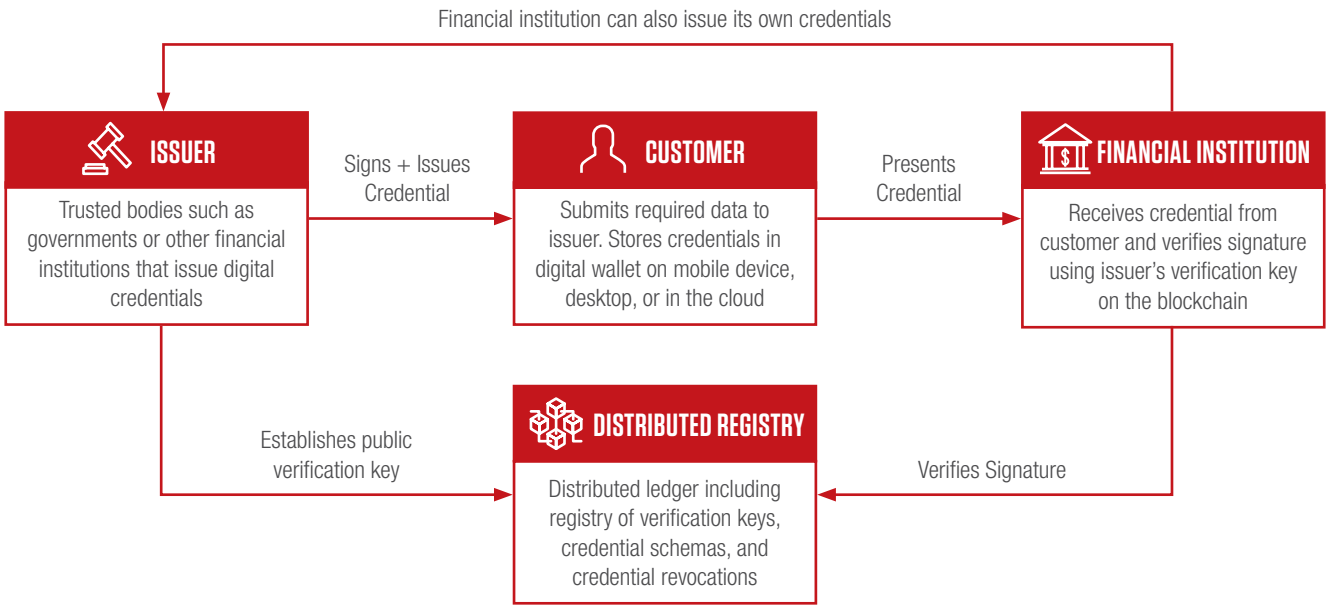
CAPCO

DECENTRALIZED IDENTITY:

HOW DIGITAL TRANSFORMATION AND DISTRIBUTED LEDGER TECHNOLOGY IS DISRUPTING KYC

Financial institutions are struggling to keep up with Know Your Customer (KYC) and Anti-Money Laundering (AML) requirements because of increasing regulatory complexity and more discerning consumer preferences. In 2017 alone, financial institutions reported a 400 percent increase in regulatory headcount yet still cited KYC and onboarding as the most significant challenges in remaining compliant[1]. In 2019, 12 of the world's top 50 banks received fines for KYC, AML, or sanction related violations with total fines across all financial institutions increasing more than 160 percent[2]. At the same time, customers are increasingly wary of sharing personal information following a series of large data breaches, including the 2017 hack of Equifax that exposed personal information on over 143 million Americans. Pew Research found that 81 percent of Americans believe the risks created by companies collecting personal data outweigh the benefits[3]. In response, many institutions are exploring a new decentralized approach based on distributed ledger technology (DLT) to break the cycle of increasing complexity and costs while giving customers more control over their data. By transforming the way organizations and customers share data, decentralized identity allows financial institutions to reduce and mutualize the costs associated with KYC while creating a better customer experience that protects privacy and reduces friction.

WHAT IS DECENTRALIZED IDENTITY?



Decentralized identity uses cryptography to allow customers to present digital credentials that can replace traditional paper and plastic credentials such as passports, driver's licenses, and birth certificates. Instead of each bank having to store and protect the information, these credentials are stored in digital wallets controlled by the customer. Institutions can verify the authenticity of these credentials by inspecting their cryptographic signatures using a public registry of verification keys managed on a distributed ledger. The algorithm used to sign each credential allows the verifier to ensure its properties have not been tampered with. This allows credentials to be presented and verified without interaction from the issuer. If a user needs to update their information, they can be issued a new credential. Credentials are shared using a persistent channel that allows the institution to request the most recent credential to satisfy periodic checks or complete transactions without having to manage and secure the information when not being used. Once established, this connection supports two-way communication to share additional information, such as updated statements and other documentation.

ROLE OF THE DISTRIBUTED LEDGER

The purpose of the ledger is to provide a reliable and tamper-resistant way to store information without a centralized administrator. This enables trust and transparency across the enterprise and national boundaries. Additionally, every transaction and public entity on the ledger can be audited and traced back to its source. This feature could have significant implications for how governments and institutions address FinCEN's Customer Due Diligence (CDD) rule, which requires them to verify the beneficial ownership chain of their clients. Distributed ledger technology is ideally suited to help manage the type of public registries that FinCEN recommends using to track entities and relationships. The government of British Columbia is already applying DLT to register businesses and digitize the issuance of permits and other legal documents. At the time of writing, more than 1.3 million legal entities had been registered, and more than 2.4 million verifiable credentials had been issued[4]. The program is currently being extended to other provinces.

IMPROVING CUSTOMER EXPERIENCE

Nearly every online interaction for today's customers begins with manually filling out the same redundant information: username, password, email, etc. For financial institutions conducting KYC, the data required is more extensive and often collected using paper-based documentation that can take significant time to process. The result is a frustrating experience for users and onboarding times that stretch into weeks. A recent survey found that financial institutions take two to four weeks to onboard a new client, and nearly 12 percent of companies have switched banks as a result of poor KYC experience[5]. Instead of requiring customers to enter the same information each time, decentralized identity enables them to provide an existing credential. The result is a frictionless user experience that increases security while significantly reducing processing times. A pilot program using decentralized identity in US credit unions reduced fraud, increased customer satisfaction, and decreased the time to verify a customer's identity by 80 percent[6].

PROTECTING DATA PRIVACY

One of the most significant benefits of decentralized identity is that it allows customers to have more control over their data while reducing the risks faced by financial institutions who would otherwise have to store it. By transferring custody of the data to the customers, institutions no longer face the risks associated with storing and protecting it between use. Institutions can request a credential when its data is required, removing the requirement for permanent storage. While it is still necessary to maintain some permanent records for auditing purposes, such data minimization is an important step to reduce the risk for the institution.

Decentralized identity also supports the use of zero-knowledge-proofs to give users more control over the data they share. Zero-knowledge proofs allow users to present credentials in such a way that they can still be verified, yet only expose the information required to complete the transaction. For example, a proof might be created from a credential representing a birth certificate that proves the holder is over the age of 18 without showing the actual birthdate. Multiple credentials can be combined into a single proof, allowing users to freely compose data from credentials they already have to meet verification requirements. Such capabilities can help bring an end to the current practice of over-collecting data that exposes firms to greater risk and increases the costs and complexity of compliance with GDPR and other privacy regulations.

ROLE OF FINANCIAL INSTITUTIONS

Financial institutions are ideally placed to help establish the ecosystem needed to support decentralized identity, given the existing requirements around verifying customer identities. The relationship between institutions and customers creates a natural cornerstone for issuing verifiable credentials with a high degree of trust. In contrast, the high costs associated with traditional KYC mechanisms create a clear incentive for financial institutions to adopt an innovative approach. While integrating decentralized identity can add value to individual organizations, the most significant benefits can be realized through coordination between multiple institutions and governments. This allows institutions to mutualize costs while supporting a complete record of financial behavior, which would drive real progress in terms of identification and prevention of financial misconduct. A recent trial including institutions across 19 countries, tested the viability of decentralized identity using simulated transactions. Based on the results, 67 percent of participants believed decentralized identity would have a 'transformational impact' on customer experience with the majority predicting processing times would be cut 30-50 percent. Given the sky-high expectations for the technology, it is remarkable that 83 percent of participants said the results exceeded their initial expectations, and 100 percent said they would recommend this pilot to their peers[7].

BARRIERS TO ADOPTION

While early trials have successfully demonstrated the impact that decentralized identity can have, widespread adoption has not yet materialized. The lack of adoption is due in large part to the relative newness of the technology. Whereas the challenges of KYC go back to the earliest days of finance, DLT has only been around since the Bitcoin whitepaper in 2008. With billions of dollars invested in existing IT infrastructure and operations, migrating to such new technology is not a decision to be made lightly, forcing institutions to adopt a wait-and-see approach.

Furthermore, the connection between distributed ledger technology and cryptocurrencies like Bitcoin and Ethereum has tainted the reputation of DLT.

Additionally, the appearance of KYC utility providers like SWIFT has already enabled some financial institutions to mutualize KYC efforts. However, a recent report from the International Chamber of Commerce found that these providers exclude nearly 34 percent of financial institutions due to high costs and complexity. Moreover, the study found little evidence that they are making a significant impact. Only 23 percent of institutions surveyed reported substantial improvement in operational risk and error rate performance in 2017, compared with more than 40 percent who claimed performance remained the same or got worse[8].

CONCLUSION

Without adopting an innovative solution, financial institutions will continue to struggle under the burden of increasing KYC regulation. FinCEN expects compliance with its own CDD rule to cost financial institutions and customers $10 billion by 2025 with additional regulations like AML5 likely to push these costs much higher[9]. There is no disputing that the ability to reduce money laundering and other illicit financial activity has significant benefits that stretch far beyond the financial system. Yet, today's centralized approaches cannot achieve this without raising serious data privacy concerns. Decentralized identity presents the tantalizing promise for financial institutions to significantly improve KYC/AML while streamlining the customer experience and protecting privacy rights.

REFERENCES

1. https://www.refinitiv.com/content/dam/marketing/en_us/documents/reports/kyc-compliance-the-rising-challenge-for-financial-institutions-special-report.pdf
2. https://www.fenergo.com/news/aml-kyc-and-sanctions-fines-for-global-financial-institutions-top-$36-billion-since-financial-crisis.html
3. https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/
4. https://www.orgbook.gov.bc.ca/en/home
5. https://www.opus.com/future-of-kyc/
6. https://www.businesswire.com/news/home/20191212005053/en/CULedger-Completes-Successful-Pilot-Program-MyCUID-U.S.
7. https://www.prnewswire.com/il/news-releases/infosys-finacle-and-r3-conclude-global-trial-of-blockchain-based-trade-finance-300923069.html
8. https://iccwbo.org/content/uploads/sites/3/2018/05/icc-2018-global-trade-securing-future-growth.pdf
9. https://www.fincen.gov/sites/default/files/shared/CDD_RIA.pdf

AUTHOR

James Hiester, Consultant
James.Hiester@capco.com

ABOUT CAPCO

Capco is a global technology and management consultancy dedicated to the financial services industry. Our professionals combine innovative thinking with unrivalled industry knowledge to offer our clients consulting expertise, complex technology and package integration, transformation delivery, and managed services, to move their organizations forward.

Through our collaborative and efficient approach, we help our clients successfully innovate, increase revenue, manage risk and regulatory change, reduce costs, and enhance controls. We specialize primarily in banking, capital markets, wealth and asset management and insurance. We also have an energy consulting practice in the US. We serve our clients from offices in leading financial centers across the Americas, Europe, and Asia Pacific.

To learn more, visit our web site at www.capco.com, or follow us on Twitter, Facebook, YouTube, LinkedIn and Instagram.

WORLDWIDE OFFICES

APAC
Bangalore
Bangkok
Gurgaon
Hong Kong
Kuala Lumpur
Mumbai
Pune
Singapore

EUROPE
Bratislava
Brussels
Dusseldorf
Edinburgh
Frankfurt
Geneva
London
Paris
Vienna
Warsaw
Zurich

NORTH AMERICA
Charlotte
Chicago
Dallas
Houston
New York
Orlando
Toronto
Tysons Corner
Washington, DC

SOUTH AMERICA
São Paulo

WWW.CAPCO.COM

CAPCO

JN_2271