International Journal of Scientific Research & Engineering Trends
Volume 7, Issue 5, Sept- Oct-2021, ISSN (Online): 2395-566X

Blockchain in the KYC Process – A Case Study

Abhishek Oberoi, Bhargav Patel, Anas Mansuri
Department of Computer Engineering,
Devang Patel Institute of Advance Technology and Research,
Charotar University of Science and Technology, Changa, Anand, India.

Abstract-This paper deals with the appropriateness of the blockchain technology to improve existing KYC procedures, which are often described as lengthy, costly and cumbersome. Moreover, similar identification processes need to be carried out repeatedly for several institutions, which creates considerable inefficiencies and avoidable costs. The use of a blockchain design with smart contracts offers the possibility to avoid redundant workflows and entails several benefits such as enhanced security, trust and flexibility. This illustrates that the blockchain technology, which is still in a maturing phase, has the potential to play an important role in streamlining and (to some extent) automating current KYC processes. In terms of security, trustworthiness or customer satisfaction, the technology may offer game changing opportunities (not only) in the realm of authenticated user identification or digital identity management.

Keywords-Blockchain, KYC, smart contract, treasury, privacy

I. INTRODUCTION

Efforts to curb money laundering and terrorist financing are becoming increasingly sophisticated around the globe. As a consequence, banks, financial service providers and corporates have to carry out extensive checks on the legitimacy of their business partners in order to meet legal compliance requirements, commonly referred to as Know-Your-Customer (KYC).

In a recent survey study, more than 90 percent of corporate treasurers stated that responding to KYC requests is far more demanding today than it was five years ago. Due to lengthy KYC processes, many companies have already reduced the number of their banking partners. More specifically, corporate treasurers complain about complex and sometimes poorly structured KYC procedures they have to go through before opening an account with a new bank. Such checks can quickly take up to several months due to duplicate queries or unconcrete requirements from the banks.

In the course of digitization, such problems do not remain unaddressed. While a survey conducted by the magazine DerTreasurer in 2020 revealed that financial managers see the greatest need for digitization in corporate banking in KYC issues, first corporates such as E.ON, a German electric utility company, presented a solution to digitize KYC processes.

In concrete terms, the energy supplier opened a bank account and delivered the data for the KYC checks completely electronically via a new electronic bank account management tool. However, the new tool will only have real added value if not just one or two, but many financial institutions share the same electronic solution. For this reason, the corporate wants and needs to convince more banks of the acceptance of the electronically transmitted KYC information.

Another major weakness in the current KYC process is that personal and company data are repeatedly requested by several institutions. This results in identical processes that customers go through at different parties but produce identical results. This in turn causes avoidable expenses for the institutions and annoys customers who have to undergo the KYC procedure several times. According to a recent survey by Thompson Reuters, such an outdated due diligence process generates direct costs for financial institutions of on average USD 60 million and overall is said to cost up to USD 500 million per bank per year.

In this regard, the plans of the banking cooperative Swift, acronym for Society for Worldwide Interbank Financial Transactions, to set up a central register for KYC-relevant corporate client data are meaningful. In detail, the KYC registry is an existing online portal for financial institutions to exchange institutional KYC information as part of the statutory due diligence process. The platform shall enable banks to exchange KYC data and documents with their correspondent banks in a secure, standardized and controlled manner and to access the complete and validated KYC profiles of their correspondents.

In a first step, Swift launched the web- based register for KYC-relevant corporate customer data at the end of 2019 for all companies that have a Swift connection within their group. The declared goal is to increase efficiency and contribute to cost savings in the KYC process. Hopes expressed by a participating corporate in May 2020 include that a platform as communication channel will be more secure and transparent than e-mail processes and that

banks would have more confidence in the information provided via the platform, as the documents would be verified by Swift. The Swift review would hopefully also lead to fewer queries.

Given that Swift has been criticized for its inefficiency and lack of transparency, the solution based on an online portal of the traditional banking system also raises doubts. Concerning the general Swift setup, for example, the Swift member Credit Suisse, global wealth manager, investment bank and financial services company headquartered in Switzerland, "believes that interbank payment systems are ripe for disruption.

Interbank payment systems such as Swift are old, inflexible, slow, and increasingly prone to cyberattacks at a time when banks are under 3 tremendous pressures to cut costs and protect customer data from hackers, which blockchain could achieve".

Critics of the Swift registry state that centralized KYC utilities struggled to gain industry-wide acceptance with over one-third of banks not participating due to cost, operational and complex technical integration issues and that such centralized models are inflexible compared to new technologies. Promoters of the stated blockchain technology assert that decentralized setups provide the basis for a truly global, efficient and secure KYC process without centralized data stores managed by third-party providers acting as (inefficient) intermediaries.

Eventually, the head of KYC and reference data at Swift recognizes new technologies: "The [Swift KYC registry] platform is constantly evolving, but transferring the registry onto blockchain will be off the cards fornow. We will continue to explore blockchain over different use cases, but for now the centralized solution is a good one".

The remainder of the article takes up this point and examines if and in what way a blockchain structure is capable of solving the current KYC problems.

II. BLOCKCHAIN IN THE KYC PROCESS – A TECHNOLOGICAL FIT?

1. Blockchain Basics:
Blocks that consist of time-stamped series of an immutable record of transaction data form the core of the blockchain technology. A blockchain makes it possible to transmit information in a forgery-proof manner using a decentralized database shared by many participants, so that manipulated copies are impossible.

Such a database is also known as distributed register or distributed ledger and requires a trustworthy and decentralized mechanism to create consensus on how new blocks are created and how they can be added to the existing blocks.

There are various consensus mechanisms, with proof-of-work being the oldest and best known (e.g., used in the public Bitcoin and until present still the Ethereum blockchain), proof-of-stake being faster and more resource-efficient (less time-consuming and computationally-intensive) and proof- of-authority being particularly applied in the realm of private or permissioned, i.e., access- restricted blockchains.

The blockchain technology is developing very dynamically and new areas of application are being opened up rapidly. So-called smart contracts are regarded as the most important conceptual development of the blockchain. Smart contracts are to be understood as computer programs that can make decisions if certain conditions are fulfilled. In other words, they enable a blockchain-based automated execution of if-then relationships.

2. Dealing with the current weaknesses of the KYC process:
How does the blockchain technology address the current problems of the KYC procedure?

3. Security:
In addition to the blockchain basics above, it is important to note that all parties involved must agree on transactions before they are recorded and that the verified blocks are cryptographically encrypted before being appended to the chain of data records (blockchain). The decentralized database is stored on many computers in a peer-to-peer network.

Since each participant or node keeps a copy of the entire blockchain instead of the information being located on a single server, the technology is resistant to hacking – changing the data record would imply hacking each individual node as there is no single point of failure. Blockchains are therefore secure, always up-to-date directories in which digital transactions can be documented reliably and comprehensibly for the participants.

Is the blockchain thus 100% tamper-proof? Theoretically, if a participant manages to control more than half of the participant nodes, he could modify the transaction history. In fact, this never happens and this is of minor relevance in the framework of private or permissioned blockchains with trusted nodes.

4. Efficiency:
Paper or e-mail-based processes for complex transactions involving many participants are slow and error-prone. A blockchain creates – with its digital ledger technology – trustworthy and forgery-proof business transactions, so that clearing and settlement can take place more quickly. However, the performance of a public blockchain does not even come close to that of a central database. For

comparison, while the VISA payment network processes an average of 2,000 transactions per second (with a maximum capacity of 56,000 transactions per second), the 6 worldwide online payment system of PayPal enables approximately 150 transactions per second, the public blockchain of Bitcoin merely processes three transactions per second and Ethereum 20 transactions per second.

Checking transactions and synchronizing them takes time, or in other words, finding a consensus in a completely distributed public blockchain system is difficult and needs certain security measures (e.g., the hash puzzle) to create trust among the participants, which eventually slow down the system's performance. This limited transaction speed is still a major limiting factor of the blockchain technology. For this reason, alternative ways of increasing scalability are being examined with promising further developments to the blockchain technology. (e.g., parachains, state-channels etc.)

Again, in private or permissioned blockchains with several trusted nodes, this problem generally does not exist because there is already trust between the participants and therefore time- and energy-intensive consensus mechanisms for the validation of transactions become redundant, which also increases the transaction speed significantly (but not to the level of central systems). Hyperledger Fabric, a permissioned blockchain project, is said to be able to process 3,000 to 20,000 transactions per second. In general, however, the question arises as to how relevant the differences in transaction figures are in a KYC use case.

5. Costs:
With the blockchain technology, the need for third parties or other instances that give certain guarantees decreases significantly. Further, the digital representation of processes is also associated with meaningful automation potential and thus again cost reductions. Relating in particular to smart contracts, this can this can reduce transaction costs and ensure a high level of process integrity because subsequent deviations from agreements once made are no longerpossible or at least made considerably more difficult.

In view of the above-mentionedredundancy of identical KYC processes and the associated costs, the blockchain technology has the potential for a single KYC identification process that generates a certified data record. Instead of regularly repeating the identification process, other institutions or customers could be granted access to the trustworthy and immutable record of KYC data.

Compared to centralized repositories of data with an intermediary between banks and their customers, the blockchain solution offers more flexibility without imposing standardized guidelines on its users in the sense of 'one-size-fits-all'.

6. Transparency:
Flexibility also plays a role in terms of transparency, which is another important and often criticized feature of blockchain technology. Blockchains are very transparent, since any member of the network can view the entire transaction history at any time. This high level of data integrity and transparency creates trust between the different actors in the blockchain network. In general, insight into historical transaction data can help to verify the authenticity of products or assets. In the KYC process, too, such traceability and thus authenticity checkshelp to prevent fraud.

However, the actually desired transparency with the blockchain could also go too far. It is important to remember that blockchains are by nature open and not anonymous, but pseudonymous. While you are able to control who gains insight into past transactions, you may want to protect your privacy to a certain extent. In this respect, tools like zk-SNARKs, which stands for 'Zero-Knowledge Succinct Non-Interactive Argument of Knowledge' and that work on so-called Zero-Knowledge-Proofs, could be a promising, but still computationally-intensive,solution.1

Put simply, zk-SNARKs or zero knowledge proofs mean that between two parties to a transaction, each party is able to verify to the other that it has a certain set of information without disclosing what that information is. This is very different from other systems where at least one party must know all the information. For example, individuals may need to prove that they hold enough money in their bank account to pay for a certain good, i.e., they meet a certain monetary threshold, but they do not want to reveal the exact balance of their account.

Another example from the online gambling business would be that individuals need to document that they are over the minimum age for gambling. So you prove this information without disclosing your full personal information such as your date or place of birth. Thus, zk-SNARKs allow you to reach your desired level of transparency, since only the necessary and required information is published on the blockchain.

7. Assessment of the potential solution:
To what extent can the blockchain technology solve the current weaknesses and other secondary aspects of the KYC process?

One major advantage of the blockchain solution is the ability to avoid redundancies. Instead of conducting KYC processes repeatedly with different institutions, a company would complete the verification procedure with one bank, with the result being securely stored on the blockchain. The result refers to a trustworthy and immutable data record with verified identity and business data stored in encrypted form, which the company could provide to all

institutions and bodies that are obliged to follow KYC procedures. This access could be granted by means of smart contracts. Storing the information in smart contracts has the advantage that a company can more easily control who accesses its data; using one-time passwords, for example, it can allow another institution to access the verified identity and business information.

As far as the choice between a public vs. a permissioned blockchain is concerned, although both approaches can be observed in the literature, there is a tendency towards the access- restricted approach, not least because of fewer security and privacy issues and significantly improved efficiency. In this regard, the General Data Protection Regulation (GDPR), for example Article 17 – Right to erasure ('right to be forgotten'), in the European Union is another important aspect.

Advocates of a permissioned blockchains state storing data directly on a public blockchain would not be GDPR-compliant, since the immutability of the blockchain hinders the fulfilment of the right to be forgotten.

There are different solutions and workarounds to this problem, e.g., storing information off-chain or a dynamic management of a blockchain based decentralized data storage, but which are subject to additional efforts and restrictions. In a permissioned blockchain, if all participants agree, a deletion of data would be feasible.

As far as ownership of the data is concerned, with the blockchain solution it can remain with the user (e.g., a corporate) itself, without any intermediary. This gives individual parties greater control over their data, excludes the possibility of unauthorized access and reduces the probability of mistakes or fraud.

Further, smart contracts based on the blockchain technology make it possible to execute control and automate operational processes, which can reduce risks by restricting the extent of human intervention.

In this respect, the properties of the blockchain, such as its immutability and security, create trust in the data stored on a blockchain, which makes secondary validation processes unnecessary and further reduces the need for manual input.

Further, conventional, centralized systems involving third parties are said to be slow in identifying, reporting, and solving mistakes, whereas a decentralized setup makes the processes more efficient, since several parties can easily rely and access reliable data.

In summary, the blockchain technology is capable of eliminating the main weaknesses and creating the conditions for simplifying the current KYC procedure. Compared to central solutions, the decentralized structure of a blockchain offers a much higher level of trust and stability without a single point of failure and, last but not least, a wide range of flexibility in this process.

III. CONCLUSION

Checks on the legitimacy of one's business partners, better known as KYC, are excessively long, expensive and inefficient. In addition, the process has to be repeated for different institutions resulting in similar processes producing identical results. Using a blockchain design with smart contracts enables users to avoid duplication of efforts and current redundancies in the process together with an adequate access control.

Overall, the blockchain could play a major role in streamlining the KYC procedure towards a secure, trustworthy and more efficient workflow that offers numerous opportunities and flexibility in many ways for seminal applications.

The blockchain, which may still be in its infancy to a certain extent, could not only be a game changer for the banking and financial industry (in terms of security, trustworthiness, customer satisfaction etc.), but potentially has a broader scope of application in fields that require authenticated user identification and beyond.

The character of the blockchain technology has the potential to automate compliance processes to a certain extent and to manage digital identities efficiently in the digital age.

REFERENCES

[1] Backhaus, D. (2018). E.on digitizes KYC processes.
[2] Backhaus, D. (2019). Swift opens KYC platform for corporate customers.
[3] Backhaus, D. (2020). Würth uses KYC registers from Swift.
[4] Bafin (2017). Blockchain-Technology.
[5] Bhaskaran, K., Ilfrich, P., Liffman, D., Vecchiola, C., Jayachandran, P., Kumar, A., … Suen, C. H. (2018). Double-blind consent-driven data sharing on blockchain. Proceedings - 2019
[6] Bundesnetzagentur.(2019). Die Blockchain-Technology: Potentials and challenges in the grid sectors of energy and telecommunications
[7] Devteam (n.d). Why Is Blockchain a Good Solution for KYC Verification?
[8] Finck, M. (2019). Blockchain and the General Data Protection Regulation.
[9] FinTech Network. (2019). Four Blockchain Use Cases for Banks. FinTech Network Report.
[10] Gorenflo, C., Lee, S., Golab, L., & Keshav, S. (2020). FastFabric: Scaling Hyperledger Fabric to 20,000 Transactions per Second.
[11] Hülsbömer, S. & Genovese, B. (2020). Was it Blockchain?

[12] Kindergan, A. (2020). Forget Bitcoin, but Remember Blockchain?
[13] Parra Moyano, J., & Ross, O. (2017). KYC Optimization Using Distributed Ledger Technology.
[14] Saigal, K. (2019). Swift KYC registry opens to corporates.
[15] Schiller, K. (2019). What is zk-SNARKs and Zero Knowledge Proof?
[16] Wass, S. (2019). Swift expands KYC registry to corporates.