Blockchain as the Newest Regtech Application—
the Opportunity to Reduce the Burden of KYC
for Financial Institutions

By Yvonne Lootsma

Abstract
The aim of this paper is to provide insight into the regulatory landscape surrounding much criticized regulatory reporting and know your customer (KYC) requirements for financial institutions and to describe how regulatory technology can be used for improvement. In terms of potential cost reduction, efficiency gains, and customer satisfaction, significant benefits are to be expected from (regulatory) technology in this domain. Additional factors that will shape the future financial environment are taken into account. First a general summary of upcoming regulation, regulatory technology, blockchain, and KYC are outlined. Subsequently blockchain application in the field of KYC is explained, including an overview of the major benefits and related challenges.

Introduction
The backlash of the 2008 financial crisis and new technology are the main drivers that have given shape to the new paradigm in the financial industry. Regulators maintain record-low interest rates while establishing a firm legal grip on financial institutions. On top of this, technological innovations lead to changed demands and new forms of competition. Recently FINTECH (financial technology) companies, whose business model revolves around providing automated alternatives to mainstream banking products, have received much attention. With their offer they appeal to the younger generation (millennials) of customers that demands quick, digital, and personalized service. Surveys confirm that this generation has a low degree of trust in traditional banks, which makes them receptive to those alternatives and a bottleneck to traditional banks.

Whereas in the first instance after the crisis the regulator emphasized financial risk control with regulations such as the Basel Framework, regulation in response to financial technology has followed quickly. In 2007 the EU introduced the payment services directive (PSD) regulating third-party services providers within the EU, and the US included comparable rules in the extensive 2010 Dodd-Frank act introduced by the Obama Administration. Following new developments the EU introduced the PSD 2 directive in 2016, which is to be implemented by January 2018. The directive will enhance rules for payment service providers, and also force banks to allow third-party providers access to customer data with the aim of enabling competition to expand their offers. The expectation is that PSD 2 will have a far reaching impact on banks that in time will transform the financial industry. These, and further changes to come, force banks to respond with costly changes to their business model.

Know Your Customer (KYC)
In addition to regulating financial and technological matters, regulators have also actively introduced policies in the domain of customer due diligence. The US is pioneering in introducing regulation in this area. From the late 1980s onward the US has introduced KYC (know your customer) policies that have obliged banks to collect and store substantial information about their customers and monitor their transaction flows in order to inform authorities of suspicious behavior. In addition, the US has become very strict in sanctions and trade embargo policy, enforcing compliance by imposing high fines on major banks for regulatory breaches. In 2014 the US introduced the Foreign Accounts Tax Compliance Act (FATCA) regulations, demanding banks report US taxable customers.
On a global scale states cooperate through international organizations (OECD, FATF, Wolfsberg group). on due diligence standards and exchange of tax information (OECD, FATF, Wolfsberg group). The EU has followed with a set of anti-money laundering regulations and series of tax exchange treaties modelled on these international standards (AML 4; DAC 4).

This has resulted in increasing complex and extensive KYC requirements, with a cost that is estimated through a recent survey to amount to $60 million annually on average, while the customer experience was evaluated as poor. Despite spending a substantial sum on KYC, customer satisfaction is suffering from increased regulatory requirements. Before entering into a banking relation, clients—and in particular corporate clients—have to go through lengthy paperwork procedures, for which financial institutions have insufficient skilled resources to handle the process.

REGTECH

As these regulatory constraints constitute a major pain point for banks, technological solutions are in high demand. Corresponding to this demand and the complexity of the current financial environment is the rise of regulatory technology (REGTECH) that offers promising solutions to reduce the compliance burden. REGTECHs differ from FINTECHs in their scope and business model. They offer solutions to financial institutions instead of competing with them; in addition, they target other sectors affected by regulations. REGTECHs have cooperated and also been sponsored by regulators. An example of this is the sponsoring of hundreds of firms by the UK Financial Conduct Authority (FCA) in 2014, which was followed by similar initiatives by regulators worldwide. Examples of areas in which REGTECHs offer solutions are client identification and transaction monitoring.

New developments in artificial intelligence, robotics, and blockchain are expected to introduce far-reaching automation up to complete replacement of human intervention. As outlined in this article, in particular blockchain technology is showing potential for solutions in the KYC domain.

Current challenges that are complicating REGTECH development is the overwhelming regulatory complexity, with rules defined by different legislative bodies. Despite international cooperation there is a lack of unification in regional specifications. Banks will have to comply with all international regulations as well as the specific laws of all the states in which they offer their products and services.

Blockchain

Blockchain (originally developed for mining bitcoins) is described as a distributed database, meaning that data is stored on the blockchain network and can be accessed by computers that are connected to it. One single file of data is split into parts, termed blocks. All blocks have to be separately validated by the entire network, which happens algorithmically. An example is a so-called smart contract that has programmed contractual conditions. In order for a contractual process to proceed, involved parties will have to provide their “digital signature,” which will be validated through the entire network. Encryption is applied to secure the data.

The blockchain database can be publically or alternatively, privately accessible. The second possibility is expected to prevail for commercial usage or in the case of KYC. What follows is an overview of the different elements of KYC/AML [anti-money laundering] together with the possible impact blockchain technology could have on it.

Client Identification and Verification

The first step of KYC is the identification of the customer and the verification of the person’s identity. For individuals this consists of the usual data such as the name, birthdate, nationality, address, and so on. This can be verified through an ID card or official (state) document. Blockchain allows for the use of digital identities. Electronic information associated with an individual in a particular identity system is called digital identity. Individuals tend to have several synchronic yet separated online digital identities in use. Examples can be straightforward such as mail, social media, and Internet banking, however, many other forms of digital identities for practically any Web application are imaginable.

Identity systems can be used for authentication and authorization. Persons can authenticate through use of a password, an object such as a smartcard, or their fingerprint. Consumers have several digital identities they
use for a wide range of purposes, which have varying means of authentication. In response applications to simplify the user experience by enabling the use of one identity for several purposes have appeared. Thus far, they have failed to be adopted on a large scale. Recent technological advancements have led to further initiatives that aim to enable more efficient use of digital identities, one of those initiatives is blockchain.\textsuperscript{15}

Blockchain can be used for the management of digital identities and has great potential for application in various fields such as in banking. Digital identities can be used to facilitate data exchange between financial institutions as well as exchange with third parties. An example of this is IDIN, an initiative developed by Dutch banks that allows consumers to use their banking ID with other merchants. It works similar to interbanking payments (see Exhibit 1) where instead of payment, identity information is exchanged. The way this would work is that via a private or permissions blockchain a Digital Identity Management System (DIMS) is created, in which several financial and eventually other actors can participate. The KYC information can be linked to the digital identity of the customer and shared through the system. The amount of information stored and shared can be regulated through the customer’s settings, which also defines what information is shared and with whom.\textsuperscript{16}

The way this would work in practice is illustrated in Exhibit 1.

Important to note is that in this example the customer decides with whom to share the digital identity.

**KYC for Professional Entities**

Exhibit 1 describes the process for individual clients, but for entities the process is more complex. In addition to verifying the details from the enterprise, related entities also have to be identified and verified. Some key persons such as the directors, those that have access to accounts, those who act or sign on behalf of the company, as well as the UBOs also have to be identified and verified. UBO stands for ultimate beneficial owner and concerns those that exercise a substantial form of control (the applied threshold usually is 10 percent to 20 percent) in an enterprise.

Another obligatory requirement for companies is to have an overview of the company organigram and all the intermediary entities that exercise a determined amount of control in the company, as well as the entities in which the company holds a certain threshold of shares.\textsuperscript{18} As such, a great part of KYC consists of identifying and verifying the correct relationships between companies. This information is subject to frequent change due to the increase or decrease of control or ownership stakes. In terms of blockchain for entities, several digital identities of individuals should be linked and stored in the blockchain database together with the entity.

Another possibility is the creation of a real-time organizational chart database in which shareholder structures are linked together and can be updated whenever something in the structure changes. A more basic option here would be to share an unconnected organigram per entity that is onboarded. The authenticity of the org chart can be verified through the signature of someone linked to it using their (individual) digital identity for this purpose.

The issue that arises here is the privacy of the individual and the entity. This could be solved through the use of personalized settings that can be applied to determine the degree to which provided information can be distributed and when signatures are required. As much of this information is increasingly becoming publicly available, this will not always be required.
Customer Screening

Financial institutions are linked internally to screening lists while using external providers for screening purposes. Names of relevant entities and individuals that have a relation to the bank are screened for hits to governmental sanctions, terrorism, other illegal activities, political exposure, and negative press. This search is automated, and it hits block onboarding until the hit is investigated and cleared. In addition, screening is part of ongoing surveillance and is carried out in real time.19

With respect to blockchain, screening could be included in the blockchain database. Hits would automatically “block” the authentication and would have to be cleared before continuing the process. Banks could supplement this with their internal screening process.

Additional Information and Customer Risk Analysis

Depending on the customer type and bank, the customer has to provide further information and fill in a questionnaire. Another aspect of KYC is the analysis of the customer through the due diligence team. This entails the interpretation of screening outcomes, negative press releases, and assessing the risk based on the captured information. The intensity of check-ups will depend on the inherent risk the customer poses. The criteria determining the inherent risk are prescribed by the regulator, whereas banks can further specify this according to their own policy.

Examples of factors that play a role in the inherent risk are the country in which the customer is based, is originally from, or operates in, as well as the business or profession of the customer. For companies, the process is usually more onerous than for individuals. Based on the information received and the analysis done by the KYC team, further check-ups may be required until the criteria determining the risk are satisfied. This will result in the final risk outcome and the overall customer profile. KYC input, therefore, consists of information provided by the customer and analysis performed by an employer, or in the future eventually a computer. The output, the customer risk profile, will determine the future treatment of the customer.

As the risk assessment is the responsibility of each institution and this information is typically not shared with the customer, the bank-specific part will likely remain out of scope of the distributed database in the short term. The part that is most fit to be distributed is the information provided by the customer, which could entail specific information regarding his operations. As different banks likely will have the same inquiries, the customer could opt to make this information visible per default as well as on specific request.

Publicly Accessible Information

An important part of the EU’s newest anti-money-laundering directive is the set-up of a central UBO register. Every EU country will be obliged to keep track of the owners of the company, together with the usual company information in the trade register such as the main directors. This and other already publicly accessible information, such as trade registers and all company information about regulated institutions and listed companies, does not specifically need to be provided by the customer. This information can be added to the shared customer data and can be freely distributed.

Surveillance Reviews, Updates and Transaction Monitoring

KYC data has to be kept up to date through scheduled reviews or ad-hoc reviews in case of significant changes. New information can be added to the blockchain and used by multiple institutions in order to keep their files in order.

In terms of AML the use of blockchain can be envisioned with respect to transaction data.20 With the use of blockchain, transaction data can be stored and become better traceable. In addition, it is suggested that here efficiency gains can be expected through codification of the transaction data, which will enable the data to be better interpreted. The question is whether privacy concerns will allow transaction data to be distributed. Distribution of transaction data among several institutions provides better input in identifying suspicious transaction patterns. Although this is likely a step too far in terms of privacy, a possible intermediate approach would be to create a shared standard for transaction monitoring and store all the possible hits in the database that will be made available to authorities.

Tax Reporting

Another aspect that falls in the scope of KYC is the determination of reportable accounts to government
authorities of a multitude of countries. This process requires banks to classify the tax status of the client toward the country of which they are a fiscal resident. The client will declare this information to the bank as part as the client’s identification information. The fiscal residence of the client can be stored along with the client’s other KYC information in the blockchain. In addition, the client’s tax status in relation to the governments can be derived from this. Blockchain also could be used for tax reporting.\textsuperscript{21}

**Conclusion**

The possibilities for KYC distribution through a blockchain database are plentiful. Through cooperation with other Financial institutions and with third parties such as the regulator, banks can save costs and time for themselves and their clients. Recently, progress has been made in this area through the digital trade chain consortium consisting of several major banks that have announced that for their trade finance operations IBM will create a mutual blockchain platform.\textsuperscript{22} This could foster further cooperation initiatives. In addition, the use of a digital identity outside of the financial institutions, as the example of IDIN in the Netherlands shows, can spill over into new business opportunities that are particularly relevant in the light of the developments of the upcoming PSD2 directive and the rise of third-party payment service providers. The condition for the use of data is the standardization of requirements among the participants as well as alignment with other digital applications. In order for banks to realize efficiency gains, it is recommended to align with the regulator and in this way increase the scope for consensus on the demand and supply side. With the implementation of blockchain databases for KYC data, customers can be offered a fast on-boarding process, and bankers can attend more to their core business of managing money instead of KYC.

**Works Cited**


**Notes**

1. Lomazzo. Fintech’s impact on wealth management.
2. KPMG. 2016 Banking sector briefing. Banking the customer experience divided.

4. Evry. PSD2. Strategic Opportunities beyond compliance.


8. Thomson Reuters.


10. Lomazo.

11. Erovic. Regtechs—the regulatory toolkit.


13. Vandepitte. How Blockchain is disrupting the financial sector.


16. Id.

17. Id.

18. Alan, supra n.5.

19. Id.

