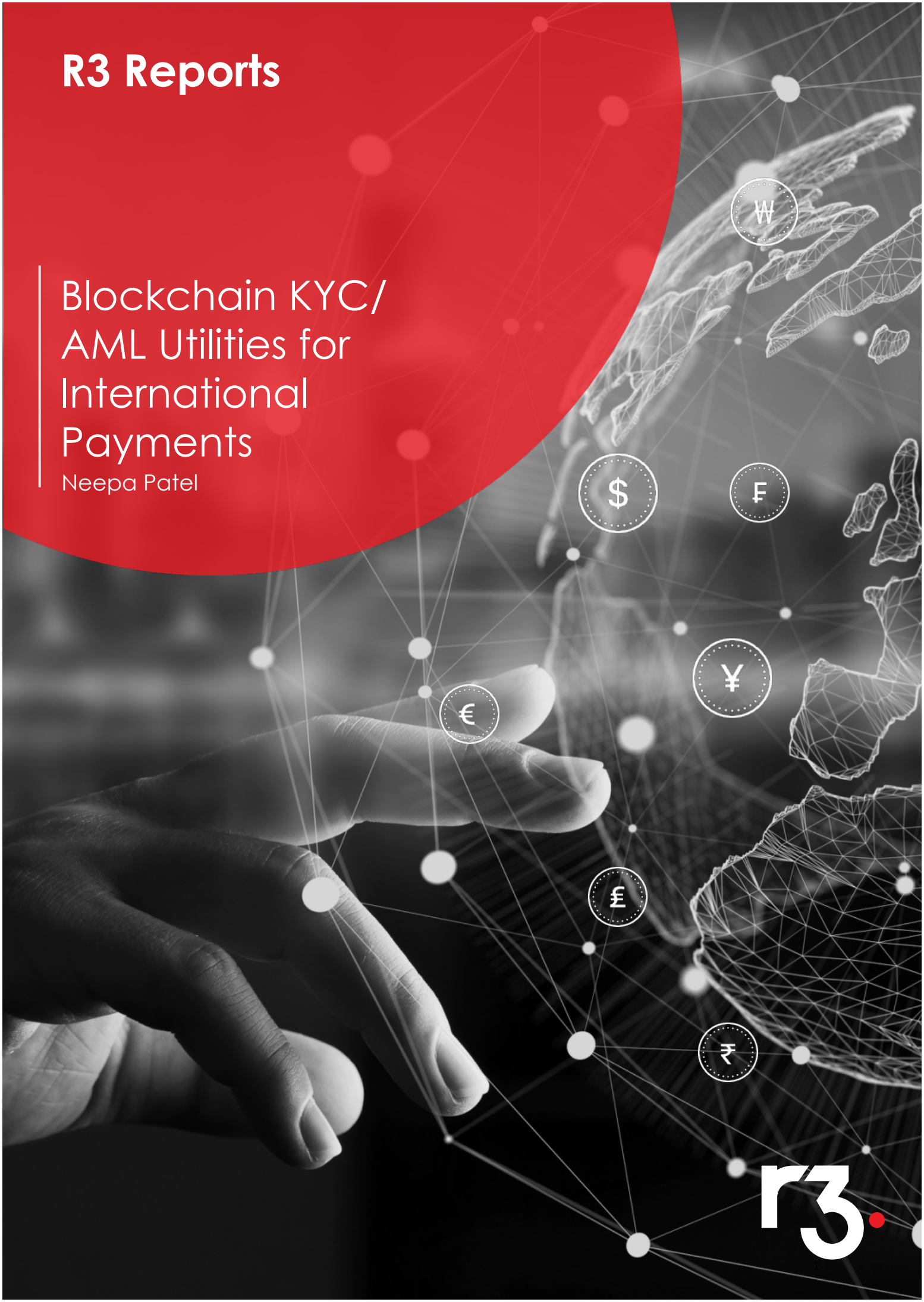
R3 Reports

Blockchain KYC/ AML Utilities for International Payments

Neepa Patel



Contents

R3 Research aims to deliver concise reports on DLT in business language for decision-makers and DLT hobbyists alike. The reports are written by experts in the space and are rooted in practical experience with the technology.

For more Research, please visit R3's Wiki here.

Blockchain KYC/AML Utilities for International Payments:
A Regulatory Solution for Anti-Money Laundering and Financial Inclusion?

Neepa Patel

November 6, 2017

Abstract

Can a distributed ledger solve the problem of de-risking correspondent banks while also helping with the fight against money laundering and terrorist financing?[1] Financial inclusion is a global problem that technology can solve, if implemented properly. We argue that distributed ledger-based systems can enable banks to re-engage with customers and correspondent banks excluded as result of de-risking. But design matters. Distributed ledger technology (DLT) must be coupled with regional KYC/AML standards in order to improve transaction traceability and identify potential suspicious activity related to money laundering or terrorist financing. We introduce the idea of creating both a global correspondent banking utility for correspondent banks and a linked KYC registry for individuals and businesses. This can reintegrate excluded entities into the financial system and improve government oversight on their activities.

1 Can mutualizing KYC costs solve de-risking?

Since 2010, 28 major banks have been fined for breaching U.S. sanctions, with 7 banks receiving fines exceeding $500 million, of which the highest was $8.9 billion. In one example, the Financial Conduct Authority and the New York Department of Financial Services issued KYC/AML fines for one institution, forming a cumulative $628 million fine. In response, banks have moved to reduce their risk by shedding correspondent banking relationships in developing countries. The high and rising risk of fines and the costs of increased scrutiny have destroyed the proud tradition of some banks to extend services throughout the world, particularly to its poorest and difficult to analyze regions (King et. al, 2016).

Despite concerns around global de-risking, regulatory requirements are getting stricter and regulators continue to remind financial institutions of the importance of understanding customers and their transactions. Issues with the current cross border payment system include inaccurate client information, lack of complete visibility over customer activity, jurisdictional differences with common identity standards, and data and privacy concerns.

To lower the risk of fraudulent or illicit transactions, banks must know where money is coming from and where it is going. Financial institutions are required to validate their customers' identity, monitor all transactions, and report any suspicious activity to a designated government body. To effectively comply with this requirement, financial institutions need to have a clear picture of their customer's profile, identity, spending habits and the kinds of transactions he or she is likely to engage in.

Recent technological innovation in blockchain or DLT-based systems promises improvement in payments without extensive networks with central administrators. DLT can facilitate the direct exchange of tokens of value and enable real-time messaging and clearing within a cryptographically secure and resilient environment (Rutter, 2016).

[1] All blockchains are distributed ledgers, but not all distributed ledgers "batch" information together into a chain of blocks. For simplicity the term blockchain and distributed ledger technology are used interchangeably in this paper.

Data on a distributed ledger is verifiable and immutable, providing increased transparency to relevant participants. Regulators can plug into the ledger and pull necessary data relating to payments and identity. Additionally, regulators could pull payment data for reporting / auditing purposes, instead of the current push process today that requires banks to submit data to regulators (Stark, 2017).

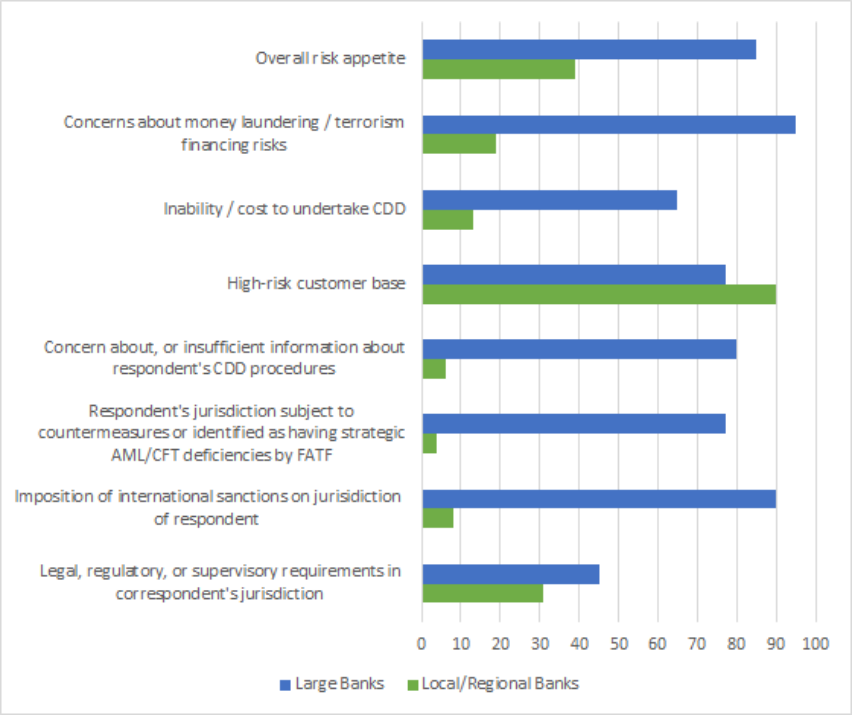
Distributed ledgers have the potential to improve the speed, transparency and end-to-end tracking of cross-border payments (Koning, 2017). A distributed ledger could ultimately facilitate large size cross border settlement on the ledger itself (Zhao et. al, 2018). If this occurs, the type of customer base and volume of transactions can be derived using actual transactional information rather than relying on foreign banks to complete a questionnaire to identify its customer base and average volume of transactions.

Regulators impose fines and penalties on banks that do not conduct appropriate due diligence on the entities and individuals they directly deal with; therefore, banks use intermediaries and shift some of the risk to the middle men or reject processing the transaction altogether. The more information a bank in a well-developed country has on the end user and the end user's bank in an unbanked region, the more comfortable it will be with facilitating the transaction.

2 Correspondent banking relationship decline

While different DLT and blockchain initiatives propose a potential for faster and cheaper payments, banks in well-developed countries still continue to need a way to verify that banks, money service operators and end users in remote locations are using the funds for non-fraudulent transactions. In the past, foreign correspondent accounts have been used for drug trafficking and terrorist financing to hide the true ownership of accounts. The Federal Financial Institutions Examination Council (FFIEC) manual states, "Because of the large amount of funds, multiple transactions, and the U.S. bank's potential lack of familiarity with the foreign correspondent financial institution's customer, criminals and terrorists can more easily conceal the source and use of illicit funds. Consequently, each U.S. bank, including all overseas branches, offices, and subsidiaries, should closely monitor transactions related to foreign correspondent accounts" (2014).

Figure 1: Reasons for terminating correspondent banking relationships



Source: Erbenová, et. al, 2016

In order for U.S. banks to establish foreign correspondent banking accounts, banks must com-

plete a risk assessment of the foreign bank's profile, obtain documentation related to the AML supervisory regime of the jurisdiction that issued the bank license, answer questions related to the relationship between the foreign bank and shell banks, payable through accounts, nested accounts and sanctioned banks, and also maintain an overview of the bank's customer base.[2] Once established, banks are required to closely monitor transactions related to these accounts. Depending on the risk profile, onboarding documentation must be updated frequently.

For many banks, the cost and resources spent on monitoring transactions and maintaining KYC documentation is expensive and not worth the correspondent relationship. Correspondent banking relationships are declining, especially for banks that (i) do not generate sufficient volumes to recover compliance costs; (ii) are located in jurisdictions perceived to be too risky; (iii) provide payment services to customers for which the necessary information for an adequate risk assessment is not available; or (iv) have customers that pose a higher risk for AML/counter-terrorism financing (CFT) and are therefore more difficult to manage (Bank for International Settlements, 2016).

3 Correspondent banking utility

In order to re-engage with customers excluded from higher risk jurisdictions, banks need to identify ways to trust foreign banks and have more transparency into a recipient's profile. One way to address foreign bank documentation difficulties is to create a correspondent bank utility shared by multiple banks. This solution could provide a single unified view of a foreign correspondent bank's onboarding documentation.

The utility would require a governance structure that incentivizes or requires participants to maintain active information. The foreign correspondent bank would receive an annual alert to update and attest the information on the utility. Banks in the network utilizing the data would be notified if a bank failed to update and attest. This would mutualize onboarding costs amongst banks and improve data quality by forcing the foreign correspondent bank to update information in a timely manner. Entities participating in the correspondent banking utility would be required to comply with preexisting rules, and attest their data is accurate. Red flags can be built into the system making it known when a participant hasn't updated or attested to documents annually or has missing documents.

The use of a correspondent banking utility on a distributed ledger would provide several advantages:

- Reducing the number of times a bank must send the same information; In Figure 2 below, Diamond Bank, a Nigerian Commercial Bank, will need to send onboarding information separately to all 21 of its correspondent banks both at account opening, and periodically.

Figure 2: Diamond Bank's correspondent banks

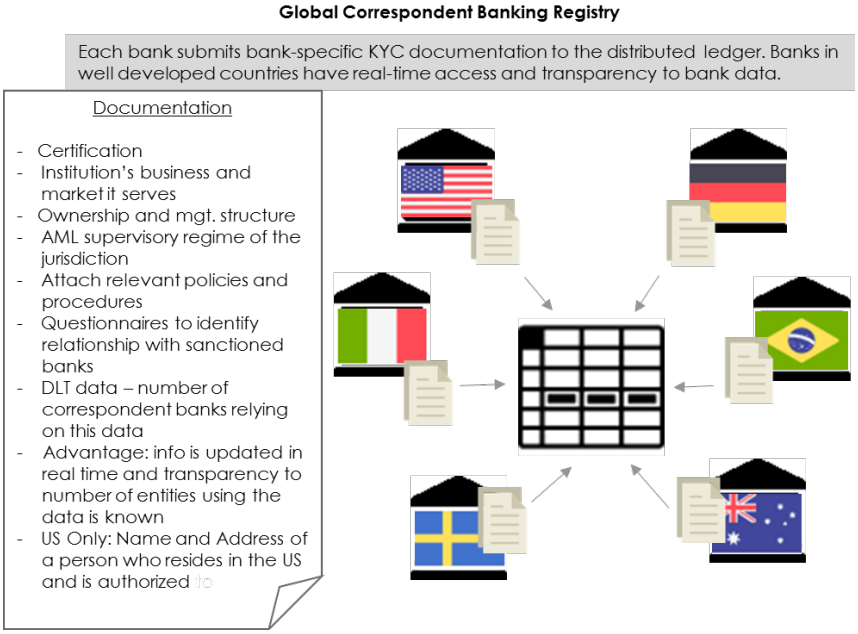
Source: http://www.diamondbank.com

- Improved accuracy and consistency of data;

[2]Nested accounts occur when a foreign financial institution gains access to the U.S. financial system by operating through a U.S. correspondent account belonging to another foreign financial institution. If the U.S. bank is unaware that its foreign correspondent financial institution customer is providing such access to third-party foreign financial institutions, these third-party financial institutions can effectively gain anonymous access to the U.S. financial system – e.g. a local bank conducts correspondent banking business indirectly via its regional savings bank.

- The use of a single template to promote the standardization of KYC information that banks provide to other institutions would propagate the need of movement in this space[3];
- Increase speed of due diligence by reduction in the amount of documentation exchanged over email.

Figure 3: KYC global correspondent banking utility



Source: Federal Financial Institutions Examiners Council, 2014

A global correspondent banking registry could also include the number of correspondent relationships that each single entity maintains. The registry could provide the domestic regulator a holistic view of correspondent banking relationships established by banks under their jurisdiction. The registry could provide a means for banks on the network to alert one another if fraudulent activity by a network bank is detected. Further, while current privacy regulations limit the amount of interaction and information that banks can share with other banks outside their country borders, banks could always alert domestic regulators via DLT.

A registry could help with regulator coordination and information sharing. Regulators have the ability to notify other regulators on the network or alert banks within their jurisdiction of fraudulent activity. Regulators around the world are working separately to fight money laundering and terrorist financing so sharing information would improve the current process. Further, such action would be aligned with the Financial Action Task Force's (FATF) 40 recommendations which encourage international cooperation and providing legal assistance in relation to money laundering, associated predicate offences and terrorist financing investigations and prosecutions. The FATF recommends countries develop a sufficient legal basis for providing assistance and, where appropriate, should have in place treaties, arrangements or other mechanisms to enhance cooperation (2012).

4 KYC / AML registry for customers

A KYC / AML registry for customers established by a country would allow a bank to have access to private personal information and transactional information on their own bank customers. Information on other bank customers would not be accessible unless a bank was participating in a transaction as an originator, beneficiary or intermediary of funds. An aggregated ledger used for payments would provide bank regulators a holistic view of a client's profile and funds transfer activity across multiple banks which would be vastly different from current AML reporting

[3]Setting global standards on the KYC documentation required for submission by correspondent banks was mentioned in the Committee on Payments and Market Infrastructures paper on correspondent banking.

requirements that are built on a "one-to-one" model, where each institution typically reports to an authority on singular customers and transactions. See Appendix - Figure 1.

Having KYC and AML information readily available allows banks to spend more time analyzing information rather than collecting and verifying the data received – a key issue in onboarding delays. Challenges may remain with trusting the information on the registry, but this could be solved by including reputable third-party validators or attesters on the ledger.

The Panama Papers investigation would have benefited from the process described above. The Panama Papers leak exposed the purposeful opacity in corporate formation and the placement and layering of money and transactions that can facilitate all forms of financial crime and the evasion of sanctions. During the Panama Papers investigation, more than a dozen mid-size and large banks had to turn over details of their dealings with Panama law firm Mossack Fonseca and certain shell companies to authorities and regulators. This was a long painstaking process for banks as client KYC documents and transaction information were dispersed amongst multiple banking systems. To make matters more difficult, regulators could not confirm the veracity of the details provided or even be confident all customer details were provided. A customer KYC registry with AML analytics described above would have allowed regulators access to ledger data that would have accurately determined which banks held accounts with fraudulent parties.

A digital ID linked to payment transfers could help banks comply with funds payment regulations such as the "U.S. Travel Rule" or "EU Funds Transfer Rule" and help build a robust customer profile. Funds transfer regulations require originating, intermediary and beneficiary banks to collect data on all participants involved in a cross-border transaction. This includes the sender's name, sender's address, amount of transfer, execution data, beneficiary's name and beneficiary's bank. A payment transfer linked to a digital ID with sender and beneficiary data could be used to comply with funds payment regulations without any manual intervention. The underlying information of a digital identity in a KYC utility would be crucial to prevent a customer from creating multiple fake names using the same ID number (Social Security # or Passport #) or even prevent a bank from attaching misspelled or incorrect data to a wire transfer message.

5 Digital ID, payment transfers, and regulatory compliance

A contentious topic between banks and regulators is the topic of knowing your customer's customer. Although regulations do not require this, banks feel the pressure of understanding the risk and transaction profile of all participants in a transaction – this includes the end customer and the end customer's bank. This lack of KYC and AML transparency in current systems deter a bank from processing a cross border transaction, which ultimately pushes the unbanked population to use nontraditional payment services.

DLT could potentially provide banks with more data, which may lower their costs for screening marginal entities and transactions, potentially leading to more cross border transactions. For example, what if a bank has access to enough new data to form a more complete risk profile of the sender, beneficiary bank and beneficiary? Would they be more likely to process a transaction? Of course! If a bank had access to a profile that included the top five counterparties, average currency amount and number of transactions sent and received by a client this would help a bank trust the end customer without having a relationship. Delving deeper into a customer transaction allows banks and regulators to analyze cash inflows and outflows of clients, partners and countries. With this information banks could determine whether a client's transaction make sense. Data collected can also be compared against behavior of clients in similar industries or in similar regions. See Appendix - Figure 1.

The detailed information from a KYC global correspondent bank registry linked to a KYC customer registry would provide a single unified view of a client profile, mutualize onboarding costs amongst banks, improve data auditability and transparency and increase regulatory oversight. See Appendix – Figure 2 for an illustration of a cross border payment process.

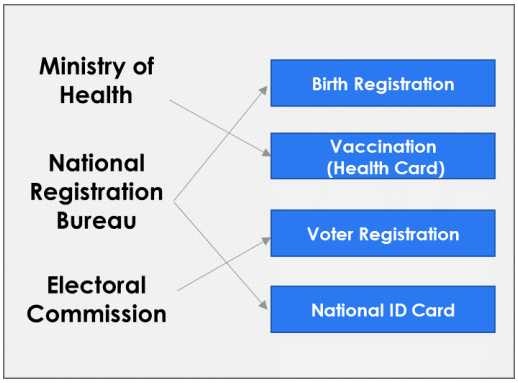
6 KYC registry for the unbanked

Several fintech companies and banks are working on approaches to financial inclusion by creating digital identities for the unbanked on a distributed ledger. According to World Bank's 2016 ID for Development initiative, approximately 1.5 billion people around the world cannot prove their

identity. The majority of these people live in Asia and Africa and are cut off from accessing basic services and rights. The data suggests that less than half of all adults in the poorest 40% of households have a bank account and around 375 million unbanked adults in developing countries (18%) are constrained by not having the necessary ID documentation (Mesropyan, 2016). Creating an identity on a DLT can provide individuals greater control over their personal information and how they access it. By combining the decentralized blockchain principle with identity verification, a digital ID can be created to act as a digital watermark that can be assigned to every online transaction of any asset.

A major challenge with implementing digital identities for the unbanked is that foreign banks in less developed regions do not always capture identity information and evaluate potential risks with the same rigor of the U.S. regulatory system. Foreign correspondent banks operating in unbanked jurisdictions might not require verified identities given a widespread lack of passports and government identification in the local jurisdiction. In order to include the unbanked, U.S. regulators would likely have to change identity standards of certain regions and use other verifiable means in lieu of passports and birth certifications such as biometrics or other government verifiable methods. ID2020 is a public-private partnership seeking to solve the challenges of identity exclusion for the 1.5 billion people who live without an officially recognized identity. The alliance model coordinates diverse stakeholders and efforts to ensure efficient and scalable implementation of digital identity solutions in nontraditional ways. Also, regulators in developed nations should consider adopting these non-traditional solutions for customers in unbanked regions.

Figure 4: Digital identity solutions: non-traditional solutions



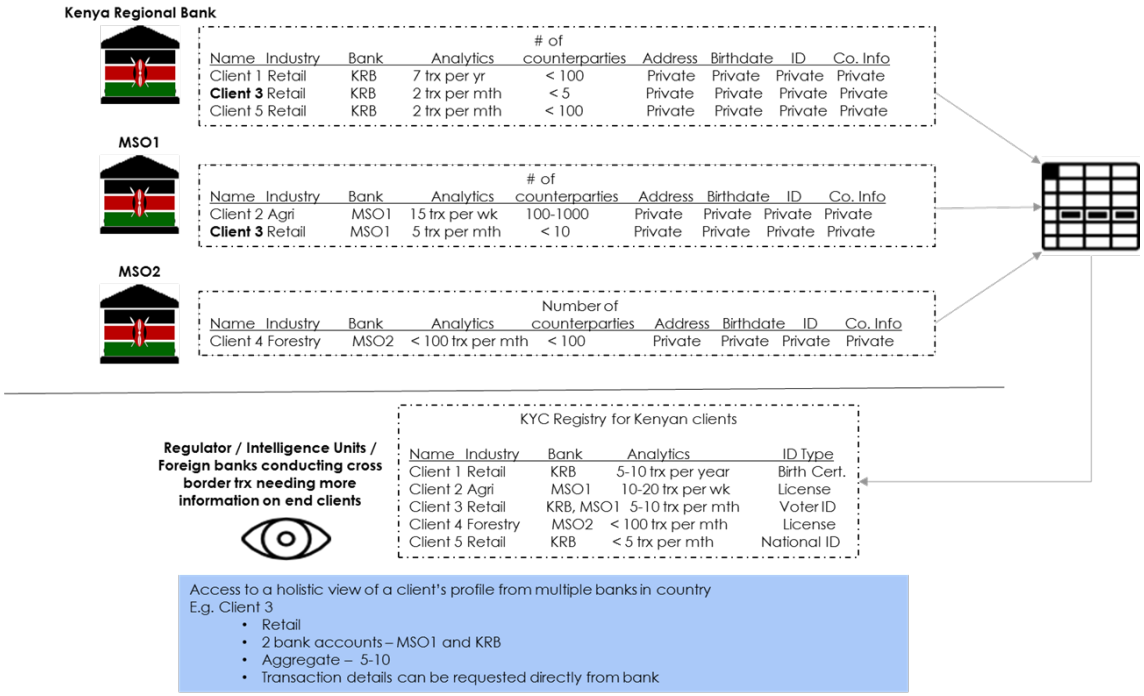
Source: www.ID2020.org

In conclusion, regulators and the intelligence community should permit banks to use alternate KYC methods for the unbanked and support the use of distributed ledger technology to increase financial inclusion. Currency thresholds and the number of transactions for customers in unbanked regions should be set in advance since the KYC data collected is limited. Further, utilizing a distributed ledger for payment transfers and having access to a holistic view of the payment system is beneficial for banks, regulators and intelligence units to identify money launderers and terrorist financing. The current de-risking problem has pushed individuals and entities out of the traditional banking system and caused them to explore non-traditional payment methods that have little or no government oversight. The right distributed ledger technology design coupled with KYC/AML standards consistent across regions will significantly increase traceability to support financial inclusion and identify accounts used by money launderers.

Appendix

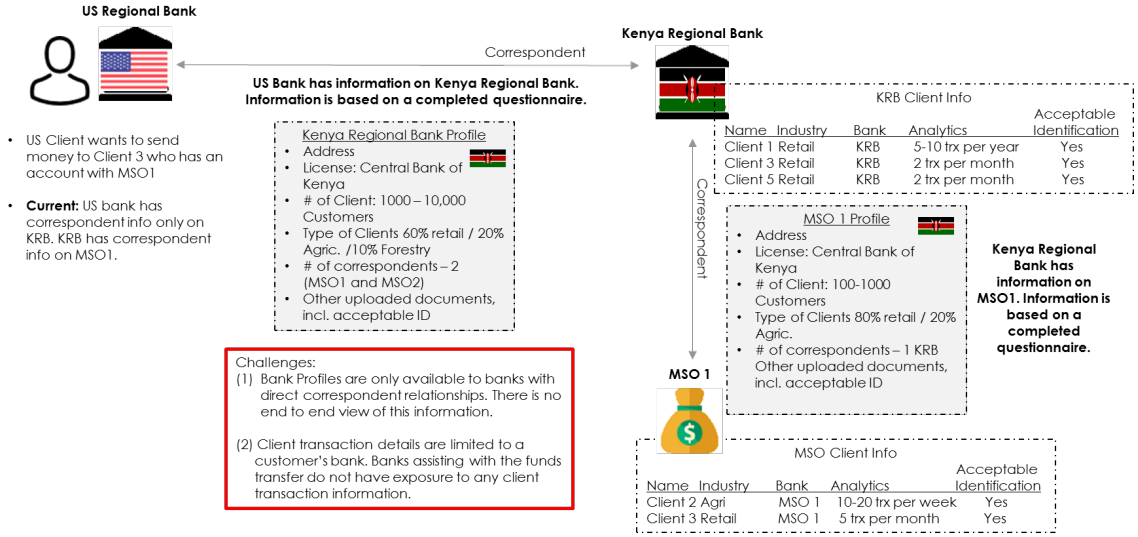
A KYC Registry created by aggregating real transaction data from multiple banks can be beneficial to regulators and intelligence agencies. Aggregated information from multiple banks on a single customer would provide a more precise picture of a customer's profile and transaction activity. If a bank in a well developed region has access to this high level view of a customer's profile, they would probably be more comfortable and willing to conduct a transaction.

Figure 1: Country specific KYC registry



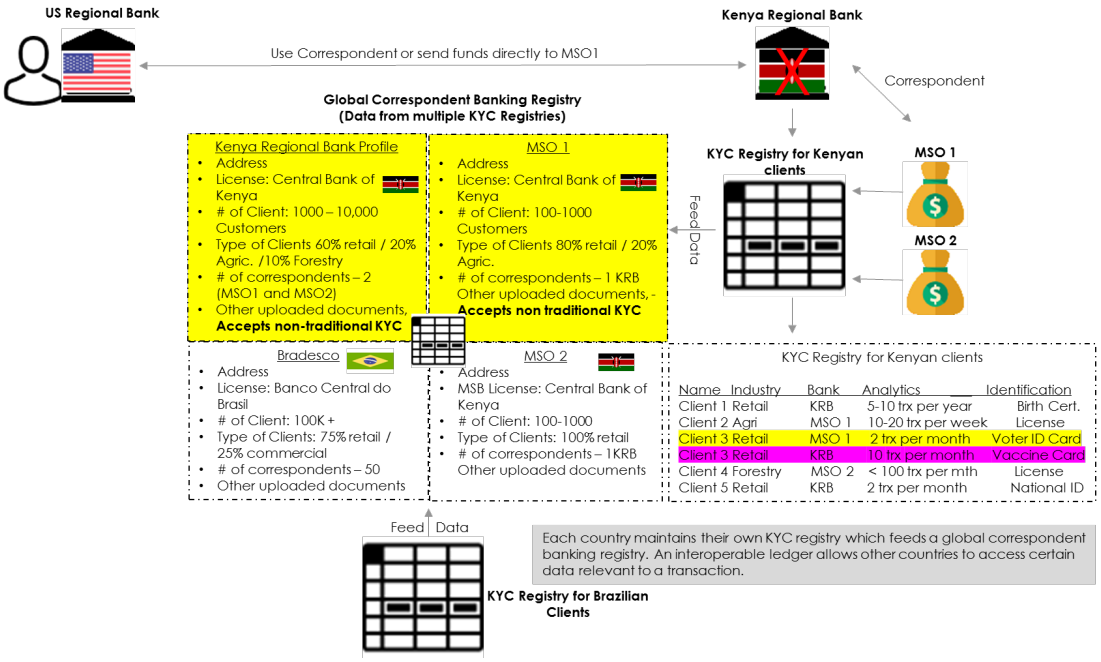
To illustrate the current cross border payment process, Appendix - Figure 2 demonstrates a client of a U.S. bank submitting a payment request to send funds to Money Service Operator 1 (MSO1) in Kenya. The U.S. bank does not have a direct relationship with MSO1 and therefore, must use a correspondent bank to help transmit the funds. Currently, the U.S. bank only has details on the correspondent bank, Kenya Regional Bank (KRB), no details on MSO1 and limited information on the end client.

Figure 2: Current cross border payments using correspondent banks



The optimal benefit of using a distributed ledger for cross border payments would be linking a Global Correspondent Banking Registry (See Figure 3) with a country specific KYC registry (See Appendix - Figure 1). This would provide the U.S. bank high level information on MSO1 and the end client (see highlighted info). This level of transparency would instill more trust and confidence in the beneficiary and the beneficiaries' bank, while still complying with privacy regulations. The U.S. bank can even choose to send funds directly to MSO1, thereby eliminating the need of having a correspondent bank. Additionally, identification on the ledger should be more robust for a client conducting a $10,000 transaction vs. a client conducting a $1,000 transaction.

Figure 3: Cross border payments using distributed ledger technology



Example 1:

- A U.S. client at a U.S. Regional Bank submits a payment request to send $5,000 to Client 3 who has an account at MSO1.
- U.S. Regional Bank does not have a direct banking relationship with MSO1 and must use KRB as a correspondent bank.
- With a DLT, U.S. bank can have real time access to correspondent banking info on KRB, MSO1 and high level, non-private info on Client 3.
- U.S. Bank can determine if this transaction is reasonable.

Reg Check (Complete): MSO1 has a valid banking license. MSO 1 has a small customer base (100-1000) with most clients in the retail space. They take non-traditional identification which probably means they cater to the unbanked populated. The end customer (Client 3) is a retail client receiving a relatively small dollar amount ($5,000) with low levels of account activity (2 trx per mth). Even though the ID on file is non-traditional (voter ID card), the customer is probably not laundering funds. With this level of data, the U.S. Regional bank may choose to send funds directly to MSO 1 and eliminate the use of the correspondent bank - KRB. In the off chance the client is using the $5,000 to launder money, it will be recorded on the ledger and can be reviewed if this client is ever identified as suspicious in the future. Regulators should push for all activity to be conducted through normal payment methods on a DLT so an audit trail can be maintained if client activity needs to be reviewed later.

Example 2:

- A U.S. Client at U.S. Regional Bank wants to send $30,000 to Client 3 who has an account at KRB.
- U.S. Regional bank has a direct relationship with KRB.
- With a DLT, U.S. Bank has real time access to correspondent banking info on KRB and high, level non-private info on Client 3.
- U.S. Bank needs to determine if this transaction is reasonable.

Reg Check (Failed): KRB has appropriate licenses in place. Client 3 is receiving a small, but sizeable dollar amount ($30,000) in an active account (10 trx amount). The ID on file is a vaccination card. The U.S. bank should probably request more information or reject the transaction since the funds are a substantial amount, the account is relatively active and the ID on file is non-traditional. Funds over a certain amount should have stronger KYC documents on file.

References

Bank of International Settlement (2016). Committee on Payments and Market Infrastructures - Correspondent Banking.

Erbenová, Michaela, Yan Liu, Nadim Kyriakos-Saad, Alejandro López-Mejía, Giancarlo Gasha, Emmanuel Mathias, Mohamed Norat, Francisca Fernando, and Yasmin Almeida (2016). The Withdrawal of Correspondent Banking Relationships: A Case for Policy Action. IMF Staff Discussion Note.

FATF (2012). International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation. The FATF Recommendations.

Federal Financial Institutions Examiners Committee (2014). BSA / AML Examination Manual.

King, Nigel, Nick Skinner, Ian Grigg, Stephen Lane-Smith, Atefeh Mashatan, Paul Bayer, Craig Maladra, John Vondrachek, Henry Roxas, Christopher Swanson, Abbas Ali (2016). Foundations of DLT Whitepaper Series – Identity. R3 Research.

Koning, JP (2017). Fedcoin: A Central Bank-Issued Cryptocurrency. R3 Research.

Mesropyan, Elena (2016). 1.5 Billion People Around the World Cannot Prove Their Identity. Let's Talk Payments.

Rutter, Kevin (2016). Vision Series: Cash and Payments. R3 Research.

Stark, Josh (2017). Applications of Distributed Ledger Technology to Regulatory and Compliance Processes. R3 Research.

World Bank Group (2016). Identification for Development. World Bank.

Zhao, Xiaohang, Haici Zhang, Kevin Rutter, Clark Thompson, Clemens Wan Cross-Border Settlement Systems: Blockchain Models Involving Central Bank Money. R3 Research.

R3 is an enterprise software firm using distributed ledger technology to build the next generation of financial services infrastructure.

R3's member base comprises over 80 global financial institutions and regulators on six continents. It is the largest collaborative consortium of its kind in financial markets.

Consortium members have access to insights from projects, research, regulatory outreach, and professional services.

Our team is made of financial industry veterans, technologists, and new tech entrepreneurs, bringing together expertise from electronic financial markets, cryptography and digital currencies.

corda is an open source, financial grade distributed ledger that records, manages and executes institutions' financial agreements in perfect synchrony with their peers.

Corda is the only distributed ledger platform designed from the ground up to address the specific needs of the financial services industry, and is the result of over a year of close collaboration between R3 and its consortium of over 80 of the world's leading banks and financial institutions.