Ostern, Nadine Kathrin; Riedel, Johannes

Know-Your-Customer (KYC) Requirements for Initial Coin Offerings

Business & Information Systems Engineering

Provided in Cooperation with:
Springer Nature

Suggested Citation: Ostern, Nadine Kathrin; Riedel, Johannes (2020) : Know-Your-Customer (KYC) Requirements for Initial Coin Offerings, Business & Information Systems Engineering, ISSN 1867-0202, Springer Fachmedien Wiesbaden, Wiesbaden, Vol. 63, Iss. 5, pp. 551-567, https://doi.org/10.1007/s12599-020-00677-6

Bus Inf Syst Eng 63(5):551–567 (2021)
https://doi.org/10.1007/s12599-020-00677-6

RESEARCH PAPER

Know-Your-Customer (KYC) Requirements for Initial Coin Offerings

Toward Designing a Compliant-by-Design KYC-System Based on Blockchain Technology

Nadine Kathrin Ostern · Johannes Riedel

Received: 14 August 2019 / Accepted: 21 September 2020 / Published online: 8 December 2020

Abstract Blockchain technology is often proposed as an infrastructure for decentralized Know-Your-Customer (KYC) verification, i.e., a process determining whether a customer is eligible for a given transaction. The benefit of using blockchain technology lies in the expected compliance costs reduction for companies by automatically enforcing KYC-requirements, whose results are accessible by multiple financial institutions. While information systems researchers have proposed conceptual models and prototypes of blockchain-based KYC-systems, they do not yet consider severe penalties that are applicable to companies if KYC-requirements are not met. Hence, if the legal requirements for KYC-processes cannot be met, these systems are not applicable. The paper uses an objective-centered design science research approach to develop a blockchain-based KYC-system for the conduct of ICOs that is compliant-by-design. To this end, the authors first identify existing KYC-requirements and define corresponding system design objectives that are used to develop a KYC-system that automatically enforces KYC-regulations, thereby preventing money laundering and other forms of identity fraud. Second, the authors contribute to the literature by providing a blueprint for compliant-by-design blockchain-based KYC-systems, in the paper, integrated into the investment flow of an ICO. Third, the authors propose a KYC-system that is applicable in the real world, by making – due to legal certainty – KYC-processes cost-effective, i.e., the proposed blockchain-based KYC-system expectably reduces compliance costs for customers and financial organizations.

Keywords Blockchain · Distributed ledger · Know-your-customer · Anti-money-laundering · Initial coin offering · Compliance-by-design · Design science research

1 Introduction

Initial coin offerings (ICOs) constitute a novel mechanism, typically used for the funding of highly innovative ventures that issue and sell virtual tokens to a crowd of investors (Fisch 2019). While ICOs share similarities with conventional crowdfunding, the differentiating feature is the use of blockchain technology, providing a decentralized database and a distributed software architecture that enables the direct exchange of money against tokens without the need of financial intermediation (Notheisen et al. 2017). Given the disruptive potential brought along by the blockchain-based funding mechanism, ICOs attracted a massive influx of investments summing up to US $7,8 billion in 2018 alone (ICOData 2019). To put this into context, the world's largest reward-based crowdfunding platform, Kickstarter, raised about US $3.4 billion from inception through to April 2018 (Adhami et al. 2018).

While peer-to-peer crowdfunding steers investment, the capability to conduct pseudonymous transfers through non-

Accepted after two revisions by Jörg Becker.

Electronic supplementary material The online version of this article (https://doi.org/10.1007/s12599-020-00677-6) contains supplementary material, which is available to authorized users.

N. K. Ostern (✉)
Frankfurt School of Finance and Management, Adickesallee 32-34, 60323 Frankfurt, Germany
e-mail: nadine.ostern@wiwi.uni-marburg.de

J. Riedel
Technical University Darmstadt, Mornewegstraße 23a, 64293 Darmstadt, Germany
e-mail: uni@j-riedel.de

face-to-face relationships (FATF 2018) attracts the attention of legal authorities (Fridgen et al. 2018; Arnold et al. 2019). In particular, its virtuality and the variety of possible token designs give authorities a hard time enforcing tax and bank laws (Arnold et al. 2019), thereby considerably increasing the risk for large-scale money laundering schemes and terrorist funding (European Union 2018; FATF 2018). European legislators reacted to this situation by updating the European Anti-Money-Laundering (AML) regulations, amending the current legal framework to specifically address money laundering risks of ICOs (Haffke et al. 2019). Coming into force in 2020, EU-based companies wanting to raise funds via ICOs need now to ensure customer due-diligence measures by implementing appropriate Know-Your-Customer (KYC) processes (Haffke et al. 2019).

Given these developments, this paper is dedicated to identify KYC-requirements in order to develop a compliant-by-design, blockchain-based KYC-system integrated into the investment flow of an ICO. Compliant-by-design means that we use regulations as input to design a system that automatically enforces KYC-requirements or otherwise terminates the ICO investment process (Lohmann 2013). From a technical point of view, designing a blockchain-based KYC-system for ICOs is straightforward given a common technological backbone; however, we first need to identify requirements for ICOs that affect the KYC-system design, which automatically enforces requirements. Thus, we ask ourselves: *What are the design requirements for a blockchain-based joint KYC/ICO-system, and how can we meet these requirements in our prototype design?*

To answer this research question, we apply an objective-centered design science research (DSR) approach to identify KYC-requirements for ICOs based on EU-AML regulations as well as German federal regulations (Peffers et al. 2008). We use Germany as one example of an EU member state in which an ICO is conducted and, thus, is subject to federal regulations. By working on the intersection of IS, legal, and computer science research, we contribute to the latest state of research, in which blockchain-based KYC-systems have been suggested but not designed or tested for legal compliance. Consequently, our research attempt is in line with recent recommendations of Hinz et al. (2019), emphasizing that IS researchers need to take care of policy-related topics to ensure the applicability of scientific IT artifacts.

The remainder of this paper is structured as follows: Sect. 2 provides an overview of related work. We then describe our research method and proceed to describe legal requirements and design objectives in Sects. 3 and 4. Section 5 presents the higher-level architecture of the developed prototype as well as implementation details for demonstration purposes. Subsequently, the technical feasibility, legal compliance, and applicability of the KYC-system are discussed in Sect. 6. Eventually, a conclusion is provided in Sect. 7.

2 Related Work

Blockchain technology is frequently proposed to serve as regulatory technology (Gozman et al. 2019), where a formal contract and programming language is used as a tool to enforce regulations automatically (Egelund-Müller et al. 2017; Parra Moyano and Ross 2017). Thereby, processes can be created in such a way that they are compliant-by-design, i.e., regulations are taken as input for process model design so that they automatically enforce the respective rules (Lohmann 2013). The compliance-by-design approach makes subsequent proofs and potential correction of processes unnecessary while ensuring flexibility, i.e., the ability to implement and modify system requirements (Lohmann 2013), which is necessary when considering a field subject to rapid technical and legal developments.

Before we consider KYC-regulations, however, we will seek to provide an overview of already proposed solutions for blockchain-based and, potentially, compliant-by-design KYC-systems on which the intended prototype can probably build. In particular, following vom Brocke et al. (2020), we understand DSR as a method that deliberately builds on and demonstrates how previous design knowledge can be consumed to produce new design knowledge that contributes to existing knowledge within and across research projects.

We, therefore, screened the AIS eLibrary using the keywords (blockchain* OR "distributed ledger*" AND "know your customer" OR KYC*), searching for peer-reviewed articles between 2008 and 2020. This search delivered 40 articles, which were first screened for exclusion criteria (i.e., panel setups, workshops, proposal or research-in-progress, abstract-only) and for whether the articles were actually concerned with KYC-processes. Based on the initial screening, 28 articles remained which determine the KYC-process as a prerequisite for the acceptance and use of ICOs. We commenced with a second round of screening, identifying articles that develop or propose conceptual models, proof-of-works, or prototypes of blockchain-based KYC-systems, excluding papers that only mention the importance of KYC-processes. Notably, this left us with a single article, i.e., Parra Moyano and Ross (2017), who introduce a prototype for a blockchain-based, optimized KYC-system for financial organizations.

Given the scarcity of IS research related to blockchain-based KYC-processes in the AIS eLibrary, we extended the literature search to the computer science and engineering

research domain, applying the same keywords to the IEEE Xplore database. While the AIS eLibrary is one of the most relevant databases and a knowledge base for the IS research domain, we chose to query the IEEE Xplore database to include more technical sources, helping us to identify the foundations on which we can build the envisaged prototype.

This search resulted in 10 articles, 3 of which focus on the design and development of blockchain-based KYC-systems. For instance, Bhaskaran et al. (2018) discuss a shared KYC-process for financial institutions based on blockchain technology, focusing on the implementation of a proposed double-blind, consensus-driven data-sharing model that is built on the Hyperledger Fabric. Developing a sample contract, Sinha and Kaul (2018) propose a KYC-system based on Ethereum, where blockchain is used as a general database on which customer data are encrypted using public–private key cryptography, thus proposing an encryption scheme similar to Bitcoin. Eventually, Kumar and Anand (2020) exemplify the implementation of the blockchain-based KYC-system proposed by Parra Moyano and Ross (2017) while identifying new issues, including a missing token-based incentive for participating members that should help to avoid free-riders.

Comparing the articles identified during the literature review, Parra Moyano and Ross (2017) yet offer the most sophisticated prototype in terms of the technical details presented. We therefore reconstructed and visualized every step of the KYC-process proposed by Parra Moyano and Ross (2017), and discussed its transferability and applicability to an ICO investment flow. While the refined KYC-process was deemed to be suitable to be integrated into an ICO investment flow from a technical viewpoint, it became evident that regulatory issues arise from not yet considering the above-described developments of KYC- and AML-regulations, which might have severe consequences not only for the implementation but also the real-world applicability of a KYC-system. To put this into numbers, a KYC-system that is not compliant with, e.g., European AML-regulations, leads to severe fines that typically amount up to double-digit millions of euros in France and Germany, and single digit millions everywhere else (Kirschenbaum 2018).

Consequently, even if regulatory aspects are typically not in the focus of IS researchers concerned with the design of blockchain-based KYC-systems, we need to consider regulations as they might affect the architecture and the system design of our artifacts. Thus, to ensure the applicability of the envisaged prototype, this paper takes the KYC-system of Parra Moyano and Ross (2017) as an impetus and commences – after describing our method – with the analysis of the laws relevant for the design of KYC-processes, in order to build a compliant-by-design blockchain-based KYC/ICO-system.

3 Research Method

This paper follows the DSR methodology proposed by Peffers et al. (2008), suggesting a six-staged process towards the development of an IT artifact (Fig. 1). Notably, we start with an objective-centered approach toward the development of a blockchain-based KYC/ICO-system, which is triggered by regulatory requirements for the conduct of ICOs and, consequently, leads to the development of design objectives.

The development of design objectives is informed by what Gregor and Hevner (2013) stated as descriptive (Ω) and prescriptive (λ) knowledge. Our Ω-knowledge base covers "what we know already" (Gregor and Hevner 2013) and comprises human phenomena, i.e., money laundering as stated by several reports published by the FATF and the BaFin (FATF 2014,2018; BaFin 2017) and the increasing costs of KYC-processes or, more generally, regulatory compliance for financial organizations (Thomson Reuters 2017a, b). The λ-knowledge comprises – among others – instantiations, i.e., existing systems and processes, which, in this paper, are constituted in the prototype offered by Parra Moyano and Ross (2017).

Using the Ω-and λ-knowledge bases as a starting point, we identified applicable regulations, starting with recommendations issued by the European Securities and Markets Authority (ESMA), which was the first supervisory authority to give an overview of applicable laws associated with the regulation of ICOs (ESMA 2017a). In particular, the ESMA referred to various legal frameworks which could become relevant in the context of ICOs, including organizational and transparency requirements stemming from the Markets in Financial Instruments Directive (MiFID), capital and operational rules from the Alternative Investment Fund Managers Directive (AIFMD), as well as requirements resulting from the Anti-Money Laundering Directive (AMLD) (ESMA 2017a, b). Simultaneously, we screened an advisory letter of the BaFin providing initial guidance on applicable German laws, referring to the German Investment Code, the German insurance supervision act, as well as the German Payment Services Supervision Act (BaFin 2017). Moreover, the BaFin emphasized that issuers of payment and security tokens are explicitly named as applicable to the German Money Laundering Act (GwG), meaning that they are required to perform due diligence methods for their investors (BaFin 2017).

Using these initial pointers from the ESMA and BaFin, we followed a structured literature review approach (Webster and Watson 2002), i.e., we started a forward

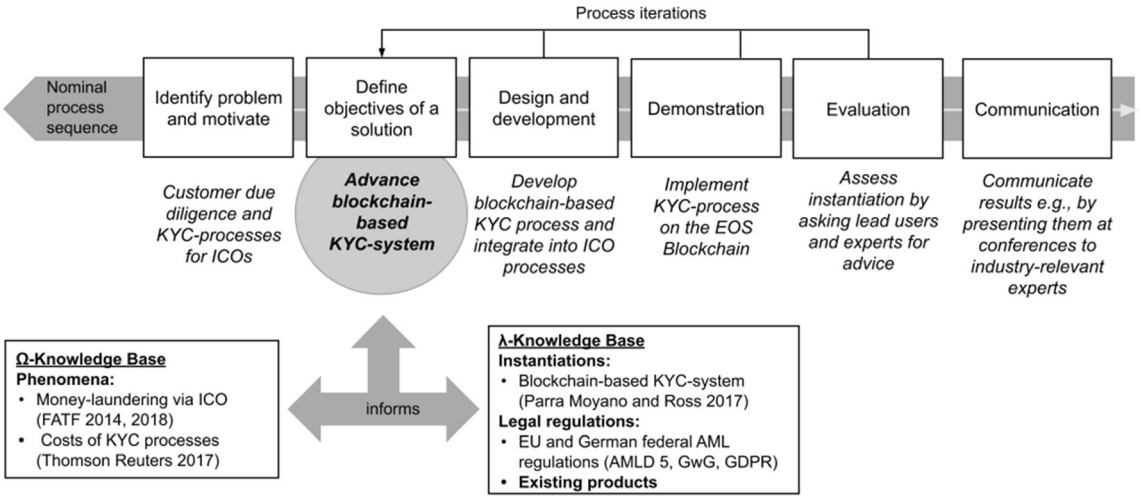

Fig. 1 Design science research process and knowledge bases

search, as backward search was not feasible due to the timeliness of the emerging regulatory assessment of ICOs. To this end, both authors independently screened the regulations and assessed them in terms of their relevance and urgency for the KYC/ICO-system design, determined by the expected penalty for companies in case of non-compliance. The identified regulations were discussed between the authors until a preliminary set of regulations was reached. Thereby, the AMLD5 and GwG were identified and classified as particularly important for the development of the KYC/ICO-system.

We analyzed each article of the identified regulations and translated them into design objectives, these being discussed and adapted by the authors in four discussion rounds, which amounted to 2 months for the identification and translations of regulations into initial design objectives. Thereby, we first agreed on the formulation of system design objectives for each article and then began to merge objectives whenever possible. Afterwards, the high-level architecture for the prototype was designed by the second author, and both authors discussed the results during two discussion rounds within one month, including discussions on issues such as the verification method for identity data as well as identity data storage locations. Eventually, the process steps were developed and depicted using a sequence diagram, and the interface was designed for demonstration purposes, which lasted three months. Following the approach of Chatterjee et al. (2005), we presented implementation details as well as the interface design to demonstrate and subsequently to evaluate the blockchain-based KYC/ICO-system. Thereby, a Tech-Startup supported the prototype development phase by providing us with an eID-system, which we integrated into our developed KYC/ICO-system, as well as by being available for questions concerning the concrete implementation of processes steps, the creation of the sequence diagram, and the user interface.

Having developed the initial version of our prototype, two rounds of evaluations were conducted, which each lasted for two months and included the consultation of lawyers, IT-experts, and potential users of KYC/ICO-system. Finally, we will communicate our results not only in this article but strive toward the dissemination of our results among both IS researchers and practitioners. To this end, we will disseminate our work additionally through presentations at practice-oriented conferences, especially those with a focus on financial services or a regulatory focus.

4 Requirements Analysis and KYC/ICO-System Design

This section starts by discussing legal requirements and corresponding design objectives. Note that these already include the final set of identified regulations, including adjustments from the ex-ante evaluations. For instance, the EU General Data Protection Regulation (GDPR) was deemed relevant during the first evaluation phase due to enhanced due diligence requirements by the AMLD5, leading to additional design objectives. While we will explain the evaluation process in Sect. 6, we consider it relevant at this point to mention all regulations that have been incorporated into the design of the prototype. Despite legal regulations, it became evident that design objectives will have consequences for further design decisions, even if these do not originate directly from the KYC- or other legal requirements. When these consequential requirements emerge from the analysis of regulations and subsequent design of the process, we call them progressive requirements and present them after elaborating KYC- and other

legal requirements. Progressive requirements, thereby, refer to design decisions made to preserve the applicability and functionality of the ICO investment flow from the perspective of an emitter or investor while legal requirements are automatically enforced.

4.1 Legal Requirements and Design Objectives

Designing a compliance-by-design approach necessitates gathering profound knowledge on regulations with which processes need to comply (Lohmann 2013). We, therefore, analyzed the AMLD5, which comes into force in 2020 and requires companies that want to raise funds via ICOs to take action in order to comply with EU-regulations as well as federal regulations, to which the EU-Directive refers. This paper assumes that an ICO is conducted in Germany, making it not only subject to EU-regulations but also federal laws, among others the GwG, which is the German equivalent to AMLD5. In the following, we discuss legal KYC-requirements that are summarized and transferred into design objectives, as shown in Table 1. In total, we identified six legal requirements relevant for a KYC/ICO-system that are briefly described in the following.

Article 8 of the AMLD5 specifies that proper due diligence measures need to be applied when a business relationship between an ICO emitter and an ICO investor is established, i.e., if money and tokens are exchanged. AMLD5 thereby refers to federal law and regulations in the internal market (European Union 2018). In line with the GwG, identity verification of an ICO investor needs to be conducted using electronic identification and trust service for electronic transactions compliant with the so-called eIDAS regulation. EIDAS deals with the EU-wide acceptance of national identity verification schemes. We refer to the German eID-scheme as an example, which is notified as eIDAS compliant since the 22nd August 2017 (BSI 2017).

Furthermore, the GwG requires that data on business relationships and transactions must be kept for five years, especially transaction receipts, if they are necessary for the analysis of transactions. § 10 GwG explains the general due diligence requirements for this case (BMJV 2019), for which it is also essential to identify the contracting party (BMJV 2019). One possibility to verify an identity is the identification using an electronic verification scheme as described by § 18 of the Personal Identification Act [§12(1) GwG], which refers to the aforementioned German eID scheme. The collected identity should thereby comprise the

Table 1 KYC-, legal requirements and design objectives

No	Source	Requirement	Design objective
Subject: identification and verifying information			
(1)	§ 11(a) EU-AMLD5 Article 8, § 2 GwG	The customer should be identified, and the customer's identity should be verified based on documents, data, or information obtained from a reliable and independent source	Within the KYC-system, the initial recording of identity data must base on information that originates from a person's identity card that is demonstrably verified by German authorities (e.g., through German eID)*
(2)	§ 1 GwG (3), § 11 GwG	Collected identity data should comprise the first name and surname, place of birth, date of birth, nationality, and a physical address	To ensure that all necessary identity data are collected, the KYC-system must be linked to an eIDAS compliant identity verification scheme to provide a rigorous data collection and verification process
(3)	§ 15 GwG (4) sentence 2	For high-value transactions, the source of funds needs to be identified	An investor who transfers more than a pre-defined limit needs to fill in an additional data field during the KYC-process stating information on the source of funds
Subject: data handling			
(4)	§ 6 GwG (2), § 8 GwG	Data on business relationships and transactions, especially transaction receipts, should be kept for the analysis of transactions for five years	Data on business relationships and transactions must be stored at least five years on the local database of one of the contracting parties or on the blockchain, which allows for shared access
(5)	Sect. 3, Article 16 GDPR	It should be possible to correct inaccurate data	An ICO investor must have the opportunity to ask for the correction of inaccurate data. To this end, data captured during the blockchain-based KYC-process need to be stored in a way that allows for revocation
(6)	Sect. 3, Article 17 GDPR	It should be possible to erase personal data	An ICO investor must have the opportunity to ask the KYC-provider and emitter to delete any records of investment progress once the five-year storage obligation (see requirement 5) is over. Data that is stored locally in the KYC-provider's and emitters database must be deleted

*German eID was notified as compliant with EU eIDAS regulation on the 22th August 2017 (BSI 2017)

first name and surname, place of birth, nationality, and physical address in the case of natural persons (BMJV 2019).

Moreover, the German legislation distinguishes between transactions of low risk and high risk for money laundering. In moderate risk cases, simplified due diligence measures can be applied, meaning that it is then sufficient that the proof of identity of an investor is based on documents from credible sources. In contrast, enhanced due diligence measures are demanded if a transaction is especially significant, if the contracting party is a politically exposed person, or if the party is based in a country associated with a high risk for money laundering, according to §15(3) GwG. To assess whether these requirements apply, proper KYC-measures need to be taken before the business relationship is established. One example of an enhanced due diligence measure is to identify the source of funds [§15(4) GwG] (BMJV 2019).

EU regulations concerning data privacy need to be obeyed as well, especially if personal data should be stored temporarily. Notably, since the 25th May 2018, the European General Data Protection Regulation (GDPR) is in force, which regulates the processing of personal data relating to individuals in the EU by an individual, a company, or an organization (European Union 2016; European Commission 2018). According to GDPR, processing entities need to inform the subject which data is collected and how it is used. Furthermore, individuals have the right to ask for information about all personal data saved by an entity (Sect. 2, Article 13, GDPR).

While compliance with these regulations can be met by choosing a blockchain-based approach, there are other data subject rights that are more difficult to integrate in a blockchain-based solution. For instance, GDPR specifies that data subjects have the right to ask for incorrect, inaccurate or incomplete personal data to be corrected as well as the right to demand data-processing entities to erase personal data when it is no longer needed or if the processing is unlawful (Sect. 3, Article 16, GDPR). However, the design principles of a blockchain try to establish immutability of data, meaning that the deletion or correction of data on the blockchain is typically not supported. Thus it is necessary to combine blockchain with off-chain solutions to cope with the requirement of revocation and erasure of personal data as stated by the GDPR (European Commission 2019).

4.2 Progressive Requirements and Design Objectives

The ESMA and the BaFin have both issued alerts to investors, making them aware of the risks associated with investments into ICOs (ESMA 2017a, b). In particular, they state that it is risky for an investor to transfer money to an unknown blockchain address since it is uncertain whether tokens will be received. To encounter this risk, most ICOs are based on smart contracts which eventually ensure that investors receive tokens in exchange for the money transferred. As legal requirements necessitate that KYC-processes are conducted before tokens are exchanged for money during an ICO, typically tokens are not sent to the investor right away. From the perspective of the investor, thus, a maximum of transparency is required to reduce the perceived risks associated with investing in an ICO. To do so, the investor needs to have insights into the current state of the token sale before tokens are provided (e.g., through automatically triggered status updates).

Given the fact that KYC-results are stored on a blockchain, if the identity verification is successful, the KYC-process is expected to be more efficient in terms of money [i.e., due to KYC-verification process cost-sharing among financial organizations (Parra Moyano and Ross 2017)] as well as faster. In particular, if the KYC-process is integrated into the ICO investment flow by storing the KYC results on the blockchain, we expect a faster cycle time compared to a solution where a KYC-process is triggered only after the investment. This is because by integrating the KYC-process, we explicitly declare its completion as a requirement for a token swap. Furthermore, we require that the investor should be able to always complete the KYC-process itself in less than 10 min, because longer waiting times typically lead to displeased users (Elst et al. 2017). Hence, additional to investors' requirement that status updates on the KYC-process need to be available, the KYC-processes should be conducted in a way that speeds up and automates both the KYC- as well as the ICO-process. Notably, this objective is shared by several products on the market, e.g., IdentityMindGlobal (2019) or SumSub (2019).

Eventually, access to KYC-results and investments stored on the blockchain needs to be managed, meaning that investors typically require that their investments are not trackable, i.e., linkable to their identity by third parties (European Commission 2019). Preventing transaction flow analysis, however, can be realized by technical measures (e.g., using an address shuffling based anonymization approach) or non-technical means (e.g., providing guidelines how to make the transaction flow analysis harder) (Khalilov et al. 2018). Linked to the need to manage data is key management, which helps to prevent privacy gaps, but at the same time is aimed at being user-friendly (Thwin and Vasupongayya 2019). Thus, while Parra Moyano and Ross (2017) do not discuss key management, our prototype should facilitate as-easy-as-possible verification as several studies showed that manual, user-centric access control and an immutable access log, as well as attribute-based encryption schemes, might create barriers to use

blockchain-based systems (Thwin and Vasupongayya 2019). Thus, we propose a KYC-system in which users can manage their key over a web interface that allows for privacy-friendly, fast and easy to use communication with parties that are part of the KYC/ICO-process.

Table 2 summarizes the above-explained requirements relevant to the design of our KYC/ICO-system. Together with the legal requirements, summarized in Table 1, these requirements and objectives provide the input for the design of our prototype.

5 Prototype Design and Demonstration

The following section provides an overview of the high-level architecture of the prototype and how involved parties interact with each other.

5.1 High-Level Architecture Features

The ICO investment process is orchestrated by a smart contract running on a blockchain platform. This component handles the financial exchange of the investors' money and emitter tokens, acting as an escrow holder. While the smart contract is already a common component for running ICOs, we propose to integrate the KYC-process with the financial flow by deploying the smart contract on the same blockchain on which the ICO is performed. In particular, the smart contract serves as an intermediary that holds on to the funds until the emitter has finally decided whether the investment is accepted or not. In return, the investor has the guarantee that funds are secured: Either the investor receives tokens or at least gets all invested funds back.

By requiring the KYC-provider to record the status of successful completion of the KYC-process on the smart contract, we achieve a legally compliant solution and offer enhanced transparency to the investor. In particular, the ICO investor uses a web interface to interact with the smart contract. This web interface is used to provide the ICO investor with information regarding the status of the KYC-completion. This increases transparency for the investor as the successful completion of the KYC-process is communicated as a prerequisite for exchanging funds and tokens.

To be compliant with GDPR, the actual identity data of the investor are stored off-chain. This is because an on-chain solution would allow other parties to reuse or copy the identity-related information for potential misuse. Furthermore, these data could not be deleted once stored on the blockchain, which would against provoke a conflict with the GDPR. Thus, data is mutually shared off-chain between the KYC-provider and the ICO emitter. This step necessitates that the ICO emitter trusts the KYC-provider that it verifies the identity of the investor in compliance with the applicable laws. To allow a later correction of the data, we refrained from storing a hash value on the blockchain. While we acknowledge that there exist proposals that allow for a later modification (e.g., Ateniese et al. 2017), public blockchains that are used for ICOs currently lack this possibility.

For this prototype, we assume that the KYC-process is linked to the German eID scheme. Notably, the GwG principally distinguishes between cases where the identity has to be captured in detail (i.e., high-value transactions) and cases where regulations are less strict. For ICOs, however, currently no clear guideline exists for which transaction value eased verification processes are sufficient. Thus, as safeguarding principle, KYC-providers should

Table 2 Progressive requirements and design objectives

No	Source	Requirement	Design objective
Subject: investors privacy and ICO-process transparency			
(7)	Investor	It should not be possible for other people to track the investor in the future	The KYC-system must prevent transaction flow analysis through proper technical and non-technical solutions
(8)	Investor	The investor needs to know in which phase the token sale process currently is and when tokens will be provided	The KYC-system must provide status updates of the KYC-process available for the investor
Subject: process design			
(9)	Investor/ICO emitter	The ICO investor should not manually conduct public/private key management	The KYC-system should allow key management facilitated via a web interface; proper incentives for investors need to be set
(10)	Investor/ICO emitter/existing products	The KYC-process should be integrated into the investment process and should not take longer than ten minutes to complete	The KYC-process should run on a decentralized, public blockchain solution, which allows parties involved in the ICO to access the results of the KYC-process as fast as possible through the elimination of third parties

strive for a solution that satisfies the highest legal regulations and methods listed in § 15 GwG, of which eID is one possible solution. To communicate with the eID backend server, the investor uses an eID Provider app, which is used to verify the identity without any human interaction. In particular, every identity card that is issued to German citizens and foreigners that live permanently in Germany has an integrated chip that, together with Near Field Communication (NFC) capabilities available for most of today's smartphones, is capable of verifying identities electronically. Hence, if investors own such a phone, they can use their identity card to verify their identity electronically. As the eID system has proven compliant with eIDAS regulation, it can be used for every EU-based ICO.

5.2 Sequence of Process Steps

Figure 2 depicts the high-level architecture of the prototype, indicating the sequence of process steps. We explain the process steps of the combined ICO/KYC-process in the following. For a detailed description of the architecture and process steps, we refer to "Appendix" A (available online via https://springerlink.com), showing a sequence diagram of the KYC/ICO-process according to the UML-standard.

1. The investor starts the ICO-investment and KYC-process by sending a specific amount of money to the smart contract which records the investment. Tokens that the investor is expected to receive in exchange for his money are not transferred to the investor right away. First, the customer's identity needs to be checked, and the ICO emitter needs to accept the investor (i.e., an ICO emitter can refuse to send tokens in exchange for money received if, for instance, a country prohibits ICOs). For this purpose, the smart contract prevents the direct transfer of funds against tokens until the verification process is completed.
2. After the initial transfer of money, the investor needs to verify his or her identity by starting a new identity verifying session by using the ICO Investment Web Interface. This web interface provides information about the status of the investment and the KYC-process to the investor.
3. The investor uses the eID-providers' app, his or her identity card or residence permit, and the secret PIN to prove his or her identity.
4. Once the identity data is proofed via the eID-providers App, it is shared with the KYC-provider that is in charge of verifying the correctness of personal information. The KYC-provider stores the identity data off-chain.
5. After the data is recorded with the KYC-provider, the status, i.e., the completion of the KYC-process, is recorded on the blockchain.
6. The investor uses the ICO investment web interface to ensure that the KYC-process was appropriately recorded.
7. Afterward, detailed identity data needs to be shared with the ICO emitter because the emitter needs to decide whether the investment is to be accepted or not.
8. Depending on the emitter's decision whether to accept the investor, two variants are possible for the last step: If the emitter accepts the investor (8a), the ICO emitter provides the tokens and receives the investment in return. If the investor is denied by the emitt(8b)er, the investor is refunded the invested money. In this case, no token exchange takes place.

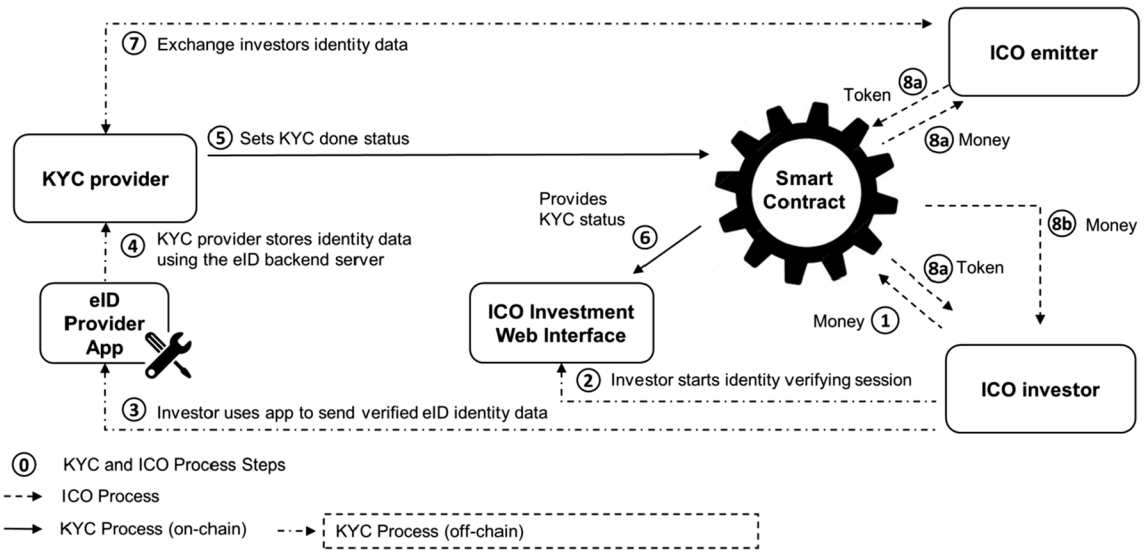

Fig. 2 High-level architecture of the prototype

5.3 Implementation and Demonstration

We implemented the prototype on a decentralized blockchain platform. We compared available public blockchain platforms based on the CCID's Global Public Blockchain Technology Assessment Index published by the Ministry of Industry and Information in China (Das 2019), whose index scores distributed ledger projects in the subcategories basic technology, applicability, and creativity. We required the overall rating of the blockchain to be in the top ten list. Additionally, for integrating the KYC-process into the token/money swap, we expected parties relevant to the KYC/ICO-process to be able to record the state of the investment and the KYC-process, which excludes payment-only blockchains like Bitcoin. We found that both Ethereum and EOS fulfill these criteria.

We developed a cost prediction for these platforms for the prototype presented in Table 3. The table shows which and how many resources are consumed per process step. As both blockchains use different cost models, the corresponding units for the different consumed resources are given as well, with costs per unit based on average prices in the time frame 01.07.2018–30.11.2018.

Based on these considerations, EOS turned out to be less expensive, i.e., identity verification costs U.S.$ 0.09per investor. Furthermore, while Ethereum requires the investor to cover all costs of the investment process, EOS allows sharing the costs incurred by the used platform resources. Therefore, we decided to build our KYC/ICO-system on the EOS platform. However, there are no technical reasons why a similar system could not be developed on the Ethereum platform as well.

Figure 3 shows the main user interface of the prototype. The user interface is split into three areas for the different user groups and technical components, i.e., investors, emitter, KYC-provider, and the smart contract. Notably, in a real scenario, a user only gets to see one interface, as a user typically has only one role.

An investment is started as soon as the investor starts the KYC/ICO-process by entering the EOS username into an input field, which is "investor1" in Fig. 3. A click on "update" will show the investor's current balance. If there is currently no investment, an input field appears where the number of EOS coins can be chosen. As soon as the investor clicks on "invest EOS," the coins are transferred to the account of the smart contract. A click on "update" in the box of the smart contract will show that the balance of the contract has increased by the amount that has been invested. After the coins are transferred, the UI asks the investor to start the KYC-process, as shown in the investor's box in Fig. 3. If the investor clicks on the link, the web page is opened, providing a QR code that needs to be scanned using the eID-Providers App (Fig. 4, left picture). For our prototype, we used an existing eID system provided by a Tech-Startup, which also supplies the app. If the invested amount of funds exceeds a predefined threshold, the app requires the investor to enter information on the funds' source (e.g., by writing a statement or by attaching documents that prove the source of funds). After the investor has entered the PIN of his identity card, the card is connected to the phone so that communication via NFC can take place.

Once the KYC-process is finished, the app shows a TAN which needs to be entered on the website. The EOS

Table 3 Cost estimation for the prototype for Ethereum and EOS

Step	Costs for Ethereum	Costs for EOS
Investor sends funds to smart contract	21,000 gas for transaction + 20,000 gas for storage	0.3 KiB RAM 0.132 KiB/Day Network 1.035 ms/Day CPU
Investor finishes KYC and claims KYC-token	21,000 gas for transaction + 5,000 gas for storage update	0.117 KiB/Day Network 0.471 ms/Day CPU
KYC-provider sets KYC "Done" flag	21,000 gas for transaction + 5,000 gas for storage update	0.103 KiB/Day Network 0.600 ms/Day CPU
Emitter sends token, receives back money	3 * 21,000 gas for transactions	0.134 KiB/Day 3.070 ms/Day CPU
Refund after investment done	− 15,000 gas for deleting data entry	− 0.2 KiB RAM − 0.486 KiB/Day Network − 5.176 ms/Day CPU
Total of required resources	141,000 gas	0.1 KiB RAM
Costs per unit	19.169 Gwei per gas, 1 Gwei = 0.000 000 2766 $	0.88 $ per KiB
Total costs per accepted investor	0.75 $	0.09 $

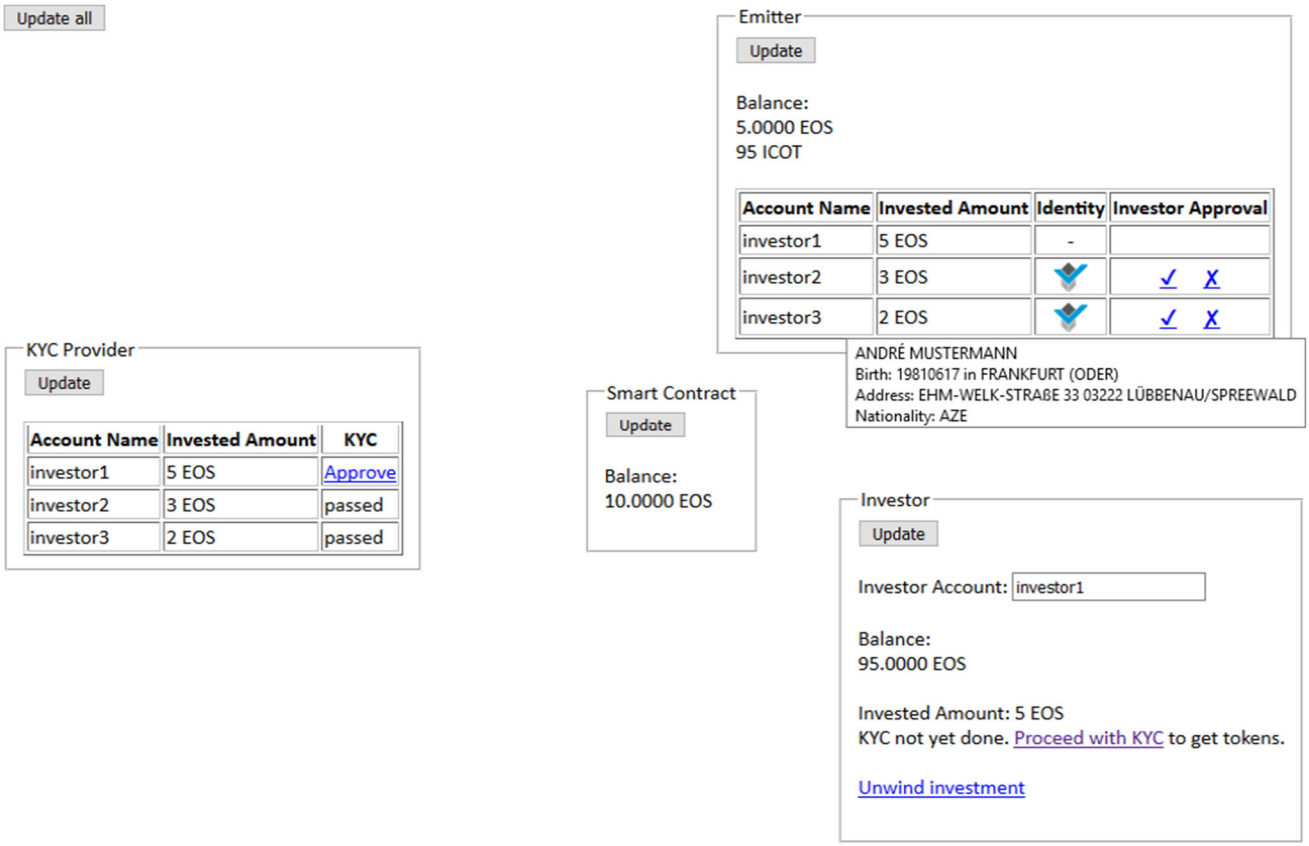

Fig. 3 Screenshot of the main user interface (identity data are shown once the mouse hovers over the icon in the "identity" column)

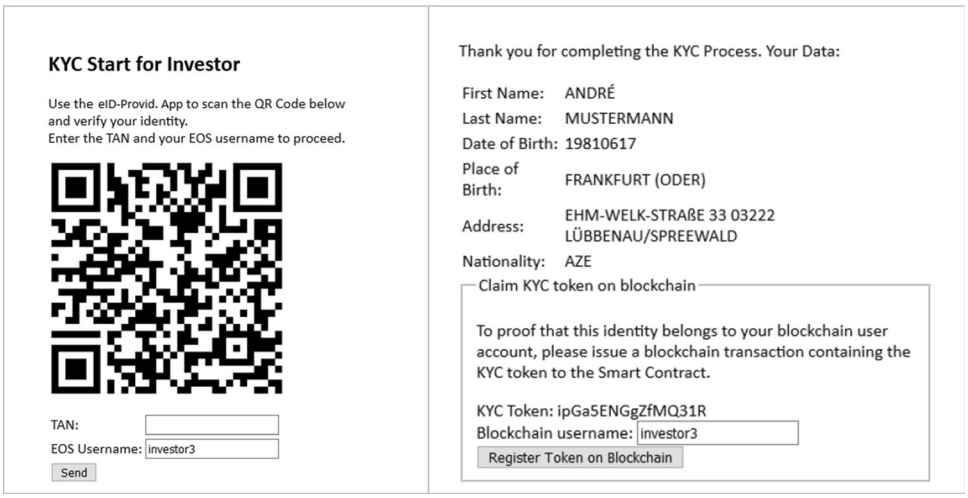

Fig. 4 Start and end of the KYC-process for the ICO investor

username will be captured as well so that the KYC-provider already knows which user will claim the captured identity. However, since the investor has not yet used his or her blockchain private key to sign a transaction, the KYC-provider cannot be sure yet that the entered username belongs to the captured identity. After the investor has inserted the TAN from the app and the EOS username, a click on "send" will lead to the screen shown in Fig. 4 (right picture). There the investor can see all of the data that have been read out from the card. These data are already stored in the off-chain database of the KYC-provider but are not yet connected to an EOS username. A connection is established by registering the "KYC-Token," which is generated randomly by the KYC-provider and references a single identity data set. The investor now

sends a blockchain message to the smart contract with this token inside.

The advantage of sending this message on the blockchain is that it has the investor's signature, which ensures the authenticity of the message. It is possible to send this message with a click on the button "Register Token on Blockchain." After the click, the investor is informed that the KYC-process window can be closed. In the main UI of the prototype, a click on "Update" in the investor box will now report that the KYC-process has successfully been carried out. As long as the emitter has not provided the tokens, the investor can unwind the investment at any time. This will trigger a transfer of the initially invested EOS amount from the smart contract back to the investor.

The emitter sees a table with all investments that have been made into the ICO in the main UI, as shown in Fig. 3. In the example, "investor1" has not yet completed the KYC-process. In contrast, "investor2" and "investor3" have already completed the KYC-process, which means that their investment is ready for acceptance. The emitter can hover over the blue icon to see the identity data of an investor. If the investor is accepted, a click on the checkmark triggers a swap. The ICO tokens ("ICOT" in the example) are then transferred to the smart contract by the emitter, that forwards the tokens to the investor. At the same time, the smart contract sends the EOS coins to the emitter. Eventually, all data regarding the investment (investor, invested amount) is deleted from the list of ongoing investments in the smart contract.

6 Evaluation

In this section we evaluate the developed prototype of a blockchain-based KYC/ICO-system. Notably, we conduct requirements as well as applicability checks to assess both the rigor and relevance of the developed KYC/ICO-system (Rosemann and Vessey 2008). We summarize this process in Table 4.

6.1 Legal and System Design Evaluation

To assess the rigor of the developed prototype, we conducted two types of assessments, on the one hand one regarding legal requirements and, on the other, a system design check. Whereas the first serves as a tool to ensure that all relevant legal requirements are considered, meaning that the developed KYC/ICO-system uses the right regulations as input, the latter ensures that the system is technically feasible and compliant-by-design. The consultations with lawyers were not audio-recorded due to legal reasons, therefore the reported feedback described in the following is based on conversation notes.

The first round of the legal requirements check was conducted during two 1-h consultations each with a lawyer experienced in the conduct of ICOs, including necessary KYC-processes which were identified through an Internet search. After having outlined the objectives of our prototype, we explained the process with which we had identified regulations and the resulting set of legal requirements and objectives. We asked the lawyer for an assessment concerning whether or not the identified regulations were appropriate and complete given the legal situation. During the consultation, it was pointed out that given the preliminary information provided by the BaFin, a final statement on the completeness of regulations can only be made for the time being. Additionally, it became evident that potential violations of the GDPR may arise due to the implementation of AML-regulations, especially the increased due diligence requirements. This insight triggered the renewed start of the requirement search focusing on GDPR and related regulations. Using forward search, relevant requirements related to the privacy of ICO participants were identified and subsequently translated into design objectives, leading us to the final set of ten objectives presented previously (Table 1). The second consultation with the lawyer in the first evaluation round led to minor linguistic adaptations as well as to the approval of the completeness of privacy-related legal requirements.

We conducted a second round of evaluation focusing on the legal requirements by approaching two additional lawyers as recommended by the first lawyer. We conducted separate interviews which lasted 1 h and 0,5 h respectively, again explaining the KYC/ICO-system and asking for their assessment concerning the completeness and appropriateness of the identified regulations. While both lawyers agreed on the completeness and appropriateness of the identified regulations and design objectives, one lawyer stressed the provisional nature of these findings. In particular, the lawyer stressed that it is essential to have the possibility of adapting rules, and thus smart contracts, fast and conveniently as the legal situation can change quickly. Moreover, it was discussed that, at the moment, the prototype is only compliant-by-design for the European and mainly the German legal area.

Including these objections in the technical evaluation, we performed two rounds of system design evaluation by IT-experts, the description of which can be found in Table 5. These experts were not previously involved in the construction of the artifact (Frank 2007) and had considerable experience in designing identity solutions in the context of KYC-systems. The experts were identified using snowball sampling, i.e., we used recommendations from each of the identified experts, with the supporting Techstartup recommending the first expert. While we are aware that this method could lead to biases in some cases, it was

Table 4 Evaluation process and criteria

Evaluation purpose	Evaluation step	Evaluation criteria	Iterations and participants	
			Round 1	Round 2
Rigor	Legal requirements and system design check	Relevance and completeness of legal requirements	Interview with 1 lawyer (2 consultations)	Interviews with 2 lawyers (1 consultation each)
		Appropriateness of design objectives		
		Fulfillment of requirements (1)–(10)	Interviews with 3 IT professionals (for details, see Table 5)	Interviews with 2 IT professionals (for details, see Table 5)
		Technical feasibility of automatic rule enforcement		
Relevance	Applicability checks	Importance	Interviews with 16 potential users (1 interview each)	
		Accessibility		
		Suitability		

Table 5 Descriptive characteristics of IT-experts

Round	Professional background	Organizational position	Years of experience (in the field of work)	Frequency of consultation
1	Engineer	C-level manager	13	1
	Computer Scientist	C-level manager	4	2
	Computer scientist	Software Lead developer	12	4
2	Engineer	Software engineer	6	1
	Computer scientist	Software developer	3	1

deemed appropriate given the few IT-experts who possess a comprehensive understanding of both the conduct of ICOs and KYC-processes.

We explained the KYC/ICO-system objectives as well as graphical representations (i.e., the high-level architecture, sequence diagram, and the interface) to the experts, asking for their assessment. We conducted semi-structured interviews that were audio-recorded, transcribed, and coded subsequently (Wolfswinkel et al. 2013). Importantly, we informed the experts that we seek honest expert evaluation which provides us with advice on how to improve the prototype.

The results of the system design evaluation are summarized in Table 6. According to the results of the evaluation, the prototype is capable of enforcing five out of ten requirements related to the identification and verification of information, process design, and KYC/ICO-process transparency. We marked automatically enforceable objectives in Table 4 using an"F," indicating that these objectives are compliant-by-design. Partially fulfilled objectives refer to objectives and associated rules that can be technically enforced, which were however not yet sufficiently legally specified, i.e., the threshold for large funds was not specified up until the current date, or rules required the enforcement of regulations beyond the KYC/ICO-systems boundaries, e.g., the global deletion of personal data on local servers.

During the interviews, experts claimed that three objectives could not be enforced, e.g., we were not able to deploy the fourth legal requirement, stating that data on business relationships and transactions should be kept for a subsequent analysis for five years. Moreover, while the transaction log of blockchain makes a receipt of the token-money swap accessible, there is no mechanism implemented that stores the captured identity of approved or denied investors in order to avoid investor tracking and, especially, transaction flow analysis. Thus, a full transaction record, including not only information on the amount of money and tokens transferred but also identity-related information, is not intended due to privacy protection regulations (European Commission 2019). This issue becomes even more relevant when looking at proposed solutions to avoid transaction tracking and to protect investors' privacy. Khalilov et al. (2018) analyze tools that strive toward improving ICO investors' privacy based on, for instance, decryption mix-nets, fair exchange protocols, or zero-knowledge proofs, but the majority of these solutions are still in their conceptual development phase.

Also, blockchain technology typically supports only pseudo-anonymous transactions, which means that identities of the transacting parties are not known to the public. Consequently, recording investors' identities along with the funds is a task left to the ICO emitter, who is expected to implement a document management system with which he or she may support transaction analysis. The main issue here, however, is that of interoperability. Future research should thus focus on how we can create interfaces to combine blockchain and other centralized or decentralized infrastructures to maximize efficiency and cost-saving potentials of blockchain-based KYC solutions.

Lastly, our prototype ensures that the outcome of a KYC-process and information related to an individual cannot be revoked by any party other than the KYC-provider. While we stated this requirement before the development of our prototype, the implementation of these features requires a careful evaluation of possible permission structures and the development of a governance framework. While this was out of scope for this research project, IT-experts emphasized that future research needs to develop governance structures that support KYC and ICO-processes on a public blockchain while distributing permission rights in such a way that, as far as possible, no single party involved in the joint KYC/ICO-process can change data unnoticed. At the same time, the current legal situation requires that state authorities verify identities. Thus, while complete decentralization might be technically feasible (Parra Moyano and Ross 2017), the legal situation requires partial centralization, i.e., a trusted authority responsible for verifying identities and for deciding upon the success of the KYC-process. Given the current European and, in particular, German jurisprudence, the blockchain-based KYC-system proposed in this paper, consequently, allows as much decentralization as technically *and* legally possible.

In our second round of the technical evaluation, we received the feedback to analyze the coding of the smart contract from a security perspective, as cases of lost funds have resulted from smart contract design issues in the past. Thus, we performed a security assessment by checking for common pitfalls in smart contract coding (Atzei et al. 2017). One of the flaws identified relates to the fact that KYC-providers map the captured identity data and the corresponding blockchain username only by trusting the saved KYC-token found in the smart contract. A malicious miner could steal the KYC-token that a user was about to enter and could himself claim this token by adding the

Table 6 Requirements and design objectives evaluation (Status (Stat.): F – fulfilled, PF – partial fulfilled, NF – not fulfilled)

No	Stat	Remarks/limitations
Subject: Identification and verifying information		
1.	F	We addressed this need by linking our prototype to the German identity card and the respective backend server, i.e., base our approach on data that is verified by authorities. This approach also ensures the accuracy of the data
2.	F	There are rare cases in which authorities do not have all the information. In this case, Objective 2 cannot be fulfilled
3.	PF	If funds exceed a certain threshold, the eID Provider's App requires the investor to make a statement on the source of funds or add corresponding documents. There is no legal rule what is deemed sufficient for this. Thus the emitter needs to decide whether the information is adequate or not
Subject: data handling		
4.	NF	While the transaction as such is stored on-chain, information on the emitter or investor is not. Enriching the KYC-process with additional information is an implementation task for the emitter, who is expected to have an off-chain document management system
5.	NF	Currently, the prototype does not provide data processing. From a technical viewpoint, however, the implementation of permissions to modify personal data can be easily implemented
6.	PF	An investor can ask the KYC-provider and ICO emitter to delete personal data after the five-year storage obligation has expired. Automated enforcement mechanisms cannot be implemented. Transaction-related information cannot be deleted without significant expenditure
Subject: investors privacy and KYC/ICO-process transparency		
7.	NF	No technical solution is available yet that prevents the privacy violations – possible solutions are currently in the development phase, but not applicable to web services, see, for example, Khalilov et al. (2018). GDPR prevents the KYC-provider and ICO emitter from tracking future investments. The investor can implement precautions, e.g., use token mixers or different storing wallets
8.	F	Investors can quickly inform themselves about the status of the KYC and investment process using the app. The completion of the KYC-process is a prerequisite for the token-money swap between an investor and an emitter
Subject: process design		
9.	F	Public/private key management is handled via the ICO investment web interface, providing a one-click solution
10.	F	The process of downloading the eID provider's app, scanning the QR-Code on the website of the KYC-provider, entering the PIN, attaching the identity card, and finally entering the TAN is estimated by experts to be completed in less than 10 min

KYC-token to the information of his investment. Then the KYC-provider would erroneously assign the captured off-chain identity data to the blockchain account of the miner instead of to the one of a legitimate investor.

We addressed this issue by adding off-chain information from the investor to the KYC-provider containing the investor username. This way, the KYC-provider can check whether the KYC-token found in the smart contract on-chain belongs to the same investor name transmitted off-chain. The on-chain information is taken into account because of the proven message authenticity by the investor. Another improvement for the coding was an added warning if a smart contract is fraudulently used to emulate an investor, which possibly leads to attacks because of limited computing resources. Furthermore, we ensured that status checks and status updates in the coding are always performed before funds or tokens are transferred to prevent reentrancy or unpredictable state attacks.

6.2 Applicability of KYC/ICO System

We assessed the relevance of the designed KYC/ICO-system, conducting an applicability test (Rosemann and Vessey 2008). We conducted 16 semi-structured interviews with potential users of the KYC/ICO-systems, focusing on ICO investors who had already experienced a KYC-verification process. Our interview partners were mostly male (68%) and participated on average in 3 ICOs. Before the interviews started, we explained the objectives and the design of the KYC/ICO-system to participants, laying special emphasis on how they would interact and use the system once it was implemented. Doing this, we constantly made sure that the interview partner understood the basic functionalities and the objectives of the designed KYC/ICO-system. During the interviews, we asked participants whether the designed KYC/ICO-system is *important*, i.e., tackles key issues when investing via ICOs, whether it addresses a real-world problem, and if it is timely (Rosemann and Vessey 2008). Second, we evaluated whether the designed solution is *accessible*, i.e., whether the design is understandable and outcomes, e.g., the user interface, are perceived as usable. Third, we asked for the assessment of the prototype's *suitability,* i.e., whether the designed KYC/ICO-system is perceived to be a solution to the problem at hand. Eventually, it was emphasized that there were no right or wrong answers and that the goal of the interview was to assess the relevance of the prototype from the users' perspective.

The evaluation of the interviews indicated the relevance of the developed solution from the user's perspective. 75% of the interview partners reported slow identity checks when registering on platforms or websites based on which users can trade and invest in ICOs, with the main problem being that identity checks had to be repeated several times due to technical problems leading to non-identifiability. 25% even claimed to have aborted the process, as the re-verification of the identity verification was either too time-consuming or – with 16% of the interview partners – led to distrust. 38% of the interview partners stated that they had problems connecting their trading activities with their bank account, as the bank terminated such a connection for security reasons. Overall, the majority of respondents (94%) indicated that they would use a KYC/ICO-system offered by financial organizations to verify their identity if the system solved the problems mentioned above, i.e., ensured speed and reliability of identity verification.

Potential users were less clear in terms of their assessment of the accessibility of the designed ICO/KYC-process. While 56% of the participants stated that they generally appreciated a solution based on QR codes given the ease of use with which the identity can be proofed, 13% were worried about the security of the system. While security checks must be in place, especially at interfaces (and have to be further developed and checked when the prototype is implemented), 19% of interview partners, claimed that a solution in cooperation with eID-providers which are compliant with eIDAS regulation increase confidence in the security of the ICO/KYC-system in general. Moreover, 44% of the interview partners stated that while they generally thought that the demonstrated system seemed to be intuitive to use, they would have to use the system on their laptop or mobile phone when investing in an ICO for a final evaluation.

Lastly, we evaluated the suitability of the designed KYC/ICO-system by asking whether the designed solution was perceived to actually solve problems of ICO investors. Our interview partners were quite clear about this point, i.e., 94% claimed that the proposed system was suitable to solve identity verification issues assuming that the system works as described, i.e., that no major technical problems occur and that the implementation of identity verification works rapidly and reliably. In fact, potential users stated that they perceived the solution as especially suited as it reduced the complexity for the user, while potentially reducing the costs for KYC-processes depending on the amount of participating financial organizations. Thereby, 19% of the interview partners primarily see financial organizations in the responsibility to take care of proper KYC-verification processes, meaning that KYC-processes are demanded to be fast, reliable as well as connectable with ICO processes by integrating innovative solutions. Thus, the majority of interview partners perceived the proposed KYC/ICO-system as suitable to solve experienced issues, assuming the faultless functioning of the prototype once fully implemented.

7 Limitations

This paper proposes a joint KYC/ICO-system that strives for compliance-by-design with the recently updated regulatory provisions of the European Union (European Union 2018) concerned with customer due diligence duties and the prevention of money laundering. To this end, we performed a requirement analysis of EU and German regulations that served as design objectives for the envisaged KYC/ICO-systems. While we see contributions made by this paper mainly arising from research at the intersection of information system design and legal issues, we need to view our results in the light of its limitations.

First, we did not manage to implement all objectives stemming either from not yet fully developed regulations or, most importantly, from other pieces of legislation that prevent the implementation of objectives. While we acknowledge that especially the latter limits the automation of compliance, we argue that these conflicts are in the realm of lawyers and the government who need to take on a clearer stance when it comes to conflicting regulations. Having said this, we admit that the presented KYC/ICO-system is a snapshot of the current legal situation, meaning that objectives and, consequently, the system design need to be adapted to possibly changing KYC/AML and ICO-regulations that can evolve over the next years. The same applies to the currently proposed combination of on- and off-chain solutions, whereby the current data handling solution must be subject to a constant review of further technical developments of blockchains.

Second, the evaluation of the prototype builds on experts' assessment of the objectives as well as the system design. Experts capable of assessing compliance for a KYC-system in the context of an ICO are scarce, meaning that the evaluation of the legal objectives and compliance-by-design resides on assessments of nine experts. While we acknowledge that for a typical IT artifact the amount of experts assessing a system should be larger, we lay special emphasis on the quality and capability of experts assessing our KYC/ICO-system, which is why we deem the evaluation to be adequate for the time being. While the same holds for the applicability checks, we however see the need to implement the system in a real-world context in order to conduct further evaluations.

While the designed KYC/ICO-system is a blueprint for a compliant-by-design KYC-system that might also be applied to other contexts than ICOs, future work needs to focus on the implementation of a system used by multiple financial organizations. During this work, several further questions can and need to be answered, including whether and how the KYC/ICO-system can be implemented into existing infrastructures of financial organizations and what issues need to be dealt with, especially focusing on potential security issues that emerge at interfaces. Second, while applicability checks have been made with potential users, further research needs to assess the applicability of the KYC/ICO-system focusing on financial organizations. While we are convinced that the assessment of users is equally important, due to arising network effects, applicability checks with financial organizations might yield further insights. The assessment of financial organizations, thereby, potentially affects the design of governance rules, including decision rights, accountability, and incentives (Beck et al. 2018) that need to be designed and tested before and post-implementation.

The need to specify governance rules and incentives leads to the third limitation of this paper, which is that we currently cannot assess the exact pecuniary benefits of using a KYC/ICO-system. While it would be possible to theoretically approximate these costs (Parra Moyano and Ross 2017), exact calculations require insights into the actual cost structure of organizations' KYC-processes. While this is out of the scope for this paper, we see the necessity to tackle this issue before implementing the system in real-world settings. Additionally, a comprehensive evaluation of the added value would require to assess alternative solutions, which also includes the assessment of other than blockchain infrastructures. While this might be especially important if we strive for compliant-by-design KYC-systems that are not designed for the conduct of ICOs, we argue that for a joint KYC/ICO-system, the blockchain probably provides the most efficient solution due to a minimum of interfaces and media discontinuity.

8 Conclusion

This paper uses design science research to develop a compliant-by-design blockchain-based KYC-system that is integrated into the investment flow of an ICO. While we provide insights into the system design, the main contribution of this paper is the identification and integration of legal KYC-requirements that are used as input for the design of the KYC/ICO-system. We design a prototype that promotes the development of legally secure blockchain-based KYC-systems and provides a starting point for future research, especially toward the development of governance and legal frameworks for decentralized KYC-systems based on blockchain technology. While we are convinced that the system is transferable to other contexts, we see further work emerging around the issue of designing governance rules as well as for the further evaluation of the rigor and applicability of this or future versions of the prototype, referring to both participating financial organizations as well as ICO investors.

Acknowledgements The company AUTHADA contributed to this work through ideational support. No financial support was received.

Funding Open Access funding enabled and organized by Projekt DEAL.

Compliance with ethical standards

Conflict of interest The authors declare that they have no conflict of interest.

References

Adhami S, Giudici G, Martinazzi S (2018) Why do business go crypto? An empirical analysis of initial coin offerings. J Econ Bus 100:64–75

Arnold L, Brennecke M, Camus P et al (2019) Blockchain and initial coin offerings: blockchain's implications for crowdfunding. In: Treiblmaier H, Beck R (eds) Business Transformation Through Blockchain. Palgrave Macmillan, Basingstoke, pp 233–271

Ateniese G, Magri B, Venturi D, Andrade ER (2017) Redactable blockchain—or—rewriting history in bitcoin and friends. In: Proceedings 2nd IEEE European symposium on security and privacy, EuroS and P 2017

Atzei N, Bartoletti M, Cimoli T (2017) A survey of attacks on Ethereum smart contracts (SoK). In: Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)

BaFin (2017) Initial coin offerings: Hohe Risiken für Verbraucher. https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Fachartikel/2017/fa_bj_1711_ICO.html. Accessed 19 Jun 2019

Beck R, Müller-Bloch C, King JL (2018) Governance in the blockchain economy: a framework and research agenda. J Assoc Inf Syst 19:1020–1034

Bhaskaran J, Ilfrich P, Liffman D, et al (2018) Double-blind consent-driven data sharing on blockchain. In: IEEE International Conference on Cloud Engineering (ICE2), pp 1–7

BMJV (2019) Money-Laundering Act. https://www.gesetze-im-internet.de/gwg_2017/. Accessed 5 Jul 2019

BSI (2017) eIDAS-Notifizierung der Online Ausweisfunktion. In: Fed. Off. Inf. Secur. https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/ElektronischeIdentitaeten/Online-Ausweisfunktion/eIDAS-Notifizierung/eIDAS-Notifikation_node.html. Accessed 29 Jun 2019

Chatterjee S, Tulu B, Abhichandani T, Li H (2005) SIP-based enterprise converged networks for voice/video-over IP: implementation and evaluation of components. IEEE J Sel Areas Commun 23(10):1921–1933

Das S (2019) TRON ranks #2, way ahead of bitcoin in china's latest crypto rankings. In: CCN News. https://www.ccn.com/tron-eos-bitcoin-china-crypto-rankings/. Accessed 22 Mar 2020

Egelund-Müller B, Elsman M, Henglein F, Ross O (2017) Automated execution of financial contracts on blockchains. Bus Inf Syst Eng. https://doi.org/10.1007/s12599-017-0507-z

Elst RV, Heckel M, Vauclin N (2017) Digital onboarding for financial services – customer survey, https://www2.deloitte.com/content/dam/Deloitte/lu/Documents/technology/lu-digital-onboarding-financial-services-digital-natives-112017.pdf. Accessed 23 Mar 2020

ESMA (2017a) ESMA alerts firms involved in initial coin offerings (ICOs) to the need to meet relevant regulatory requirements https://www.esma.europa.eu/document/esma-alerts-firms-involved-in-initial-coin-offerings-icos-need-meet-relevant-regulatory, Accessed 16 Jul 2019

ESMA (2017b) ESMA highlights ICO risks for investors and firms. France, Paris

European Commission (2018) Neue Regeln für die grenzüberschreitende Verwendung elektronischer Identifizierung. https://ec.europa.eu/germany/news/20180928-elektronische-identifizierung_de. Accessed 5 Jul 2019

European Commission (2019) GDPR: rules for businesse and organizations. https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations_en. Accessed 26 May 2019

European Union (2016) Regulation (EU) 2016/679 of the European parliament and of the council of 27 April 2016. Off J Eur Union L119

FATF (2018) FATF report to the G20 Leader's Summit. https://www.fatf-gafi.org/media/fatf/content/images/G20-June-2019.pdf

FATF (2014) Virtual currencies: key definitions and potential AML/CFT Risks. https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf

Fisch C (2019) Initial coin offerings (ICOs) to finance new ventures. J Bus Ventur 34:1–22

Frank U (2007) Evaluation of reference models. In: Fettke P, Loos P (eds) Reference modeling for business systems analysis. Idea Group Publishing, pp 118–140

Fridgen G, Schweizer A, Regner F, Urbach N (2018) Don't slip on the initial coin offering (ICO)—a taxonomy for a blockchain-enabled form of crowdfunding. In: Proceedings of the Twenty-Sixth European Conference on Information Systems (ECIS 2018), Porthmouth, UK

Gozman D, Liebenau J, Aste T (2019) A case study of using blockchain technology in regulatory technology. MIS Q Exec 19:19–37

Gregor S, Hevner AR (2013) Positioning and presenting design science type of knowledge in design science research. MIS Q 37:337–355. https://doi.org/10.2753/MIS0742-1222240302

Haffke L, Fromberger M, Zimmermann P (2019) Virtual currencies and anti-money laundering—the shortcomings of the 5th AML directive (EU) and how to address them. J Bank Regul pp 1–21

Hinz O, van der Aalst WMP, Weinhardt C (2019) Blind spots in business and information systems engineering. Bus Inf Syst Eng 61:133–135

ICOData (2019) Funds raised in 2018. https://www.icodata.io/stats/2018. Accessed 27 May 2019

IdentityMindGlobal (2019) IdentityMindGlobal. https://identitymindglobal.com/. Accessed 5 Jul 2019

Khalilov K, Can M, Levi A (2018) A survey on anonymity and privacy in Bitcoin-Like Digital Cash Systems. IEEE Commun Surv Tutor 20:2543–2585

Kirschenbaum J (2018) Europe needs money laundering penalties that hurt. In: Ger. Marshall Fund United States. https://www.gmfus.

org/blog/2018/09/13/europe-needs-money-laundering-penalties-hurt. Accessed 22 Jun 2019

Kumar M, Anand N (2020) A blockchain based approach for an efficient secure KYC process with data sovereignty. Int J Sci Technol Res 9:3403–3407

Lohmann N (2013) Compliance by design for artifact-centric business processes. Inf Syst 38:606–618

Notheisen B, Hawlitschek F, Weinhardt C (2017) Breaking down the blockchain hype towards a blockchain market engineering approach. In: Proceedings of the 25th European Conference on Information Systems (ECIS)

Parra Moyano J, Ross O (2017) KYC optimization using distributed ledger technology. Bus Inf Syst Eng. https://doi.org/10.1007/s12599-017-0504-2

Peffers K, Tuunanen T, Rothenberger MA, Chatterjee S (2008) A design science research methodology for information systems research. J Manag Inf Syst 24:45–78. https://doi.org/10.2753/mis0742-1222240302

Rosemann M, Vessey I (2008) Toward improving the relevance of information systems research to practice: the role of applicability checks. MIS Q 32:1–22

Sinha P, Kaul A (2018) Decentralized KYC systems. Int Res J Eng Technol 5:1206–1211

SumSub (2019) SumSub. https://sumsub.com/. Accessed 05 Mar 2019

Thomson Reuters (2017a) Reducing the costs of compliance: a bold move towards Know your Customer (KYC) managed services. https://ctmfile.com/assets/ugc/documents/FINAL_Reducing_the_cost_of_compliance.pdf

Thomson Reuters (2017b) Thomson Reuters 2017 Global KYC surveys attest to even greater compliance pain points. https://www.thomsonreuters.com/en/press-releases/2017/october/thomson-reuters-2017-global-kyc-surveys-attest-to-even-greater-compliance-pain-points.html. Accessed 6 Apr 2020

Thwin TT, Vasupongayya S (2019) Blockchain-based access control model to preserve privacy for personal health record systems. Secur Commun Networks 5:1–15

Union E (2018) Directive (EU) 2018/843 of the European parliament and of the council of 30 May 2018 amending directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives. Off J Eur Union 156:1–32

vom Brocke J, Winter R, Hevner AR, Maedche A (2020) Accumulation and evolution of design knowledge in design science research – a journey through time and space. J Assoc Inf Syst 21:520–544

Webster J, Watson RT (2002) Analyzing the past fo prepare for the future: writing a literature review. MIS Q 26:13–23

Wolfswinkel JF, Furtmueller E, Wilderom CPM (2013) Using grounded theory as a method for rigorously reviewing literature. Eur J Inf Syst 22:45–55. https://doi.org/10.1057/ejis.2011.51