A Blockchain Enabled KYC Solution: New Horizon or False Dawn?

the answer company™
THOMSON REUTERS®

Contents

Introduction

Against a backdrop of escalating costs, complex manual processes and increased regulatory scrutiny, financial institutions are required to critically evaluate their operating procedures and look to innovative technologies to retain profitability and ensure compliance with global regulations.

Blockchain as one of the most well-known examples of Distributed Ledger Technology, has been hailed across the industry as the key to future success within the financial services industry: 91% of the 1520 global financial services executives surveyed by Cognizant in 2017 cited Blockchain as either "critical or important to their firm's future."[1]

As a technology predicated on collaboration, Blockchain enables parties across the industry to come together to achieve a shared goal, without the need for intermediaries or paper trails to ensure trust. This simplifies and streamlines interactions.

Blockchain is a platform that supports multiple use cases within Financial Services, and it has the ability to transform a number of processes, including peer-to-peer payments, trade settlements and supply chain tracking. One such use case being explored is in the area of Know Your Customer (KYC). The benefits of Blockchain are aligned with industry attempts to solve the KYC challenges of: complex, inefficient processes; access to accurate data; and an increasingly stringent regulatory environment, all of which have led to excessive operational overheads and poor client experiences.

Some see Blockchain technology as a method of revolutionizing the way in which financial institutions conduct KYC, by empowering industry players to work together to ensure the simple, but secure movement of sensitive information between counterparties; mutualizing the effort to manually conduct KYC on each client; and reducing the burden on clients to provide documentation to their banking counterparties.

However, whilst theoretically appealing, the end-to-end KYC use case for Blockchain requires a number of interim steps to transform market thinking before such a solution can be successful. Primarily, many Blockchain use cases are predicated on removing a central intermediary, for example a clearing house, to improve efficiency, whilst maintaining mutual trust between two transacting entities.

In the context of KYC, the concept of a central intermediary has yet to be widely accepted, with the industry still relying on bilateral interactions.

Consequently, in order for a Blockchain enabled KYC solution to be successful in solving the challenges that surround end-to-end KYC processes as opposed to providing an alternative platform on which to manage interactions, first the concept of a utility needs to be adopted as an interim step to drive a standard and establish governance.

The utility is a central player that performs the collection, verification and monitoring of the data and documentation associated with client due diligence and provides a platform for distribution amongst subscribers of mutualized profiles.

[1] Cognizant (2017) Financial Services: Building Blockchain One Block at a Time
https://cognizant.com/whitepapers/financial-services-building-blockchain-one-block-at-a-time-codex2742.pdf

Outlining KYC challenges

Ever-increasing anti-money laundering (AML) regulations, coupled with more aggressive enforcement activities have led many financial institutions to implement lengthy, expensive processes in a bid to remain compliant. These slow the pace of business and have had an increasingly negative impact on the client experience.

As a consequence of the complex regulatory environment and challenge of accessing quality public data, the collection and verification of client entity information is increasingly burdensome. Ensuring the accuracy of information is further exacerbated by the 4th Anti-Money Laundering Directive requirement that data is monitored and updated.

Financial Institutions have traditionally increased staffing as the mechanism for managing complexity in KYC requirements, but with large financial institutions reportedly spending on average $150m[2] on KYC processes in 2017, this operating model is no longer sustainable.

With the introduction of General Data Protection Regulation (GDPR) in 2018, there is significant pressure on financial institutions to monitor their internal controls, particularly those that pertain to client data security, and to provide evidence of robust internal audits to regulators and boards. Assessing the extent to which control guidelines are being followed can be difficult to monitor, especially in large, complex organizations. As a result, firms are challenged with ensuring that concerns such as data security and privacy with respect to the collection and storage of client information are managed and that the overall governance of their operational processes is sound.

Our 2017 Thomson Reuters Global KYC Survey, which gathered responses from both financial institutions and their corporate clients, revealed that the global average time to onboard a new client is 26 days, up from an average of 24 days in 2016.[3]

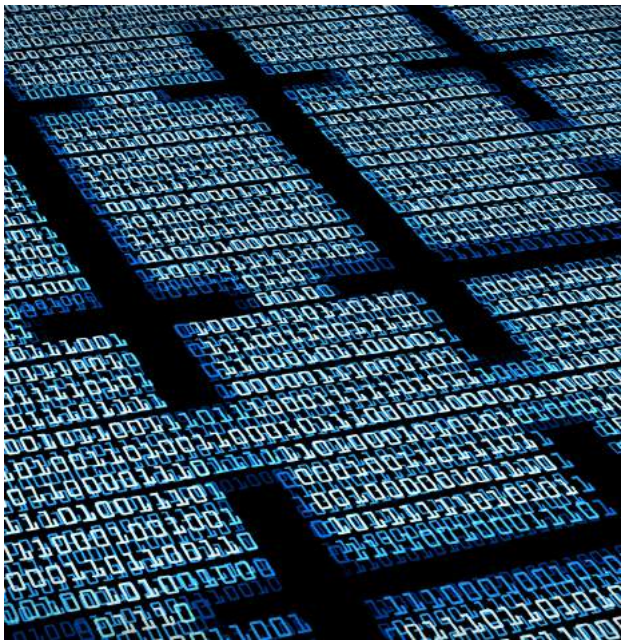
[2] Thomson Reuters (2017): KYC Compliance: The rising challenge for financial institutions https://risk.thomsonreuters.com/en/resources/special-report/kyc-compliance-the-rising-challenge-for-financial-instutitions.html

[3] As above

Blockchain to the rescue?

Whilst there are a number of potential ways to solve KYC challenges, a Blockchain enabled KYC utility model holds particular appeal, with many banks and industry consortiums exploring this option.

A market opportunity has been identified to leverage Blockchain as an enablement layer in the KYC utility model. This would deliver trust and data security on a platform that enables efficiencies in KYC processes. Standardizing and sharing the storage of account opening information on a Blockchain creates a single tamper proof KYC record that mutualizes the effort of conducting KYC and demonstrates compliance with AML regulations, potentially generating $3 – $5 billion in cost savings across the industry.[4]



Characteristics of Blockchain that make it a theoretically advantageous technology to leverage include:

- **Immutability**
  Records are given a unique ID and stored cryptographically in a way that ensures lineage and eradicates the opportunity to tamper with information without alerting the rest of the network.
- **Privacy**
  Encryption through complex cryptography and obfuscation techniques ensures that clients maintain control of their sensitive information and can decide which parties are granted permission to access this information via access to the correct key.
- **Shared ledger**
  Consensus mechanisms ensure that shared data is agreed upon, improving access to accurate information across the industry.
- **Transparency**
  Any participant in the network can access a record, with the correct permission from the client. This is an opportunity for regulators to be nodes on the Blockchain and monitor information directly, ensuring compliance.

[4] Goldman Sachs (2016): Profiles in Innovation; Blockchain: Putting Theory into Practice https://finyear.com/attachment/690548/

What could a Blockchain enabled KYC solution look like?

Conceptually, a Blockchain enabled solution could rely on a network of third parties to build KYC records, without the requirement for clients to provide documentation.

Generating a trusted single client record in an automated fashion delivers an optimized client experience as well as operational efficiencies. It also enhances regulatory compliance by ensuring that all financial counterparties have access to identity information from an official source.

> 'Leveraging open-source intelligence into a single platform could offer myriad benefits, from reducing reliance on multiple vendors to greater transparency and accuracy'.
>
> Jasmine Sicular, Director,
> Global Financial Crimes Compliance, S&P Global

A potential Blockchain enabled KYC solution could take the following shape:

- **Collection of entity data**
  If golden data sources, such as government agencies, create a node and provide a single authoritative source of information on a client, the requirement for the client to provide information to multiple counterparties is removed. Such a model would deliver significant client experience benefits, as an entity would only have to submit their information to the required government agency and then grant access permission to their financial institutions. This means that data traditionally understood as private documentation would be provided through official sources with the consent of the client. Alternatively, for multi-banked clients, a consensus mechanism could be implemented to highlight which financial institutions hold client information that differs from others, creating transparency and consistency in identifying a client.

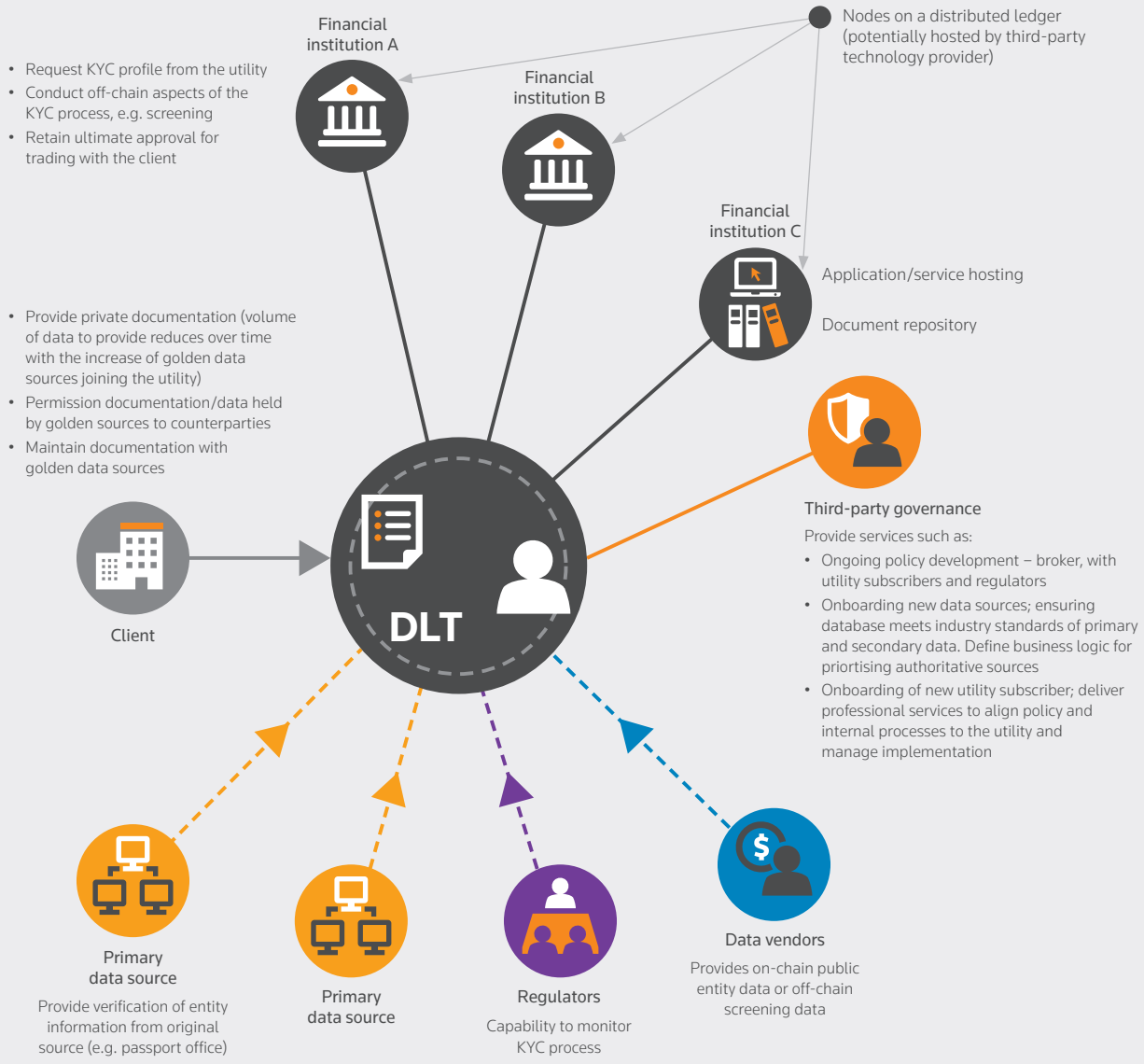
- **Verification of entity data**
  A significant amount of KYC data is currently sourced on paper or from easily replicated 'digital copies'. This has resulted in an entire industry built around third-party data verification services. Through access to primary sources and applying cryptography, identity information can be made self-verifiable, removing the need for forensic validation (for example: examining copies of documentation for authenticity). This would allow financial institutions to instantly verify identity data without having to rely on external information. Utilizing self-verifiable data issued by authoritative sources, financial institutions could at best completely automate their onboarding processes, or at the very least significantly reduce onboarding times. This also has the potential to evolve to deliver enhanced privacy benefits, where verification of an entity or individual from an originating source does not require access to the underlying data, but purely confirmation that the record exists and matches the information expected, for example, verifying an individual's age without having access to their date of birth.

- **Screening**
  Whilst this process may still need to be conducted offchain, a unique ID created for a client as part of the identification and verification process, or through existing IDs, could reduce false positives by accurately identifying the entity or individual. It could also connect a greater number of sources of information relating to an individual client to build a richer picture of their behavior and relationship network, potentially uncovering hidden risks.

- **Monitoring**
  Creating a single record and unique ID enables financial institutions on the network to automatically receive updates to client entity information or changes to risk exposure.

- **Reporting**
  This would enable an immutable audit trail of all activities relating to a KYC profile, including permissions, access and edits.

A potential Distributed Ledger Technology (DLT) or Blockchain enabled KYC Solution.



R3, a consortium of over 70 of the world's biggest financial institutions has recently developed a prototype of a Blockchain enabled KYC utility. The solution was built on Corda, R3's open source distributed ledger technology platform built specifically for regulated financial institutions. Unlike traditional Blockchains, information on Corda is only shared amongst the parties to a transaction. This ensures that regulated financial institutions are remaining compliant with increasingly complex data security and privacy laws.

Is the industry ready for a Blockchain enabled KYC solution?

Given the systemic importance and complexity of the KYC process and the criticality of accurate information for risk decision making and regulatory compliance, there are a number of dependencies and considerations that need to be worked through before a Blockchain enabled KYC utility can be launched.

These considerations not only span technical capabilities, but also regulatory acceptance and a shift in market attitude.

Dependencies required to make a blockchain-enabled KYC Utility feasible include:

- **Proving the viability of the technology**
  To deliver a global KYC utility requires a Blockchain infrastructure that can manage high levels of complexity and business logic as well as accommodate potentially thousands of nodes. Whilst there is significant activity amongst fintechs working on solutions in this space, there are ongoing questions about Blockchain's capability to manage large volumes of transactions at a given time, limiting the scalability of a solution at this stage.

  - KYC-Chain Ltd., a Hong Kong based start up has been building identity technology leveraging distributed ledgers and blockchain. KYC-Chain believe the need for large volume processing capacity can be greatly reduced by managing a number of components off chain (i.e. identity wallets, external service endpoints, etc). In this solution, distributed ledgers would be used mostly for verifying identifiers, public keys, and storing document references (cryptographic hashes).

- **Delivering Return on Investment**
  The cost of developing, implementing and migrating systems to a Blockchain enabled solution is high. Financial institutions need to consider the long term benefit of significant upfront investment to support a platform for a non-revenue generating bank activity. In an environment where financial institutions are struggling to maintain profit margins and have been implementing wide spread cost saving exercises across their organizations, such investments may be difficult to justify.

- **Regulatory reform**
  There has been a shift by some regulatory bodies towards adopting innovative technologies to improve the ease of doing business in their jurisdiction. However, regulation itself is still a few steps behind. For a Blockchain enabled KYC utility to be achievable, requires an industry agreement to leverage technology (whether it be metadata or confirmation through Blockchain) as a form of verification and it is essential to have support from the regulators in revising guidance and regulation on this topic.

- **Access to government databases**
  Open access to data, especially from primary sources including government databases, is critical to achieving a Blockchain enabled KYC utility and will be required in order to facilitate verification. For the Blockchain model, these sources require not only open access but also an ability to provide data to the Blockchain to deliver automated verification.

From Thomson Reuters experience automating the ingestion of public data in key markets and from the 8000+ sources our services use globally for KYC data collection and verification, we have seen considerable effort being required to align data structures and also automate the access to these data sets, many of which are yet to offer API connectivity.

- **Standardisation of the data model**
  A common policy around identification and verification drives a common data set which, in turn, enables the realization of greater onboarding and refresh efficiencies and improved client experience for all utility participants. Given inconsistencies arising from varied interpretations of Financial Action Task Force (FATF) principles, regional regulatory requirements and different interpretation of risk based approach between financial institutions, there is a considerable process and market evolution required to achieve standardization. This is a concept which financial institutions and their clients are very support of and agree on conceptually, however it is very challenging to achieve in practice, remaining somewhat elusive at a global level. Whilst a decentralized Blockchain solution does not necessarily require standardization to operate, not developing a common standard for KYC data requirements significantly impacts the solution's capability to address some of the challenges outlined earlier in this paper, namely client experience and process efficiency.

As well as dependencies, there are also some additional considerations that may form barriers to wide spread adoption to a Blockchain enabled utility model. These include:

- **Governance in a decentralised model**
  Traditionally utilities involve a central player performing the collection, verification and monitoring of KYC data and documentation. This reduces duplication of operational effort and improves the client experience by providing a single point of contact. Typically this central player has been a third party vendor, who provides independent governance of the solution, or a government department, where access to government data is a fundamental requirement, for example for KYC on individuals.

Ultimately to realize a decentralized model, the role of the central party in determining standards, acceptability of sources and establishing the overall data model and data storage is removed. This has been one of the key barriers to establishing a Blockchain solution that optimizes process efficiency, the client experience and regulatory compliance, as mutualization is not achieved. In saying this,

> KYC-Chain see a way of solving for the governance challenge is through implementing different trust and reputation mechanisms on the network, giving some claims or signatures more value than others. Highly trusted entities, such as governments, can adhere to the network to provide attestation of identity data and service providers can act as claim issuers or verifiers, potentially connected to (or even part of) government agencies.

- **Accessibility of infrastructure**
  For a Blockchain enabled utility to operate effectively, market wide adoption is required across financial institutions, their clients and data sources, something many industry solutions have struggled to achieve. Whilst larger, sophisticated players have Blockchain expertise within their organizations, for others, especially end clients, sourcing the technical expertise to set up a node and manage the storage of their documentation and permissions may be a significant barrier to entry.
- **Trust in technology**
  Although the technology conceptually enables trust between counterparties and in the underlying information, there has been hesitancy by many in moving beyond proofs of concept into implementation. Financial institutions face significant scrutiny of their KYC processes and consequently the cost of failure is high. As liability relating to non-compliance with KYC regulations will always lie with financial institutions, migrating business critical processes to a platform based on fairly a nascent technology, especially one that has an association with the Bitcoin brand, which has experienced some negative media – has been approached with caution.

The path to a Blockchain enabled solution

Whilst Blockchain has yet to find its niche in solving KYC challenges, the theoretical use case is clear. There has been a flurry of activity across the industry in an attempt to pave the way for such a solution.

Such attempts have followed two strands of execution, testing different aspects of the concept, which may later converge. The first strand explores the utility concept, the second piloting the technology as an enablement layer across subsections of the KYC process, specifically with regard to the exchange of client documentation.

Utility concept

Over the last 18 months there has been an increase in activity from major banks, regulators and governments investigating the viability of and implementing global and country level KYC utilities, managed by a central player. They solve the issue of duplication amongst financial institutions in mutualizing the operational effort of collecting, verifying and monitoring the data associated with client due diligence to a shared policy standard at a global or jurisdictional level. Such a model provides an intermediary step for a Blockchain enabled KYC utility that requires many of the same considerations to be addressed: centralization; the digitization of documentation requirements; access to trusted data sources; and standardization of policy - but which accommodates more flexibility in the model and provides a blueprint process for building trust, accelerating adoption and managing industry readiness.

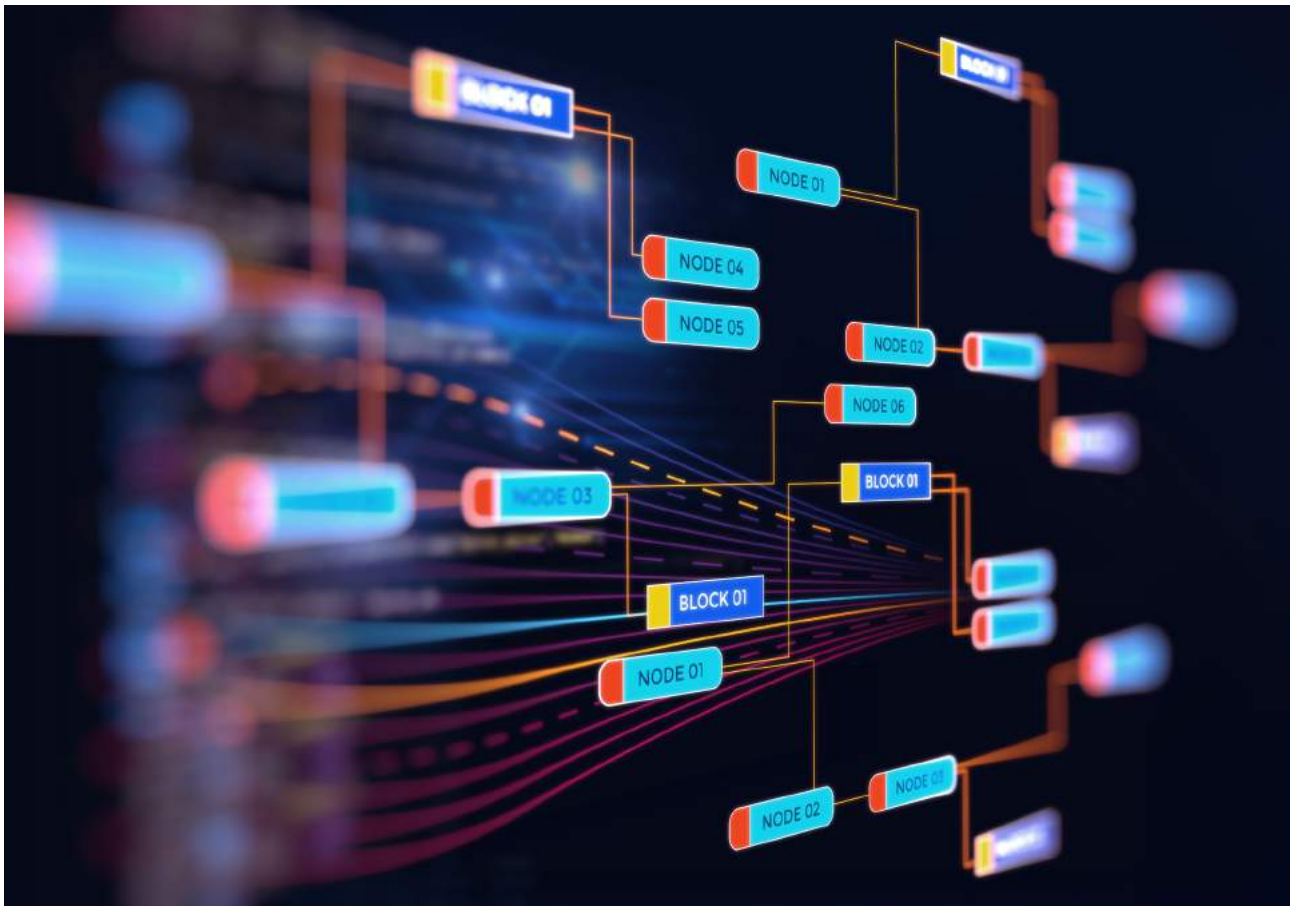
Examples of KYC utilities include: global, vendor-led models such as Thomson Reuters KYC as a Service; regional, bank-led models that leverage a broad set of solution components from vendors, such as the South African KYC utility, co-designed by Standard Bank, Amalgamated Banks of South Africa (ABSA), Rand Merchant Bank (RMB) and Thomson Reuters; and regional government-led initiatives focused on retail KYC, such as India's Central Know Your Customer Registry (CKYCR).

Blockchain enabled document exchange pilots

There has been significant collaboration across the industry, with fintechs, banks, data vendors and regulators working to pilot Blockchain solutions for sub-sections of the KYC process. Whilst many of these solutions will not solve all the KYC challenges encountered by market participants, they are effectively introducing the technology into the KYC space.

Several technology providers like Thomson Reuters, in partnership with financial institutions and their end clients, are piloting KYC document exchange capabilities. These tend to leverage Blockchain technology and a platform to securely store and distribute KYC related documentation to multiple banking counterparties from a central interface. The model Thomson Reuters is piloting, provides a Blockchain enabled audit trail of who has distributed, accessed and amended a client's KYC related documentation. This looks to engender trust in the technology, which is nascent in its application to this use case, without requiring clients to upload their private documentation to a Blockchain.

> KYC-Chain have observed decentralized approaches gaining good pace, and can provide the grounds for building solid and efficient KYC mechanisms that take into account the particular needs of financial institutions while also empowering the individual entities as sole owners of their data.



Whilst pilot Blockchain solutions to date are solving issues surrounding data security and internal control challenges, a path towards standardization is required to address many of the other core challenges of conducting KYC. Some see this as evolving organically, after a community has been established on the Blockchain and a critical mass of participants is available to drive towards an accepted standard.

Digital identity

Governments in countries such as Estonia and Singapore are exploring replacing centralized registries with decentralized ledgers to create a trusted, tamper-proof repository of information on an individual[5], which spans multiple facets of their identity. From a KYC perspective, digital identities provide the capability to automate the verification of an individual's identity. They also enable the use of digital signatures, improve data quality and deliver operational efficiencies when onboarding retail clients. However, owing to the complexity of the identification requirements for corporate entities, there is a limitation on the application of digital identities in solving institutional KYC challenges.

[5] DBS (2016): Understanding Blockchain Technology, https://www.dbs.com.sg/treasures/templatedata/article/generic/data/en/GR/022016/160225_blockchain.xml

Conclusion

A blockchain enabled KYC solution could be on the horizon, but the journey towards achieving it requires significant collaboration across industry participants and a number of hurdles to be overcome.

Conceptually Blockchain provides the perfect platform to deliver an automated, secure, trustworthy KYC solution that improves client experience, streamlines operational processes and enhances regulatory compliance.

However, Blockchain in itself cannot solve all the industry challenges surrounding KYC or achieve the goals outlined earlier in this paper without market participants agreeing to adopt a new infrastructure with regulatory approval, whilst continuing to focus on the day today pressures of supporting a business critical process. The responsibility lies with the entire industry (banks, regulators, third party vendors, partners) to deliver this innovation. This is a dynamic that other industry initiatives in this space have struggled to achieve.

Initiatives that are paving the way towards such a model can be summarized into two main approaches: the utility managed service concept, which looks to standardization to mutualize the effort of conducting KYC for all utility participants; and document exchange Blockchain platforms, which look to enhance data security and streamline the distribution channels for KYC documentation.

Whilst the two approaches solve certain KYC challenges, the utility model addresses, at the outset, the most prominent. Delivering a single KYC record that leverages public information as much as possible, to a standard accepted across banking participants, minimizes the burden on clients to provide documentation and delivers operational efficiencies by mutualizing the end-to-end KYC process. As it stands, such a model has delivered cost efficiencies in excess of 30% to large banks.

In this model, Blockchain forms the underlying technology infrastructure that can be leveraged to optimize a solution, but it is the overall utility concept that is built on this technology that would solve such industry challenges.

R3 proposes taking an incremental approach to delivering Blockchain enabled solutions across the industry by first moving existing KYC utilities onto a Blockchain infrastructure. This would enable efficiencies in the data collection and sharing processes. Once the underlying platform has successfully been implemented, additional participants and features can be added one by one, replacing legacy sources of data with direct digital assertions from authoritative sources. As the world moves towards adopting true digital identity, existing KYC processes will become automated and carried out in real-time. Banks could encapsulate their KYC policies and risk profiles in a smart-contract, which would automatically lead to onboarding decisions being driven by the data being fed into it.

In summary, Blockchain may well be a new horizon for KYC. The infrastructure would lend itself well to the ongoing challenges in this space and could achieve many of the same stated goals of the utility model. However, the hurdles which would prevent such a platform from achieving success are similar in nature to those faced by the managed service providers in this space. In short, lessons need to be learned if we are to avoid a false dawn.

Thomson Reuters KYC as a Service

KYC as a Service offers an innovative platform which integrates regulatory technology, market leading entity data and accredited operational capabilities. It delivers and maintains a set of collected information based on public and private data, unwrapped, screened and validated KYC profiles. Our clients across the industry can rely on us as a critical component of their customer due diligence process.

R3

R3 is an enterprise software firm working with a network of over 200 financial institutions, regulators, trade associations, professional services firms and technology companies to develop on Corda, their blockchain platform designed specifically for businesses.

KYC-Chain

KYC-Chain is a B2B managed workflow application that enables organizations to better manage their KYC processes for both individuals and corporates. A white labelled end-to-end solution to streamline the onboarding process for your customers, and greatly improve efficiency for your compliance team.

Find out more at **risk.tr.com**