Blockchain in the KYC Process

An Answer for Everything?

By **Dr Andreas Hecht**, Manager Corporate Finance – Risk Management and Reporting, MAHLE International GmbH, Certified Blockchain Expert

Know Your Customer requirements have long been a headache for corporate treasurers. Could blockchain resolve the pain points in the KYC journey? Are there any downsides to using distributed ledger technology in this instance? This article answers these important questions – and more.

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, or Know Your Customer (KYC). In a recent survey, more than 90% of corporate treasurers stated that responding to KYC requests is far more demanding today than it was five years ago[1]. The lengthy KYC processes mean that 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 take up to several months due to duplicate queries or various requirements from the banks.

While a survey conducted by a German treasury magazine in 2018 revealed that financial managers see the greatest need for digitisation in corporate banking in KYC issues[2], E.ON, a German electric utility company, offered one solution: it opened a bank account and delivered the data for the KYC checks electronically via a new electronic bank account management tool. However, this will only have real added value if many financial institutions share the same electronic solution.

Another major weakness in the current KYC process is that personal and company data are repeatedly requested by several institutions, with customers having to complete identical processes with different counterparties which produce identical results, causing avoidable expense for the institutions and annoying customers. According to a recent survey by Thomson Reuters, this outdated due diligence process generates average direct costs for financial institutions of $60m and overall is said to cost up to $500m per bank per year[3].

To address this problem the banking co-operative SWIFT is in the process of setting up a central register for KYC-relevant corporate client data. The KYC registry is an online portal for financial institutions to exchange institutional KYC information as part of the statutory due diligence process. The platform enables banks to exchange KYC data and documents with their correspondent banks in a secure, standardised and controlled manner and to access the complete and validated KYC profiles of their correspondents. In a first step, SWIFT launched the web-based registry for KYC-relevant corporate customer data at the end of 2019 for all companies that have a SWIFT connection within their group, aiming to increase efficiency and contribute to cost savings in the KYC process. In May 2020 one participating corporate said that it hoped that a platform as communication channel will be more secure and transparent than email 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 will hopefully also lead to fewer queries.

However, SWIFT has been criticised for its inefficiency and lack of transparency, and the solution based on an online portal of the traditional banking system also raises doubts. Concerning the general SWIFT set-up, for example, SWIFT member Credit Suisse "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 tremendous pressure to cut costs and protect customer data from hackers, which blockchain could achieve". Critics of SWIFT's KYC registry state that centralised 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 centralised models are inflexible compared to new technologies.

Promoters of blockchain technology assert that decentralised set-ups provide the basis for a truly global, efficient and secure KYC process without centralised data stores managed by third-party providers acting as (inefficient) intermediaries. The head of KYC and reference data at SWIFT has acknowledged the new technologies, stating "The [SWIFT KYC registry] platform is constantly evolving, but transferring the registry onto blockchain will be off the cards for now. We will continue to explore blockchain over different use cases, but for now the centralised solution is a good one".

How blockchain can address weaknesses of the current KYC process

Security

All parties involved must agree on transactions before they are recorded and ensure that the verified blocks are cryptographically encrypted before being appended to the chain of data records (blockchain). The decentralised 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

Promoters of blockchain technology assert that decentralised set-ups provide the basis for a truly global, efficient and secure KYC process.

BLOCKCHAIN BASICS

Blocks that consist of time-stamped series of an immutable record of transaction data form the core of blockchain technology. A blockchain makes it possible to transmit information in a forgery-proof manner using a decentralised database shared by many participants, so that manipulated copies are impossible. Such a database, also known as distributed register or distributed ledger, requires a trustworthy and decentralised 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, so far, in Ethereum), proof-of-stake being 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.

Blockchain technology is developing dynamically and new areas of application such as smart contracts are rapidly opening up. Smart contracts are computer programmes that can make decisions if certain conditions are fulfilled, enabling a blockchain-based automated execution of 'if-then' relationships.

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.

Is blockchain 100% tamper-proof? Theoretically, if a participant manages to control more than half of the participant nodes, it could modify the transaction history. In practice this never happens and has little relevance to private or permissioned blockchains with trusted nodes.

Efficiency

Paper or email-based processes for complex transactions involving many participants are slow and error-prone. A blockchain creates trustworthy and forgery-proof business transactions, so that clearing and settlement can take place more quickly. However, the performance of a public (as opposed to private) blockchain does not come close to that of a central database. For example, while the VISA payment network processes an average of 2,000 transactions per second (with a maximum capacity of 56,000 transactions per second) and the worldwide online payment system of PayPal enables approximately 150 transactions per second, the public blockchain of bitcoin processes just three transactions per second and Ethereum processes 20 transactions per second. Checking transactions and synchronising them takes time: finding a consensus in a completely distributed public (again, we are not talking about private blockchains here) blockchain system is difficult and needs certain security measures to create trust among the participants, slowing down the system's performance. This restricted transaction speed is still a major limiting factor of blockchain technology and alternative ways of increasing scalability such as parachains, state-channels etc. are promising developments.

For those who aren't familiar with the terminology, parachains improve the scalability and speed of the network. As the chains run and process all transactions in parallel, bottlenecks are avoided as with individual blockchains that process transactions one after the other. Meanwhile, the term 'state channels' refers to an 'off-chain' process with users transacting with each other directly outside the blockchain, which reduces the use of 'on-chain' operations.

In contrast to public blockchains, private or permissioned ones with several trusted nodes, mean that this performance problem does not usually exist because there is already trust between the participants. In turn, this means that time- and energy-intensive consensus mechanisms for the validation of transactions become redundant, significantly increasing transaction speeds but not to the level of central systems. Hyperledger Fabric, a permissioned blockchain project, is reported 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.

Costs

Blockchain technology significantly reduces the need for third parties or other guarantees, and the digital representation of processes is also associated with meaningful automation potential and thus cost reductions. With smart contracts this can reduce transaction costs and ensure a high level of process integrity, because subsequent deviations from agreements once made are no longer possible, or at least made considerably more difficult. In view of the redundancy of identical KYC processes and the associated costs, 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.

Transparency

Transparency is another important and often criticised feature of blockchain technology. Blockchains are very transparent, since any member of the network can view the entire transaction history at any time. This 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 such traceability and thus authenticity checks help to prevent fraud.

However, the desire for transparency could go too far. 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, (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge) which work on so-called zero knowledge proofs, could be a promising, but still computationally-intensive, solution. Zero knowledge proofs mean that each party in a transaction is able to verify to the other that it has a certain set of information without disclosing what that information is, unlike 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, but they do not want to reveal the exact balance of their account. So, you prove this information without disclosing your full personal information such as your date or place

Blockchains are therefore secure, always up-to-date directories in which digital transactions can be documented reliably and comprehensibly.

of birth. zk-SNARKs allow you to reach your desired level of transparency, since only the necessary and required information is published on the blockchain.

How effective is blockchain in the KYC process?

One major advantage of blockchain compared to current KYC processes is the ability to avoid redundancy in the system. Instead of conducting KYC processes repeatedly with different institutions, a company would complete the verification procedure with one bank, 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, the advantage of which is 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.

In the choice between a public vs permissioned blockchain there is a tendency towards an access-restricted approach because of fewer security and privacy issues and significantly improved efficiency. 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 to this problem, e.g., storing information off-chain or a dynamic management of a blockchain-based decentralised data storage, subject to additional efforts and restrictions. In a permissioned blockchain, if all participants agree, a deletion of data would be feasible.

In a blockchain solution ownership of the data can remain with the user (e.g., a corporate) without any intermediary. This gives individual parties greater control over their data, excludes the possibility of unauthorised access and reduces the probability of mistakes or fraud. Smart contracts make it possible to execute control and automate operational processes. Blockchain properties such as immutability and security create trust in the data, making secondary validation processes unnecessary and further reducing the need for manual input. Conventional, centralised systems involving third parties can be slow in identifying, reporting, and solving mistakes, whereas a decentralised set-up makes the processes more efficient.

In summary, blockchain technology is capable of eliminating the main weaknesses and creating the conditions for simplifying the current KYC procedure. Compared to centralised solutions, the decentralised structure of a blockchain offers a much higher level of trust and stability and a wide range of flexibility without a single point of failure.

Parting thoughts

KYC checks on the legitimacy of business partners are long, expensive and inefficient. The process has to be repeated for different institutions resulting in similar processes producing identical results. Using a blockchain with smart contracts enables users to avoid duplication of efforts and current redundancies in the process, together with adequate access control. Overall, blockchain is not the answer for everything, but it 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.

Blockchain, which is and must be constantly further developed, could not only be a gamechanger 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 with its ability to automate many compliance processes and to manage digital identities efficiently in the digital age. ■

DR ANDREAS HECHT

Manager Corporate Finance – Risk Management and Reporting, MAHLE International GmbH, Certified Blockchain Expert

> ***Transparency is another important and often criticised feature of blockchain technology.***

Note
This is an edited version of Dr. Hecht's article. The full text including references is available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3609496

1 https://www.it-finanzmagazin.de/firmenkunden-bekommen-zugang-zum-swift-kyc-register-99069/
2 https://www.dertreasurer.de/news/cash-management-zahlungsverkehr/eon-digitalisiert-kyc-prozesse-2001901/
3 https://link.springer.com/article/10.1007/s12599-017-0504-2