Demo: Blockchain for the Simplification and Automation of KYC Result Sharing

Robert Norvill, Mathis Steichen, Wazen M. Shbair, Radu State
University of Luxembourg (SnT)
29, Avenue John F. Kennedy
L-1855 Luxembourg
Email: {robert.norvill, mathis.steichen, wazen.shbair, radu.state}@uni.lu

***Abstract*—Know Your Customer (KYC) processes performed by banks on their customers are redundant, cumbersome and costly. Therefore, a system is proposed to automate menial tasks and allow sharing of data related to KYC. A blockchain dictates the collaboration between different participants and several services are built around it to support the functionality of the system as a whole. An access control system is used to share data legitimately.**

I. Introduction

Know Your Customer (KYC) is a process usually required to be performed by banks on their customers. Therefore, banks need to collect data on their customers, for example on their identity and on their home address. This data is then used to perform security and background checks on the customers. KYC is required by EU law, in order to ensure that banks deal only with legitimate customers.

However, the KYC process is cumbersome and costly, and needs to be performed repeatedly by every bank for each of their customers. This includes redundant work that can be alleviated by trusted automation. Furthermore, the KYC process needs to be compliant with data protection regulations.

Therefore, this work introduces a system that leverages blockchain to automate tasks and allow the sharing of data related to the KYC process. Some considerations regarding the system are discussed in Section II, and the architecture is explained in Section III. The demonstration is detailed in Section IV. This paper ends with the conclusion in Section V.

II. Sharing data through the blockchain

Sharing data through blockchain requires careful considerations regarding privacy and applicable law.

a) GDPR: The European Union's General Data Protection Regulation (GDPR) [1], [2] introduces several requirements that banks have to satisfy when dealing with personal data of their customers. Customers can request the deletion of their personal data or the sharing of documents with a third party, for example another bank. This enables cooperation, however this permission is required, if the bank wants or needs to share a customer's data.

b) Data on the blockchain: Blockchains can be used to share data, however, this is usually costly and inefficient in terms of storage space. In addition, storing any customer's personal data directly on the blockchain is not compliant with GDPR. Therefore, the herein proposed system stores customer information and documents off-chain, but stores hashes on the blockchain. Thus, if needed, they can be removed from the system, and their dissemination controlled. The blockchain itself is used to store events and permissions. Events are the on-boarding of new customers into the system and requests for documents from participants. This provides a trail that allows auditors to follow the actions performed on or through the blockchain. Permissions are set by the customer whose data is concerned. Whenever a bank requests a document, these permissions are consulted and the document is then either shared or not. The permissions form a hierarchy in the form of tiers that give different accesses to different types of documents. For example, a lower tier provides access to identity information that is also contained on id cards. A higher tier, gives access to tax documents or proofs of residency. Blockchain-based access control systems have already been proposed, for example [3].

c) Information sharing: Information is shared through the blockchain. Whenever a bank wants to access customer data, it does so by sending a request, within a transaction, to the blockchain. The blockchain executes the transaction and updates its state. Consensus is formed on whether or not the request is legitimate, i.e. on whether or not it is in line with set permissions. If the requester is allowed to receive the customer data, it is shared with the requester.

d) Private, permissioned blockchains: Different types of blockchains exist [4]. Because the system is using sensitive information, a private blockchain is employed. This allows the selection of participants as well as limiting who can access the blockchain data. Customers access the blockchain or the off-chain storage through their respective banks' services.

III. System architecture

Figure 1 illustrates the system architecture. Participating banks operate their own such system, such that many of them form one self-verifying network. The components within one such system are described in the following.

a) Geo-address validation: An API for geo-address validation is provided by the Luxembourgish government for addresses within Luxembourg and is available online [5]. It provides a percentage that represents how close a given address is to an existing one. Furthermore, GPS data can be

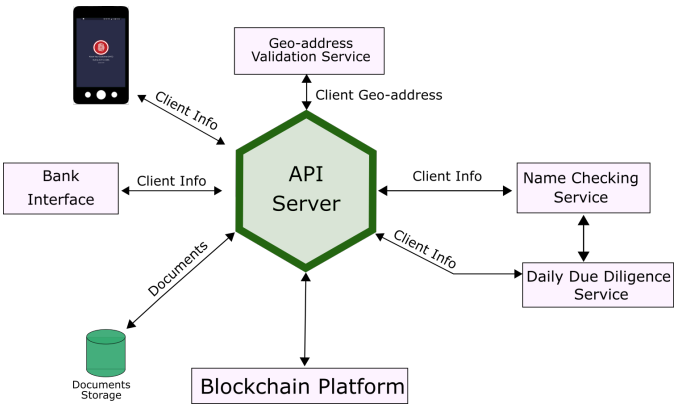

Fig. 1. The system architecture comprising the blockchain, the document storage, name checking and daily check service, an interface with the geo-address validation service and the API service. The latter allows customers and banks to interact with the components of the system.

used for additional checks and for automatically inserting the correct address within the system.

b) Name checking service: KYC requires banks to regularly check if a customer's name appears on list[1] of known suspicious persons. This is the task of this service.

c) Daily due diligence service: Together with the name checking service, this component automatically verifies that the bank only conducts legitimate business.

d) Documents storage: The document storage is used to store all documents that a customer provided to their bank. They are thus stored off-chain and can be removed from the system if necessary. Documents include scans or id cards, passports or residency proofs.

e) User interface: The customer interface is provided by a bank for its customers. It allows the customers to give and revoke permissions and to see which bank has access to their information.

f) Bank interface: The bank interface allows the bank to interact with the system. Information can be viewed, documents accessed and requested.

g) API server: The API server acts in between the different services and is the main access point to the system. It handles requests, serves documents, and with the blockchain.

h) Blockchain: As described in Section II, the blockchain stores events, such as document requests and permissions. It is not directly accessed by customers, but by participating banks. The required blockchain functionality is implemented as smart contracts on top of an Ethereum blockchain [6].

This section concludes with a discussion of the advantages and drawbacks of this system. As mentioned in Section II, the system enables a wide range of automation of redundant and menial tasks. Customer provided addresses are automatically verified, daily checks are performed, GPS information is leveraged for security purposes and Id cards or passports can be scanned using the smartphone. All of these lead to reduced costs and alleviation of redundant work for banks and customers. Moreover, auditors can view the system and the events, immutably stored by the blockchain.

As future work, the leakage of business information and data duplication is to be addressed. Information regarding one bank's customer numbers may be leaked through the blockchain, because users and documents are registered within the blockchain. In the future, we intend to explore solutions to this issue involving the use of multiple accounts.

Data duplication can occur if a customer registers with two different banks, without stating that an account on the system has already been created. This would partially defeat the purposes of the system, but could be addressed using a customer identifier stored on the blockchain.

IV. Demonstration

The described system is set up in a docker container environment. Several banks are present in the system and can be used immediately. The demonstration includes the following steps. First, a new customer is registered within the system and mock data is uploaded. The mock customer data is obtained by scanning an id card or a passport. Second, a user can interact with the system, both as customer and as a bank. For this purpose, a document is uploaded to the system. The bank then requests access to this document, whereupon according permissions are set by the customer. The correctness of the file is then verified. Third, the customer withdraws the permission and the bank's access to the document is revoked.

Thus, the demo highlights key elements of the proposed system and allows a user to see the interaction with the latter, both as a customer and as a bank.

V. Conclusion

This demo paper presents a system that allows automation and simplified, permissioned document sharing between banks. It is specifically designed to reduce the redundant and menial workload required by the KYC process.

The demo gives insights into the operation of the system. It shows how the system works from different angles, the customers' and the banks'.

Future work includes the investigation of data leakage and duplication issues, for which potential solutions have been discussed.

[1]For example: https://www.refinitiv.com/en/products/world-check-kyc-screening.

References

[1] "Regulation (eu) 2016/679 of the european parliament and of the council of 27 april 2016." https://eur-lex.europa.eu/eli/reg/2016/679/oj. Accessed: 2019.03.14.

[2] "Eu gdpr.org." https://eugdpr.org/. Accessed: 2019.03.14.

[3] D. Di Francesco Maesa, P. Mori, and L. Ricci, "Blockchain based access control," in *Distributed Applications and Interoperable Systems* (L. Y. Chen and H. P. Reiser, eds.), (Cham), pp. 206–220, Springer International Publishing, 2017.

[4] K. Wüst and A. Gervais, "Do you need a blockchain?," in *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)*, pp. 45–54, June 2018.

[5] "La plate-forme de données luxembourgeoise." https://data.public.lu. Accessed: 2019.03.14.

[6] G. Wood, "Ethereum: A secure, decentralised generalised transaction ledger," 2018.