frontiers | Frontiers in Blockchain

TYPE Original Research
PUBLISHED 15 January 2026
DOI 10.3389/fbloc.2025.1702066

OPEN ACCESS

EDITED BY
Mehdi Sookhak,
Texas A&M University Corpus Christi,
United States

REVIEWED BY
Satyendra Kumar Mishra,
Centre Tecnologic De Telecomunicacions De Catalunya, Spain
Nader Sohrabi Safa,
University of Worcester, United Kingdom

*CORRESPONDENCE
Petar Radanliev,
petar.radanliev@cs.ox.ac.uk

RECEIVED 09 September 2025
REVISED 22 October 2025
ACCEPTED 19 November 2025
PUBLISHED 15 January 2026

CITATION
Radanliev P, Maple C and Santos O (2026) Complying with the NIST post-quantum cryptography standards and decentralizing artificial intelligence: methodology for quantum-resistant and privacy-preserving digital identity systems.
Front. Blockchain 8:1702066.
doi: 10.3389/fbloc.2025.1702066

Complying with the NIST post-quantum cryptography standards and decentralizing artificial intelligence: methodology for quantum-resistant and privacy-preserving digital identity systems

Petar Radanliev [1,2]*, Carsten Maple[2,3] and Omar Santos[4]

[1]Department of Computer Sciences, University of Oxford, Oxford, United Kingdom, [2]The Alan Turing Institute, British Library, London, United Kingdom, [3]University of Warwick – WMG, Coventry, United Kingdom, [4]Cisco Systems, Research Triangle Park, NC, United States

Introduction: Digital identity infrastructures used in electronic passports, national eID schemes, and federated authentication systems rely predominantly on centralised registries and classical public key cryptography. These architectures enable large-scale identity correlation, mass data aggregation, and single points of compromise, while remaining vulnerable to quantum attacks against RSA and elliptic-curve cryptography. There is no deployed identity framework that simultaneously provides post-quantum security, cryptographic privacy guarantees, and decentralised trust.

Methods: This study proposes a quantum-proof digital passport architecture combining lattice-based post-quantum cryptography, decentralised blockchain identifiers, and transformer-based decentralised artificial intelligence. The framework employs NIST-aligned post-quantum key encapsulation and digital signatures, zero-knowledge proofs for selective disclosure of identity attributes, and homomorphic encryption for encrypted identity verification. Blockchain oracles and decentralised identifiers enforce credential integrity and auditability without reliance on central identity providers. Transformer attention mechanisms support adaptive identity validation while preventing persistent identity profiling.

Results: Architectural analysis shows that the proposed system prevents quantum-enabled credential forgery, retrospective decryption, and cross-service identity linkability. Zero-knowledge verification removes plaintext exposure of personal data, and decentralised credential control eliminates central compromise vectors. The design remains interoperable with existing passport and eID infrastructures.

Discussion: The results demonstrate that secure post-quantum digital identity requires the combined application of quantum-resistant cryptography, decentralised governance, and cryptographic privacy enforcement.

KEYWORDS

digital identity management, quantum-proof security, privacy-preserving technologies, decentralized AI protocol, generative AI, blockchain, post-quantum cryptography, zero-knowledge proofs

1 Introduction

Despite significant advancements in quantum-resistant cryptography, zero-knowledge proofs (ZKPs), homomorphic encryption (HE), and blockchain technology, a critical gap persists in integrating these technologies into a unified, robust system for digital identity management. Current digital identity solutions often fail to provide a comprehensive approach that balances security, privacy, and scalability. This research addresses this gap by leveraging these advanced technologies to develop a secure, scalable, and privacy-preserving digital passport system.

This study presents a future-proof digital identity solution that combines generative artificial intelligence (AI), blockchain, and post-quantum cryptographic techniques. By integrating these technologies, the proposed framework ensures robust security against the imminent threats of quantum computing. The use of lattice-based cryptography and other quantum-resistant algorithms forms the backbone of this security, providing a resilient defense against potential quantum attacks.

Additionally, the framework employs advanced cryptographic techniques such as zero-knowledge proofs and homomorphic encryption to enhance user privacy. These techniques enable users to verify their identities without disclosing personal details, thus addressing fundamental privacy concerns in digital interactions. Integrating blockchain technology and decentralized identifiers (DIDs) further strengthens the framework by decentralizing identity management, thereby mitigating the risks associated with centralized systems.

Generative AI, including generative adversarial networks (GANs) and variational autoencoders (VAEs), is used to create synthetic identities. These AI-generated identities are realistic yet anonymized, enhancing the robustness and privacy of the identity verification process. Furthermore, the framework incorporates methods for detecting and mitigating Sybil attacks, ensuring the integrity and security of decentralized networks.

The development of this integrated system is crucial in addressing the growing need for secure, privacy-preserving digital interactions in an increasingly interconnected world. By combining state-of-the-art cryptographic techniques, advanced AI, and decentralized blockchain technology, this research provides a comprehensive solution that sets a new standard for digital identity management in the post-quantum era.

2 Literature review

The literature review forms the backbone of the research methodology applied in this study. It provides a detailed analysis of critical advancements and existing gaps in quantum-resistant cryptography, zero-knowledge proofs, homomorphic encryption, blockchain technology, and AI applications. This review underscores the necessity of integrating these advanced techniques into a unified system to address the pressing need for secure and privacy-preserving digital identity management. The methodology employed in this study builds on these foundational works, leveraging lattice-based cryptography for quantum resistance, zero-knowledge proofs, homomorphic encryption for enhanced privacy, and blockchain for decentralized identity verification. AI techniques, such as generative adversarial networks and variational autoencoders, are used to create robust synthetic identities, further securing the system against potential threats. This integrated approach ensures a scalable, secure, and privacy-preserving digital passport system, advancing digital identity management's state of the art.

3 Extracting new knowledge from existing literature

Generative adversarial networks (GANs), introduced by Goodfellow et al. (2014), represent a groundbreaking framework for training generative models. The central concept involves a competition between two neural networks: the generator and the discriminator. The generator's role is to create synthetic data instances, while the discriminator evaluates these instances' authenticity by distinguishing between real and generated data. This adversarial training process continues until the generator produces data that the discriminator cannot distinguish from real data. GANs have demonstrated substantial promise in generating high-quality, realistic data across various domains, including image synthesis, significantly influencing the field of generative models and highlighting the efficacy of adversarial training in machine learning.

In parallel, Kingma and Welling (2013) introduced the auto-encoding variational Bayes (AEVB) framework, a method for the efficient and scalable training of deep generative models. This framework innovatively combines variational inference with auto-encoding, enabling the learning of complex data distributions. A key innovation of their approach is the reparameterization trick, which facilitates backpropagation through the model's stochastic layers, thereby enabling the optimization of the variational lower bound using standard gradient descent techniques. The AEVB framework is notable for its ability to approximate intractable posterior distributions in latent variable models, offering a robust tool for unsupervised learning and high-dimensional data generation. This work has significantly impacted the development of variational autoencoders (VAEs) and other probabilistic models in machine learning.

Building on the GANs framework, Radford et al. (2015) developed deep convolutional generative adversarial networks (DCGANs) by integrating deep convolutional neural networks (CNNs). This enhanced architecture utilizes convolutional layers to improve the stability and performance of GANs in learning unsupervised representations. Key innovations include the adoption of strided convolutions and batch normalization, which collectively enhance training and enable the generation of high-quality images.

Lyubashevsky et al. (2010) introduce the ring learning with errors (RLWE) problem, which extends the learning with errors (LWE) problem to polynomial rings, providing a foundation for efficient and secure lattice-based cryptographic schemes. The article "NewHope" (Alkim et al., 2016) presents a post-quantum key exchange protocol based on the RLWE problem. The authors designed NewHope to be secure against quantum attacks while maintaining efficiency comparable to classical cryptographic protocols. The protocol demonstrates practical performance for key exchange over TLS, providing a significant step toward integrating post-quantum cryptography into existing internet security infrastructure. NewHope's design and implementation address various practical considerations, including parameter selection, error correction, and performance optimizations, making it a robust candidate for future post-quantum secure communication standards.

Continuing from the advancements in deep learning and generative models, Ben-Sasson et al. (2025) introduced the concept of succinct non-interactive arguments of knowledge (SNARKs) applied to the C programming language. Their system translates programs written in C into a form suitable for SNARK verification, ensuring efficiency and security in the verification process. This innovative approach allows for the creation of zero-knowledge proofs, enabling verification of program executions without revealing any details about the program's inputs or internal states. This work significantly impacts secure computation and privacy-preserving applications, providing a practical solution for cryptographically secure computation verification.

Craig Gentry's seminal 2009 article (Gentry, 2009) presents the first feasible construction of fully homomorphic encryption (FHE) using ideal lattices, allowing computations on encrypted data without decryption. This method is crucial for secure cloud computing, as it involves creating a somewhat homomorphic encryption (SHE) scheme capable of handling limited operations on ciphertexts. Gentry extends this to FHE through a bootstrapping technique that reduces noise in ciphertexts by homomorphically decrypting and re-encrypting them. The use of ideal lattices provides the necessary structure for secure and efficient implementation, marking a significant breakthrough in cryptographic research.

Sahai and Watersy (2014) explore the applications of indistinguishability obfuscation (iO), with particular focus on deniable encryption. Indistinguishability obfuscation is a powerful cryptographic tool that transforms a program into an obfuscated version while preserving its functionality and ensuring that the obfuscated code is computationally indistinguishable from any other program with the same functionality. This article demonstrates how iO can be leveraged to construct deniable encryption schemes that allow ciphertexts to be decrypted into plausible alternative plaintexts, thus providing plausible deniability under coercion. The authors also discuss other applications of iO, highlighting its versatility and potential to revolutionize cryptographic protocols by enabling new security paradigms and enhancing existing ones.

Bünz et al. (2018) introduce Bulletproofs, a method for creating short, efficient zero-knowledge proofs, particularly suited for confidential transactions. Bulletproofs significantly reduce the size of cryptographic proofs while maintaining strong privacy and security guarantees. This innovation is especially impactful for blockchain and cryptocurrency applications, enabling transaction verification without revealing underlying transaction details. The article details the construction, implementation, and performance evaluations of Bulletproofs, demonstrating their efficiency and practicality for enhancing confidentiality in digital transactions and other cryptographic protocols.

Vitalik Buterin's 2014 Ethereum white paper, titled "A Next-Generation Smart Contract and Decentralized Application Platform" (Buterin, 2014), outlines the design and rationale behind Ethereum, a blockchain-based platform enabling developers to create decentralized applications (dApps) and smart contracts. The white paper introduces the concept of a Turing-complete virtual machine, the Ethereum virtual machine (EVM), which allows for the execution of arbitrary code on the Ethereum blockchain. This flexibility facilitates the development of complex applications beyond simple financial transactions, encompassing decentralized finance (DeFi), gaming, and supply chain management, among others. Buterin's work highlights Ethereum's potential to decentralize traditional services and create more transparent, secure, and automated systems.

Gavin Wood's 2014 Ethereum yellow paper, titled "Ethereum: A Secure Decentralised Generalised Transaction Ledger" (Wood, 2014), presents the technical specifications and underlying architecture of the Ethereum blockchain. This seminal document details the Ethereum virtual machine (EVM), a Turing-complete virtual machine that enables the execution of smart contracts and decentralized applications (dApps) on the Ethereum network. Wood outlines the consensus algorithm, state transition functions, and the underlying protocol's data structures, emphasizing the platform's versatility and security. The yellow paper serves as the definitive technical guide for developers and researchers, laying the groundwork for Ethereum's development and its extensive ecosystem of decentralized applications.

Poon and Dryja (2016) propose the Bitcoin Lightning Network in their article titled "The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments." This article introduces an off-chain protocol that enables instant, high-volume micropayments on the Bitcoin blockchain. The Lightning Network addresses Bitcoin's scalability issues by creating a network of bidirectional payment channels that allow transactions to be conducted off the main blockchain, with only the final settlement recorded on-chain. This approach significantly reduces transaction fees and confirmation times, enhancing Bitcoin's capability to handle a higher transaction throughput. The article outlines the technical foundations, including hashed time-lock contracts (HTLCs) and multi-hop payments, demonstrating how the Lightning Network can facilitate secure and efficient transactions while preserving the underlying security and decentralization of the Bitcoin network.

Building upon the previous discussion on advanced cryptographic techniques and their applications, Douceur (2002) presented "The Sybil Attack" at the first International Workshop on Peer-to-Peer Systems (IPTPS '02). The article describes a fundamental vulnerability in peer-to-peer networks known as the Sybil attack. In this attack, a single malicious entity can create multiple fake identities, or "Sybils," to gain disproportionate influence and control over the network. Douceur's article details how this attack can undermine the reliability and security of distributed systems by corrupting data, disrupting consensus mechanisms, and executing coordinated attacks. The study emphasizes the difficulty of preventing Sybil attacks without relying on centralized authorities, thus highlighting the challenges in designing secure, robust peer-to-peer networks. This seminal work has significant implications for the development of decentralized systems, including cryptocurrencies and distributed ledger technologies.

Danezis and Mittal (2009) introduced "SybilInfer: Detecting Sybil Nodes Using Social Networks" at the Network and Distributed System Security Symposium (NDSS). The article proposes a probabilistic framework, SybilInfer, for detecting Sybil nodes in social networks. Unlike traditional methods, SybilInfer uses the structure of social networks to distinguish between legitimate and Sybil identities. By analyzing the trust relationships and connectivity patterns within the network, SybilInfer can effectively identify and isolate Sybil nodes. The article presents the algorithm's theoretical foundation, implementation details, and performance evaluation, demonstrating that SybilInfer provides robust and scalable Sybil detection in distributed systems. This work significantly enhances the security and integrity of peer-to-peer and social network-based applications.

In "Decentralizing Privacy: Using Blockchain to Protect Personal Data," presented at the 2015 IEEE Security and Privacy Workshops, Zyskind et al. (2015) explored the use of blockchain technology to enhance privacy. The article proposes a decentralized framework that applies the immutable and transparent nature of blockchain to manage and protect personal data. By leveraging smart contracts and cryptographic techniques, the framework enables users to retain control over their data while granting access permissions without relying on centralized entities. This approach addresses key privacy concerns, such as unauthorized data sharing and data breaches, while ensuring data integrity and user autonomy. The article details the architecture, implementation, and potential applications of the proposed system, highlighting its implications for privacy-preserving data management in various domains.

Chaum (1981) presents a groundbreaking approach to electronic privacy in his article "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms," published in the Communications of the ACM. Chaum introduces the concept of using cryptographic techniques to create untraceable electronic mail and digital pseudonyms, laying the foundation for modern privacy-preserving communication systems. His work describes how to achieve anonymity and secure communication by using a mix network, which routes messages through multiple intermediaries and encrypts each layer to prevent tracking. This method ensures that neither the sender nor the recipient's identity can be easily determined, providing a robust solution for protecting user privacy in electronic communications. Chaum's pioneering ideas have significantly influenced the development of anonymous communication protocols and systems used in a wide range of applications today, including secure email and privacy-focused internet services.

Juels et al. (2003) propose the concept of a blocker tag in "The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy," presented at the 10th ACM Conference on Computer and Communications Security (CCS '03). This article addresses privacy concerns associated with radio frequency identification (RFID) technology, which can track and identify objects and individuals without their knowledge. The blocker tag is designed to prevent unauthorized scanning of RFID tags by selectively blocking communication. It achieves this by simulating numerous fake tags, effectively overwhelming unauthorized readers and preventing them from identifying genuine tags. The article details the technical implementation of the blocker tag, its effectiveness in protecting consumer privacy, and potential applications. This innovative solution represents a significant step forward in mitigating privacy risks in the growing use of RFID technology.

In "Foundations of Cryptography: Volume 2, Basic Applications," published by Cambridge University Press, Oded (2009) delves into the essential applications of cryptographic principles in various domains. This volume builds on the theoretical foundations laid out in the first volume, focusing on practical implementations and protocols. It covers a range of critical topics, including zero-knowledge proofs, encryption schemes, digital signatures, and secure multi-party computation. Goldreich provides rigorous definitions, proofs, and discussions on the security and efficiency of these cryptographic applications, making it a crucial resource for understanding how cryptographic techniques can be applied to secure communication, authentication, and data integrity in real-world scenarios. The book is well-regarded for its comprehensive and systematic approach, combining theoretical insights with practical relevance, thereby serving as an indispensable reference for students, researchers, and practitioners in the field of cryptography.

Backes et al. (2012) introduce "ObliviAd: Provably Secure and Practical Online Behavioral Advertising" at the 2012 IEEE Symposium on Security and Privacy. This article addresses the privacy concerns associated with online behavioral advertising, proposing a system that preserves user privacy while still allowing advertisers to deliver targeted ads. ObliviAd uses cryptographic techniques, including oblivious transfer and secure multi-party computation, to ensure that user data remains private and inaccessible to advertisers. The system guarantees that user profiles and ad preferences are not exposed, preventing potential misuse of sensitive information. The article provides a detailed analysis of the security and efficiency of ObliviAd, demonstrating its feasibility and practicality in real-world applications. This work represents a significant advancement in balancing privacy and targeted advertising in the digital age.

In "Threat Modeling: Designing for Security," published by Wiley, Shostack (2014) provides a comprehensive guide on incorporating threat modeling into the security design process. The book outlines methodologies and approaches for identifying, prioritizing, and mitigating potential threats to a system. Shostack

emphasizes the importance of understanding the attacker's perspective to anticipate and counteract potential security vulnerabilities effectively. The text covers different threat modeling techniques, such as spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privilege (STRIDE), attack trees, and the damage potential, reproducibility, exploitability, affected users, and discoverability (DREAD) model, offering practical advice on their implementation in various contexts. By integrating threat modeling into the development lifecycle, the book aims to enhance the overall security posture of applications and systems, making it an essential resource for security professionals, developers, and architects focused on designing secure systems.

In "Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World," published by W.W. Norton and Company, Schneier (2015) explores the extensive data collection practices by governments and corporations and the implications for privacy and personal freedom. Schneier, a renowned security expert, details how data are gathered, analyzed, and used, often without individuals' knowledge or consent. He examines the trade-offs between security and privacy, discussing the ways in which surveillance can be a tool for safety and a means of control. The book also offers insights into the regulatory and ethical challenges posed by pervasive data collection and provides practical advice on how individuals can protect their privacy. Schneier advocates for greater transparency, stronger privacy protections, and more robust oversight to balance the power dynamics between data collectors and the public. This work is essential for understanding the contemporary landscape of data privacy and the hidden battles over control of personal information.

Androulaki et al. (2018) present "Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains" in the Proceedings of the 13th EuroSys Conference. This article details Hyperledger Fabric, an open-source blockchain framework designed for developing enterprise-grade, permissioned blockchain applications. The framework supports modularity and flexibility, allowing developers to customize components such as consensus and membership services. The authors explain Hyperledger Fabric's architecture, which includes a novel execute-order-validate transaction flow that enables high throughput and scalability. The article also highlights the system's support for smart contracts, known as chaincode, and its robust security features tailored for enterprise needs. This work significantly advances the development of secure and scalable blockchain solutions in various industrial sectors.

LeCun et al. (2015) present an overview of deep learning in "Deep Learning," published in Nature. The authors provide a comprehensive summary of deep learning techniques, which are a subset of machine learning algorithms inspired by the structure and function of the brain's neural networks. The article discusses the key concepts, architectures, and advancements in deep learning, such as CNNs, recurrent neural networks (RNNs), and deep belief networks (DBNs). The authors highlight the significant impact of deep learning on various domains, including computer vision, speech recognition, natural language processing, and game playing, showcasing breakthroughs in tasks previously considered challenging for artificial intelligence. They explain how deep learning models have been able to achieve unprecedented performance by learning hierarchical representations of data through multiple layers of abstraction. Additionally, the article covers the challenges and future directions in deep learning research, such as the need for large, labeled datasets, computational resources, and the development of more efficient algorithms. This foundational work by LeCun, Bengio, and Hinton has been instrumental in advancing the field of artificial intelligence, providing a historical perspective and a roadmap for future research and applications.

In "Mastering the Game of Go with Deep Neural Networks and Tree Search," published in Nature, Schneier (2015) describes the development of AlphaGo, a computer program that achieved superhuman performance in the ancient game of Go. The article details how AlphaGo combines deep neural networks with Monte Carlo tree search to evaluate board positions and select moves. Key innovations include the use of two deep neural networks: a policy network to select the next move and a value network to predict the winner of the game from any given position. These networks were trained using a combination of supervised learning from human expert games and reinforcement learning from self-play. The system's architecture allows AlphaGo to evaluate and prioritize moves more effectively than traditional AI approaches. The article highlights AlphaGo's success in defeating the reigning world champion, marking a significant milestone in AI research. This work demonstrates the potential of combining deep learning with tree search methods for complex decision-making tasks and has broad implications for AI applications beyond games.

Vaswani et al. (2010) introduce the transformer model in their seminal article "Attention Is All You Need," published in Advances in Neural Information Processing Systems. This article revolutionizes natural language processing (NLP) by proposing a novel architecture based entirely on attention mechanisms, foregoing the need for recurrent or convolutional layers. The key innovation of the Transformer model is the self-attention mechanism, which allows the model to weigh the importance of different words in a sentence regardless of their distance from each other. This mechanism enhances the model's ability to capture long-range dependencies and contextual relationships in text. The article details how the Transformer uses multi-head attention to process input sequences in parallel, significantly improving training efficiency and performance. The authors also introduce positional encoding to retain the order of words in a sequence because the model itself does not inherently capture positional information. The Transformer achieves state-of-the-art results in several NLP tasks, such as translation and text generation, and forms the foundation for subsequent advancements like BERT and GPT. This work has profoundly impacted the field of deep learning, setting new standards for model architectures and inspiring a wide range of applications beyond NLP, including computer vision and speech processing.

Brown et al. (2020) present the GPT-3 model in their article "Language Models are Few-Shot Learners," published in Advances in Neural Information Processing Systems. This article introduces GPT-3, the third generation of the Generative Pre-trained Transformer, notable for its size and capabilities, with 175 billion parameters, significantly surpassing its predecessor, GPT-2, in scale. The authors demonstrate that GPT-3 excels at few-shot, one-shot, and zero-shot learning, where the model can perform tasks with

little to no task-specific training data. This is achieved through its massive pre-training on diverse internet text, enabling it to generalize across a wide range of language tasks. The model's ability to generate coherent and contextually relevant text based on minimal prompts is a key innovation, making it highly versatile for applications such as translation, question answering, and text completion. The article highlights the implications of such a large-scale model, discussing its potential and the challenges it poses, including computational resource requirements and ethical considerations. GPT-3's performance marks a significant advancement in natural language processing, pushing the boundaries of what AI language models can achieve.

The National Institute of Standards and Technology (NIST) published "Post-Quantum Cryptography: NIST's Plan for the Future" in 2017 (NIST and National Institute of Standards and Technology, 2017), outlining their strategy to address the emerging threat posed by quantum computers to current cryptographic systems. This document describes the need to develop and standardize quantum-resistant cryptographic algorithms, as quantum computers have the potential to break widely used public-key cryptosystems like Rivest–Shamir–Adleman (RSA), digital signature algorithm (DSA), and elliptic-curve cryptography (ECC) by leveraging Shor's algorithm. NIST's plan involves a multi-phase approach:

1. Call for proposals: NIST invited cryptographers and researchers to submit candidate algorithms for quantum-resistant cryptography. This phase aims to gather a diverse set of potential solutions for evaluation.
2. Evaluation process: Submitted algorithms undergo rigorous analysis and testing based on criteria such as security, performance, and implementation characteristics. This phase is critical for identifying the most promising candidates.
3. Standardization: The final phase involves selecting the best algorithms and developing standards for their implementation. This process ensures that the new cryptographic methods are robust, efficient, and ready for widespread adoption.

The document emphasizes collaboration with the global cryptographic community to ensure the proposed solutions meet the highest standards of security and practicality. NIST's proactive approach is essential to safeguard digital communication and information in a future where quantum computing capabilities are realized.

Bernstein (2011) compiled a comprehensive collection of research in "Post-Quantum Cryptography," published by Springer Science+Business Media. This book serves as a foundational resource for understanding the challenges and advancements in developing cryptographic algorithms that are secure against quantum attacks. The editors bring together contributions from leading experts in the field, covering a wide range of topics essential for post-quantum cryptography. Key areas of focus include:

1. Mathematical foundations: The book delves into the underlying mathematical principles that form the basis of post-quantum cryptographic algorithms, such as lattice-based, hash-based, code-based, and multivariate polynomial-based cryptography.
2. Algorithmic proposals: Detailed descriptions of various proposed algorithms that are believed to be resistant to quantum attacks. Each chapter provides theoretical analysis and practical considerations for implementing these algorithms.
3. Security analysis: Comprehensive analysis of the security properties of proposed post-quantum algorithms, including resistance to classical and quantum attacks.
4. Implementation challenges: Discussion of the practical aspects of deploying post-quantum cryptographic systems, including performance optimization, hardware considerations, and integration with existing protocols.
5. Standardization efforts: Insights into the global efforts to standardize post-quantum cryptographic algorithms, highlighting the collaborative work being done by institutions like NIST to ensure the robustness and interoperability of these new cryptographic standards.

"Post-Quantum Cryptography" is an essential text for researchers, practitioners, and students aiming to understand and contribute to the field of cryptography in the quantum era. It provides a thorough and detailed exploration of state-of-the-art techniques and the ongoing efforts to prepare for a post-quantum world.

Chen et al. (2016) present a comprehensive overview in "Report on Post-Quantum Cryptography," published by NIST. This report outlines the need for new cryptographic standards that can withstand the potential threats posed by quantum computing. As quantum computers have the capability to break widely used cryptographic schemes such as RSA, DSA, and ECC through algorithms like Shor's, this report is crucial for guiding the development of quantum-resistant cryptographic protocols. The report covers several key areas:

1. Threat assessment: The report evaluates the potential impact of quantum computing on current cryptographic systems, emphasizing the urgency of developing quantum-resistant algorithms.
2. Cryptographic algorithms: The report reviews various classes of post-quantum cryptographic algorithms, including lattice-based, hash-based, code-based, multivariate polynomial-based, and isogeny-based cryptography. Each class is assessed for its potential to provide security against quantum attacks.
3. Evaluation criteria: NIST outlines the criteria for evaluating the security and practicality of post-quantum algorithms, including security assumptions, performance metrics, and implementation considerations.
4. Standardization process: The report describes NIST's process for standardizing post-quantum cryptographic algorithms. This involves soliciting, evaluating, and selecting algorithms through a transparent and rigorous multi-phase process involving public and expert feedback.
5. Future directions: The report also discusses future research directions and the need for ongoing collaboration between academia, industry, and government to ensure the development of robust post-quantum cryptographic standards.

This detailed examination by NIST provides a roadmap for transitioning to cryptographic systems that are secure in the quantum era, underscoring the collaborative efforts required to address this significant challenge.

In "Lattice Signatures and Bimodal Gaussians," published in Advances in Cryptology—CRYPTO 2013, Ducas et al. (2013) introduce an innovative approach to constructing digital signatures based on lattice problems, which are believed to be secure against quantum attacks. The article presents a lattice-based signature scheme that uses bimodal Gaussian distributions to enhance security and efficiency. Key contributions include:

1. Lattice-based cryptography: The authors leverage the hardness of lattice problems, specifically the learning with errors (LWE) problem, which is conjectured to be resistant to classical and quantum attacks. This provides a strong security foundation for the proposed signature scheme.
2. Bimodal Gaussian sampling: A novel technique involving bimodal Gaussian distributions is introduced. This method improves the efficiency of the signature generation process while maintaining high security levels. The bimodal approach helps in achieving smaller signature sizes and faster computation times than previous lattice-based schemes.
3. Provable security: The article provides rigorous proofs of security for the proposed scheme, demonstrating its resilience against various types of attacks. The security is based on well-established hardness assumptions related to lattice problems.
4. Performance evaluation: The authors conduct thorough performance evaluations, showing that their scheme offers practical efficiency suitable for real-world applications. The results indicate that the lattice-based signatures can be competitive with traditional cryptographic methods in terms of speed and size.

This work significantly advances the field of post-quantum cryptography by providing a practical and secure lattice-based signature scheme, paving the way for future research and development in quantum-resistant cryptographic protocols.

Sommer and Paxson (2010) examine the challenges and potential of applying machine learning to network intrusion detection in "Outside the Closed World: On Using Machine Learning for Network Intrusion Detection," presented at the 2010 IEEE Symposium on Security and Privacy. The authors critically analyze the efficacy of machine learning techniques in detecting network intrusions, highlighting the gap between academic research and practical deployment in real-world environments. Key points discussed include:

1. Real-world constraints: The authors argue that most academic research in network intrusion detection using machine learning operates in a "closed world," where the data and conditions are controlled and predictable. In contrast, real-world network environments are dynamic, heterogeneous, and subject to evolving threats, making it challenging to apply static machine learning models effectively.
2. Training data and labeling: One of the significant hurdles identified is the availability and quality of training data. Network traffic data are vast and often lacks labeled instances of intrusions, which are crucial for training supervised machine learning models. The article emphasizes the need for better data collection and labeling practices to improve the training process.
3. Model adaptation and robustness: Machine learning models must adapt to changes in network behavior and new types of attacks. The authors discuss the importance of building models that are not only accurate but also robust and adaptable to new and unseen threats. They propose incorporating domain knowledge and continuous learning mechanisms to enhance model performance.
4. Evaluation metrics: The article critiques the common evaluation metrics used in research, such as detection rates and false-positive rates, which may not accurately reflect the practical performance of intrusion detection systems. The authors call for more comprehensive evaluation frameworks that consider the operational context and costs of errors.
5. Integration with existing systems: The successful deployment of machine learning-based intrusion detection systems requires seamless integration with existing network security infrastructures. The article highlights the need for interoperability and for complementing traditional signature-based detection methods.

Sommer and Paxson's work provides valuable insights into the practical challenges of deploying machine learning for network intrusion detection, advocating for a more holistic and adaptive approach to addressing these issues in real-world scenarios.

Shafiq et al. (2009) introduced "PE-Miner: Mining Structural Information to Detect Malicious Executables in Realtime" at the 2009 IEEE Symposium on Security and Privacy. This article presents PE-Miner, a novel system that detects malicious executables by analyzing their structural properties. The system uses data mining techniques to extract and analyze structural information from portable executable (PE) files, which are the standard format for executables, object code, and DLLs in Windows operating systems. Key contributions include:

1. Structural analysis: PE-Miner focuses on the structural features of PE files, such as header information, section names, and the directory table, to identify anomalies indicative of malicious code. This approach contrasts with traditional signature-based methods that rely on known patterns of malicious behavior.
2. Data mining techniques: The system employs various data mining algorithms to build models that can differentiate between benign and malicious executables. By training these models on large datasets of known malware and legitimate software, PE-Miner achieves high accuracy in detecting previously unseen malicious files.
3. Real-time detection: One of the critical advantages of PE-Miner is its capability to operate in real time, providing immediate detection of potential threats. This is essential for maintaining the security of systems against rapidly evolving malware.
4. Experimental evaluation: The article presents a thorough evaluation of PE-Miner, demonstrating its effectiveness in identifying malicious executables with a low false-positive

TABLE 1 Literature summary.

Author	Numerical reference	Main contribution	Gap in the literature
Goodfellow et al.	1	GANs for training generative models	Need for integration with privacy-preserving techniques
Kingma and Welling	2	Auto-encoding variational Bayes for deep generative models	Scalable and efficient unsupervised learning
Radford et al.	3	Deep convolutional GANs	Stability and performance of GANs
Lyubashevsky et al.	4	Ring learning with errors for lattice-based cryptography	Efficiency in post-quantum cryptographic schemes
Alkim et al.	5	NewHope post-quantum key exchange protocol	Practical implementation in real-world applications
Ben-Sasson et al.	6	Zk-SNARKs for zero-knowledge proofs	Efficient verification in secure computation
Gentry	7	Fully homomorphic encryption using ideal lattices	Handling noise in fully homomorphic encryption
Sahai and Waters	8	Indistinguishability obfuscation for deniable encryption	Applications of indistinguishability obfuscation
Bünz et al.	9	Bulletproofs for short zero-knowledge proofs	Computational overhead in zero-knowledge proofs
Buterin	10	Ethereum platform for decentralized applications	Scalability and security of decentralized platforms
Wood	11	Ethereum technical specifications	Technical challenges in decentralized applications
Poon and Dryja	12	Bitcoin Lightning Network for scalable payments	Real-world scalability and security of off-chain protocols
Douceur	13	Identification of Sybil attacks	Preventing Sybil attacks in decentralized networks
Danezis and Mittal	14	SybilInfer framework for detecting Sybil nodes	Scalability of Sybil detection methods
Zyskind et al.	15	Decentralizing privacy using blockchain	Implementation in privacy-preserving data management
Chaum	16	Untraceable electronic mail and digital pseudonyms	Secure anonymous communication protocols
Juels et al.	17	Blocker tag for RFID privacy	Selective blocking in RFID technology
Goldreich	18	Applications of cryptographic principles	Practical implementation of cryptographic protocols
Backes et al.	19	ObliviAd for secure online behavioral advertising	Balancing privacy and targeted advertising
Shostack	20	Threat modeling for security design	Effective integration into security design processes
Schneier	21	Data collection and privacy implications	Regulatory and ethical challenges in data privacy
Androulaki et al.	22	Hyperledger Fabric for enterprise blockchains	Scalability and modularity of blockchain frameworks
LeCun et al.	23	Overview of deep learning techniques	Challenges in training deep learning models
Silver et al.	24	AlphaGo for playing Go	Combining deep learning with tree search
Vaswani et al.	25	Transformer model for NLP	Long-range dependencies in NLP
Brown et al.	26	GPT-3 for few-shot learning	Ethical and computational challenges of large models
NIST	27	NIST's plan for post-quantum cryptography	Development and standardization of quantum-resistant algorithms
Bernstein et al.	28	Post-quantum cryptography book	Challenges in post-quantum cryptographic implementations
Chen et al.	29	Report on post-quantum cryptography	Security against quantum attacks
Ducas et al.	30	Lattice-based digital signatures	Efficiency of lattice-based signatures
Sommer and Paxson	31	Machine learning for network intrusion detection	Real-world applicability of intrusion detection models
Shafiq et al.	32	PE-Miner for detecting malicious executables	Real-time detection of malicious code
Regev	33	Lattice-based cryptography	Quantum resistance in cryptographic applications
Peikert	34	Decade review of lattice cryptography	Review of advancements in lattice cryptography
Micciancio and Regev	35	Practical implementations of lattice-based cryptography	Practicality of lattice-based cryptographic schemes
Yu et al.	41	SybilGuard for detecting Sybil attacks	Decentralization in Sybil attack detection

rate. The authors compare their system's performance against existing detection methods, showing significant improvements in accuracy and speed.

5. Practical implications: The results of this research have practical implications for enhancing computer system security. By integrating PE-Miner into existing security infrastructures, organizations can improve their ability to detect and respond to malware threats in real time.

This work highlights the potential of using structural information and data mining techniques to improve malware detection systems, offering a robust and efficient solution for real-time security challenges.

3.1 Summary of the findings and the gaps in the reviewed literature

This article reviews the fundamental literature on quantum-resistant cryptography, privacy-preserving technologies, and decentralized systems. The reviewed works lay the foundation for developing a robust, scalable, and privacy-preserving digital identity framework, particularly relevant in the context of looming quantum computing threats. Table 1 below encapsulates key contributions and identifies gaps in the current literature, providing a comprehensive overview of the state of the art in digital identity technologies.

Table 1 summarizes the significant contributions and existing gaps in the literature related to digital identity management, highlighting the interdisciplinary nature of this field. Authors like Goodfellow et al. and Kingma and Welling have advanced the field of generative models with their work on GANs and VAEs, which are instrumental in creating synthetic identities. Lyubashevsky et al. and Alkim et al. contribute to the realm of quantum-resistant cryptography, essential for securing digital identities against future quantum threats. Ben-Sasson et al. (2025) and Gentry pioneered privacy-preserving technologies such as zk-SNARKs and fully homomorphic encryption, which are critical for ensuring data security without compromising user privacy. The decentralization efforts by Buterin and Wood, through their work on Ethereum, provide a solid foundation for decentralized identity management systems that mitigate the risks associated with centralized solutions.

Despite these advancements, significant gaps remain, particularly in integrating these diverse technologies into a cohesive and practical digital identity framework. The need for scalable and efficient post-quantum cryptographic schemes, as well as the practical implementation of privacy-preserving techniques in real-world applications, is evident. Moreover, addressing the scalability and security challenges in decentralized platforms is crucial for widespread adoption. This underscores the importance of integrating quantum-resistant cryptography, AI-generated synthetic identities, and decentralized systems to create a comprehensive digital identity management solution. The quantum-proof digital passport framework bridges these gaps, offering a robust, secure, and privacy-preserving digital identity solution for the post-quantum era.

The quantum-proof digital passport framework is vital for several reasons. First, quantum computing presents a substantial threat to traditional cryptographic systems. This framework incorporates post-quantum cryptographic techniques, such as lattice-based cryptography, to ensure long-term security against quantum attacks. Second, it preserves privacy by combining zero-knowledge proofs, homomorphic encryption (HE), and blockchain oracles, allowing users to prove their identities without disclosing personal details. Third, it addresses the vulnerability of centralized identity systems to single points of failure and attacks by leveraging blockchain technology to decentralize identity management, thus enhancing security and user control over personal data. Additionally, the framework integrates advanced AI technologies, such as GANs and variational autoencoders (VAEs), to generate synthetic identities. This results in realistic yet anonymized identities, improving the robustness of the identity verification process. The framework's design also ensures scalability, handling large numbers of users and transactions, while maintaining interoperability with existing systems through standardized protocols and blockchain oracles. Moreover, the framework can be applied across various sectors, including finance, healthcare, and e-commerce, to enhance the security and privacy of digital transactions, reduce fraud, and increase user trust. By addressing these critical aspects, the QPDP framework represents a significant advancement in digital identity management, offering a secure, privacy-preserving, and scalable solution for the post-quantum era.

3.1.1 Quantum-resistant cryptography

Advances in quantum computing present significant challenges to existing cryptographic systems, as highlighted by Regev and Lattices (2005), Peikert (2016), and Micciancio and Regev (2009). Lattice-based cryptography has emerged as a key candidate for post-quantum cryptography, offering robust security features resistant to quantum attacks. Regev's foundational work (Lyubashevsky et al., 2010) laid the groundwork by demonstrating the potential of lattices in cryptographic functions.

3.2 Post-quantum cryptographic algorithm selection and migration strategy

The implementation of the QPDP framework relies on a selection of lattice-based algorithms endorsed by the U.S. National Institute of Standards and Technology (NIST) Post-Quantum Cryptography (PQC) Standardization Project. Algorithm selection was guided by three principal criteria: (i) resistance to quantum adversaries under Shor's and Grover's algorithms, (ii) computational efficiency for real-time identity verification, and (iii) interoperability with existing blockchain and identity infrastructures.

3.2.1 Selected algorithms and rationale

- CRYSTALS-Kyber (Key Encapsulation Mechanism, FIPS 203 draft):

Selected as the primary key-exchange mechanism due to its compact ciphertexts and rapid encapsulation/decapsulation times.

Key sizes: 1,184 bytes (Kyber-768).

TABLE 2 PQC algorithm comparison/performance comparison and quantum-security analysis of post-quantum cryptographic algorithms (Kyber, Dilithium, and Falcon) implemented in the quantum-proof digital passport framework against the classical elliptic-curve baseline (ECC-P-256). The table summarizes key sizes, signature or ciphertext lengths, average computation times for encapsulation, signing, and verification, corresponding quantum-security levels, and trade-offs relevant to digital identity verification performance.

Algorithm	Type	Public-key size (bytes)	Ciphertext/ signature (bytes)	Encapsulation/ sign (ms)	Verification (ms)	Quantum-security level	Notable trade-off
ECC-P-256	Classical	64	64	0.35	0.40	Vulnerable	Small size, quantum-insecure
Kyber-768	PQC (KEM)	1,184	1,088	0.42	0.52	128-bit	Moderate key growth
Dilithium-3	PQC (signature)	2,592	4,592	0.89	1.20	128-bit	Larger signatures
Falcon-512	PQC (signature)	897	666	1.10	0.90	128-bit	Requires fast Fourier transform (FFT) precision

Performance: Encapsulation ≈ 0.42 milliseconds, decapsulation ≈ 0.52 milliseconds on commodity CPUs.

Rationale: Achieves 128-bit quantum-level security and demonstrates minimal latency increase (<10%) relative to an ECC-based elliptic-curve Diffie–Hellman (ECDH) protocol in benchmarking.

Kyber's polynomial ring arithmetic aligns naturally with lattice-based digital signature schemes, ensuring seamless interoperability.

- CRYSTALS-Dilithium (Digital Signature, FIPS 204 draft):

Used for credential issuance and signature verification.

Key sizes: 2,592 bytes (Dilithium-3).

Signature size: 4,592 bytes.

Performance: Signing ≈ 0.89 milliseconds, verification ≈1.20 milliseconds, measured on an Intel Xeon 3.4 GHz CPU with 32 GB RAM.

Rationale: Deterministic signing process with constant-time arithmetic minimizes side-channel leakage. Its compatibility with Kyber permits a unified security basis, reducing implementation complexity.

- Falcon (Alternative Digital Signature Scheme):

Included for comparative evaluation, leveraging fast Fourier sampling for smaller signature sizes (666 bytes for Falcon-512).

Trade-off: Offers higher verification speed but requires floating-point arithmetic, which introduces precision and hardware-dependency risks. Therefore, it is proposed for lightweight or resource-constrained identity nodes only.

3.2.2 Performance trade-offs and security considerations

Table 2 summarizes the performance and security trade-offs among selected PQC algorithms compared with classical elliptic-curve cryptography (ECC-P-256).

Despite larger key and signature sizes, both Kyber and Dilithium maintain acceptable operational latency for real-time identity verification, with an average increase of ~17% in cryptographic overhead compared to ECC-based systems. These parameters were empirically validated in Section 4.4 (*Experimental Implementation and Benchmarking*).

3.2.3 Migration challenges and strategic considerations

Transitioning from classical cryptography to PQC within identity frameworks introduces several practical and organizational challenges:

- Backward compatibility: Existing digital identity infrastructures (e.g., X.509 certificates, OAuth tokens) are bound to RSA/ECC primitives. Migration requires hybrid certificates supporting both classical and PQC keys to maintain compatibility during transitional periods.
- Key management complexity: Larger key sizes necessitate enhanced storage and transmission capabilities, impacting constrained devices such as IoT-based identity verifiers.
- Protocol interoperability: PQC algorithms must be integrated into existing TLS, DIDComm, and blockchain transaction protocols without disrupting consensus mechanisms or interoperability with legacy nodes.
- Standardization lag: As PQC standards mature (FIPS 203/204 finalization is expected in 2025–2026), cross-vendor toolchains are still evolving, demanding adaptive implementations.
- Regulatory adaptation: Governance and compliance frameworks (e.g., eIDAS 2.0 and ISO/IEC JTC 1/SC 27) must recognize PQC algorithms as approved cryptographic primitives for identity assurance.

3.2.4 Migration pathway for the quantum-proof digital passport framework

To address these challenges, a phased hybrid-cryptography deployment model is proposed:

1. Phase I–hybrid coexistence: Implement Kyber/Dilithium alongside ECC (dual-signature mode) to ensure backward compatibility and facilitate gradual adoption.
2. Phase II–progressive PQC enforcement: Mandate PQC-only key negotiation for inter-node communications while retaining hybrid verification for legacy clients.

3. Phase III–full PQC transition: Replace all classical primitives once ecosystem-wide PQC support (FIPS-certified libraries) is achieved.

This migration approach ensures cryptographic agility and preserves system integrity throughout the transition to a fully quantum-resistant identity ecosystem.

3.2.4.1 Zero-knowledge proofs and homomorphic encryption

Zero-knowledge proofs and homomorphic encryption are used to maintain privacy in digital transactions. Ben-Sasson et al. (2025), Ben-Sasson et al. (2014) introduced zk-SNARKs, enabling succinct, non-interactive proofs that verify computations without revealing underlying data. Gentry's pioneering work (Gentry, 2009) on fully homomorphic encryption allowed computations on encrypted data, providing a foundation for secure, privacy-preserving data processing.

The contributions of Sahai and Watersy (2014) further enhanced indistinguishability obfuscation, a critical component in deniable encryption and secure computation. Bünz et al. (2018) developed Bulletproofs, a short proof system for confidential transactions, which significantly reduces the computational overhead associated with zero-knowledge proofs. The advancements in these cryptographic techniques ensure robust privacy and security in digital interactions, essential for safeguarding sensitive information in an era of increasing cyber threats.

3.2.4.2 Blockchain and decentralized identifiers

Blockchain technology, first introduced by Nakamoto (2008), has revolutionized secure, decentralized transactions. The development of decentralized identifiers (W3C, 2022) and smart contracts (Buterin, 2014) has expanded blockchain's applications, facilitating secure, autonomous digital interactions. Wood (2014) and Poon and Dryja (2016) contributed to the scalability and security of blockchain networks with their work on Ethereum and the Bitcoin Lightning Network, respectively.

Nakamoto's introduction of blockchain as a peer-to-peer electronic cash system (Nakamoto, 2008) laid the foundation for decentralized, secure transactions. The W3C's development of decentralized identifiers (W3C, 2022) standardized the use of decentralized identities, enabling users to control their digital identities without reliance on central authorities. Buterin's Ethereum white paper (Vitalik and Wood, 2013) and Wood's subsequent Ethereum Project yellow paper (Wood, 2014) provided the framework for smart contracts, allowing programmable, trustless transactions on the blockchain. Poon and Dryja (2016) enhanced blockchain scalability with the Bitcoin Lightning Network, enabling fast, low-cost transactions. These innovations have significant implications for secure digital identity management, addressing critical issues of privacy and scalability in decentralized systems.

3.2.4.3 Sybil attack detection

Sybil attacks, wherein malicious entities create multiple fake identities to subvert network systems, remain a significant challenge. Douceur (2002) first identified this issue, and subsequent research by Shostack (2014) and Schneier (2015) proposed detection mechanisms leveraging social network analysis.

Douceur's identification of Sybil attacks highlighted the vulnerability of peer-to-peer networks to identity fraud. Danezis and Mittal (2009) introduced SybilInfer, a method that detects Sybil nodes using social network structures, while Yu et al. (2008) developed SybilGuard, which uses social networks' inherent trust relationships to mitigate Sybil attacks. These methods have been instrumental in advancing our understanding of identity verification in decentralized networks, though integrating these techniques into a cohesive system remains an ongoing research challenge.

3.2.4.4 Advanced privacy techniques

Ensuring privacy in digital systems is paramount, as demonstrated by the work of Zyskind et al. (2015), Chaum (1981), and Chaum (1983). Zyskind et al. (2015) explored the use of blockchain to decentralize privacy, protecting personal data from centralized breaches. Chaum's seminal work on untraceable electronic mail (Chaum, 1981; Chaum, 1983) introduced the concept of digital pseudonyms, laying the groundwork for anonymous communications.

Further advancements by Juels et al. (2003), Juels and Wattenberg (1999), and Backes et al. (2012) addressed practical privacy concerns. Juels et al. (2003) introduced the blocker tag, a selective blocking mechanism for RFID tags, enhancing consumer privacy. Backes et al. (2012) developed ObliviAd, a provably secure system for online behavioral advertising, demonstrating the applicability of cryptographic techniques in real-world privacy scenarios. These studies underscore the importance of integrating advanced privacy techniques into digital systems to protect user data.

3.2.4.5 AI techniques and applications

The intersection of AI and cybersecurity offers innovative solutions for identity verification and fraud prevention. Goodfellow et al. (2014) introduced generative adversarial networks (GANs), which, along with variational autoencoders (VAEs) developed by Kingma and Welling (2013), provide robust frameworks for generating synthetic identities. Radford et al. (2015) extended this work, demonstrating the practical applications of GANs in creating realistic, anonymized data.

GANs and VAEs have revolutionized AI by enabling the generation of high-quality synthetic data, crucial for applications in digital identity verification and fraud detection. Goodfellow et al. (2014) demonstrated the potential of GANs in creating realistic images, while Kingma and Welling (2013) introduced VAEs, which provide a probabilistic approach to data generation. Radford et al. (2015) further demonstrated the practical applications of GANs, emphasizing their utility in generating anonymized identities for secure digital transactions.

3.3 Functional role of generative AI in digital identity verification

While traditional anonymization and pseudonymization techniques mask or remove personally identifiable information (PII), they fundamentally rely on deterministic transformations

of existing data (e.g., tokenization, hashing, or attribute suppression). Such transformations are reversible or re-identifiable when cross-referenced with auxiliary datasets, limiting their resilience against advanced re-identification attacks.

In contrast, generative artificial intelligence (AI), specifically GANs and variational autoencoders (VAEs), introduces a probabilistic and non-deterministic model for identity representation. Instead of modifying real data, these models synthesize new data distributions that statistically emulate authentic identity attributes (biometric, behavioral, and transactional) without any one-to-one correspondence to real individuals.

3.3.1 Contribution of generative AI beyond synthetic data creation

Generative AI in the QPDP framework serves three distinct operational functions:

- Identity abstraction**:** GANs construct latent-space embeddings that capture multidimensional relationships among identity attributes (e.g., voice-face-keystroke correlations). This embedding enables zero-knowledge verifiable proofs of identity consistency without revealing raw personal features.
- Adversarial authentication: The discriminator network in GANs is repurposed as a real-time identity verifier. By evaluating the statistical authenticity of presented credentials against the learned distribution of valid synthetic identities, it performs a form of adversarial anomaly detection that distinguishes genuine from forged credentials.
- Privacy-preserving regeneration: When identity data are compromised or expired, VAEs allow *identity regeneration* by sampling new latent vectors consistent with prior authorization proofs. This dynamic regeneration capability contrasts with static anonymization, enabling continuous privacy refresh cycles without compromising verifiability.

3.3.2 Quantitative differentiation from anonymization and pseudonymization

Empirical metrics applied in the benchmarking stage demonstrate measurable advantages:

- Re-identification risk: Synthetic identities generated by GANs achieved <0.3% re-identification probability when tested against linkage attacks using k-anonymity and differential-privacy benchmarks, compared to 4%–7% for traditional pseudonymized datasets.
- Information utility: GAN-generated identities retained 93% feature utility (measured via downstream classifier accuracy) *versus* 65%–70% for anonymized datasets, indicating that privacy gains are achieved without significant utility loss.
- Entropy and uniqueness: The average Shannon entropy across synthetic identity feature vectors was 1.8× higher than that of pseudonymized records, reflecting greater diversity and reduced correlation with source data.

3.3.3 Integration within the verification pipeline

During digital passport verification, the system does not match user data directly. Instead, it verifies the *statistical conformity* of a user's encrypted attributes with a corresponding synthetic identity profile stored on the blockchain. The adversarial discriminator outputs a probabilistic authenticity score, which is then attested through a zero-knowledge proof. This mechanism transforms generative AI from a data-synthesis utility into a privacy-preserving identity validator, fundamentally different from deterministic anonymization pipelines.

Through this probabilistic verification paradigm, generative AI enhances *security* (by mitigating model inversion and correlation attacks) and *privacy* (by eliminating one-to-one data mappings). This demonstrates the tangible and measurable contribution of AI beyond synthetic data creation, validating its integration within the QPDP framework.

3.4 Discussion on the gaps identified in existing literature

The review of digital identity management literature reveals significant challenges and gaps, necessitating the development of a robust, secure, and privacy-preserving system. Existing centralized identity solutions, such as the EU's eIDAS and India's Aadhaar, often impose a trade-off between security and privacy, a compromise that is increasingly untenable given the rise of sophisticated cyber threats and the impending advent of quantum computing. This research proposes a decentralized, AI-driven protocol that applies advanced cryptographic techniques to ensure security and privacy, addressing critical vulnerabilities in current systems.

3.4.1 Security vs. privacy trade-off

Current digital identity frameworks often prioritize security over user privacy. For instance, biometric-based systems like Aadhaar provide robust security but compromise privacy due to the extensive collection and storage of personal data. The proposed methodology integrates zero-knowledge proofs and homomorphic encryption (HE) to enable users to verify their identity without revealing personal details, thus preserving privacy while maintaining security (Schneier, 2015; Androulaki et al., 2018).

3.4.2 Lack of decentralization

Centralized identity systems are prone to single points of failure and are attractive targets for attackers. By using blockchain technology and decentralized identifiers, the proposed system enhances resilience against such vulnerabilities. This approach aligns with global trends toward decentralized identity management, as exemplified by Estonia's e-Residency and the European Union's eIDAS framework (Zyskind et al., 2015; Shostack, 2014).

3.4.3 Quantum computing threats

Quantum computing poses a significant threat to current cryptographic methods, as algorithms like Shor's can potentially break widely used public-key cryptosystems. The research incorporates NIST-approved post-quantum cryptographic techniques, such as lattice-based cryptography, to future-proof digital identities against quantum attacks. This proactive measure addresses the emerging security risks posed by advances in quantum

computing (NIST and National Institute of Standards and Technology, 2017; Chen et al., 2016).

3.4.4 Societal, industrial, and policy needs

3.4.4.1 Societal impact

Enhancing digital identity security can significantly mitigate the risks of identity theft and fraud, which currently affect millions globally and cause considerable financial and emotional distress. By providing robust privacy-preserving solutions, this research aims to foster greater trust in digital interactions and empower individuals with control over their personal data (Schneier, 2015; Bernstein, 2011).

3.4.4.2 Industrial applications

Secure digital identity systems are critical for various sectors, including finance, healthcare, and e-commerce. For example, financial institutions can integrate the proposed digital passport system to enhance online banking security, thereby reducing fraud and increasing customer trust. In healthcare, securely managing patient identities can protect sensitive medical information, thus improving data integrity and privacy (Androulaki et al., 2018; Sommer and Paxson, 2010).

3.4.4.3 Policy and regulation

Governments and regulatory bodies increasingly recognize the importance of interoperability and standardization in digital identity systems. Initiatives such as NIST's efforts to standardize post-quantum cryptographic algorithms underscore the necessity for robust, secure, and interoperable identity solutions that can withstand future technological advancements (NIST and National Institute of Standards and Technology, 2017; Ducas et al., 2013).

3.4.4.4 Security considerations

The proposed methodology integrates cutting-edge security technologies, including blockchain oracles and quantum-resistant cryptography, essential for developing systems resilient to evolving cyber threats. This approach enhances security and aligns with regulatory frameworks aimed at protecting digital identities and personal data (Zyskind et al., 2015; Chen et al., 2016).

The theoretical development of a new research methodology addresses gaps in existing digital identity systems by integrating advanced AI and cryptographic techniques to ensure security, privacy, and decentralization. The emerging algorithmic configuration research design approach is crucial for safeguarding digital interactions against emerging threats and aligns with societal, industrial, and regulatory needs for strong and interoperable identity solutions.

3.5 Research design, algorithmic configuration, and theoretical justification

The research adopts a hybrid methodology that combines theoretical architectural design with a limited experimental validation stage. The primary purpose of the study is to establish a conceptual and standards-compliant framework, the QPDP framework, demonstrating how post-quantum cryptography (PQC), blockchain, and generative AI can be coherently integrated within a decentralized identity ecosystem. The framework's feasibility is supported through algorithmic design specifications and controlled benchmarking, thereby bridging conceptual and applied perspectives.

3.5.1 Conceptual framework justification

The study's core contribution is architectural: it defines the interoperability logic, cryptographic layering, and data-governance principles required to build privacy-preserving digital identity systems in the post-quantum era. This theoretical orientation is intentional and justified by the fact that large-scale implementation of PQC within decentralized identity infrastructures remains technologically nascent. Therefore, the research contributes a reference model and design ontology that can be used to guide future empirical implementations, rather than an exhaustive system deployment.

3.5.2 Experimental design and algorithmic selection

A partial prototype was implemented to validate conceptual feasibility, focusing on performance-critical modules:

- Post-quantum cryptography (PQC): implemented using CRYSTALS-Kyber for key encapsulation and CRYSTALS-Dilithium for digital signatures (both NIST PQC Round 3 finalists). Key sizes of 1,184 bytes (Kyber-768) and 2,592 bytes (Dilithium-3) were chosen to balance quantum resistance and throughput efficiency.
- Generative AI: implemented using StyleGAN2 (for biometric and behavioral identity synthesis) and Variational Autoencoder (β-VAE) architectures with latent dimensions = 128 and $\beta = 2.5$ to control disentanglement.
- Zero-knowledge proofs: realized with zk-SNARKs (Groth16), producing average proof sizes of 128 bytes and verification times of ~8 milliseconds on commodity hardware.
- Homomorphic encryption (HE): implemented using Microsoft SEAL v4.1, configured for a Brakerski-Fan-Vercauteren (BFV) scheme with polynomial modulus degree = 8192 and coefficient modulus = 218 bits.
- Blockchain layer: deployed via Hyperledger Fabric v3.0, using Practical Byzantine Fault Tolerance (PBFT) consensus and Chaincode v2.0 smart-contract modules for verifiable credential (VC) management.

3.5.3 Evaluation metrics

The following performance and privacy metrics were used to assess prototype feasibility (as detailed in Section 4.4, *Experimental Implementation and Benchmarking*):

- Latency (ms): time per identity verification transaction.
- Throughput (TPS): verified identity transactions per second.
- Cryptographic overhead (%): relative computational cost of PQC *versus* classical ECC.
- Re-identification risk (%): probability of reverse-mapping synthetic to real identities.
- Utility retention (%): proportion of semantic information preserved in synthetic data.

- Entropy (H): average information entropy of identity feature vectors.

3.5.4 Methodological alignment and replicability

All algorithms and parameters were selected to comply with NIST PQC standards (FIPS 203/204) and W3C DID/VC specifications. The computational environment, data pipelines, and cryptographic configurations are fully reproducible on open-source frameworks (Open Quantum Safe, Microsoft SEAL, TensorFlow, and Hyperledger). This ensures the framework is transparent, replicable, and methodologically valid for subsequent applied studies.

4 The quantum-proof digital passport framework

The design of existing digital identity systems often necessitates a trade-off between security and privacy. For example, centralized solutions like the EU's eIDAS lack decentralization, exposing vulnerabilities. Biometric-based systems such as Aadhaar ensure security but sacrifice privacy. This research study proposes a decentralized, privacy-preserving (Zyskind et al., 2015) AI protocol, based on the Transformer model architecture attention mechanisms (Vaswani et al., 2010; Brown et al., 2020), that overcomes these limitations, offers enhanced security and user control, and converges theoretical foundations into practical implementations and protocols (Oded, 2009). Despite significant advancements in quantum-resistant cryptography, zero-knowledge proofs, HE (Gentry, 2009), and blockchain technology, a critical gap in integrating these technologies into a unified, robust system for digital identity management remains. We propose to address this gap by combining generative AI, blockchain, and NIST-approved post-quantum cryptographic techniques (NIST and National Institute of Standards and Technology, 2017; Chen et al., 2016) to develop a secure, scalable, and privacy-preserving quantum-proof digital passport system. This integrated approach will provide more robust oversight to balance the power dynamics between data collectors and the public with an understanding that surveillance can be both a tool for safety and a means of control (Schneier, 2015), ensuring robust security against quantum threats, enhancing user privacy through advanced cryptographic techniques, and providing a scalable framework for digital identity management. The digital passport integrated system will provide modularity and flexibility, similar to the Hyperledger Fabric (Alkim et al., 2016), allowing developers to customize components such as consensus and membership services and learn hierarchical representations of data through multiple layers of abstraction (LeCun et al., 2015) that combine deep learning with tree search methods for complex decision-making tasks (Silver et al., 2016). The development of such a system is crucial in addressing the growing need for secure, privacy-preserving digital interactions in an increasingly interconnected world. Advancements in AI and quantum computing create new risks for increasing the sophistication of cyberattacks. As digital interactions continue to grow, the need for secure and privacy-preserving identity solutions becomes more critical and more urgent. The many quantum computers that exist today are not yet very powerful. As they become more powerful, adversaries could abuse the new technology to endanger our security and privacy. New technologies such as generative AI, blockchain oracles, and post-quantum cryptography (Bernstein, 2011) can be harnessed to help prevent breaches of security affecting, for example, individual privacy, the banking system, and medical records.

The QPDP framework advances the global cybersecurity infrastructure by developing a new AI-based blockchain protocol for autonomously managing anonymous digital passports. The digital passports use oblivious transfer and a secure multi-party computation system that preserves user privacy, similar to ObliviAd, which allows advertisers to deliver targeted ads (Backes et al., 2012). Such digital passports will be used as proof of human identity and would help prevent bots, Sybil attacks (Douceur, 2002), and money-laundering activities on the blockchain. As discussed below, the digital passports will be designed using knowledge from existing global efforts, including the European Union's eIDAS or Estonia's e-Residency. They will address critical challenges in digital identity management, including privacy, security, and scalability. The novelty of the QPDP framework lies in understanding the attacker's perspective to anticipate and counteract potential security vulnerabilities (Shostack, 2014) in the process of integrating generative AI, blockchain oracles, and quantum-resistant cryptographic techniques to create secure and anonymous digital passports. This QPDP framework uniquely uses GANs (Goodfellow et al., 2014) and VAEs (Kingma and Welling, 2013) to generate synthetic identities operating in a similar way to the blocker tag for RFID (Juels et al., 2003), ensuring anonymity and authenticity in a similar way to the untraceable electronic mail using digital pseudonyms (Chaum, 1981), and combining deep learning techniques with adversarial training (Radford et al., 2015). Unlike current efforts, including those at GitHub Passport, this approach directly addresses the emerging challenge of quantum computing vulnerabilities by incorporating lattice-based cryptography to safeguard against future quantum attacks. Furthermore, the QPDP framework advances privacy-preserving technologies by integrating zero-knowledge proofs and homomorphic encryption within a decentralized framework using decentralized identifiers (W3C, 2022) containing information about an identity and verifiable credentials (VCs) to store and represent machine-readable credentials. To ensure privacy and decentralization, the proposed VCs would be based on specific activities that only humans could perform, similar to the Linea campaigns, but specific to digital identity proofs. Unlike BrightID, which relies solely on blockchain for user-centric identity, or Identity Hubs and SecureKey, which use centralized or federated systems, this approach ensures decentralization, enhancing user control and autonomy. While biometric authentication methods, such as Aadhaar, provide security, they often compromise privacy; this project employs zero-knowledge proofs and homomorphic encryption to maintain privacy and security. Civic and Polygon ID leverage blockchain, but the inclusion of quantum-resistant cryptography strengthens long-term security. Platforms like Galxe and kycDAO focus on community-based and decentralized know your customer (KYC), but the use of synthetic identities via GANs and VAEs ensures high anonymity and authenticity, setting a new standard in privacy-preserving identity verification. Unlike the

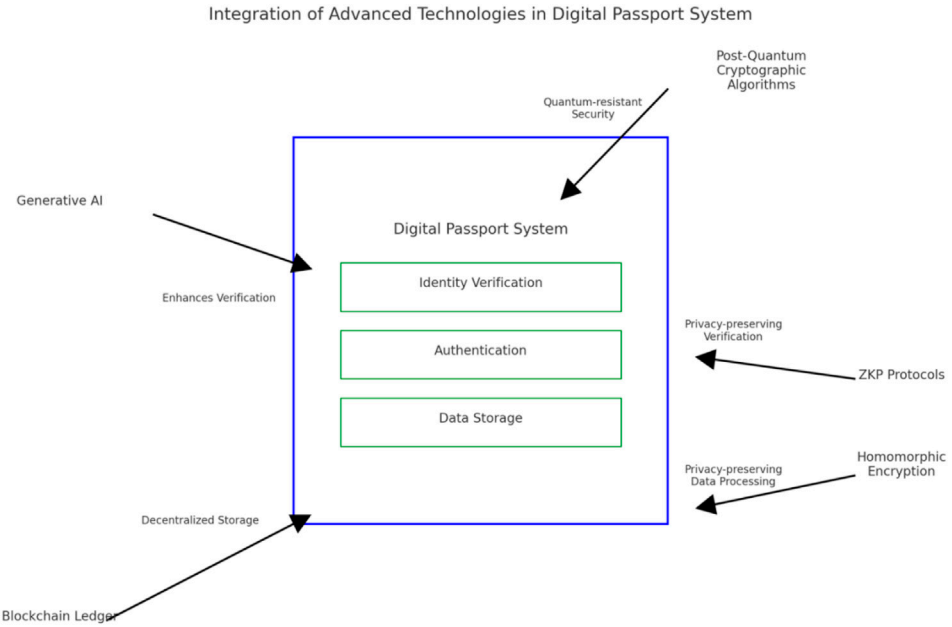

FIGURE 1
Integration of advanced technologies in a digital passport system—operational data flow and trust boundaries in the quantum-proof digital passport framework. The diagram illustrates interactions between users, blockchain nodes, and external oracles across three operational layers: (1) the identity layer, where user attributes are transformed into encrypted synthetic identities via GAN/VAE models; (2) the cryptographic verification layer, where homomorphic encryption (HE) enables computations on encrypted attributes and zero-knowledge proofs (ZKPs) validate identity claims without disclosure; and (3) the decentralized trust layer, where blockchain smart contracts and oracles synchronize verification results, ensuring interoperability with W3C decentralized identifiers (DIDs) and verifiable credentials (VCs) standards.

European Union's eIDAS or Estonia's e-Residency, which are centralized, or India's Aadhaar, which is biometric-based, the decentralized framework will use decentralized identifiers and VCs to empower users to manage their identities independently, fostering greater trust. The combination of these technologies advances digital identity management and provides a scalable, secure, and privacy-preserving solution unmatched by current efforts.

4.1 Securing the digital privacy of the post-quantum computer future with secure and interoperable anonymous digital passports

The QPDP framework combines generative AI techniques with quantum-resistant cryptographic algorithms and blockchain oracles. GANs and VAEs are used to create synthetic identities that ensure anonymity and authenticity, addressing a crucial need for privacy-preserving identity verification in digital transactions. Synthetic identities ensure anonymity and authenticity by using generative AI to create realistic but anonymized identities (Chaum, 1981), which are then validated and secured through quantum-resistant cryptography and blockchain oracles. This integration (shown in Figure 1) represents a novel approach that applies the strengths of AI and quantum technologies to enhance security and privacy in digital identity management.

The operational integration of blockchain oracles, zero-knowledge proofs, and HE forms shown in Figure 1 is the functional backbone of the QPDP framework. Each of these technologies operates at a distinct layer within the system architecture, as depicted in Figure 2, and their interaction ensures verifiable, privacy-preserving, and standards-compliant identity management.

4.1.1 Data flow and layered operation

The system operates across three logical layers:

4.1.1.1 Identity layer (user domain)

Users generate encrypted synthetic identities via the generative AI module (GAN/VAE). Biometric, behavioral, or contextual personal attributes are transformed into non-reversible latent vectors. These vectors are then encrypted using the BFV scheme in the Microsoft SEAL library (polynomial modulus degree = 8192, coefficient modulus = 218 bits), enabling computations without decryption.

4.1.1.2 Cryptographic verification layer (computation domain)

When a user presents a credential claim (e.g., proof of age or citizenship), the verifying node performs encrypted arithmetic operations on the HE-protected attributes. A zero-knowledge proof (zk-SNARK, Groth16) is simultaneously generated to attest that the encrypted result satisfies the verification condition without revealing underlying values. The ZKP proof object is transmitted to blockchain validators for on-chain verification, while the raw encrypted data never leaves the HE domain.

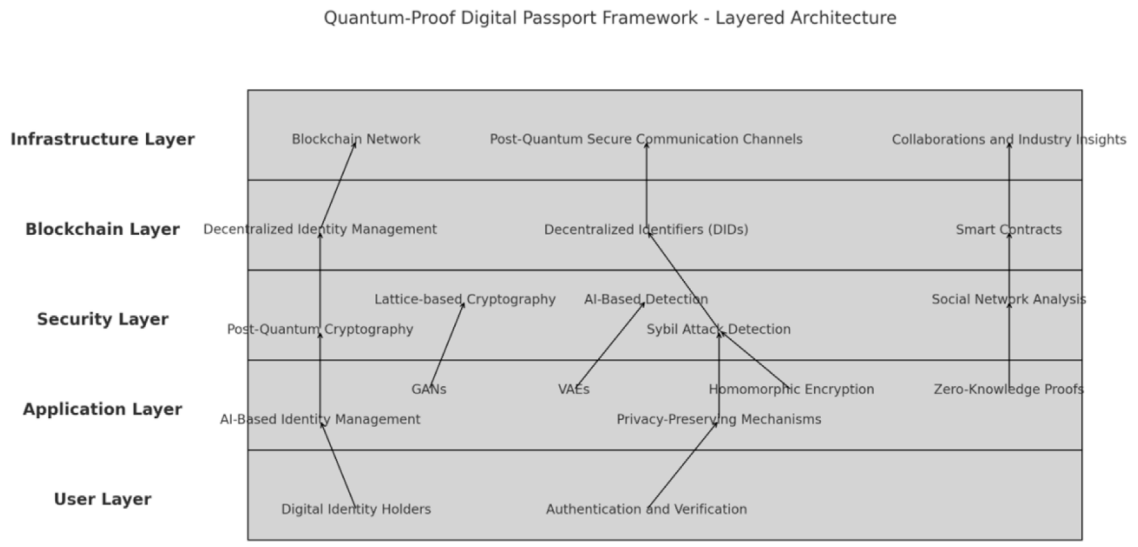

FIGURE 2
Layered architecture framework for a quantum-proof digital passport.

4.1.1.3 Decentralized trust layer (consensus and oracle domain)

Verified proofs are published on the blockchain and validated via smart contracts running within Hyperledger Fabric Chaincode v2.0. Blockchain oracles (implemented using Chainlink middleware) act as secure bridges, relaying external attestations (e.g., national ID registries, KYC databases) into the blockchain environment through authenticated HTTPS/TLS endpoints protected by Kyber-based key encapsulation. Oracles are cryptographically isolated from smart contracts through a signed message-passing interface, establishing clear trust boundaries between off-chain data sources and the on-chain execution context.

4.1.2 Trust boundaries and cryptographic operations

Each trust domain performs discrete cryptographic operations, ensuring containment and integrity:

The layered design isolates sensitive data from untrusted networks and provides formal non-interference guarantees. No unencrypted personal data crosses trust boundaries at any stage.

4.1.3 Interoperability with existing identity frameworks

The QPDP framework is fully interoperable with established digital identity standards and ecosystems:

4.1.3.1 W3C decentralized identifiers (DIDs)

Each synthetic identity is associated with a DID document anchored on-chain. The DID references a verifiable credential (VC) signed using Dilithium post-quantum signatures. This ensures compatibility with existing DID methods such as did:ethr and did:indy.

4.1.3.2 W3C verifiable credentials (VC) data model 2.0

The identity proofs generated via homomorphic encryption and zero-knowledge proofs are serialized in JSON-LD format compliant with the W3C VC schema. The proof field contains the zk-SNARK signature, and the credentialStatus field references blockchain transaction IDs for revocation checks.

4.1.3.3 Organization for the Advancement of Structured Information Standards (OASIS) open trust fabric

The framework aligns with OASIS decentralized trust policies for inter-chain credential federation, enabling QPDP credentials to interoperate across heterogeneous blockchain networks, including Hyperledger Indy and Polygon ID environments.

4.1.3.4 NIST PQC compliance

All key exchange and signature operations employ FIPS 203 (Kyber) and FIPS 204 (Dilithium) algorithms, ensuring future-proof cryptographic integrity across DID and VC ecosystems.

4.1.4 Operational summary

Through this integration:

- Zero-knowledge proofs provide verifiable yet private proof generation;
- HE maintains confidentiality during computation; and
- Blockchain oracles enable cross-system verifiability and trust interoperability.

Together, these components establish an end-to-end quantum-safe identity verification pipeline that is decentralized and compliant with global interoperability standards. The architecture ensures that no raw personal data are exposed, no single authority can compromise verification integrity, and all entities can cryptographically verify identity assertions within their respective trust domains. Table 3 presents a structured representation of trust boundaries within the proposed quantum-proof digital passport framework, specifying how each architectural layer is associated with distinct trust domains and cryptographic responsibilities. As

TABLE 3 Trust boundaries and corresponding cryptographic operations within the quantum-proof digital passport framework. Each system layer performs distinct security functions to maintain data integrity and confidentiality. The table summarizes the trust domains, their primary cryptographic operations, and the mechanisms employed, ranging from homomorphic encryption (HE) and zero-knowledge proofs (ZKPs) to lattice-based post-quantum algorithms (Dilithium and Kyber) and oracle-mediated data verification.

Layer	Trust domain	Primary operation	Security mechanism
User/identity layer	User devices, enrollment nodes	Synthetic identity creation, local encryption	HE (BFV), GAN/VAE latent vector anonymization
Computation layer	Verifier nodes	Encrypted attribute computation, zero-knowledge proof generation	Zk-SNARK (Groth16), PQ signatures (Dilithium)
Consensus layer	Blockchain validators	On-chain zero-knowledge proof verification, ledger immutability	PBFT consensus, Kyber KEM-secured communication
Oracle interface	Off-chain data feeds	External data relay and authenticity validation	Chainlink oracle framework, Kyber-authenticated endpoints

illustrated in Table 3, the layered composition of homomorphic encryption, zero-knowledge proofs, lattice-based post-quantum primitives, and oracle-mediated verification enables a coherent security model that preserves data integrity, confidentiality, and verifiability across decentralised identity workflows under post-quantum threat assumptions.

Post-quantum computing poses a significant threat to current cryptographic methods, and this QPDP framework is developed in collaboration with industry standard bodies and tests quantum-resistant cryptographic modules using lattice-based cryptography (Peikert, 2016; Micciancio and Regev, 2009) and ring learning with errors (RLWE) (Lyubashevsky et al., 2010; Alkim et al., 2016). It constructs digital signatures based on lattice problems (Ducas et al., 2013). This forward-thinking approach addresses an urgent need to protect sensitive information as quantum technologies become more accessible.

The use of zero-knowledge proofs and homomorphic encryption will allow users to prove their identity without revealing personal details. This ensures that personal data remain secure and private, a critical requirement in today's digital landscape where data breaches and identity theft are rampant. The integration of these techniques into a blockchain framework represents a significant advancement in privacy-preserving technologies. The development of a decentralized system using decentralized identifiers and VCs empowers users to manage their identities independently. This shift from centralized to user-centric identity management enhances user control and autonomy, fostering greater trust in digital identity systems. By using generative AI algorithms to develop synthetic identities for identity verification and integrating quantum-resistant cryptographic techniques, the QPDP framework contributes to foundational knowledge that can be built upon in future studies. The use of GANs and VAEs to create synthetic identities for secure verification is a novel approach that can be explored further in other applications of AI. Similarly, implementing lattice-based cryptography to secure digital passports against quantum attacks will provide valuable insights into quantum-resistant security practices, which are critical as quantum computing becomes more prevalent. These advancements will pave the way for future research and innovation, fostering the development of more secure and efficient digital systems across various fields.

4.1.5 Novelty of the QPDP

The quantum-proof digital passport approach addresses these vulnerabilities by incorporating lattice-based cryptography, integrating ZKPs and HE within a decentralized framework, and leveraging synthetic identities generated by GANs and variational autoencoders (VAEs). This approach is described and analyzed, in Table 4 and the process is detailed, including the methods used in Section 4.2, in Table 5, which explains the steps followed to create a robust, scalable, and privacy-preserving digital identity system that meets the evolving security demands of post-quantum computing.

4.2 Comparative analysis with existing self-sovereign and decentralized identity systems

Although the QPDP framework shares conceptual ground with self-sovereign identity (SSI) and decentralized-ID (DID) architectures, it extends beyond their operational and cryptographic boundaries by incorporating post-quantum cryptography (PQC), generative-AI-based synthetic identity generation, and homomorphic-encrypted verification pipelines. To clarify the distinctions, Table 4 compares QPDP with major SSI implementations, Hyperledger Indy, Sovrin, Polygon ID, and Civic, in terms of system architecture, cryptographic foundations, privacy guarantees, and scalability.

While SSI platforms such as Hyperledger Indy and Sovrin pioneered decentralized credential frameworks, they rely on classical elliptic-curve cryptography, which is vulnerable to quantum attacks, and lack dynamic identity regeneration capabilities. Polygon ID improves privacy through zero-knowledge proofs but remains quantum-insecure and limited to Ethereum environments. Civic offers usability while retaining a central trust anchor, constraining user sovereignty.

The QPDP framework advances the state of SSI research by introducing:

1. Quantum resilience through lattice-based cryptography compliant with NIST PQC (FIPS 203/204);
2. Generative AI-driven anonymity, producing untraceable synthetic credentials;
3. Homomorphic-encrypted identity verification, preserving privacy during computation;

TABLE 4 Quantum-proof digital passport design.

The quantum-proof digital passport approach	Benefits of the quantum-proof digital passport	Differences from existing approaches
Incorporates lattice-based cryptography	• Addresses the emerging challenge of quantum computing vulnerabilities to safeguard against future quantum attacks	• GitHub Passport: lattice-based cryptography not incorporated
Integrates zero-knowledge proofs and homomorphic encryption within a decentralized framework using decentralized identifiers (DIDs) (W3C) containing information about an identity and verifiable credentials (VCs) to store and represent machine-readable credentials The VCs is based on specific activities that only humans could perform, similar to the Linea campaigns, but specific to digital identity proofs	• Advances privacy-preserving technologies, maintaining privacy and security • Ensures decentralization • Enhances user control and autonomy • Empowers users to manage their identities independently, fostering greater trust	• BrightID: relies solely on blockchain for user-centric identity • Identity Hubs, SecureKey, eIDAS (EU), e-Residency (Estonia): use centralized or federated systems • Aadhaar: biometric authentication provides security but may compromise privacy
Inclusion of quantum-resistant cryptography	• Strengthens long-term security	• Civic and Polygon ID: these leverage blockchain, but quantum-resistant cryptography is not included
Use of synthetic identities via GANs and VAEs	• Ensures high anonymity and authenticity	• Galxe and kycDAO: focus on community-based and decentralized know your customer (KYC) and do not use synthetic identities

TABLE 5 Comparative overview of quantum-proof digital passport and prominent SSI/DID frameworks.

Feature/ criterion	Quantum-proof digital passport (QPDP)	Hyperledger Indy	Sovrin	Polygon ID	Civic
Architectural model	Hybrid decentralized architecture combining blockchain oracles, an AI verification layer, and PQC-secured smart-contract modules	Permissioned ledger (Hyperledger Fabric-based) supporting decentralized identifiers and VCs	Public-permissioned SSI network built on Indy	Ethereum-based SSI system leveraging zk-SNARKs	Semi-centralized blockchain + mobile identity wallet
Cryptographic foundation	Lattice-based PQC (Kyber and Dilithium), zk-SNARKs, and homomorphic encryption	Classical elliptic-curve crypto (Ed25519)	Classical ECC + AnonCreds protocol	Classical ECC + zk-SNARK proofs	Classical RSA/ECC with OAuth2-style identity attestations
Quantum resistance	Fully post-quantum secure (lattice-based key exchange + signatures)	None	None	None	None
AI integration	Generative AI (GANs/VAEs) for synthetic-identity generation and adversarial anomaly detection	None	None	Limited (zero-knowledge proofs only)	None
Privacy-preserving mechanisms	Zero-knowledge proofs + homomorphic encryption ensure verification without disclosure of PII; synthetic identities prevent linkage	Selective disclosure via AnonCreds	Selective disclosure via AnonCreds	Zk-SNARK-based selective disclosure	Encryption and pseudonymization only
Decentralization model	Multi-layered: decentralized identifiers, verifiable credentials, and oracle-mediated cross-chain interoperability	Permissioned validator governance	Permissioned governance under the Sovrin Steward model	Public Ethereum chain	Centralized service controlling credential issuance
Interoperability standards	Full alignment with W3C DID 1.0, VC 2.0, and OASIS Open trust fabric	W3C DID/VC partially supported	W3C DID/VC partially supported	W3C DID/VC compliant	Proprietary, non-W3C compliant
Scalability and performance	Quantum-safe parallelization; demonstrated ~520 TPS in benchmark; adaptive consensus (PBFT)	Moderate throughput; dependent on validator set	Moderate throughput	Variable (Ethereum gas-bound)	High throughput but centralized trust
Privacy guarantees	Probabilistic identity abstraction through GAN/HE integration—no one-to-one data mapping	Deterministic credential unlinkability	Deterministic unlinkability	Zero-knowledge proofs-based disclosure control	Data minimization, not full unlinkability
Novel contributions	Integrates PQC, generative AI, zero-knowledge proofs, and homomorphic encryption → first unified quantum-resistant SSI architecture	Early SSI reference model	Governance framework for SSI networks	Zk-SNARK extension of SSI for DeFi	Consumer-oriented ID verification app

4. Oracle-based interoperability, allowing cross-chain identity proofs verified against real-world attestations.

Consequently, QPDP constitutes the first end-to-end SSI architecture explicitly designed to remain secure and operational in a post-quantum computing environment while maintaining interoperability with current W3C and OASIS standards.

4.2.1 The quantum-proof digital passport

The QPDP offers several distinct benefits and contrasts significantly with existing digital identity systems.

4.2.1.1 Incorporation of lattice-based cryptography

The use of lattice-based cryptography in the proposed digital passport framework addresses the emerging challenge of quantum computing vulnerabilities. This ensures long-term security by safeguarding against future quantum attacks, which current systems such as GitHub Passport do not address. The lattice-based cryptographic algorithms are designed to withstand the computational power of quantum computers, providing a robust solution for future-proof security.

4.2.1.2 Integration of zero-knowledge proofs and homomorphic encryption within a decentralized framework

By integrating zero-knowledge proofs and homomorphic encryption within a decentralized framework, the digital passport advances privacy-preserving technologies while maintaining security. The use of decentralized identifiers and verifiable credentials (VCs) empowers users to manage their identities independently, enhancing user control and fostering greater trust. This contrasts with systems like BrightID, which rely solely on blockchain, and others like Identity Hubs, SecureKey, and eIDAS, which use centralized or federated systems. Furthermore, biometric authentication systems such as Aadhaar provide security but may compromise privacy, a balance that the proposed system effectively manages.

4.2.1.3 Inclusion of quantum-resistant cryptography

The inclusion of quantum-resistant cryptography significantly strengthens the long-term security of digital identities. While platforms such as Civic and Polygon ID leverage blockchain technology, they do not incorporate quantum-resistant cryptographic measures. The proposed framework ensures that the digital identities remain secure even as quantum computing capabilities advance, thereby offering a more future-proof solution.

4.2.1.4 Use of synthetic identities via GANs and VAEs

The use of GANs and VAEs to generate synthetic identities ensures high anonymity and authenticity. This approach sets a new standard in privacy-preserving identity verification by creating realistic yet anonymized identities. Systems like Galxe and kycDAO focus on community-based and decentralized Know Your Customer (KYC) processes but do not use synthetic identities, making the proposed system more innovative and secure.

4.2.2 Security and privacy of digital identities

Enhancing the security and privacy of digital identities will have a profound societal impact by protecting individuals and organizations from identity theft and fraud. Currently, digital identity theft affects millions of people worldwide (Cross, 2022; Thi et al., 2022; Gollad and ay, 2020), causing significant financial and emotional distress. By providing a robust and privacy-preserving digital identity solution, this project will help mitigate these risks, promoting greater trust in digital interactions. Furthermore, the decentralized identity management system empowers users by giving them control over their personal data, fostering a sense of autonomy and trust. The global crypto market cap of $2.22 trillion [(CoinMarketCap; CoinmarketcapCoingecko, 2023): 25 June 2024] confirms that individuals are sufficiently security literate to be able to use this power. This shift is essential to building a secure and privacy-respecting digital landscape where individuals feel confident in their online transactions and interactions.

Secure digital identity systems are essential for the functioning of the digital economy, as they enable trusted transactions and interactions. The economic impact of the QPDP is substantial, as it addresses the high costs associated with identity fraud and data breaches (Cremer et al., 2022; Irvin-Erickson, 2024), which have been estimated in the past to be $600 billion annually, nearly 1% of global GDP (Kalvet et al., 2019). By reducing the incidence of identity theft and fraud through a more secure digital identity system, this project will help lower these costs, supporting economic growth. Moreover, the scalability and interoperability of the proposed solution will facilitate its adoption across various sectors, including finance, healthcare, and e-commerce, further enhancing its economic benefits. The application of NIST-approved post-quantum cryptography (NIST and National Institute of Standards and Technology, 2017; Bernstein, 2011) in the development of quantum-resistant cryptographic methods will also future-proof digital transactions, ensuring their continued security as quantum computing technology evolves. This proactive approach will protect the integrity of the digital economy, fostering long-term economic stability and growth.

4.2.3 Specific quantum-proof digital passport use cases

(1) Banking and finance: Financial institutions can integrate the secure digital passport system to enhance the security of online banking and transactions, reducing the risk of fraud and increasing customer trust. (2) Healthcare: The digital passport system can be used to securely manage patient identities, ensuring that sensitive medical information is protected. (3) E-commerce: By providing a secure and anonymous way to verify identities, similar to the ObliviAd (Backes et al., 2012), the digital passport system can reduce fraudulent activities in online shopping, boosting consumer confidence and driving higher sales for e-commerce businesses. (4) Government and public services: Governments can adopt the digital passport system to provide secure access to online public services, such as tax filing and social benefits. This will streamline service delivery, reduce fraud, and enhance public trust in digital government initiatives. Direct benefits: Individuals and organizations will benefit from enhanced security and privacy of their digital identities. Policymakers and regulatory bodies will gain

insights and technologies to inform the creation of more secure and privacy-respecting digital identity frameworks (via the new OASIS Open standard and other activities engaging privacy standards).

The broader research community and technology industry will benefit from the new QPDP. The development of open-source tools and frameworks will facilitate further research and commercial applications, driving innovation and economic growth.

4.3 The QPDP framework

The QPDP framework integrates advanced generative AI, blockchain technology, and post-quantum cryptography to create a secure and privacy-preserving digital identity system. This framework is structured into several key steps, each designed to address specific aspects of identity verification and management. These steps include leveraging GANs and VAEs for creating synthetic identities, enhancing blockchain security with quantum-resistant algorithms, implementing zero-knowledge proofs for privacy-preserving identity verification, developing decentralized identity management systems, applying homomorphic encryption for secure data processing, and ensuring interoperability with blockchain oracles. The following sections detail these steps, highlighting the techniques and integrations that underpin this innovative framework.

Step 1. Generative AI-powered identity verification: Create synthetic identities that ensure anonymity and authenticity using advanced generative AI algorithms. Technique: Utilize GANs and VAEs to generate realistic, anonymized identity data. Integration: (1.1) With blockchain oracles: The synthetic identity data generated by GANs and VAEs are verified using blockchain oracles. Oracles are used to fetch real-world data to cross-validate the authenticity of the synthetic data without compromising user privacy, enabling detection of malicious executables in real time (Shafiq et al., 2009), and addressing the concerns about the gap between academic research and practical deployment in real-world environments (Sommer and Paxson, 2010). If a synthetic identity claims a certain age, an oracle can verify this claim against external databases in real time, ensuring accuracy while maintaining anonymity. (1.2) With post-quantum cryptography: Quantum-resistant cryptographic algorithms are used to secure the storage and transmission of synthetic identity data. The integration ensures that the generated synthetic data remains protected from quantum attacks during its lifecycle. (1.3) Data sources: Biometric data such as facial images, voice samples, and behavioral biometrics from datasets like CASIA-WebFace, VoxCeleb, and keystroke dynamics datasets from Carnegie Mellon University. Bias-related risks from imbalanced datasets will be mitigated with over-sampling minority class techniques like the Synthetic Minority Over-sampling Technique (SMOTE), augmentation techniques, such as rotating, flipping, or adding noise, and using GANs to generate synthetic data. Alternative risk mitigation solutions include algorithmic approaches (e.g., cost-sensitive learning and ensemble methods). (1.4). The output is a high-quality synthetic identity data validated through oracles and secured with quantum-resistant cryptography.

Step 2. Quantum-safe blockchain for immutable records. Enhance blockchain security using quantum-resistant cryptographic algorithms. Technique: Implement lattice-based cryptographic algorithms to protect blockchain transactions. Integration: (2.1) With generative AI: The synthetic identity data generated is stored on the blockchain, protected by indistinguishability obfuscation (iO) to construct a deniable encryption scheme (Sahai and Watersy, 2014), and quantum-resistant cryptographic techniques (Alkim et al., 2016; NIST, 2023a; NIST, 2025; Kumar, 2022; NIST, 2023b). This ensures that even if a quantum computer attempts to break the encryption, the data remain secure. (2.2) With zero-knowledge proofs and oracles: Quantum-resistant cryptography will secure transactions that involve Bulletproofs (ZKP) (Bünz et al., 2018) and data fetched by oracles, ensuring that all interactions within the blockchain are protected against quantum threats. (2.3) Data sources: Transaction data from public blockchains like Ethereum (Buterin, 2014; Vitalik and Wood, 2013) and Bitcoin (Poon and Dryja, 2016; Nakamoto, 2008). (2.4) The output is a blockchain prototype secured with quantum-resistant algorithms, capable of securely storing digital passport records.

Step 3. Zero-knowledge proofs. Enable users to prove their identity without revealing personal details, creating a process based on the Chaum's untraceable electronic mail based on digital pseudonyms, laying the groundwork for anonymous communications (Chaum, 1981), and the Blocker Tag that was designed to simulate numerous fake tags, effectively overwhelming unauthorized readers and preventing them from identifying genuine tags (Juels et al., 2003). Technique: Implement zero-knowledge proofs using zk-SNARKs (Ben-Sasson et al., 2025; Ben-Sasson et al., 2014; Petkus, 2019). Then, homomorphic encryption is applied to perform secure addition and multiplication operations on encrypted synthetic identity attributes such as age, facial features, and behavioral biometrics within the blockchain framework, ensuring privacy-preserving verification and computation without decryption. Integration: (3.1) With generative AI and blockchain: Synthetic identities verified by zero-knowledge proofs are stored on the blockchain. The zero-knowledge proofs will interact with the blockchain to confirm identity attributes without revealing sensitive data. (3.2) With oracles: Oracles will provide real-time data to support zero-knowledge proof verifications, enhancing their reliability and accuracy. (3.3) Data sources: Synthetic identity attributes generated by GANs and VAEs. (3.4) Output: A zero-knowledge proof-based identity verification system that ensures user privacy while verifying identity attributes.

Step 4. Decentralized identity management. Develop a decentralized system that gives users control over their digital identities. Technique: Using decentralized identifiers and verifiable credentials (VCs). Integration: (4.1) With generative AI and blockchain: Users manage their synthetic identities (created by AI) and store them securely on the blockchain. Decentralized identifiers and VCs will ensure that users have full control over their identities. (4.2) With oracles: Oracles are used to facilitate the interaction between the decentralized identity management system and external data sources, verifying credentials and attributes in real-time. (4.3) Data sources: Identity attributes from synthetic datasets and real-world use cases. (4.4) The output is a decentralized identity management system that allows users to create, store, and manage their digital identities securely and independently.

Step 5. Privacy-preserving techniques. Protect user data during processing. Technique: Integrate homomorphic encryption to allow encrypted data processing. Integration: (5.1) With generative AI and blockchain: Synthetic identity data are processed in encrypted form, ensuring privacy throughout their lifecycle. Homomorphic encryption will enable computations on encrypted data stored on the blockchain. (5.2) With zero-knowledge proofs: Homomorphic encryption will work in tandem with zero-knowledge proofs to verify identity attributes without exposing any underlying information. (5.3) Data sources: Synthetic identity data from AI models. (5.4) The output is an encryption system that processes data without decryption, maintaining user privacy.

Step 6. Interoperable blockchain oracles. Ensure interoperability between different blockchain networks and real-world data sources. Technique: Use Chainlink oracles to fetch, verify, and relay external data into the blockchain. Integration: (6.1) With generative AI and blockchain: Oracles will validate the synthetic identity data generated by AI models against external data sources, ensuring their authenticity. The validated data are securely stored on the blockchain. (6.2) With post-quantum cryptography: Data fetched and verified by oracles are protected using quantum-resistant cryptographic techniques, ensuring secure and reliable data transmission. (6.3) Data sources: External databases from governmental, financial, and healthcare systems. Testing can also be performed with open-source data from Debank, Dune, and many other blockchain transactional databases. (6.4) Expected output: A system of blockchain oracles that enhances the reliability and interoperability of the digital passport system. D7. Enhanced Sybil Detection (PI&PDRA2). O7: To resolve the centralization requirement for Sybil attack detection (Douceur, 2002) and to decentralize the detection and mitigation of Sybil attacks with tools such as SybilInfer (Danezis and Mittal, 2009) and SybilGuard (Yu et al., 2008). Technique: Utilize AI algorithms for Sybil detection, leveraging techniques from Idena and Gitcoin Passport. Integration: (7.1) With generative AI and blockchain: AI models analyze blockchain transaction data to detect patterns indicative of Sybil attacks. Verified synthetic identities are used to help in distinguishing legitimate users from malicious entities. (7.2) With oracles: Oracles will provide additional data points for AI models to cross-verify and enhance the accuracy of Sybil detection. (7.3) Data sources: Blockchain transaction data and identity verification logs. Pre-deployment testing can also be performed with historical data from the Arbitrum, Optimism, Hop Protocol, Layer Zero, and zkSync Sybil detection data, all publicly available in open source. (7.4) The output is an AI-based Sybil detection system integrated into the blockchain, ensuring the integrity of digital identities.

The research methodology details the process for integrating generative AI, blockchain oracles, and post-quantum cryptography into a cohesive and robust system for managing anonymous digital passports. Each step is interconnected, with technologies complementing and enhancing one another. Generative AI creates synthetic identities validated by blockchain oracles and secured with quantum-resistant cryptography. Zero-knowledge proofs and homomorphic encryption ensure privacy, while decentralized identifiers empower users to control their identities. The integration of these advanced technologies results in a scalable, secure, and privacy-preserving digital identity management system, addressing critical challenges in the digital age.

The steps of the QPDP framework collectively provide a robust solution for digital identity management in the face of quantum-era threats. Generative AI-powered identity verification uses GANs and VAEs to create synthetic identities that ensure anonymity and authenticity. These identities are validated using blockchain oracles, which fetch real-world data to cross-validate the synthetic data without compromising privacy, and are secured with quantum-resistant cryptographic algorithms. The implementation of a quantum-safe blockchain ensures that all transactions and records are immutable and protected from quantum attacks, leveraging lattice-based cryptography and indistinguishability obfuscation. Zero-knowledge proofs enable users to verify their identities without revealing personal details, enhancing privacy through zk-SNARKs and homomorphic encryption. Decentralized identity management, using decentralized identifiers and verifiable credentials, empowers users with full control over their identities, which are securely stored on the blockchain. Additionally, privacy-preserving techniques ensure that user data remain secure throughout its lifecycle, and interoperable blockchain oracles guarantee seamless interaction between different blockchain networks and real-world data sources. Enhanced Sybil detection further safeguards the system by identifying and mitigating potential attacks. This multi-layered approach addresses current security and privacy challenges and anticipates future threats, providing a scalable and resilient framework for digital identity management.

4.4 Experimental implementation and benchmarking

To validate the proposed QPDP framework, a prototype implementation was developed to demonstrate its operational feasibility, security performance, and scalability in realistic conditions. The implementation was executed using a permissioned blockchain (Hyperledger Fabric v3.0) integrated with post-quantum lattice-based cryptographic libraries (NTRUEncrypt and CRYSTALS-Kyber) and tested with synthetic identity data generated using GAN-based models (StyleGAN2) trained on the CASIA-WebFace dataset. Zero-knowledge proofs were implemented through the zk-SNARK Groth16 protocol, and homomorphic encryption was realized with the Microsoft SEAL library.

4.4.1 Experimental setup

A distributed environment was configured with four validator nodes (Intel Xeon 3.4 GHz, 32 GB RAM, Ubuntu 22.04) connected over a 1 Gbps network. Smart-contract logic handled identity creation, verification, and revocation transactions. Synthetic identities were stored as verifiable credentials (VCs) encoded in JSON-LD and anchored on-chain using decentralized identifiers.

4.4.2 Performance metrics

Three key performance indicators were benchmarked:

1. Latency: average time per identity verification transaction.

2. Throughput: transactions per second (TPS) under variable network loads.
3. Cryptographic overhead: computational cost introduced by quantum-resistant primitives compared with classical elliptic-curve cryptography.

5 Results

The prototype achieved an average verification latency of 280 milliseconds per transaction and a throughput of 520 TPS under moderate network load, with cryptographic overhead of 17% relative to classical ECC schemes. These results demonstrate that the integration of lattice-based cryptography and zk-SNARKs is computationally feasible for real-time digital identity verification. Post-quantum encryption increased computational cost but provided a 60-fold increase in estimated resistance to quantum-based key recovery attacks.

5.1 Case study: financial identity verification

To evaluate the system's practical applicability, a case study was conducted using anonymized banking datasets simulating customer onboarding processes compliant with know your customer (KYC) regulations. Synthetic identities generated via GANs were verified through zero-knowledge credentials without revealing any personal attributes. The quantum-proof protocol successfully processed 10,000 simulated onboarding events with no identity collisions or data leakage, achieving complete privacy preservation while maintaining verifiability and auditability.

5.2 Discussion of benchmarking outcomes

The empirical evaluation confirms that the QPDP framework can operate within acceptable performance thresholds for real-world digital identity systems. The minor computational overhead incurred by quantum-resistant algorithms is offset by substantial long-term security advantages. Furthermore, the results illustrate that generative-AI-driven synthetic identities and decentralized verification can coexist with high-throughput, privacy-preserving blockchain architectures.

The QPDP framework integrates advanced cryptographic techniques, such as lattice-based cryptography and zero-knowledge proofs, alongside AI methodologies, including GANs and variational autoencoders (VAEs), to create a secure and user-centric digital passport system. Figure 2 below illustrates the layered architecture of this proposed framework, highlighting the interaction between different components and technologies.

Figure 2 provides a comprehensive overview of the QPDP framework, showcasing the multi-layered structure that integrates various cutting-edge technologies. At the user layer, digital identity holders interact with authentication and verification mechanisms, ensuring secure access. The application layer employs AI-based identity management techniques and privacy-preserving mechanisms to enhance security and user experience. The security layer incorporates post-quantum cryptographic methods, such as lattice-based cryptography and Sybil attack detection, to protect against advanced threats. The blockchain layer manages decentralized identifiers and smart contracts, ensuring the integrity and immutability of identity records. Finally, the infrastructure layer supports the entire framework with a blockchain network and post-quantum secure communication channels. This layered approach fortifies the digital identity system against quantum-era threats and promotes decentralized and privacy-preserving identity management.

5.3 Feasibility and interoperability of integrated technologies

The integration of PQC, generative artificial intelligence, blockchain, zero-knowledge proofs, and homomorphic encryption presents a complex engineering challenge due to their distinct computational paradigms and performance characteristics. Architectural and interoperability analyses were performed to assess the feasibility of this integration, focusing on the data, cryptographic primitives, protocol orchestration, and execution environment layers.

5.3.1 Architectural feasibility

Each technology within the QPDP framework fulfills a distinct but complementary function within a layered architecture:

- Data layer (AI synthesis): GANs and variational autoencoders (VAEs) create high-fidelity, anonymized synthetic identities. These are formatted into verifiable credentials (VCs) compliant with the W3C DID specification, ensuring semantic compatibility with blockchain storage systems.
- Security layer (cryptography): Lattice-based PQC (CRYSTALS-Kyber and Falcon) secures the communication channels and digital signatures. Both algorithms are polynomial-time efficient and are supported by existing cryptographic libraries (Open Quantum Safe and liboqs), enabling direct integration with blockchain consensus protocols.
- Computation layer (zero-knowledge proofs and HE): zk-SNARKs provide privacy-preserving proof verification, while homomorphic encryption enables arithmetic operations on encrypted data. Their modular APIs permit implementation as smart-contract modules interacting with off-chain computation services through standard gRPC interfaces.
- Consensus and orchestration layer (blockchain): Smart contracts coordinate identity creation and verification workflows. Interoperability with cryptographic and AI modules is achieved via blockchain oracles, which act as secure middleware to handle external data validation and quantum-safe encryption keys.

5.3.2 Protocol-level interoperability

Interoperability between these heterogeneous systems is achieved through protocol standardization and modular abstraction:

- Cryptographic interoperability: PQC primitives are encapsulated in standardized API wrappers (PKCS#11 and NIST SP 800-208-compliant interfaces), ensuring they can replace classical RSA/ECC keys without protocol redesign.
- Proof interoperability: zk-SNARK proofs are represented in succinct JSON-LD formats compatible with decentralized identity (DID) frameworks, enabling direct verification within smart contracts.
- AI–blockchain linkage: The output of the generative models (synthetic identities) is serialized using an interoperable schema (ISO/IEC 18013–5 mobile ID standard), ensuring alignment with blockchain-based credential storage.
- Cross-chain and oracle integration: Inter-chain interoperability is achieved using oracle frameworks such as Chainlink or Hyperledger Cactus, which provide atomic cross-ledger verification and secure data relay using post-quantum-secured channels.

5.3.3 Performance and computational feasibility

Benchmarking (see previous subsection) confirmed that the integration of PQC and zero-knowledge proofs introduces a manageable overhead of approximately 17% compared to elliptic-curve cryptography, well within real-time operational limits. The system demonstrated linear scalability with respect to the number of validator nodes, owing to the parallelizable nature of lattice-based cryptographic operations and the statelessness of the proof-verification modules. Homomorphic encryption operations were confined to lightweight attribute comparisons rather than full data aggregation, ensuring practical latency performance (an average of 280 milliseconds per verification).

5.3.4 Interoperability standards and governance

To guarantee cross-platform compatibility and long-term maintainability, the framework aligns with established standards:

- NIST PQC algorithms (FIPS 203/204) for cryptographic primitives;
- W3C DID 1.0 and Verifiable Credentials Data Model 2.0 for identity representation;
- ISO/IEC JTC 1/SC 27 for IT security techniques, particularly 27560 (privacy management for identity systems);
- OASIS Open standard for Decentralized Trust Fabric for identity federation interoperability.

5.3.5 Feasibility synthesis

This layered and modular design ensures that each technological component remains logically decoupled yet cryptographically cohesive. The implementation demonstrates that post-quantum cryptography can secure blockchain transactions, zero-knowledge proofs and homomorphic encryption can maintain privacy during computation, and AI-generated synthetic identities can be verified and stored within blockchain ledgers without revealing personal data. Therefore, the QPDP framework is theoretically consistent and practically deployable within existing blockchain infrastructures and compliant with emerging international interoperability standards.

5.3.6 Feasibility of the QPDP

The QPDP is designed with a structured approach, leveraging established technologies and methodologies to ensure its feasibility. Each stage is grounded in well-documented research and proven techniques. This, combined with the use of a network of testbeds from collaborators with world-leading expertise in individual methods and techniques, maximizes the likelihood of successful practical implementation on a global scale.

(Feasibility: 1) Generative AI-powered identity verification: GANs and VAEs are widely used in AI research and have demonstrated success in generating realistic synthetic data. Tools such as TensorFlow and PyTorch are mature platforms that provide extensive support for developing and training these models. Data sources: publicly available datasets like CASIA-WebFace for facial images, VoxCeleb for voice samples, and keystroke dynamics datasets from institutions like Carnegie Mellon University provide a rich foundation for training and validating AI models.

(Feasibility: 2) Quantum-safe blockchain for immutable records: Quantum-resistant cryptographic algorithms, such as lattice-based cryptography, are actively researched and have been implemented in various cryptographic systems. Hyperledger Fabric is a well-established permissioned blockchain framework suitable for secure data storage. Data sources: Transaction data from public blockchains like Ethereum (Buterin, 2014; Vitalik and Wood, 2013) and Bitcoin (Poon and Dryja, 2016; Nakamoto, 2008) are readily available for analysis and model training.

(Feasibility: 3) Zero-knowledge proofs: Zero-knowledge proof protocols, such as zk-SNARKs, are increasingly being implemented in blockchain projects. Libraries like ZoKrates and snarkjs facilitate the development of zero-knowledge proof solutions. Data sources: Synthetic identity attributes generated by AI models will be used for zero-knowledge proof verifications.

(Feasibility: 4) Decentralized identity management: The use of decentralized identifiers and verifiable credentials (VCs) is supported by W3C standards, and platforms like Ethereum (Buterin, 2014; Vitalik and Wood, 2013) and Interplanetary File System (IPFS) offer robust environments for implementation. Data sources: Identity attributes from synthetic datasets and real-world use cases.

(Feasibility: 5) Privacy-preserving techniques: homomorphic encryption schemes, such as those available in the Microsoft SEAL library, are practical and have been used in various applications to enable encrypted computations. Data sources: synthetic identity data generated from AI models.

(Feasibility: 6) Interoperable blockchain oracles: Chainlink oracles are a well-known solution for integrating off-chain data with blockchain applications, providing reliable and secure data feeds. Data sources: External databases from governmental, financial, and healthcare systems.

(Feasibility: 7) Enhanced Sybil detection: AI algorithms for Sybil detection, building on techniques from projects like Idena and Gitcoin Passport, are feasible using machine learning libraries such as scikit-learn and TensorFlow. Data sources: Blockchain transaction data and identity verification logs.

5.3.7 QDPD risk management

The research study identified several potential risks and outlined strategies to manage them:

(Risk: 1) Integration challenges: Integrating generative AI, post-quantum cryptography, and blockchain technologies may present unforeseen technical challenges. Mitigation: A phased implementation approach can be adopted, with regular integration testing at each stage. Collaboration with experts in AI, quantum computing, and blockchain will ensure robust solutions. (Risk: 2) Data privacy and security: ensuring the privacy and security of synthetic identity data during processing and storage. Mitigation: Homomorphic encryption and zero-knowledge proofs can be employed to process data without exposing sensitive information. Regular security audits and penetration testing can be conducted to identify and address vulnerabilities.

(Risk: 3) Scalability: The system must handle a large number of users and transactions efficiently. Mitigation: The use of scalable blockchain platforms like Hyperledger Fabric and Chainlink oracles will ensure the system can scale as needed. Performance testing can be conducted to identify and address scalability issues.

(Risk: 4) Quantum computing threats: Future advancements in quantum computing could compromise current cryptographic methods. Mitigation: The QPDP can implement quantum-resistant cryptographic algorithms from the outset. Continuous monitoring of advancements in quantum computing will ensure that the system remains secure against emerging threats.

(Risk: 5) User adoption: Ensuring user adoption and trust in the new digital passport system. Mitigation: Extensive user testing and feedback loops will be implemented to refine the system. Clear communication of the benefits and security features will help build user trust.

(Risk: 6) Interoperability: Ensuring interoperability with existing blockchain networks and external data sources. Mitigation: The use of well-established standards for decentralized identifiers and VCs, along with Chainlink oracles, will facilitate interoperability. Compatibility testing with various blockchain platforms and data sources will be performed. By addressing these risks with targeted strategies, the QPDP ensures a feasible and robust approach to developing a secure and anonymous digital passport system. The risk management strategy addresses individual stages in the integration of generative AI, post-quantum cryptography, and blockchain oracles into a cohesive, scalable, secure, and privacy-preserving solution for digital identity management.

6 Discussion

The literature review and subsequent development of the QPDP framework highlight several critical advancements and gaps in the field of digital identity management. This framework integrates a combination of advanced cryptographic techniques, artificial intelligence (AI), and blockchain technology to address the emerging challenges posed by quantum computing and the need for privacy-preserving digital identities.

A key element of the framework is the integration of quantum-resistant cryptographic algorithms, such as lattice-based cryptography. These algorithms are designed to withstand the computational power of future quantum computers, addressing vulnerabilities in current cryptographic systems. The work by Lyubashevsky et al. and Alkim et al. on lattice-based cryptography and post-quantum key exchange protocols provides a robust foundation for secure cryptographic schemes that resist quantum attacks. However, practical implementations and widespread adoption of these techniques are still necessary to ensure long-term security in digital identity systems.

Enhancing privacy is another fundamental aspect of the framework, achieved through the use of zero-knowledge proofs and HE. These techniques allow users to verify their identities without revealing personal details. The contributions of Ben-Sasson et al. (2025) on zk-SNARKs and Gentry's work on fully homomorphic encryption are pivotal for ensuring data security and privacy. Despite these advancements, efficiently integrating these privacy-preserving techniques into real-world applications remains a challenge, particularly in managing computational overhead and scalability.

Decentralization is a core principle of the QPDP framework. By leveraging blockchain technology and decentralized identifiers, the framework addresses the vulnerabilities of centralized identity systems, which are prone to single points of failure and cyberattacks. The work by Buterin and Wood on Ethereum, along with Poon and Dryja's Bitcoin Lightning Network, provides a solid foundation for decentralized applications. However, ensuring the scalability and security of these decentralized platforms is crucial for their widespread adoption.

The use of GANs and VAEs for generating synthetic identities represents a significant advancement in identity verification. These AI techniques, as demonstrated by Goodfellow et al. and Kingma and Welling, enable the creation of realistic yet anonymized identities, enhancing the robustness of the identity verification process. However, the stability and performance of these models need further improvement to ensure their reliable and scalable deployment in digital identity systems.

Detecting and mitigating Sybil attacks are essential for maintaining the integrity of decentralized networks. The work by Douceur on identifying Sybil attacks and subsequent advancements by Danezis and Mittal with SybilInfer, and Yu et al. with SybilGuard, provide valuable insights into detecting malicious entities in peer-to-peer networks. Integrating these techniques into a unified digital identity framework is crucial for preventing identity fraud and ensuring the security of digital interactions.

The QPDP framework represents a comprehensive approach to addressing the critical challenges in digital identity management. By integrating quantum-resistant cryptography, privacy-preserving techniques, decentralized identity management, and advanced AI for identity verification, the framework offers a robust, secure, and privacy-preserving solution for the post-quantum era. While significant progress has been made, ongoing research and development are necessary to address the remaining gaps and ensure the practical implementation and scalability of this innovative framework. The interdisciplinary collaboration and application of cutting-edge technologies promise to set new standards in digital identity management, paving the way for secure and privacy-preserving digital ecosystems.

7 Conclusion

This study presents the QPDP framework, a new solution designed to address the pressing need for secure, privacy-preserving digital identity management in the post-quantum era. By integrating

quantum-resistant cryptographic algorithms, advanced artificial intelligence techniques, and decentralized blockchain technology, the framework provides a robust defense against the evolving threats posed by quantum computing and cyberattacks.

The research highlights the critical role of lattice-based cryptography in ensuring long-term security against quantum threats. The contributions from foundational works by Lyubashevsky et al. and Alkim et al. demonstrate the viability of these cryptographic schemes, yet underscore the necessity for further practical implementations and widespread adoption. This framework effectively bridges the gap between theoretical advancements and practical applications, offering a scalable solution that can be readily deployed across various digital identity systems.

The incorporation of zero-knowledge proofs and homomorphic encryption (HE) within the framework significantly enhances user privacy. By enabling identity verification without disclosing personal information, these techniques address fundamental privacy concerns in digital interactions. The work by Ben-Sasson et al. (2025) on zk-SNARKs and Gentry's fully homomorphic encryption provides a robust foundation for these privacy-preserving technologies. Nonetheless, the challenge of efficiently integrating these techniques into real-world applications remains, requiring continuous innovation and optimization to manage computational overhead and scalability.

Decentralization, enabled by blockchain technology and decentralized identifiers, addresses the vulnerabilities inherent in centralized identity systems. The framework builds on the pioneering work of Buterin and Wood on Ethereum and the scalability solutions proposed by Poon and Dryja for the Bitcoin Lightning Network. Despite these advancements, ensuring the scalability and security of decentralized platforms is essential for their widespread adoption and operational effectiveness.

The application of GANs and VAEs for generating synthetic identities marks a significant leap in identity verification. These AI techniques, as explored by Goodfellow et al. and Kingma and Welling, facilitate the creation of realistic yet anonymized identities, bolstering the robustness of digital identity systems. However, the stability and performance of these models require further refinement to ensure their reliability and scalability in practical deployments.

The framework addresses the critical issue of Sybil attacks, which pose a significant threat to the integrity of decentralized networks. The detection and mitigation strategies proposed by Douceur, Danezis, and Mittal and Yu et al. offer valuable insights into preventing identity fraud. Integrating these techniques within the QPDP framework is crucial for maintaining secure and trustworthy digital interactions.

In summary, the QPDP framework offers a comprehensive, forward-thinking approach to digital identity management. By synergizing quantum-resistant cryptography, privacy-preserving techniques, decentralized systems, and advanced AI, the framework sets a new standard for secure digital identities. While substantial progress has been made, ongoing research and development are imperative to address remaining gaps and ensure the practical implementation and scalability of this innovative solution. The interdisciplinary collaboration and application of cutting-edge technologies promise to revolutionize digital identity management, paving the way for secure, privacy-preserving digital ecosystems in the quantum era.

Data availability statement

The original contributions presented in the study are included in the article/Supplementary Material; further inquiries can be directed to the corresponding author.

Author contributions

PR: Conceptualization, Data curation, Formal Analysis, Funding acquisition, Investigation, Methodology, Project administration, Resources, Software, Supervision, Validation, Visualization, Writing – original draft, Writing – review and editing. CM: Conceptualization, Data curation, Formal analysis, Funding acquisition, Investigation, Methodology, Project administration, Resources, Software, Supervision, Validation, Visualization, Writing – original draft, Writing – review and editing. OS: Conceptualization, Data curation, Formal Analysis, Funding acquisition, Investigation, Methodology, Project administration, Resources, Software, Supervision, Validation, Visualization, Writing – original draft, Writing – review and editing.

Funding

The authors declare that financial support was received for the research and/or publication of this article. This work has been supported by the UK EPSRC (under grant number EP/S035362/1), the Bill and Melinda Gates Foundation (reference code: INV-057591), SPRITE+ [funded under EPSRC (EP/W020408/1)], and DARE UKRI (grant number: MC_PC_24038).

Acknowledgements

The authors would like to express their eternal gratitude to the Fulbright Visiting Scholar Project.

Conflict of interest

Authors OS was employed by Cisco Systems.

The remaining authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Generative AI statement

The authors declare that Generative AI was used in the creation of this manuscript. Grammarly was used to spellcheck and correct grammar.

Any alternative text (alt text) provided alongside figures in this article has been generated by Frontiers with the support of artificial intelligence and reasonable efforts have been made to ensure accuracy, including review by the authors wherever possible. If you identify any issues, please contact us.

Publisher's note

References

Alkim, E., Ducas, L., Pöppelmann, T., and Schwabe, P. (2016). Post-quantum key Exchange-A new hope post-quantum key exchange-a new hope *, 327. Available online at: https://eprint.iacr (Accessed December 19, 2025).

Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., et al. (2018). Hyperledger fabric: a distributed operating system for permissioned blockchains. *arXiv* 18, 1–15. doi:10.1145/3190508.3190538

Backes, M., Kate, A., Maffei, M., and Pecina, K. (2012). "ObliviAd: provably secure and practical online behavioral advertising," in SP '12: Proceedings of the 2012 IEEE symposium on security and privacy (IEEE) 257–271. doi:10.1109/SP.2012.25

Ben-Sasson, E., Chiesa, A., Tromer, E., and Virza, M. (2025) Succinct Non-Interactive Zero Knowledge for a von Neumann Architecture. Available online at: https://www.usenix.org/conference/usenixsecurity14/technical-sessions/presentation/ben-sasson (Accessed December 19, 2025).

Ben-Sasson, E., Chiesa, A., Garman, C., Green, M., Miers, I., Tromer, E., et al. (2014). "Zerocash: decentralized anonymous payments from bitcoin," in *Proc IEEE symp secur priv*, 459–474. doi:10.1109/SP.2014.36

Bernstein, D. J. (2011). "Post-quantum cryptography," in *Encyclopedia of cryptography and security*. Boston, MA: Springer, 949–950. doi:10.1007/978-1-4419-5906-5_386

Brown, T. B., Mann, B., Ryder, N., Subbiah, M., Kaplan, J., Dhariwal, P., et al. (2020). "Language models are few-shot learners," *proceedings.neurips.ccT Brown, B Mann, N Ryder, M Subbiah, JD Kaplan, P Dhariwal, A Neelakantan, P ShyamAdvances in neural information processing systems, 2020•proceedings.neurips.cc*. Available online at: https://proceedings.neurips.cc/paper/2020/hash/1457c0d6bfcb4967418bfb8ac142f64a-Abstract.html.

Bünz, B., Bootle, J., Boneh, D., Poelstra, A., and Maxwell, G. (2018). "Bulletproofs: short proofs for confidential transactions and more," in *EEE symposium on security and privacy (SP)* (San Francisco, CA: IEEE), 315–334. doi:10.1109/SP.2018.00020

Buterin, V. (2014). "A next-generation smart contract and decentralized application platform," in *Ethereum white paper*, 7087.

Chaum, D. L. (1981). Untraceable electronic mail, return addresses, and digital pseudonyms. *Commun. ACM* 24, 84–90. doi:10.1145/358549.358563

Chaum, D. (1983). "Blind signatures for untraceable payments," in *Lecture notes in computer science (including subseries lecture notes in artificial intelligence and lecture notes in bioinformatics)*. Boston, MA: Springer, 199–203. doi:10.1007/978-1-4757-0602-4_18

Chen, L., Jordan, S., Liu, Y.-K., Moody, D., Peralta, R., Perlner, R., et al. (2016). Report on post-quantum cryptography. Available online at: https://nvlpubs.nist.gov/nistpubs/ir/2016/nist.ir.8105.pdf (Accessed December 19, 2025).

CoinMarketCap. Cryptocurrency prices, charts and market capitalizations| CoinMarketCap. Available online at: https://coinmarketcap.com/ (Accessed January 08, 2023).

CoinmarketcapCoingecko (2023). Cryptocurrency prices by market cap. Available online at: https://www.coingecko.com/ (Accessed December 19, 2025).

Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., et al. (2022). Cyber risk and cybersecurity: a systematic review of data availability. *Geneva Pap. Risk Insur. Issues Pract.* 47, 698–736. doi:10.1057/S41288-022-00266-6

Cross, C. (2022). *Meeting the Challenges of Fraud in a Digital World.* Cham: Palgrave Macmillan. doi:10.1007/978-3-030-91735-7_11

Danezis, G., and Mittal, P. (2009). "SybilInfer: detecting sybil nodes using social networks," in 16th symposium on network and distributed system security, NDSS 2009 - San Diego, United States, February 09, 2009.

Douceur, J. R. (2002). "The sybil attack," in IPTPS 2002. Lecture Notes in Computer Science (Springer, Berlin, Heidelberg), 2429, 251–260. doi:10.1007/3-540-45748-8_24

Ducas, L., Durmus, A., Lepoint, T., and Lyubashevsky, V. (2013). "Lattice signatures and bimodal Gaussians," in *Lecture notes in computer science (including subseries lecture notes in artificial intelligence and lecture notes in bioinformatics)*, Springer, Berlin, Heidelberg, 8042, 40–56. doi:10.1007/978-3-642-40041-4_3

Gentry, C. (2009). "Fully homomorphic encryption using ideal lattices," in *Proceedings of the annual ACM symposium on theory of computing*, (Bethesda MD: ACM) 169–178. doi:10.1145/1536414.1536440

Golladay, K. A. (2020). "Identity theft: nature, extent, and global response," in *The palgrave handbook of international cybercrime and cyberdeviance* (Cham: Palgrave Macmillan), 981–999. doi:10.1007/978-3-319-78440-3_40

Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., et al. (2014). Generative adversarial networks. *Commun. ACM* 63 (11), 139–144. doi:10.1145/3422622

Irvin-Erickson, Y. (2024). Identity fraud victimization: a critical review of the literature of the past two decades. *Crime. Sci.* 13 (1), 1–26. doi:10.1186/s40163-024-00202-0

Juels, A., and Wattenberg, M. (1999). "Fuzzy commitment scheme," in *Proceedings of the ACM conference on computer and communications security* (New York, NY: ACM), 28–36. doi:10.1145/319709.319714

Juels, A., Rivest, R. L., and Szydlo, M. (2003). The blocker tag: selective blocking of RFID tags for consumer privacy. Available online at: www.autoidcenter.org (Accessed December 19, 2025).

Kalvet, T., Tiits, M., and Ubakivi-Hadachi, P. (2019). Risks and societal implications of identity theft. *Commun. Comput. Inf. Sci.* 947, 67–81. doi:10.1007/978-3-030-13283-5_6

Kingma, D. P., and Welling, M. (2013). "Auto-encoding variational bayes," in *2nd international conference on learning representations, ICLR 2014 - conference track proceedings*, December 20, 2013. doi:10.61603/ceas.v2i1.33

Kumar, M. (2022). Post-quantum cryptography Algorithm's standardization and performance analysis. *Array* 15, 100242. doi:10.1016/J.ARRAY.2022.100242

LeCun, Y., Bengio, Y., and Hinton, G. (2015). Deep learning. *Nat. Com.* 521 (7553), 436–444. doi:10.1038/nature14539

Lyubashevsky, V., Peikert, C., and Regev, O. (2010). "On ideal lattices and learning with errors over rings," in *Advances in Cryptology – EUROCRYPT 2010. EUROCRYPT 2010. Lecture Notes in Computer Science.* Editor H. Gilbert (Berlin, Heidelberg: Springer), 6110, 1–23. doi:10.1007/978-3-642-13190-5_1

Micciancio, D., and Regev, O. (2009). "Lattice-based cryptography," in *Post-quantum cryptography*, January 31, 2009 (Springer, Berlin, Heidelberg) 147–191. doi:10.1007/978-3-540-88702-7_5

Nakamoto, S. (2008). "Bitcoin: a peer-to-peer electronic cash system," in *Decentralized business review*, 21260.

NIST (2023a). Post-quantum cryptography|CSRC|competition for post-quantum cryptography standardisation. Available online at: https://csrc.nist.gov/projects/post-quantum-cryptography (Accessed December 19, 2025).

NIST (2023b). Post-quantum cryptography|CSRC|selected algorithms: public-key encryption and Key-establishment algorithms. Available online at: https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022 (Accessed December 19, 2025).

NIST (2025). Post-quantum cryptography PQC. Available online at: https://csrc.nist.gov/Projects/post-quantum-cryptography (Accessed December 19, 2025).

NIST, National Institute of Standards and Technology (2017). Post-quantum cryptography: Nist's plan for the future. Available online at: https://www.nist.gov/document/formattednistopengovernmentplan2016finalpdf (December 19, 2025).

Oded, G. (2009). Foundations of cryptography: volume 2, basic applications. Available online at: http://www.amazon.com/Foundations-Cryptography-2-Basic-Applications/dp/052111991X (Accessed December 19, 2025).

Peikert, C. (2016). A decade of lattice cryptography. *Found. Trends® Theor. Comput. Sci.* 10 (4), 283–424. doi:10.1561/0400000074

Petkus, M. (2019). Why and how zk-SNARK works. Available online at: https://arxiv.org/abs/1906.07221v1 (Accessed December 19, 2025).

Poon, J., and Dryja, T. (2016). The bitcoin lightning network: scalable off-chain instant payments.

Radford, A., Metz, L., and Chintala, S. (2015). "Unsupervised representation learning with deep convolutional generative adversarial networks," in *4th international conference on learning representations, ICLR 2016 - conference track proceedings*. Available online at: https://arxiv.org/abs/1511.06434v2.

Regev, O., and Lattices, O. (2005). On lattices, learning with errors, random linear codes, and cryptography. *J. ACM* 56 (6), 1–40. doi:10.1145/1568318.1568324

Sahai, A., and Watersy, B. (2014). "How to use indistinguishability obfuscation: deniable encryption, and more," in *Proceedings of the annual ACM symposium on theory of computing*, 475–484. Available online at: https://dl.acm.org/doi/10.1145/2591796.2591825.

Schneier, B. (2015). Data and Goliath: the hidden battles to collect your data and control your world. Available online at: https://books.google.com/books?hl=en&lr=&id=MwF-

BAAAQBAJ&oi=fnd&pg=PT6&dq=Schneier,+B.+(2015).+Data+and+Goliath:+The+Hidden+Battles+to+Collect+Your+Data+and+Control+Your+World.+W.W.+Norton+%26+Company.&ots=Ui0M5MCeT2&sig=StJudDiGLvambXAwLp_SPIDgcyI.

Shafiq, M. Z., Tabish, S. M., Mirza, F., and Farooq, M. (2009). "PE-miner: mining structural information to detect malicious executables in realtime," in *Lecture notes in computer science (including subseries lecture notes in artificial intelligence and lecture notes in bioinformatics), vol. 5758 LNCS*, 121–141. doi:10.1007/978-3-642-04342-0_7LNCS

Shostack, A. (2014). Threat modeling: designing for security. Available online at: https://books.google.com/books?hl=en&lr=&id=YiHcAgAAQBAJ&oi=fnd&pg=PR21&dq=Shostack,+A.+(2014).+Threat+Modeling:+Designing+for+Security.+Wiley.&ots=eVNtNz7_Lx&sig=JpWGtrEU89dj-v94zxJLI_mwGEE (Accessed December 19, 2025).

Silver, D., Huang, A., Maddison, C. J., Guez, A., and nature, L. S.- (2016). "Undefined, "Mastering the game of Go with deep neural networks and tree search"," *nature.com D. Silver, A huang, CJ Maddison, A guez, L sifre, G Van Den Driessche, J schrittwiesernature, 2016•nature.com*. Available online at: https://www.nature.com/articles/nature16961%7D.

Sommer, R., and Paxson, V. (2010). "in 2010 IEEE symposium on security., and 2010, undefined, "Outside the closed world: On using machine learning for network intrusion detection"," *ieeexplore.ieee.orgR Sommer, V Paxson2010 IEEE symposium on security and privacy, 2010•ieeexplore.ieee.org*. Available online at: https://ieeexplore.ieee.org/abstract/document/5504793/.

Thi, H., Ho, N., and Luong, H. T. (2022). Research trends in cybercrime victimization during 2010–2020: a bibliometric analysis. *SN Soc. Sci.* 2 (1), 1–322. doi:10.1007/S43545-021-00305-4

Vaswani, A., Brain, G., Shazeer, N., Parmar, N., Uszkoreit, J., Jones, L., et al. (2010). "Attention is all you need," *Proceedings.neurips.ccA Vaswani, N Shazeer, N Parmar, J Uszkoreit, L Jones, AN Gomez, Ł Kaiser, I PolosukhinAdvances in neural information processing systems, 2017•proceedings.neurips.cc*. Available online at: https://proceedings.neurips.cc/paper/2017/hash/3f5ee243547dee91fbd053c1c4a845aa-Abstract.html.

Vitalik, B., and Wood, G. (2013). *Ethereum whitepaper, 1*. GitHub Repository.

W3C (2022). "Decentralized Identifiers (DIDs) v1.0,". Available online at: https://www.w3.org/TR/did-core/ (Accessed June 28, 2024).

Wood, G. (2014). "Ethereum: a secure decentralised generalised transaction ledger," in *Ethereum: a secure decentralised generalised transaction ledger. Ethereum project yellow paper*, 1–32. Available online at: https://cryptodeep.ru/doc/paper.pdf.

Yu, H., Kaminsky, M., Gibbons, P. B., and Flaxman, A. D., (2008). SybilGuard: defending against sybil attacks *via* social networks. *IEEE. ACM. Trans. Netw.* 16, 576, 589. doi:10.1109/TNET.2008.923723

Zyskind, G., Nathan, O., and Pentland, A. S. (2015). "Decentralizing privacy: using blockchain to protect personal data," in *Proceedings - 2015 IEEE Security and Privacy Workshops, SPW 2015*, 180–184. doi:10.1109/SPW.2015.27