From Fintech to Regtech: The possible use of Blockchain for KYC

YVONNE LOOTSMA
INITIO BRUSSELS
Summary

From Fintech to Regtech: the possible use of Blockchain for KYC

Introduction
Know your customer
Blockchain
Client identification & Verification
KYC for professional entities
Customer screening
Additional information and customer risk analysis
Publically accessible information
Surveillance - reviews, updates and transaction monitoring
Tax reporting and investor protection

Conclusion

Works Cited

About Initio
The author
Contact
From Fintech to Regtech: the possible use of Blockchain for KYC

Introduction
Banks have not had the best of times this decennium. The backlash of the financial crisis, low interest rates, strict regulations, government control and low consumer trust have forced banks to change their general approach, shifting from money first to rules and risk first (Alan, 2016). Technological innovations referred to as “Fintech” that use technology to provide automatized financial products have the potential to undermine the traditional positioning of banks (Lomazzo). Further treats comes from the current consumer attitude towards banks. Researchers have used to term “millennial time bomb” to describe the risk posed by the current generation that is wary of financial institutions and receptive to new innovations (KPMG). Nowadays customer’s demand personalized service and products available with the speed of a mouse click. Therefore banks these days invest strong in technology. This opens up a market for what is termed “Regtech”, the technological response to regulatory requirements (Parra-Moyano and Ross).

Know your customer
While much attention has been paid to financial risk management, another area where the regulator is closing in on banks is customer due diligence related to money laundering, terrorist finance and tax evasion. The US is pioneering in this area. From the late eighties onwards they have introduced KYC (know your customer) regulations that oblige banks to properly document their customers, monitor their transaction flows and inform authorities of possible illicit conduct. In addition, they have started demanding banks to report US taxable customers. Over the last 5 years the US has stepped up their efforts to enforce these rules by imposing high fines on major banks for failure to comply (Parra-Moyano and Ross). Outside of the US, countries cooperate through international organizations on due diligence standards and exchange of information (OECD, FATF, Wolfsberg group). The EU has followed with their own set of anti-money laundering regulations and series of tax exchange treaties modelled on these international standards (AML 4; DAC 4).
These regulations resulted in banks having to implement a thorough KYC process consisting of the collection, verification and screening of customer details during onboarding and updating this throughout the client relationship. In addition, banks assess the customer risk based on which they put monitoring controls in place as part of ongoing surveillance. The cost of KYC is estimated through a recent survey to amount to annually 60 million (Parra-Moyano and Ross), while the customer experience was evaluated as being poor. The result is further explained by the fact that the customers have to supply a large amount of documents and information after which it takes banks an extensive time to process. This would mean banks spend a lot of money, due to inadequate response to regulatory obligations however this still backlashes into bad customer service.

**Blockchain**

Technologic improvements could speed up this process, as well as supplement or replace the tailor-made service currently offered by advisors. Through the use of robotics, artificial intelligence and blockchain, customer onboarding could potentially completely be automatized. The below example process flows demonstrate the difference between the current onboarding and possible future onboarding process (Lomazzo).
The future process flow would combine the best of everything: automation from robo, the advice / financial planning of artificial intelligence and compliance from blockchain.

In the first process several actors are involved, in the second example all steps are fully automatized and the client can have an immediate account opening, while receiving advice and picking his product. Although the last part is an example of a more extreme outcome without any human intervention, it is certainly imaginable. It also shows that technology will allow for the elimination of actions that have no added value. In terms of KYC this can be achieved by the use of decentralized ledger technology such as blockchain (Suszek). The potential impact this would have is large.

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. Examples of this are smart contract that have programmed contractual conditions. In order for the 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 (Vandepitte).

The block chain database can be publically or alternatively, privately accessible. The second possibility is expected to prevail for commercial usage or in the case of KYC(Goldman and Sachs). Outlined below is a sum up of the different elements of KYC/AML together with the possible impact block chain technology could have on it.
Client identification & Verification

The first step of KYC is the identification of the customer and the verification of his identity. For individuals this consists of the usual data such as the name, birthdate, nationality, address etc. 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. Here you can see an example of a person that has several synchronic yet separated online digital identities in use. These examples are the most straightforward cases such as mail, social media and internet banking, however many other forms of digital identities for practical 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 (Baars).

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 date exchange between financial institution as well as exchange with third parties. An example of this is IDIN, an initiative developed by Dutch banks which allows consumers to use their banking ID with other merchants. It works similar to interbanking payments (see illustration below) 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 customer’s settings, which also defines with whom what information is shared (Baars).
The way this would be look in practice is illustrated in the below figure:

![Diagram](image)


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

**KYC for professional entities**

The illustration above describes the process for individual clients, for entities the process is more complex. Aside of verifying the details from the enterprise, also related entities have to be identified and verified. Some key persons such as the directors, those that have access to accounts, act/sign on behalf of the company, as well as the UBO’s also have to be identified and verified. UBO stands for ultimate beneficial owner and concerns those that exercise a substantial form of control (applied threshold usually is 10-20%) 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 the company holds a certain threshold of shares in (Alan). 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 increase/decrease of control/ownership stakes. In terms of block chain for entities, several digital identities of individuals should be linked and stored in the block chain database together with the entity. Another possibility is the creation of a real-time org. chart database where 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 signature of someone linked to this using their (individual) digital identity for this purpose. The issue that arises is the privacy of the individual and entity. This can be solved through the use of personalized settings that can be applied to determine the degree that provided information can be distributed and when signatures are required. As much of this information is increasingly becoming publically available, this will not always be required.

**Customer screening**

Financial institutions are linked internally to distributed 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 automatized, hits block on boarding until the hit is investigated and cleared. In addition, screening is part of ongoing surveillance and is carried out in real time (Alan).
With respect to blockchain, screening could be included in the block chain 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 according to their own policy can further specify this.

Examples of factors that play a role in the inherent risk are the country in which the customer is based, originally from or operates in, as well as the business/profession of the customer. For companies the process is usually heavier than for individuals. Based on the info 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 info is typically not shared with the customer, the bank-specific part will likely remain out of scope of the distributed database. The part that is most fit to be distributed is the information provided by the customer, which could however 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.

**Publically accessible information**

Currently a large part of the anti-money laundering and terrorist financing regulation in the EU, 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 info in the trade register such as the main directors. This information will be publically accessible for regulated institutions such as listed companies and many FI’s and therefore 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 foreseen reviews or ad-hoc reviews in case of significant changes. New information can be added to the block chain and used by multiple institutions in order to keep their files in order.

In terms of AML and TF the use of block chain can be envisioned with respect to transaction data (Goldman Sachs). 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 between 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 and investor protection**

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 towards the country of which they are fiscal resident. The client will declare this information to the bank as part as his identification information. The fiscal residence of the client can be stored along the client’s other KYC information in the blockchain. In addition the client tax status towards the governments can be derived from this. Blockchain could in addition be used for tax reporting towards the government (Peters).

Blockchain could also be used to store information about a client’s investment preferences and knowledge that banks are legally obliged to capture. Although in terms of competition there may be hurdles to sharing this info between institutions. As this is time consuming for the client, there is much efficiency to gain when they do not have to fill this in separately for several institutions (Peters).

**Conclusion**

To conclude, the possibilities for KYC distribution over blockchain are plentiful. The information can help banks save cost by cooperating together as well as save time for the customer. In addition, the use of a digital identity outside of the financial institutions as the example of IDIN in the Netherlands shows can also be an important contribution. The condition for the use of data is the standardization of requirements amongst the participants. In order for banks to realize efficiency gains, it is recommendable to align blockchain implementation with further reg/fintech innovations. In this way cost can be saved, customers can be offered services available with a mouse click and bankers may even be able to shift their focus back to their core business of managing money.

Yvonne Lootsma
Works Cited

Goldman Sachs. “Blockchain. Putting theory into Practice”.


Lomazzo, Jessica. “Fintech’s impact on wealth management.”


KPMG. “2016 Banking sector briefing. Banking the customer experience divided.”


Suszek, Dominic. “Blockchain: reshaping the future of banking and payment processing.”


Peters, Gareth William and Vishnia, Guy R. “Blockchain Architectures for Electronic Exchange Reporting Requirements: EMIR, Dodd Frank, MiFID I/II, MiFIR, REMIT, Reg NMS and T2S”.

https://ssrn.com/abstract=2832604


http://essay.utwente.nl/71274/1/Baars_MA_BMS.pdf

Parra-Moyano, José and Ross, Omri. “KYC Optimization Using Distributed Ledger Technology.”

https://ssrn.com/abstract=2897788

Vandepitte, Riemer. “How Blockchain is disrupting the financial sector”.

About Initio

*Initio* is a business consultancy firm specialized in the Financial Industry. Every day, our consultants contribute to the successful delivery of business projects by transferring their expertise to our client's management and internal teams.

*Initio* operates in the financial sector, servicing a wide range of clients. Our offering is focused on business consultancy combined with project methodology in order to assist our clients on the whole project cycle.

We have offices in Brussels, Luxembourg & Geneva. Through close collaboration, we can react swiftly on a wide scope of services in order to meet client needs rapidly with the highest industry standards.

[www.initio.eu](http://www.initio.eu)

---

Contact

**Initio Brussels**

Boulevard Brand Whitlock, 60
Brussels, 1200
Belgium

Tel: +32 (0)2 669 77 44
Email: brussels@initio.eu

Twitter: @Initio_eu