



Could blockchain be the foundation of a viable KYC utility?

KPMG International

kpmg.com





Foreword

Know Your Customer (KYC) processes provide the backbone of financial institutions' anti-money laundering (AML) efforts to combat the financing of terrorism (CFT), helping to detect and prevent criminal behaviors over the world. According to current estimates, in excess of US\$25 billion is spent each year on financial crime risk management in the banking sector, the majority of which is due to KYC.

However, despite the critical importance of these processes, KYC at many financial institutions is extremely inefficient, mired with time-consuming and labor-intensive manual processes, duplication of effort and risk of error. It is estimated that up to 80 percent of the effort associated with KYC is dedicated to information gathering and processing, and only 20 percent to assessing and monitoring that information for critical insights. At the same time, the tiresome process, repetitive questioning and long processing times create a frustrating experience for customers.

New and evolving technologies may present solutions to these challenges. While many financial institutions look to AI and cognitive technologies to drive efficiency by automating existing KYC processes, other technologies open up different paths. The use of blockchain, currently best known as the foundational technology for Bitcoin and other cryptocurrencies, could reduce inefficiencies and

duplication of effort in KYC information gathering between legal entities within a larger financial corporation or even between competing banks.

Yet the question arises: could blockchain truly be the key to a viable KYC utility, or is this a case of a technical solution in search of a problem?

In this report we set out to consider the business case for a blockchain-enabled KYC utility for sharing information among the participating financial institutions, while institutions continue to perform due diligence on customer information obtained from the platform. KPMG in Singapore's recent proof-of-concept prototype, a collaboration between Bluzelle Networks, a consortium of three banks in Singapore (HSBC, OCBC, Mitsubishi UFJ Financial Group) and the Singaporean regulator, we were able to demonstrate the utility's functionality, security, and scalability. The prototype was tested between February and May 2017, and passed the Monetary Authority of Singapore's test scenarios. In addition to stability and security, the platform could result in estimated cost savings of 25–50 percent by reducing duplication and providing a clear audit trail.

We hope you find this paper of value as you consider your options for improving your KYC program. If you have any questions, please contact us, or your local KPMG representative.



Eamonn Maguire
**Global Financial Services
and North America Lead,
Digital Ledger Services**
KPMG International
E: emaguire@kpmg.com



Tek Yew Chia
**Head of Financial
Services Advisory**
KPMG in Singapore
E: tekyewchia@kpmg.com.sg



Could blockchain be the foundation of a viable KYC utility?

While other centralized solutions may alleviate some of the KYC challenges, the blockchain architecture provides a modern and elegant way forward with immutability and security features that help provide greater trust in, and integrity of, the data. Benefits include:

Greater operational efficiency through a digital process flow and the ability to share customer information. These improvements can significantly reduce the time and effort required in the early stages of the KYC process, speeding up customer onboarding and reducing corresponding KYC and regulatory compliance costs.

Real time up-to-date customer data, including complex company relationships, while maintaining full data security and customer privacy. Each time there is a KYC transaction at a participating institution, the latest information would be put into the shared distributed ledger, allowing multiple institutions to rely on those same checks and information up to a minimum standard.

Immutability and transparency of the data enabled by blockchain technology allows any member institution to prove to regulators that the secure blockchain platform provides trustworthy information.

A blockchain KYC utility would not remove the need for financial institutions to perform screening and monitoring of customers. Instead, it provides a streamlined way to gain swift and secure access to clean, up-to-date customer data. The result is a reduction in labor-intensive information gathering, overall KYC processing time, and associated costs.

Potential value for regulators and customers

A blockchain KYC utility could also offer regulators a better understanding of how customers have been onboarded and the application of underlying KYC information. This would, in turn, enable regulators to better understand customer activity. All actions by

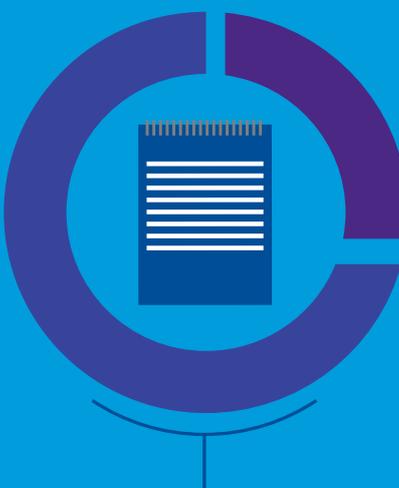
financial institutions and customers would be fully recorded and tracked, while activity data on the platform would be fully auditable.

From a customer standpoint, a financial institutions use of a KYC utility would enhance the customer experience and improve their overall satisfaction by making processes more timely and efficient.

Customers may understandably have privacy concerns about the sharing of their personal and financial data. Here, blockchain offers another advantage, with certain models giving customers the power to approve which organizations have access to their information, and when. Digital integration could make the approval process simple, such as pushing a permission request with a one-time password (OTP) to the customer's phone for approval. Other options, such as smart digital signatures, iris or facial scans may further extend customers' sovereignty of identity.

A blockchain-enabled KYC shared ledger platform benefits all stakeholders by:

Enabling greater transparency



Private and immutable ledger that enables sharing of KYC information across banks in a transparent and secure manner

Reducing operational inefficiencies



Reduces customer onboarding time and enhances customer experience

Enabling up-to-date customer data



A single source for customer data reduces potential for fraud by inhibiting data ambiguity



Proof-of-concept: The blockchain KYC utility in action

“

The banks cited the blockchain platform demonstrated ability to improve overall efficiency and reduce the time to complete necessary screening, resulting in a decreased risk of financial crime and improved responsiveness to customer needs.”

Validating the technical concept

Despite the clear potential presented by the technology, the viability of a KYC utility needs to be tested for its true applicability to be understood. To this end, KPMG in Singapore and Bluzelle Networks worked with a consortium of three banks in Singapore — HSBC, OCBC, and Mitsubishi UFJ Financial Group (MUFG) — and the Singaporean regulator Info-communications Media Development Authority (IMDA) to develop a proof-of-concept KYC utility on a blockchain platform.

This proof-of-concept prototype was developed to test the technical aspects of a blockchain platform, such as the utility’s functionality, security, and scalability. The prototype was tested between February and May 2017, and passed the Monetary Authority of Singapore’s test scenarios as planned, for example, transaction speed and concurrency (number of concurrent transactions).

Once the shared KYC platform was established, the three banks followed a process by which all new KYC requirements were first queried on the shared platform, and any existing customer details were shared with customer consent. Customer information was then validated by appropriate third-party sources, and results from the third party validation were recorded in the KYC shared ledger, further strengthening the depth of information contained within the platform. All actions, permissions and new data provided by a customer or any of the three banks was tracked and recorded.

During the testing period, KPMG ascertained that:

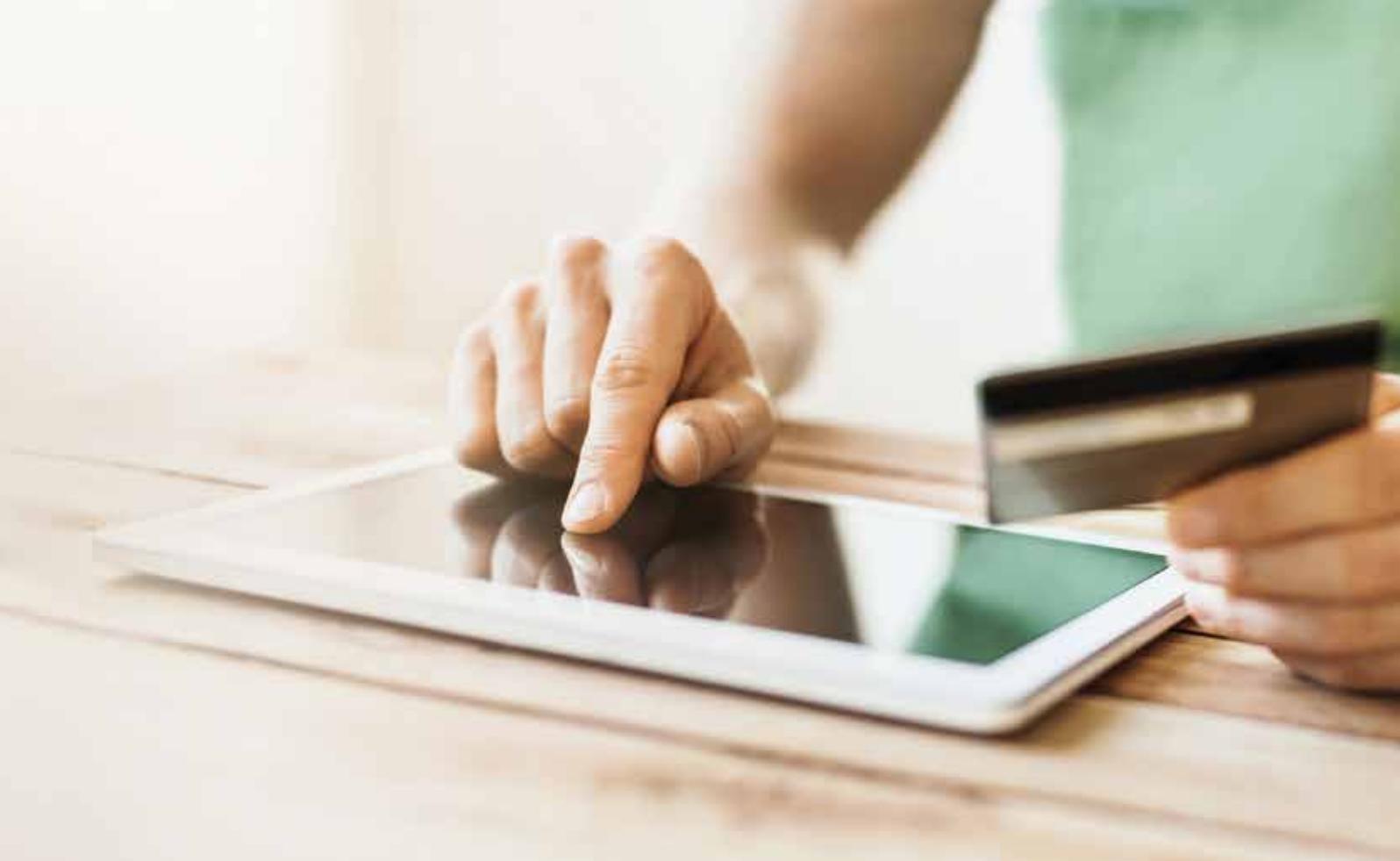
- The blockchain KYC platform remained stable and responsive even at a high volume of information flow.
- Platform performance was strong, with transaction times remaining swift even as transaction concurrency and complexity increased.
- All data was secure and confidential, with access limited only to those with the correct authentication codes.
- The platform resisted tampering by third parties.
- The platform could result in estimated cost savings of 25–50 percent by reducing duplication and providing a clear audit trail.

At the conclusion of the proof-of-concept project, the banks cited the blockchain platform demonstrated ability to improve overall efficiency and reduce the time to complete necessary screening, resulting in a decreased risk of financial crime and improved responsiveness to customer needs.

Addressing future challenges

While this proof-of-concept project validated the technical potential for a blockchain KYC utility, other areas must be further investigated for such a utility to see wider release.

In some areas, KYC processes can be very fragmented, resulting in issues with the consistency of KYC quality. Prior to working together, banks would have to agree, if not to a consistent data collection process, then at least to



consistency of data requirements. As a result, some speculate that a KYC utility model may initially be more viable when considered as a tool shared between legal subsidiaries of a banking brand versus between a consortium of banks. However, in most markets the response from interested institutions has swung strongly in the other direction, with strong support for a cross-bank utility. Many larger institutions feel that internally they have some level of both trust and information sharing through conventional databases, while they lack the ability to share with others in the external marketplace with the same level of trust or security.

Privacy regulations related to the control and sharing of personal data is another area of particular concern, especially in some regions of the globe. In Singapore, sovereign control over personal data did not pose a logistical challenge for the proof-of-concept project. However, in other jurisdictions, privacy regulations and legislation can limit what information can be shared

between institutions or beyond national borders. While privacy regulations may not pose much of a barrier in the United States or in other areas where there is a regulatory environment that permits the individual to authorize the sharing of information, regulations such as General Protection Regulation (GDPR) in Europe could pose stumbling blocks. The geographical location of the servers containing the data, as well as the data protections in place in those areas, will also be of particular relevance.

Customers, too, may have concerns over their information being shared through a platform with financial institutions with which they do not have a business relationship. Both customer education and a technical model designed to provide the individual, corporation or beneficial owner with proper sovereignty over their sensitive data need to be carefully considered.

As fintechs and challenger banks continue to disrupt the industry, questions around competition and

competitive advantage can also come into play. For example, in the Nordic countries there are ongoing conversations around KYC utilities potentially removing barriers to entry for new players. Banks with a major footprint in a particular jurisdiction are concerned that if they were to share their extensive KYC data with new entrants, those fledgling banks could potentially achieve greater levels of maturity with less cost and hassle than their established competitors.

These concerns can come to dominate conversations, sometimes in defiance of the technical structures and inter-banking agreements that would need to be in place to fully enable a shared KYC utility. However, such concerns should be viewed as stumbling blocks rather than barriers. Banks can choose whether to pursue this path, and with what competitors, while the involvement and participation of regulators in such projects can help clear the path forward.



Seeking a path forward

“

For banks and other interested parties, it is important to note that there is no one solution that will meet all needs, regardless of country, regulatory environment or size of institution.”

Based on our pilot project, we have found that use of blockchain in the creation of a KYC utility is a technologically viable solution that provides a method to safely and securely share customer information between parties. A blockchain-based KYC utility allows banks to have the confidence in the information contained within the platform, regardless of which institution originally collected the data, knowing that it cannot be changed, altered or accidentally modified. The platform also provides full visibility on how the information was entered, by whom, and how and when it was externally verified.

The concept of a KYC utility also helps to address a number of logistical issues and roadblocks faced by the banking industry today — but is it the right path forward?

For banks and other interested parties, it is important to note that there is no one solution that will meet all needs, regardless of country, regulatory environment or size of institution. There are, however, a number of options that should be given serious consideration. It could be possible to create a KYC utility using blockchain at one of three different levels:

1. Within a large financial conglomerate

The most straightforward use of a KYC utility is one created for use between subsidiaries of a large financial conglomerate within a single country. While not facing the same potential barriers as a utility shared between competing organizations, subsidiaries would nonetheless need to discern whether they are comfortable that they have discharged their KYC responsibility if the KYC process was performed by a different company subsidiary. Regulator agreement from any affected nation would also be required if the utility were to be used to share information across

borders, adding potential complications to larger-scale deployments. Conglomerates considering this path are encouraged to identify their specific KYC pain points across the organization and, based on these pain points, assess whether the internal business case warrants further investigation of a KYC utility. If so, the question then becomes selecting the right market(s) in which to potentially trial a pilot project.

2. National

For a KYC utility to work at a national level, it must be driven by an entity that can negotiate consensus across a number of competing banks, such as a consortium of banks or a banking association. Alternately, the push for a KYC utility could come from the regulator, which may seek to standardize processes or stimulate competition by allowing new market entrants to perform KYC at a more cost-effective price. However, market dynamics will vary greatly, affecting the individual viability of a national KYC utility in different nations. Parties interested in investigating this path need to consider their country's regulatory environment, market dynamics and competitive tensions, and evaluate whether the potential gains outweigh the logistical challenges in order to justify a business case for moving forward.

3. International

For a cross-border KYC utility to see success, especially between competing banks, it must be either driven by or involve significant participation from regulators. Given the complexity of such a utility and the many potential roadblocks, an international KYC utility should only be considered after the concept has been fully vetted within a single nation, whether within a financial conglomerate or between competing banks.

Is a blockchain KYC utility the answer?

Information gathering and processing consumes the greatest portion of time, cost and effort in the end-to-end KYC process, leaving fewer resources available to assess and monitor customer behavior for anomalies. It is time to flip this ratio. By providing swift access to clean, up-to-date customer data, banks can reduce the time required to screen and verify each customer, freeing up resources that can be better spent on more complex KYC challenges.

As the obstacles and inconvenience of acquiring KYC information are reduced, financial institutions will likely become better able to advance their commercial business agendas. Not only can institutions realize improvements in efficiency, but also corresponding reductions in the associated burden of cost. At the same time, the customer experience will improve and overall customer satisfaction will increase.

Nonetheless, a blockchain utility does not solve all the KYC issues faced by financial institutions today. Once KYC data is acquired, they must still validate the information provided through the utility in compliance with regulations and perform recurring monitoring. For these and other tasks, technologies such as AI and cognitive processing may help drive greater efficiency.

Especially when used in combination with other technologies, a blockchain KYC utility demonstrates strong potential to help financial institutions reduce the burden of time and cost associated with KYC processes, while providing greater visibility to regulators and a better experience for customers.



Could blockchain be the foundation of a viable KYC utility? | 7

Contacts

Authors

Eamonn Maguire
**Global Financial Services and
North America Lead,
Digital Ledger Services**
KPMG International
E: emaguire@kpmg.com

David Hicks
Global Head of Forensic
KPMG International
E: david.hicks@kpmg.co.uk

Wei Keat Ng
**Global COO (Markets)
Digital Ledger Services**
KPMG International
E: wei.keat.ng@kpmg.co.uk

Tek Yew Chia
Head of Financial Services Advisory
KPMG in Singapore
E: tekyewchia@kpmg.com.sg

Stephen Marshall
**Principal, Advisory Services
Forensics**
KPMG in the US
E: sdmarshall@kpmg.com

Additional contacts

Laszlo Peter
**Innovation & Digital Solutions,
Digital Ledger Services Lead**
KPMG Australia
E: laszlopeter@kpmg.com.au

Catherine Philippe
Partner, IT Financial Services
KPMG in France
E: cphilippe@kpmg.fr

Sven Korschinowski
Head of Fintech and Innovation
KPMG in Germany
E: skorschinowski@kpmg.com

Said Fihri
**Head of Fund Distribution Services,
Head of Digital Ledger Services**
KPMG in Luxembourg
E: said.fihri@kpmg.lu

Dennis de Vries
Digital Ledger Services Lead
KPMG in the Netherlands
E: devries.dennis@kpmg.nl

Jan Reinmueller
**Head of Digital Village
Digital + Innovation**
KPMG in Singapore
E: jreinmueller@kpmg.com.sg

Anton Ruddenklau
**Head of Digital & Innovation
Financial Services**
KPMG in the UK
E: anton.ruddenklau@kpmg.co.uk

kpmg.com

kpmg.com/socialmedia



The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2018 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network of independent firms are affiliated with KPMG International. KPMG International provides no client services. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.

The KPMG name and logo are registered trademarks or trademarks of KPMG International.

Designed by Evalueserve.

Publication name: Could blockchain be the foundation of a viable KYC utility?

Publication number: 135159a-G

Publication date: March 2018