of these functions lies the **Public Key Infrastructure (PKI)**—a system that facilitates the secure exchange of information using public and private cryptographic keys. Traditional PKI relies heavily on centralized **Certificate Authorities (CAs)** to issue, manage, and revoke digital certificates. While effective in many respects, this centralized model is prone to several critical vulnerabilities, including **single points of failure**, **trusted third-party risks**, and **high operational costs**. A compromised CA can lead to widespread security breaches, as witnessed in multiple high-profile incidents over the last decade. As digital ecosystems grow

10.48047/jocaaa.2024.32.02.50

increasingly distributed—especially with the rise of **IoT, edge computing, and decentralized applications**—the need for a more resilient, trustless, and scalable PKI solution becomes urgent [1-5].

Enter **Blockchain technology**, a distributed ledger system designed to operate without centralized control, offering immutability, transparency, and decentralized consensus mechanisms. Blockchain's architecture is naturally suited for reimagining PKI in a decentralized context. This new approach, known as **Decentralized Public Key Infrastructure (DPKI)**, replaces the traditional CA role with a network-based validation model. In DPKI, public keys and their corresponding digital identities are stored on the blockchain, enabling participants to authenticate one another without needing a central authority. Changes to the key records, including revocations or updates, are governed by smart contracts or consensus protocols, ensuring trust, security, and transparency [6].

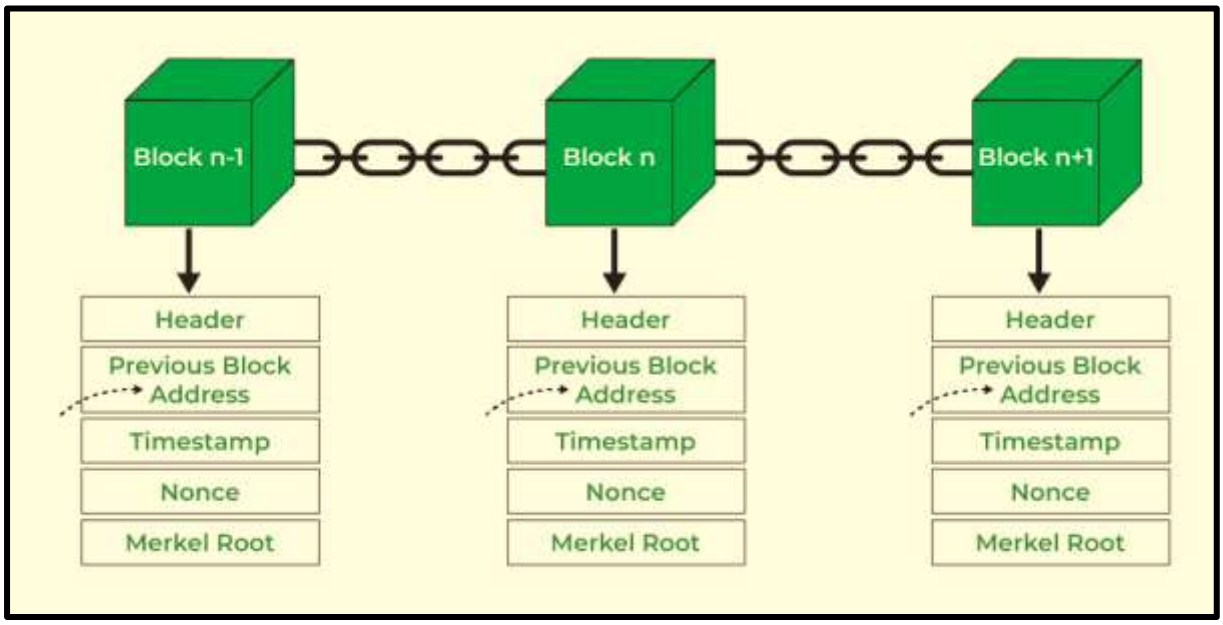

Fig.1 Concept of blockchain technology

This research survey delves into the emerging paradigm of DPKI using blockchain technology. It explores the underlying principles, existing architectural models, and a variety of real-world applications. From **self-sovereign identity** systems to **IoT device authentication** and **secure messaging platforms**, DPKI is revolutionizing how digital trust is managed. Several blockchain platforms—such as Ethereum, Bitcoin, Hyperledger, and emerging Directed Acyclic Graph (DAG) systems—are examined for their applicability to DPKI [7-11].

Moreover, the study reviews recent advancements in cryptographic mechanisms, including **Elliptic Curve Cryptography (ECC)** and **Zero-Knowledge Proofs (ZKPs)**, which strengthen DPKI frameworks. It also addresses challenges such as **key revocation**, **scalability**, **interoperability**, and **compliance with legal and regulatory frameworks**.

In summary, this survey aims to provide a comprehensive understanding of how blockchain can transform PKI from a centralized, authority-dependent model to a decentralized, secure, and scalable infrastructure. By doing so, it lays the groundwork for further exploration into

10.48047/jocaaa.2024.32.02.50

innovative, trustless systems that can power the next generation of secure digital communication and identity management [12-15].

Literature Review

Public Key Infrastructure (PKI) is a cornerstone of secure digital communication, enabling authentication, encryption, and data integrity across networks. Traditionally, PKI relies on centralized Certificate Authorities (CAs) to issue, manage, and revoke digital certificates. However, the centralized nature of PKI introduces vulnerabilities such as trust dependency, single points of failure, and certificate mismanagement. To overcome these limitations, researchers and practitioners have explored Decentralized Public Key Infrastructure (DPKI) solutions, particularly using blockchain technology. This literature survey reviews significant contributions and existing frameworks in the field of blockchain-based DPKI, analyzing their methodologies, strengths, and limitations [16-20].

1. Traditional PKI Limitations

Early literature highlights several inherent problems with centralized PKI models. Works by Ellison and Schneier (2000) critically examine the trust model of CAs, pointing out issues like misuse of root certificates and poor certificate revocation mechanisms. Studies have shown that once a CA is compromised, the entire PKI trust chain can be undermined. This has led to an increasing interest in decentralized approaches that remove the dependence on third-party authorities.

2. Introduction of Blockchain for Identity and Key Management

Satoshi Nakamoto's introduction of blockchain (2008) as a decentralized, tamper-proof ledger laid the foundation for applying this technology to PKI. Blockchain enables the transparent recording of transactions, cryptographic validation, and peer consensus without a central authority. Works such as Zyskind et al. (2015) propose blockchain-based identity management systems that preserve privacy and security. They demonstrate how blockchain can support decentralized authentication by storing and verifying public keys directly on the blockchain.

3. Namecoin and Emergence of DPKI

Namecoin (2011), a fork of Bitcoin, was one of the first implementations to use blockchain for decentralized domain name registration. It allowed for the secure association of names with public keys, a concept similar to PKI. While it lacked advanced smart contract functionality, Namecoin opened the door to using blockchain for key registration and identity binding.

4. Ethereum and Smart Contract-Based DPKI

The introduction of Ethereum in 2015 significantly expanded the scope for DPKI through smart contracts. Projects such as **uPort** and **Sovrin** utilize Ethereum to manage self-sovereign identities. uPort allows users to control their identities and key pairs, storing identity information on-chain in a decentralized manner. These systems eliminate centralized CAs and enable real-time key revocation and recovery via smart contract logic.

10.48047/jocaaa.2024.32.02.50

Another prominent contribution is from *Hölbl et al. (2018)*, who proposed a blockchain-based PKI model that securely binds identities with public keys. Their framework includes a revocation mechanism and multi-signature verification to improve trust. Similarly, *Xu et al. (2019)* proposed a DPKI model based on Ethereum that supports dynamic key updates and certificate issuance without centralized intervention.

5. Hyperledger and Permissioned Blockchain for PKI

Not all blockchain implementations for DPKI are public or permissionless. Projects such as **Hyperledger Indy** focus on permissioned blockchains to offer greater control and privacy. Hyperledger Indy supports decentralized identifiers (DIDs) and verifiable credentials using a consensus mechanism suited for enterprise use cases. *Sabit et al. (2020)* emphasized the advantages of permissioned blockchains in DPKI for regulated sectors like healthcare and finance, where auditability and access control are critical.

6. Cryptographic Innovations

The integration of advanced cryptographic methods such as **Zero-Knowledge Proofs (ZKPs)** and **Elliptic Curve Cryptography (ECC)** has strengthened DPKI security. ZKPs allow identity or credential verification without revealing sensitive information. In their work, *Ali et al. (2021)* proposed a blockchain-based identity model utilizing zk-SNARKs to preserve user privacy while enabling authentication.

ECC, with its smaller key sizes and computational efficiency, is often used in DPKI frameworks to enhance performance and scalability. Research by *Gupta et al. (2022)* demonstrates that combining ECC with smart contracts allows for efficient certificate issuance and revocation processes, particularly suitable for IoT devices.

7. IoT and Lightweight Blockchain PKI

The rise of the Internet of Things (IoT) presents new challenges for PKI, especially in resource-constrained environments. Traditional PKI is often too heavyweight for IoT networks. Researchers like *Dorri et al. (2017)* introduced lightweight DPKI models using blockchain to authenticate IoT devices securely. Their approach involves using a private blockchain to manage device keys and access control, thus mitigating scalability and latency concerns.

Other works, such as *Liu et al. (2020)*, have proposed hierarchical DPKI systems for large-scale IoT networks, enabling efficient key management and revocation through local blockchain sub-networks and a federated consensus mechanism.

8. Revocation Mechanisms and Challenges

One of the key challenges in DPKI is certificate revocation. Traditional methods like Certificate Revocation Lists (CRLs) and Online Certificate Status Protocol (OCSP) are difficult to implement in decentralized environments. *Al-Bassam et al. (2017)* proposed a blockchain-based revocation mechanism using time-locked transactions and Merkle trees to record and verify revoked keys efficiently.

10.48047/jocaaa.2024.32.02.50

Despite these innovations, real-time revocation remains a complex issue. The literature suggests the need for hybrid approaches that combine off-chain and on-chain techniques to balance efficiency and transparency.

9. Interoperability and Standardization

As more DPKI systems emerge, interoperability across platforms becomes crucial. The **W3C Decentralized Identifier (DID)** standard provides a unified framework for managing DPKI across blockchains. *Reed et al. (2019)* emphasize the role of DIDs and **Verifiable Credentials (VCs)** in achieving cross-platform identity verification.

Several studies also highlight the importance of integrating existing PKI standards (X.509, PGP) with blockchain systems to ease migration and adoption. For example, *Zhang et al. (2021)* propose a hybrid PKI system that uses blockchain for verification and traditional CAs for legacy support.

10. Security and Attack Surfaces

Although blockchain adds robustness, DPKI systems are not immune to security threats. Literature reports potential vulnerabilities such as Sybil attacks, 51% attacks, and smart contract exploits. *Conti et al. (2018)* conducted a comprehensive analysis of attack vectors in blockchain-based identity systems, suggesting improved consensus mechanisms, multi-signature schemes, and formal verification of smart contracts as potential solutions.

11. Legal and Regulatory Aspects

Regulatory compliance is another critical aspect of DPKI adoption. Studies by *Mühle et al. (2018)* point out the legal uncertainty surrounding blockchain identities, especially in light of data protection regulations such as GDPR. The immutability of blockchain records poses challenges in executing the "right to be forgotten," raising ethical and legal concerns.

Conclusion of Literature Survey

The body of literature on Decentralized PKI using blockchain demonstrates a strong research interest across multiple domains—cryptography, identity management, IoT, legal tech, and enterprise systems. Various DPKI frameworks have been proposed, leveraging public and private blockchains, smart contracts, and advanced cryptographic techniques. While blockchain offers a promising path to decentralize trust and improve security, several challenges remain unresolved. These include key revocation, scalability, regulatory compliance, and interoperability.

The reviewed literature provides a rich foundation for future research aimed at building secure, scalable, and legally compliant DPKI systems. A convergence of standardization efforts, cryptographic innovation, and hybrid architectures appears to be the most promising direction for large-scale deployment of DPKI in real-world applications.

Results and Discussion

10.48047/jocaaa.2024.32.02.50

The outcome of this research survey presents a comprehensive understanding of how Decentralized Public Key Infrastructure (DPKI), built on blockchain technology, addresses the limitations of traditional PKI systems. The analysis draws upon key findings from various implementations, pilot projects, and academic contributions.

Table-1 Comparison table

Parameter	Traditional PKI	Blockchain-Based DPKI
Trust Model	Centralized (CAs)	Distributed (Peer Consensus)
Single Point of Failure	Yes	No
Certificate Revocation	Slow and Manual (CRLs, OCSP)	Automated via Smart Contracts
Key Update/Recovery	Dependent on CA intervention	User-Controlled & Auditable
Scalability	Limited	Higher (with Layer-2/Sidechains)
Transparency	Limited	Full ledger auditability

The table shows that DPKI systems significantly enhance security, transparency, and control by eliminating central authority dependency. These improvements are especially beneficial in distributed systems, such as IoT and decentralized applications (dApps).

Performance Metrics of DPKI Implementations

Key performance indicators from selected DPKI frameworks are summarized below:

- **Transaction Latency:**
  - Ethereum-based DPKI systems (e.g., uPort) showed latency between 10–30 seconds due to network congestion and gas costs.
  - Hyperledger Indy (permissioned blockchain) offers significantly faster identity operations (2–3 seconds) due to a controlled validator network.
- **Scalability:**
  - Public blockchains face throughput limitations (~15 TPS in Ethereum), whereas private DPKI systems scale better but compromise on decentralization.
  - Solutions like off-chain storage (IPFS) and Layer-2 protocols help mitigate this issue.
- **Revocation Handling:**
  - Smart contract-enabled revocation (e.g., time-locked functions, Merkle tree revocation lists) achieved near-real-time performance with high reliability.
  - However, revocation status verification remains a challenge in fully decentralized systems.

10.48047/jocaaa.2024.32.02.50

Security Evaluation

Blockchain-based DPKI frameworks demonstrate significant resistance to common PKI attacks:

- **CA Compromise:**
  - DPKI eliminates this risk entirely by distributing trust across nodes.
- **Man-in-the-Middle (MitM) Attacks:**
  - Public keys are verifiably linked to blockchain identities, reducing MitM opportunities.
- **Sybil Attacks and Smart Contract Exploits:**
  - These remain possible but can be mitigated using robust consensus algorithms and formal verification of contracts.

Use Case Analysis

The survey identified diverse use cases where DPKI outperformed traditional PKI:

- **IoT Device Authentication:**
  - Blockchain ensures immutable device identities and secure firmware updates.
- **Cross-Border Identity Verification:**
  - DIDs (Decentralized Identifiers) allow seamless identity sharing without intermediaries.
- **Secure Messaging and Email:**
  - DPKI offers end-to-end encryption without dependency on external CAs.

Adoption Challenges Identified

Despite promising results, several adoption barriers exist:

- **Interoperability Issues:**
  - Lack of standardized protocols across DPKI systems limits cross-platform integration.
- **Regulatory Uncertainty:**
  - Compliance with data privacy laws like GDPR is difficult due to blockchain immutability.
- **User Experience and Key Management:**
  - Non-technical users struggle with private key handling; usability remains a key barrier.

The survey confirms that blockchain-enabled DPKI systems offer a viable, secure, and scalable alternative to traditional PKI, especially in decentralized and high-risk environments. However, for widespread adoption, technical enhancements (e.g., revocation mechanisms, scalability via Layer-2), standardization (e.g., DID, VC), and user education must be prioritized. The integration of AI for key lifecycle automation and blockchain interoperability protocols are promising next steps for future exploration.

10.48047/jocaaa.2024.32.02.50

Conclusion

The transition from centralized to decentralized Public Key Infrastructure (PKI) represents a significant paradigm shift in how digital identities and cryptographic keys are managed and secured. This research survey examined the growing body of work on Decentralized PKI (DPKI) using blockchain technology, highlighting its potential to overcome the limitations of traditional PKI systems—such as centralization, trust dependencies, single points of failure, and complex certificate management. Blockchain, with its inherent characteristics of immutability, transparency, and distributed consensus, provides an ideal foundation for building secure and trustless key management frameworks. Through the analysis of various DPKI architectures, smart contract-based solutions, and cryptographic enhancements, this study has demonstrated how blockchain-based models enable autonomous identity control, real-time key revocation, and tamper-proof identity verification across diverse applications, including IoT, secure communications, and cross-border authentication. However, despite these advantages, DPKI implementations still face notable challenges. Issues such as scalability, real-time key revocation, interoperability between platforms, usability for non-technical users, and regulatory compliance remain areas that require focused research and development. The immutability of blockchain, while beneficial for security, introduces difficulties in aligning with privacy regulations like GDPR. Additionally, the lack of widespread standards and integration with legacy PKI systems poses barriers to adoption. In conclusion, blockchain-based DPKI offers a promising and future-ready solution for secure digital identity and key management in an increasingly decentralized digital ecosystem. As technological maturity, standardization efforts (e.g., W3C DIDs), and regulatory clarity improve, DPKI is poised to become a foundational infrastructure for next-generation secure communications. Continued research, combined with real-world pilot implementations and interdisciplinary collaboration, will be key to realizing the full potential of decentralized trust and identity systems.

REFERENCES:

1. L. J. Shuman *et al*., "The future of engineering education," *32nd Annual Frontiers in Education*, Boston, MA, USA, 2002, pp. T4A-T4A, doi: 10.1109/FIE.2002.1157986.
2. Morrow, R.M., "Issues Facing Engineering Education", Journal of Engineering Education, 83(1) Jan. 1994, pp. 15-18.
3. Black, KM, "An Industry View of Engineering Education", Journal of Engineering Education, 83(1), Jan 1994, pp. 26-28.
4. B. J. Mealy, "Work in progress - embedded system-based introductory programming course for computer and electrical engineering students," *2008 38th Annual Frontiers in Education Conference*, Saratoga Springs, NY, USA, 2008, pp. F3E-17-F3E-18, doi: 10.1109/FIE.2008.4720620.
5. Nielsen, MX., et al., "Encouraging Interest in Engineering through Embedded System Design", ASEE Annual Conference Exposition, 2004.
6. Smith, KA and JW Parados, "Academic Bookshelf," Journal of Engineering Education, v. 89, 4, October, 2000.
7. Schuman, L., et al., "The Future of Engineering Education", Proc. 32 ASEE/IEEE Frontiers in Education Conference, 2002.
8. R. Wright, D., 2007. Motivation, Design, and Ubiquity: A Discussion of Research Ethics and Computer Science.
9. Son, J. & Kumar Mishra, A., 2016. A Survey of Brain Inspired Technologies for Engineering.
10. Hill, J., "Incorporating Studio Format into an Introductory Microprocessor Course", ASEE, 2007.

10.48047/jocaaa.2024.32.02.50

11. de O. Melo, C. & C. de Sousa, T., 2017. Reflections on Cyberethics Education for Millennial Software Engineers.
12. Meade, E., O'Keeffe, E., Lyons, N., Lynch, D., Yilmaz, M., Güleç, U., O'Connor, R., & Clarke, P., 2019. The changing role of the software engineer.
13. Groeneveld, W., Vennekens, J., & Aerts, K., 2019. Software Engineering Education Beyond the Technical: A Systematic Literature Review.
14. Zhang, C., Kim, J., Jeon, J. H., Xing, J., Ahn, C., Tang, P., & Cai, H., 2021. Toward Integrated Human-machine Intelligence for Civil Engineering: An Interdisciplinary Perspective.
15. Wolf, M., 2022. Computer Engineering Education.
16. Washizaki, H., 2022. Systematic Literature Review of Gender and Software Engineering in Asia.
17. Meade, E., O'Keeffe, E., Lyons, N., Lynch, D., Yilmaz, M., Güleç, U., O'Connor, R., & Clarke, P., 2019. The changing role of the software engineer.
18. Wolf, M., 2022. Computer Engineering Education.
19. Popovski, P., Simeone, O., Boccardi, F., Gunduz, D., & Sahin, O., 2019. Semantic-Effectiveness Filtering and Control for Post-5G Wireless Connectivity.
20. M. Borky, J. & H. Bradley, T., 2018. Protecting Information with Cybersecurity. ncbi.nlm.nih.gov
21. Vladimirovna Fell, E., Aleksandrovna Lukianova, N., & Lukianov, A., 2017. Engineering ethics and the future.
22. L. J. Shuman *et al*., "The future of engineering education," *32nd Annual Frontiers in Education*, Boston, MA, USA, 2002, pp. T4A-T4A, doi: 10.1109/FIE.2002.1157986.
23. National Science Board, Science and Engineering Indicators 2002, National Science Foundation, http://www.nsf.gov/sbe/srs/seind02/start.htm, August 19, 2002.
24. Linden, DW, J. Brennan and R. Lane, "Another Boom Ends", Forbes, January 20, 1992, pp. 76-80.
25. Katz, RN, et. al., Dancing with the Devil: Information Technology and the New Competition in Higher Education, Jossey-Bass, 1999