Technical Paper: Web3 Know Your Customer (KYC) System

Abstract

This technical paper explores the design and implementation of a Web3 Know Your Customer (KYC) system, leveraging blockchain technology to enhance security, efficiency, and user control over personal data. It details the functional requirements, process flow, and key features of a proof-of-concept (PoC) system, aiming to address the challenges of traditional KYC processes in the decentralized Web3 environment. The paper also discusses the integration of AI and web scraping for risk profiling and data verification, and the potential for on-chain audit logs and reusable KYC credentials.

1. Introduction

Know Your Customer (KYC) processes are a critical component of regulatory compliance across various industries, particularly in finance. Traditionally, KYC involves extensive data collection and verification by centralized entities to prevent illicit activities such as money laundering and terrorist financing. However, with the advent of Web3 and decentralized technologies, the conventional KYC paradigm faces significant challenges, including data privacy concerns, inefficiencies, and high operational costs.

This paper presents a comprehensive analysis of a Web3-native KYC system, designed to address these limitations by integrating blockchain technology, decentralized identity (DID), and artificial intelligence (AI). The primary objective of this system is to enable secure, efficient, and privacy-preserving identity verification for participants in the Web3 ecosystem, specifically focusing on investors and their related parties. By leveraging the immutability and transparency of blockchain, the system aims to store verified credentials on-chain, facilitating their reuse across multiple platforms and significantly reducing redundant verification efforts.

The proposed Web3 KYC Proof-of-Concept (PoC) system, as detailed in the provided Excel documentation, emphasizes a modular design that can be whitelabelled or integrated into existing processes. It incorporates features such as a web-based front-end for user interaction, customizable KYC workflows, and advanced tools for risk profiling. The system also explores the use of Optical Character Recognition (OCR) and AI for automated document review and data interpretation, alongside on-chain audit logs to maintain a transparent and immutable record of all changes.

This document will delve into the functional requirements, architectural considerations, and operational flow of the Web3 KYC PoC. Furthermore, it will discuss the broader implications of decentralized KYC, including its benefits in terms of enhanced security, user empowerment, and compliance efficiency, while also acknowledging the inherent complexities and ongoing developments in this nascent field.

2. Problem Statement

The traditional Know Your Customer (KYC) landscape, while essential for regulatory compliance and combating financial crime, is plagued by several inefficiencies and challenges that are exacerbated in the rapidly evolving Web3 environment. These issues include:

- **Redundant Verification Processes:** Users often undergo repetitive KYC checks across different financial institutions and Web3 platforms, leading to a poor user experience and increased operational costs for businesses. Each new service typically requires a fresh submission of personal documents and information, creating friction and delaying onboarding processes.
- **Data Privacy and Security Concerns:** Centralized storage of sensitive personal data makes it a prime target for cyberattacks and data breaches. Users have limited control over their data, and the potential for misuse or unauthorized access remains a significant concern. In the Web3 ethos of decentralization and user sovereignty, this centralized model is fundamentally misaligned.
- **High Operational Costs:** The manual and semi-automated processes involved in traditional KYC, including document collection, verification, and ongoing monitoring, are resource-intensive. This translates to significant financial

burdens for businesses, particularly for smaller entities or startups operating in the Web3 space.

- **Lack of Interoperability:** Data silos between different KYC providers and financial institutions hinder the seamless sharing and reuse of verified identities. This lack of interoperability prevents the creation of a truly global and efficient identity verification ecosystem.
- **Inefficient Risk Profiling:** Current risk assessment methodologies can be static and may not effectively adapt to the dynamic nature of Web3 transactions and participants. The ability to continuously monitor and update risk profiles based on real-time data and on-chain activities is often limited.
- **Compliance Complexity in a Decentralized World:** The decentralized and pseudonymous nature of blockchain transactions presents unique challenges for regulatory compliance. Regulators are still grappling with how to apply existing AML/KYC frameworks to decentralized applications (dApps) and protocols, creating uncertainty for Web3 projects.
- **Scalability Issues:** As the Web3 ecosystem expands, the current KYC infrastructure struggles to scale efficiently to accommodate a growing number of users and transactions, leading to bottlenecks and delays.

The Web3 KYC system described in this paper aims to directly address these problems by proposing a decentralized, efficient, and user-centric approach to identity verification that aligns with the core principles of Web3.

3. System Overview

The Web3 Know Your Customer (KYC) Platform, as outlined in the provided Proof-of-Concept (PoC) documentation, is designed as a modular and adaptable solution for identity verification within the decentralized ecosystem. Its core purpose is to perform KYC on investors and their associated parties, with the critical distinction of saving the verification status on-chain for subsequent reuse. This approach aims to significantly streamline the KYC process, reduce redundancy, and enhance data security and user control.

3.1. Purpose and Aims

The primary purpose of this application is to facilitate the KYC process for all investors and their related entities, ensuring that their verification status is immutably recorded on a blockchain. This on-chain verification enables the reuse of KYC credentials across various Web3 platforms, eliminating the need for repeated submissions of personal information. The overarching aim is to develop this system as a standalone module that can be easily whitelabelled or integrated into existing or new decentralized applications and processes.

3.2. Key Features

The PoC highlights several key functional requirements and features that underpin the Web3 KYC system:

- **Web-based Front-End:** The system will provide a user-friendly web interface to access and manage the KYC process, ensuring accessibility for a broad user base.
- **Customizable KYC Process:** A crucial feature is the ability to customize the KYC workflow for different customers. This includes managing and editing the flow of data, fields, forms, and entities attached to each step of the process, as referenced in the 'Flow example tab 3 (Heading A)' of the Excel document.
- **Post-Registration KYC:** The KYC process is initiated once a user has registered a new account and has not been previously verified, ensuring that all new participants undergo the necessary checks.
- **Comprehensive Profile Creation:** The system will utilize available web tools to create a detailed investor profile based on various factors, including risk assessment, network analysis, security considerations, and fraud detection. This holistic approach extends to connected and related parties of the investor.
- **OCR and AI-powered Document Review:** Optical Character Recognition (OCR) combined with interpretation tools will be employed to review uploaded documents. This functionality aims to automate the verification process, providing a pass/fail result for submitted documents, thereby increasing efficiency and accuracy.
- **Wallet Linking:** Upon successful validation, investors will have the ability to link a cryptocurrency wallet to the relevant platform, seamlessly integrating their

verified identity with their digital assets.

- **User-Updatable Details and Audit Log:** Users can update their personal details, with all changes being recorded in an audit log saved on-chain. This ensures transparency, immutability, and a verifiable history of all modifications.
- **Investor Dashboard:** A dedicated dashboard will be available for investors, providing a centralized view of their KYC status, linked wallets, and other relevant information.
- **Admin Tools:** The entity requesting the KYC will have administrative tools to manage and edit the high-level data flow and the specifics of the KYC process, including fields, forms, and entities at each step.

3.3. Commercial Phase and Future Development

The PoC also outlines a commercial phase and future development roadmap, including:

- **Full MVP Development:** Building a robust Minimum Viable Product (MVP) of the KYC platform.
- **Mobile Accessibility:** Developing Android and iOS applications for broader accessibility.
- **Robust Security Controls:** Implementing comprehensive security measures to protect sensitive data and ensure the integrity of the system.
- **Management of Connected Parties:** Features for deleting and modifying connected parties associated with an investor.
- **On-Chain KYC for Regulatory Compliance:** A key objective is to build out the entire KYC process on-chain to meet evolving regulatory requirements, emphasizing the decentralized and transparent nature of the system.
- **AI-driven Risk Flagging:** Utilizing AI and concatenated data to identify and flag high-risk investors, enhancing the system's ability to detect and prevent fraudulent activities.
- **Ongoing Risk Profiling:** Continuous monitoring and flagging of changes in the risk profile of an investor or their connected parties, with workflows to alert

relevant teams and contacts.

This comprehensive set of features and future plans demonstrates a clear vision for a Web3 KYC system that is not only compliant and secure but also user-centric and highly efficient.

4. Process Flow

The Web3 KYC system outlines a multi-stage process designed to guide users through identity verification, leveraging both traditional and blockchain-enhanced methodologies. The process flow, as detailed in the Excel document, can be broadly categorized into user interaction, data verification, and on-chain recording.

4.1. User Onboarding and Verification

1. **User Login:** The process begins with the user logging into the Web3 KYC platform. This initial step serves as the entry point for all subsequent verification procedures.
2. **User Verification:** Following login, the system initiates user verification. This phase involves a series of actions and data inputs to establish the user's identity. Key actions include:
    - **Adding Institution Details:** If applicable, users provide information related to their institution.
    - **Adding Individual Details:** Users input their personal information.
    - **Pre-populating Details:** The system aims to pre-populate institution and user details where possible, likely through integration with existing databases or user profiles, to streamline the data entry process.
    - **Uploading Documents:** Users are required to upload essential documents such as passports and scanned OCR documents. The system is designed to check the validity of these documents and trigger workflows if they are expired.
    - **Linking Address:** Users provide and link their address information.
3. **Scan User and Risk Profiling:** As users provide information, the system performs a

comprehensive scan of the user. This involves: * **Webscraping and Data Mining:** The system leverages web scraping and data mining techniques to gather additional information about the user and pre-fill data in various sections. This also includes sentiment analysis to assist users in completing the process. * **Risk Profile Generation:** Based on the collected web data, a risk profile is generated for the user. This profile is crucial for assessing potential risks associated with the investor.

1. **Onboarding Complete:** Once all necessary information is gathered and verified, the onboarding process is marked as complete.

4.2. Wallet Linking and Reporting

1. **User Create Wallet & Link to Profile:** After successful onboarding, the user can create a new cryptocurrency wallet or link an existing one to their verified profile. This step is essential for integrating their identity with their Web3 activities.

2. **Reporting:** The system includes a reporting module, likely providing web views for access examples and audit trails of all actions and changes.

4.3. Fields and Forms

The Excel document also details various fields and forms that are part of the KYC process, categorized by the type of information collected:

- **Institution Details:** Information about the institution the investor is associated with.
- **Investor Type:** Categorization of the investor (e.g., company, family office, high net-worth individual).
- **Investor Eligibility Questionnaire:** A set of questions to determine the investor's eligibility.
- **Directors Declaration:** Information related to the directors of the investor's entity.
- **Names, Roles, Email Addresses, Passports, Addresses:** Detailed personal information for individuals involved.
- **Ultimate Beneficial Owner Declaration:** Declaration of the ultimate beneficial owners.

- **Name of Parent Entity and Subsidiaries:** Information about the corporate structure.
- **Investor Legal Name:** The official legal name of the investor.
- **Authorized Persons Declaration:** Declaration of individuals authorized to act on behalf of the investor.
- **Source of Funds Declaration:** Information regarding the origin of the investor's funds.
- **Bank Details:** Banking information for financial transactions.

4.4. TractSafe - Example Risk Profiling

The Excel sheet provides an example of risk profiling, likely for a system named "TractSafe." This section outlines various risk categories and the data points used to assess them:

- **Identity Risk:** Assessed using name, date of birth, passport, address, company name, and directorships. Data is inserted from passport and API/web searches, with validation checks.
- **Industry Risk:** Examples include flagging gambling companies or companies mentioned in the same article as cartels.
- **Network Risk:** Identifying individuals or companies in the network linked to gambling, fraud, or legal proceedings.
- **Security Risk:** Flagging if a person's name/credentials appear on data breaches or the dark web, or if the person is blacklisted.

This detailed process flow and risk profiling methodology underscore the comprehensive nature of the Web3 KYC system, aiming to provide a robust and secure identity verification solution.

5. Technical Architecture

The Web3 KYC system leverages a hybrid architecture that combines traditional web technologies with blockchain and artificial intelligence to deliver a robust, secure, and efficient identity verification solution. The core innovation lies in its ability to store verified KYC credentials on-chain, enabling reusability and enhancing data integrity.

5.1. Blockchain Integration

The system's foundation is built upon blockchain technology, which serves as an immutable and transparent ledger for storing KYC verification statuses and audit logs. While the specific blockchain platform is not explicitly stated in the provided documentation, the mention of "on-chain" storage and "ERC3643 full MIT open source licence" suggests compatibility with Ethereum-based networks or similar smart contract platforms. Key aspects of blockchain integration include:

- **On-Chain Verification Status:** Once an investor successfully completes the KYC process, their verified status is recorded on the blockchain. This acts as a tamper-proof attestation of their identity, which can be referenced by various Web3 applications without re-initiating the full KYC process.
- **Audit Log on-Chain:** All changes to user details and significant events within the KYC process are logged on-chain. This provides an immutable audit trail, crucial for regulatory compliance and dispute resolution. The transparency inherent in blockchain ensures that all modifications are verifiable and traceable.
- **Wallet Linking:** The ability for users to link their cryptocurrency wallets to their verified profiles is a critical component. This establishes a direct, cryptographically secured link between a user's real-world identity and their on-chain activities, facilitating compliant participation in decentralized finance (DeFi) and other Web3 ecosystems.
- **Decentralized Identity (DID) Principles:** Although not explicitly detailed, the concept of reusable KYC credentials aligns strongly with Decentralized Identity (DID) principles. DIDs empower users with greater control over their personal data, allowing them to selectively disclose verified attributes without revealing their full identity to every service provider. The on-chain storage of verification status acts as a verifiable credential, which can be presented by the user as needed.

5.2. Artificial Intelligence (AI) and Machine Learning (ML)

AI and ML play a pivotal role in automating and enhancing various aspects of the KYC process, particularly in data extraction, verification, and risk assessment:

- **Optical Character Recognition (OCR) and Interpretation Tools:** For document verification, OCR technology is employed to extract text from uploaded

documents (e.g., passports, utility bills). This is coupled with AI-powered interpretation tools that analyze the extracted data, compare it against known patterns, and assess its authenticity. This automation significantly reduces manual effort and accelerates the verification timeline, providing a pass/fail result for documents.

- **Web Scraping and Data Mining:** The system utilizes web scraping and data mining techniques to gather supplementary information about individuals and entities from publicly available sources. This data is used to pre-populate forms, enrich user profiles, and contribute to a more comprehensive risk assessment. The integration of sentiment analysis further refines the understanding of an entity's public perception.

- **AI-driven Risk Profiling:** A sophisticated AI engine is responsible for generating and continuously updating risk profiles for investors and their connected parties. This involves analyzing a multitude of factors, including identity verification results, industry affiliations, network connections, and security indicators. The system is designed to flag high-risk investors and trigger workflows for further review by the "TractSafe team" (as mentioned in the Excel file), ensuring proactive risk management.

5.3. System Components and Interactions

The overall architecture can be conceptualized as a series of interconnected components:

- **Web Front-End:** A user-friendly web application serves as the primary interface for investors to submit their KYC information, upload documents, and monitor their verification status. This front-end interacts with the backend services to facilitate data submission and retrieval.

- **Backend Services:** These services handle the business logic of the KYC process, including user authentication, data processing, orchestration of AI/ML models, and interaction with the blockchain layer. They are responsible for managing the customizable KYC workflows and administrative tools.

- **Document Processing Module:** This module integrates OCR and AI interpretation tools to automate the review of submitted documents, ensuring their validity and authenticity.

- **Data Enrichment and Risk Assessment Module:** This module incorporates web scraping, data mining, and AI-driven analytics to build comprehensive user profiles and assess risk levels. It continuously monitors for changes in risk profiles and triggers alerts as necessary.
- **Blockchain Layer:** This layer is responsible for recording immutable KYC verification statuses, audit logs, and managing wallet linkages. Smart contracts would likely govern the logic for on-chain data storage and access control.
- **Database (Off-Chain):** While sensitive verification statuses are on-chain, it is probable that a traditional off-chain database is used to store raw user data, document uploads, and other operational information that does not require the immutability of the blockchain or is too large to store efficiently on-chain. Strict security measures would be in place to protect this data.

This layered architecture ensures a scalable, secure, and intelligent KYC solution that bridges the gap between traditional identity verification practices and the emerging requirements of the Web3 landscape.

6. Key Findings and Discussion

The analysis of the Web3 KYC Proof-of-Concept (PoC) system, combined with broader research into decentralized identity and blockchain-based KYC solutions, reveals several key findings and implications for the future of identity verification in the Web3 era.

6.1. Strengths of the Proposed Web3 KYC System

1. **Enhanced Data Security and Privacy:** By leveraging blockchain for on-chain verification status and audit logs, the system significantly reduces the risk of centralized data breaches. While raw data may still reside off-chain, the immutable record on the blockchain provides a verifiable and transparent history, increasing trust and accountability. The emphasis on user control over their identity, aligning with Decentralized Identity (DID) principles, empowers individuals and mitigates privacy concerns inherent in traditional KYC.
2. **Increased Efficiency and Reusability:** The core strength of this system lies in its ability to enable reusable KYC credentials. Once an investor is verified and their

status is recorded on-chain, this verification can be leveraged across multiple Web3 platforms without requiring repetitive data submissions. This drastically reduces onboarding times and operational costs for both users and service providers, addressing a major pain point of current KYC processes.

3. **Automated and Intelligent Verification:** The integration of OCR, AI, and web scraping tools automates significant portions of the verification process. This not only accelerates the process but also enhances accuracy and reduces the potential for human error. The AI-driven risk profiling, with its continuous monitoring capabilities, allows for more dynamic and adaptive risk assessments, crucial in the fast-paced Web3 environment.

4. **Transparency and Auditability:** The on-chain audit log provides an unparalleled level of transparency and auditability. Every significant action and change related to a user's KYC status is immutably recorded, creating a clear and verifiable trail for regulatory compliance and internal oversight. This is a significant improvement over opaque, centralized systems.

5. **Modularity and Customization:** The design as a modular, whitelabelled solution allows for flexible integration into various Web3 applications. The ability to customize KYC workflows, fields, and forms caters to diverse regulatory requirements and business needs, making the system adaptable to different use cases and jurisdictions.

6.2. Challenges and Considerations

1. **Regulatory Landscape:** While the system aims to meet regulatory requirements by building KYC on-chain, the evolving and often ambiguous regulatory landscape for Web3 and decentralized finance remains a significant challenge. Harmonizing decentralized identity with existing AML/KYC frameworks requires ongoing dialogue and innovation between technologists, regulators, and legal experts.

2. **Data Storage and Management:** The decision to store raw data off-chain, while practical for scalability and cost, introduces a point of centralization and potential vulnerability. Ensuring the secure and compliant management of this off-chain data is paramount. Strategies for data minimization and secure multi-party computation could further enhance privacy.

3. **User Adoption and Education:** The success of a Web3 KYC system heavily relies on user adoption. Educating users about the benefits of decentralized identity, the security implications, and the process of managing their on-chain credentials will be crucial. The user experience must be intuitive and seamless to encourage widespread use.

4. **Interoperability Standards:** While the system promotes reusability, true interoperability across the entire Web3 ecosystem depends on the widespread adoption of common decentralized identity standards (e.g., W3C DIDs and Verifiable Credentials). Continued collaboration within the Web3 community is essential to establish these standards.

5. **AI Bias and Accuracy:** The reliance on AI for document interpretation and risk profiling introduces the potential for algorithmic bias. Ensuring the fairness, transparency, and accuracy of AI models used in critical identity verification processes is a continuous challenge that requires rigorous testing and auditing.

6. **Scalability of On-Chain Operations:** While storing verification status on-chain is efficient, the scalability of certain blockchain operations (e.g., frequent updates to audit logs for a massive user base) needs careful consideration. Layer 2 solutions or alternative blockchain architectures might be necessary to handle high transaction volumes efficiently.

6.3. Future Implications

The Web3 KYC system represents a significant step towards a more secure, efficient, and user-centric approach to identity verification. Its emphasis on on-chain verification and reusable credentials has the potential to revolutionize how individuals and entities interact with digital services, fostering greater trust and reducing friction. As regulatory frameworks mature and technological advancements continue, such systems will play a crucial role in bridging the gap between the traditional financial world and the decentralized Web3 ecosystem, enabling compliant and secure participation for a global user base.

7. Conclusion

The Web3 Know Your Customer (KYC) system, as conceptualized and detailed in this technical paper, offers a compelling vision for the future of identity verification in a

decentralized world. By strategically integrating blockchain technology, artificial intelligence, and a user-centric design philosophy, the system addresses many of the inherent inefficiencies, security vulnerabilities, and privacy concerns associated with traditional KYC processes.

The core innovation lies in its ability to establish a reusable, on-chain verification of identity, significantly streamlining onboarding procedures and reducing the repetitive burden on users and service providers alike. The immutable audit trails provided by blockchain ensure unparalleled transparency and compliance, while AI-driven tools enhance the accuracy and efficiency of document processing and risk profiling. This hybrid approach, combining the strengths of centralized data management for raw information with the decentralized immutability of blockchain for verification status, represents a pragmatic and powerful solution.

While challenges remain, particularly in navigating the evolving regulatory landscape and ensuring widespread adoption, the foundational principles of this Web3 KYC system—user empowerment, data security, and operational efficiency—position it as a transformative force. As the Web3 ecosystem continues to mature, solutions like this will be instrumental in fostering a more secure, compliant, and accessible digital economy, where individuals maintain greater control over their digital identities and interactions.

References

[1] zkMe. (2024, November 7). *KYC Explained: Securing Your Identity in the Web3 World*. Medium. https://medium.com/@zkMe/kyc-explained-securing-your-identity-in-the-web3-world-8cc2a4b47f15 [2] Togggle. *Decentralized KYC & CDD For Web 3 Companies*. https://www.togggle.io/web3-kyc-solution [3] ComPilot. *Web3 Compatible Compliance*. https://www.compilot.ai/kyc [4] Hiro. (n.d.). *DeFi KYC: The Contradiction of Knowing Your Customer in Web3*. https://www.hiro.so/blog/defi-kyc-the-contradiction-of-knowing-your-customer-in-web3 [5] Meegle. (2025, March 17). *KYC In Web3*. https://www.meegle.com/en_us/topics/web3/kyc-in-web3 [6] Ligero Inc. (2025, July 7). *Reshaping KYC/AML in Web3*. https://ligero-inc.com/introducing-ligetron-zkvm-by-ligero-copy [7] IOTA. (2024, February 13). *KYC Done Right With IOTA*. https://blog.iota.org/kyc-done-right-with-iota/ [8] S. K. Lee. (n.d.). *The Trust Anchor of Web3: A Critical Analysis of a Global Digital ID (DID) and KYC Utility (KYCU)*. Medium. https://medium.com/@sklee206/the-trust-anchor-of-web3-a-critical-analysis-of-a-

global-digital-id-did-and-kyc-utility-kycu-236ac4850f96 [9] SecurityOnline.info. (n.d.). *New Web3 Identification Standard: IT Expert launches an innovative decentralized platform without servers and KYC*. https://securityonline.info/new-web3-identification-standard-it-expert-launches-an-innovative-decentralized-platform-without-servers-and-kyc/ [10] Fintech Futures. (n.d.). *zkMe Unveils zkKYC: A Fully Decentralized and Privacy-First KYC Solution*. https://www.fintechfutures.com/press-releases/zkme-unveils-zkkyc-a-fully-decentralized-and-privacy-first-kyc-solution [11] Transak. *Light KYC*. https://transak.com/kyc [12] NCBI. (n.d.). *A systematic literature review of blockchain-based e-KYC systems*. https://pmc.ncbi.nlm.nih.gov/articles/PMC10100622/ [13] Togggle. (n.d.). *Web 3.0 and KYC: The Changing Landscape of Customer Verification*. https://www.togggle.io/blog/web3-0-kyc-changing-customer-verification [14] Baringa. (2023, February 27). *Solving the KYC dilemma with Web 3*. https://www.baringa.com/en/insights/web-3/solving-the-kyc-dilemma-with-web-3/ [15] WebID. *KYC Solutions for Your Crypto Platform*. https://webid-solutions.com/en/sectors/crypto/ [16] Hashlock. *Crypto KYC Providers | Audit Services*. https://hashlock.com/services/crypto-kyc [17] Youverify. (2024, June 26). *Customer Due Diligence, KYC And AML Compliance For Web 3*. https://youverify.co/blog/customer-due-diligence-kyc-aml-compliance-for-web3 [18] IOTA. (2024, June 13). *IOTA Web3 ID Solution Chosen for European Blockchain Sandbox*. https://blog.iota.org/iota-web3-id-solution-sandbox/ [19] Synaps. *Unified platform for identity verification*. https://synaps.io/ [20] Toucan Protocol. (2022, October 31). *KYC in web3 carbon markets | Improving the VCM*. https://blog.toucan.earth/kyc-in-web3-carbon-markets/ [21] Dock Labs. (2025, July 10). *Decentralized Identity: The Ultimate Guide 2025*. https://www.dock.io/post/decentralized-identity [22] DeFi Prime. *Decentralized Identity Systems*. https://defiprime.com/decentralized_kyc_identity [23] Entrust. (2023, January 18). *Decentralized Identity - Know Your Customer (Kyc)*. https://www.entrust.com/blog/2023/01/decentralized-identity-know-your-customer-kyc [24] Forbes. (2024, October 25). *The Benefits And Drawbacks Of Decentralized KYC*. https://www.forbes.com/councils/forbesbusinesscouncil/2024/10/25/know-your-customer-the-benefits-and-drawbacks-of-decentralized-kyc/ [25] Identity.com. (2025, June 26). *What Is Decentralized Identity? A Comprehensive Guide*. https://www.identity.com/decentralized-identity/ [26] Togggle. *The Decentralized KYC Solution For Your Business*. https://www.togggle.io/ [27] Indicio. (2024, May 14). *How Decentralized Identity enables re-usable KYC and what it means for you*. https://indicio.tech/blog/how-decentralized-identity-enables-re-usable-kyc-and-

what-it-means-for-you/ [28] Okta. (2024, September 28). *Decentralized Identity: The future of digital Identity management*. https://www.okta.com/blog/2021/01/what-is-decentralized-identity/ [29] ScienceDirect. (n.d.). *Blockchain-based Decentralized KYC Verification Framework for*. https://www.sciencedirect.com/science/article/pii/S1877050922021263 [30] Regula Forensics. (2025, May 16). *Decentralized Identity Explained: Definition, Components, Use Cases*. https://regulaforensics.com/blog/what-is-decentralized-identity/ [31] Ping Identity. *PingOne Neo Decentralized Identity 101*. https://www.pingidentity.com/en/lp/ac/pingone-neo/decentralized-identity-101.html [32] Decentralized-id.com. (2023, June 16). *KYC|AML and Self Sovereign Identity*. https://decentralized-id.com/application/kyc/ [33] OCR Solutions. (2024, December 30). *Decentralized KYC Made Better with Blockchain and OCR*. https://ocrsolutions.com/decentralized-kyc-how-blockchain-and-ocr-revolutionize-identity-verification/?srsltid=AfmBOopU95sg98NLvxe0QdwOc6yqTMrLx8g3hgJc6_L7h6urK2OBmpsG [34] Coinmetro. (2024, April 25). *Decentralized Identity (DID) in Cross-Border KYC Processes*. https://coinmetro.com/learning-lab/decentralized-identity [35] QuestDB. *Decentralized Identity Verification*. https://questdb.com/glossary/decentralized-identity-verification/ [36] Togggle. *Decentralized Identity Solutions for Social Networking Sites*. https://www.togggle.io/blog/decentralized-identity-solutions-for-social-networking-sites [37] Infosys BPM. *Digital identity management in KYC processes*. https://www.infosysbpm.com/services/financial-crime-compliance/insights/the-rise-of-decentralised-identity-in-kyc-processes.html [38] Risc Zero. (2024, March 7). *Decentralized Identity Verification with zkKYC and Soulbound NFTs*. https://risczero.com/blog/decentralized-identity-verification-with-zkkyc-and-soulbound-nft [39] Identity.com. (2025, March 26). *What Is Reusable KYC? How It's Transforming Identity Verification*. https://www.identity.com/what-is-reusable-kyc-how-its-transforming-identity-verification/ [40] Entrust. (2023, May 18). *Breaking Down Decentralized Identity and Know Your Customer*. https://www.entrust.com/blog/2023/05/breaking-down-decentralized-identity-and-know-your-customer [41] Sanction Scanner. (2025, June 20). *What are KYC and Blockchain?*. https://www.sanctionscanner.com/blog/what-are-kyc-and-blockchain-why-is-kyc-important-for-crypto-exchanges-636 [42] KYC Chain. *Home*. https://kyc-chain.com/ [43] KPMG. *Blockchain KYC utility - KPMG Cayman Islands*. https://kpmg.com/ky/en/home/insights/2018/02/blockchain-kyc-utility-fs.html [44] FinTech Global. (2024, May 9). *How is blockchain transforming the KYC space?*. https://fintech.global/2024/05/09/how-is-blockchain-transforming-the-kyc-space/ [45]

Debut Infotech. (2024, November 6). *Blockchain KYC: Key Benefits, Challenges, and Implementation*. https://www.debutinfotech.com/blog/blockchain-kyc [46] Notabene. *What is KYC in crypto and why do crypto exchanges require it?*. https://notabene.id/crypto-travel-rule-101/kyc-crypto [47] GeeksforGeeks. (2022, May 11). *BlockChain and KYC*. https://www.geeksforgeeks.org/cloud-computing/blockchain-and-kyc/ [48] Veriff. *What Is KYC In Crypto?*. https://www.veriff.com/kyc/guides/what-is-kyc-in-crypto [49] Appinventiv. *Applications & Benefits of Blockchain Technology for KYC*. https://appinventiv.com/blog/use-blockchain-technology-for-kyc/ [50] Sumsub. *Easy Onboarding with Crypto KYC solution*. https://sumsub.com/crypto/ [51] IJNRD. *KYC Verification Using Blockchain*. https://www.ijnrd.org/papers/IJNRD2306403.pdf [52] Blockpass. *KYC For Blockchains*. https://www.blockpass.org/kyc-for-blockchains/ [53] IEEE Xplore. *Optimised KYC Blockchain System*. https://ieeexplore.ieee.org/document/9071533/ [54] SignDesk. *Blockchain Based KYC – The Future of KYC Verification*. https://signdesk.com/in/ekyc/blockchain-kyc-future-of-kyc-verification [55] Blockchain-Council. *Certified Blockchain & KYC Professional*. https://www.blockchain-council.org/certifications/certified-blockchain-kyc-professional/ [56] Trulioo. *Understanding KYC Crypto Requirements*. https://www.trulioo.com/industries/crypto-identity-verification/kyc [57] ScienceDirect. *Designing a Framework for Digital KYC Processes Built on*. https://www.sciencedirect.com/science/article/abs/pii/S0378720621001270 [58] IntellectEU. (2023, August 22). *The Future of Identity: Blockchain-based Verification in KYC Processes*. https://www.intellecteu.com/blog/the-future-of-identity-blockchain-based-verification-in-kyc-processes