



# THE RISE OF DECENTRALISED IDENTITY (DCI) IN KYC PROCESSES

## Abstract

The rise of decentralised identity verification is reshaping Know Your Customer (KYC) processes, offering enhanced security, efficiency, scalability, and user control. Traditional centralised KYC methods are often prone to inefficiencies and security vulnerabilities. Digital identity management aims to overcome these challenges by leveraging blockchain solutions in KYC that can allow for faster onboarding, improved privacy, and smooth cross-border transactions.



While challenges like regulatory complexities, data security concerns, and adoption hurdles exist, the benefits of decentralised identity systems, including reduced costs and operational risks, make them essential for protecting future-proofing financial institutions. As digital economies expand, embracing decentralised identity verification in KYC frameworks will be key to staying ahead in an interconnected global market. The global financial landscape is undergoing a seismic shift as Know

Your Customer (KYC) compliance frameworks evolve to meet the demands of a digital-first world. Traditional KYC processes, often reliant on centralised databases and manual processing, have long been fraught with inefficiencies, security vulnerabilities, and regulatory inconsistencies across borders. As businesses expand globally, centralised KYC verification continues to present significant roadblocks – ranging from data breaches to slow onboarding processes. This lack of agility has led to

the adoption of decentralised identity verification, a cutting-edge approach that leverages blockchain and OCR technology to enhance digital identity management. Experts estimate that the global decentralised identity market will grow at an astonishing rate. This rapid growth underscores the increasing need for more secure, scalable, and efficient identity verification solutions as the digital economy continues to grow.

## What Know Your Customer (KYC) compliance means

KYC regulations and compliance frameworks have been an integral part of financial institutions since 1989, helping them prevent fraud, money laundering, and financial crime. KYC is a set of processes for verifying customer identity, assessing risks, and ensuring regulatory compliance before engaging in financial

transactions. Starting from a straightforward, manual process – customers provide documents, and institutions verify them; KYC has now evolved into digital identity management and electronic verification. As financial services modernise, institutions have started using third-party databases,

biometrics, and AI-powered tools to verify customer identities. Despite the differences in jurisdictions or market-specific requirements, a typical KYC process involves four key steps, namely:

Customer onboarding	Verification	Risk assessment	Ongoing monitoring
Collecting identity documents, proof of address, and biometric data	Cross-checking customer details with third-party databases, government registries, and financial records	Assigning risk levels based on customer history, location, and transaction patterns	Evaluating transactions to detect fraudulent activities or anomalies

Although the process may seem straightforward, centralised KYC processes remain inefficient, prone to security threats and challenging to manage, necessitating a shift towards decentralised identity verification.

## Limitations of centralised KYC

While centralised KYC has been the industry standard, it has inherent flaws that can hinder efficiency, security, and user control, including:



### Manual processes

Traditional know-your-customer processes often rely heavily on manual verification, making it more time-consuming and prone to human errors. In high-volume institutions, this inefficiency can slow down onboarding and frustrate customers.



### Limited scalability for cross-border transactions

Centralised KYC systems struggle to meet the burden of global regulatory variations, making cross-border customer onboarding complex and expensive. Financial institutions often face repeated verification requirements in different jurisdictions, adding layers of inefficiency to the process.



### Single point of failure and data breach risks

Traditional KYC systems store sensitive customer information in a single location, making it an attractive target for cybercriminals. This presents a single point of failure, where data breaches can expose personally identifiable information, leading to compliance penalties and reputational damage.



### Lack of user control over personal data

Customers often have minimal control over their data once in the hands of financial institutions. Traditional KYC compliance frameworks often grant companies full custody of customer credentials, raising concerns over unauthorised access and misuse.



### Digital disenfranchisement and limited access

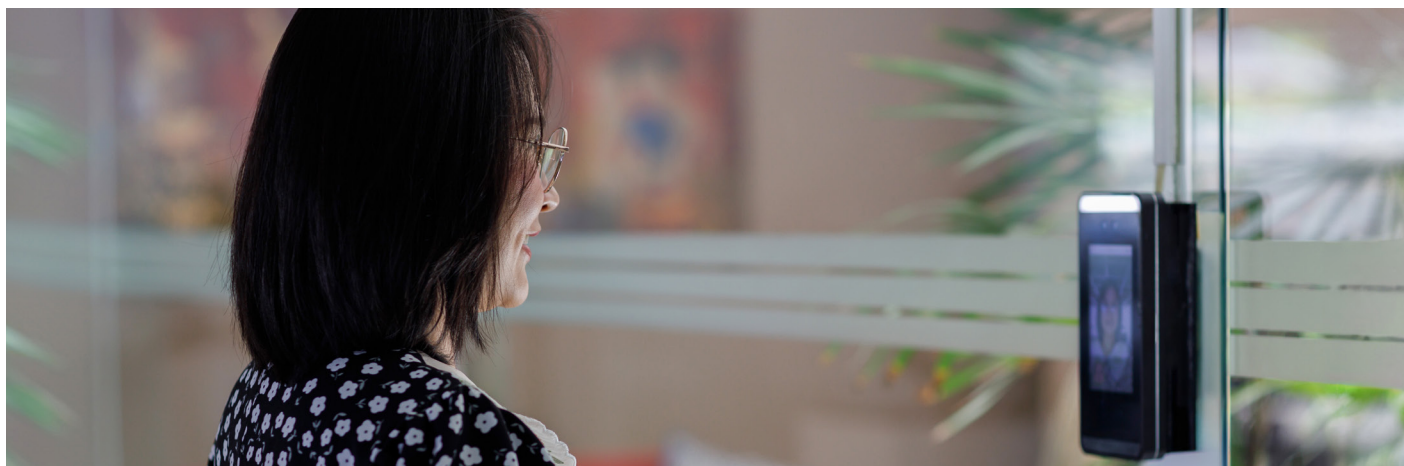
As financial institutions transition towards digital identity management, millions may lose access to financial services due to rigid verification processes. According to the World Bank, around 850 million people globally do not have an official ID, making it difficult for them to access banking and financial services and restricting financial inclusion.



### Growing regulatory burdens

Finally, financial institutions must navigate the growing burden of evolving regulations and update their KYC practices, which can lead to increased costs and operational complexity.

These limitations highlight the need for more agile and secure KYC solutions, which is where digital identity management systems, like decentralised identity verification, comes in the picture.



## Understanding digital identity management

In a bid to overcome these challenges, financial institutions have started transitioning towards digital identity management and decentralised identity verification processes. Modern digital identity solutions utilise biometrics, government-issued IDs, and OCR-based

document scanning to verify customer details with unparalleled accuracy. Unlike centralised KYC protocols, these methods enable seamless cross-referencing with public and private databases, streamlining the KYC process and enhancing security. Blockchain technology is playing a key

role in this shift, facilitating decentralised identity verification where users retain control over their data without relying on a single authority. Leveraging blockchain in KYC creates an immutable record of identity credentials, ensuring secure, tamper-proof verification.


The decentralised identity verification process starts with the credentials that the users hold. The users can then use secure digital wallets to store and manage their credentials and can present them to the verifiers. Verification relies on distributed

ledger systems, where decentralised identifiers and verifiable credentials establish the identity and authenticity of credentials while revealing minimal information. This approach to digital identity management is playing a key


role in removing barriers to access and enhancing user control, making the overall know your customer framework more flexible and efficient.

## Benefits of decentralised identity verification in KYC processes

Adopting decentralised identity verification in KYC processes offers numerous advantages for businesses and customers alike. The key benefits of using blockchain in KYC include:

**Faster and seamless onboarding**


By eliminating manual verification steps, digital identity management and decentralised KYC significantly speed up customer onboarding. This not only reduces friction and customer frustration but also improves user experience.

**Enhanced security and privacy**


Blockchain-based digital identity management ensures encrypted, tamper-proof credential storage while ensuring no unnecessary data is available to financial institutions. This minimises the risk of unauthorised access and data breaches.

**Cross-border efficiency**


With globally accepted decentralised identity solutions, businesses can verify customers easily across jurisdictions without any redundant processes. This ensures smooth international transactions and can contribute to financial inclusion in global markets.

**Greater user control over personal data**

With digital identity management, individual users can manage and share their credentials securely, choosing which entities can access what information. Such control is often the foundation for data privacy and trust.

**Reduced regulatory and organisational risks**

By automating compliance, decentralised identity verification and KYC framework reduces regulatory burdens. Moreover, by leveraging the tamper-proof decentralised ledger technology, blockchain in KYC also minimises liability for financial institutions.

**Cost reduction and operational efficiency**


Automating KYC with blockchain can cut operational costs associated with data storage, verification, and regulatory reporting while boosting overall operational efficiency.

## Challenges in implementing decentralised identity verification

While decentralised identity verification offers transformative benefits, it also comes with challenges that can make KYC processes inefficient without strategic interventions. The key hurdles financial institutions must navigate include:

**Regulatory uncertainty and compliance complexity**

Despite their widespread implementation, global KYC regulations remain fragmented. This, along with technological innovations outpacing the regulatory landscape, makes regulatory alignment difficult for financial institutions implementing decentralised identity solutions.

**Data privacy and security concerns**

While integrating blockchain in KYC enhances security and transparency, institutions must address concerns related to data storage, encryption and management. Ever-evolving cybersecurity challenges make data privacy and security pressing concerns in the digital economy.

**Adoption hurdles and technological barriers**

Transitioning from legacy KYC systems to decentralised, digital identity management requires significant investment in infrastructure, personnel, and staff training. This initial investment, along with resistance to change, often presents one of the biggest hurdles to implementing decentralised identity verification systems.





### User experience and customer education

Educating customers on decentralised identity verification and ensuring a seamless user experience is critical for adoption. Moreover, financial institutions must also acknowledge and address digital disenfranchisement to ensure financial inclusion in their digital identity management and KYC frameworks.



## Future of decentralised digital identity management

Continued advancements in blockchain technology, AI-driven identity verification, and global regulatory frameworks will shape the future of KYC compliance. Financial institutions looking to implement decentralised digital identity management solutions and future-proof their operations in this emerging shift must focus on:



### Building a scalable infrastructure

As data volumes continue to grow and customer expectations evolve, deploying robust digital identity verification frameworks will become essential. Additionally, flexible and scalable infrastructure will be crucial to support these advancements and ensure seamless integration.



### Ensuring regulatory alignment

Working with compliance experts will be crucial to navigate and stay ahead of evolving KYC regulations. This will ensure the successful implementation of compliant decentralised identity solutions for effective digital identity management.



### Educating users on decentralised identity

Many users are still unaware of or hesitant to adopt decentralised identity solutions. Raising awareness about the benefits of decentralised identity verification and ensuring user-friendly digital onboarding experiences will be crucial to ensure user buy-in.



### Choosing the right technology partner

Working with the right BPM and SaaS providers is essential for financial institutions to deploy secure, scalable, and compliant digital identity management solutions and KYC frameworks. These solutions can help leverage biometric authentication, document recognition, and real-time data enrichment to ensure rapid, accurate verification while delivering a seamless onboarding experience.

## Conclusion

The shift from centralised KYC to decentralised identity verification represents a fundamental transformation in [digital identity management](#). By leveraging blockchain technology in KYC compliance, financial institutions can enhance security, efficiency, and

regulatory compliance while giving customers greater control over their data. While challenges such as regulatory complexity and adoption hurdles remain, the long-term benefits – faster onboarding, enhanced privacy, and reduced operational costs – make

decentralised identity verification a central element for future-proofing financial operations. As the digital economy grows and evolves, embracing these solutions will be crucial for staying ahead in an increasingly interconnected world.

For more information, contact [infosysbpm@infosys.com](mailto:infosysbpm@infosys.com)



© 2025 Infosys Limited, Bengaluru, India. All Rights Reserved. Infosys believes the information in this document is accurate as of its publication date; such information is subject to change without notice. Infosys acknowledges the proprietary rights of other companies to the trademarks, product names and such other intellectual property rights mentioned in this document. Except as expressly permitted, neither this documentation nor any part of it may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, printing, photocopying, recording or otherwise, without the prior permission of Infosys Limited and/ or any named intellectual property rights holders under this document.