NOVA IMS Information Management School

MGI

Master Degree Program in
Information Management

Enhancing the Know-Your-Customer Onboarding with Blockchain

A Smart Contract-based Framework for Decentralized and Privacy-Preserving Identity Verification

Louis-Vincent Philipp-Messerschmidt

Master Thesis

presented as partial requirement for obtaining the Master Degree in Information Management

NOVA Information Management School
Instituto Superior de Estatística e Gestão de Informação
Universidade Nova de Lisboa

NOVA Information Management School

Instituto Superior de Estatística e Gestão de Informação

Universidade Nova de Lisboa

Enhancing the Know-Your-Customer Onboarding on Blockchain

A Smart Contract-Based Framework for Decentralized and Privacy-Preserving Identity Verification

by

Louis-Vincent Philipp-Messerschmidt

Master Thesis presented as partial requirement for obtaining the Master's degree in Information Management, with a specialization in Information Systems and Technologies Management

Supervised by

Ian James Scott, PHD, Nova Information Management School

February, 2025

STATEMENT OF INTEGRITY

I hereby declare having conducted this academic work with integrity. I confirm that I have not used plagiarism or any form of undue use of information or falsification of results along the process leading to its elaboration. I further declare that I have fully acknowledged the Rules of Conduct and Code of Honor from the NOVA Information Management School.

[Lisbon, 28.02.2025]

Louis-Vincent Philipp-Messerschmidt

DEDICATION

I would like to dedicate this work to my family. Thank you for your support over the years.

ACKNOWLEDGEMENTS

I would like to thank my thesis advisor, Professor Ian Scott, for providing this research opportunity. Throughout the research, he was always there to provide guidance and feedback when needed.

ABSTRACT

The increasing regulatory pressure and inefficiencies in traditional Know Your Customer (KYC) onboarding processes have driven financial institutions to explore blockchain-based solutions. Despite its potential to enhance security, reduce costs, and streamline compliance, the adoption of blockchain for KYC remains limited due to scalability challenges, privacy concerns, and regulatory uncertainties. This research applies a Design Science Research (DSR) methodology to develop and evaluate a blockchain-based KYC framework utilizing Soulbound Tokens (SBTs) for decentralized and privacy-preserving identity verification. A comprehensive literature review was conducted to assess the limitations of existing blockchain-based KYC solutions, identifying key inefficiencies such as high compliance costs, data redundancy, and security risks. The proposed artifact was implemented using Ethereum smart contracts, Truffle, and Ganache, and its feasibility was assessed through expert interviews, transaction throughput (TPS) measurements, and user perception surveys. Results indicate that while the system significantly enhances cost efficiency and data security, scalability constraints and regulatory challenges remain critical barriers to adoption. By addressing institutional adoption hurdles, exploring financial incentives for banks, and analyzing the feasibility of decentralized identity verification, this study contributes to the broader discourse on blockchain's role in compliance-driven identity management

KEYWORDS

Know-Your-Customer; Smart Contracts; Blockchain; Design-Science-Research

Sustainable Development Goals (SDG):

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS AND ACRONYMS

AML – Anti-Money-Laundering

CFT – Countering the Financing of terrorism

Defi – Decentralized Finance

DLT – Distributed Ledger Technology

DSR – Design Science Research

EVM – Ethereum Virtual Machine

FATF – Financial Action Task Force

FI – Financial Institutions

ICO – Intitial Coin Offering

IFPS – InterPlanetary File System

KYC – Know Your Customer Principle

SBT´s – Soulbound Tokens

TPS – Transactions per Second

zk-Rollups – Zero-Knowledge Rollups

zk-Proofs – Zero-Knowledge Proofs

1. INTRODUCTION

Traditional banks and financial service providers are facing major individual challenges. Growing regulatory pressure (GDPR, ESG) and competition from new types of fintech's that are establishing lean digital business models without the burden of existing structures and processes are increasing the need for established institutions to act (Kapsoulis et al., 2020). Innovative solutions are required, particularly regarding the collection of customer data in the course of anti-money laundering (AML) requirements or the know-your-customer (KYC) process. In the area of KYC, in addition to the regulatory requirements, the high costs further increase the pressure on financial institutions. The 2023 published report from Fenergo illustrates the dilemma, showing that the average KYC-cost for a corporate client is $2,598 per bank (Fenergo, 2023, p.3). However, KYC is not only a challenge for financial institutions, Customers who participate in the onboarding process also face several challenges (Moyano & Ross, 2017). The primary factors that warrant consideration in this context are, first, the inherently time-intensive nature of the process, and second, the growing sense of distrust among customers regarding the sharing of their highly sensitive personal data (Al Mamun et al., 2020). To address these issues on both sides of the process, the first research projects have been conducted in the areas of distributed ledger Technology as well as blockchain, showcasing that decentralized technology can deliver an overall more efficient KYC-process (Malhotra et al., 2022).

This thesis seeks to develop a novel blockchain-based artifact that simultaneously enhances cost efficiency in KYC onboarding and strengthens privacy-preserving identity management. The proposed artifact leverages Soulbound Tokens (SBTs) as a decentralized solution to verify KYC documents only once, enabling financial institutions to reduce operational redundancies and compliance costs. By implementing SBTs for identity management, individuals gain control over their digital identities, eliminating the need for repetitive document submissions across multiple financial entities (Tran et al., 2023). Furthermore, the artifact ensures that once a KYC verification has been completed and bound to a non-transferable SBT, it remains immutable and verifiable across participating financial institutions, enhancing security and regulatory compliance. This approach not only minimizes onboarding costs but also tackles critical privacy concerns by reducing data exposure and empowering customers with greater control over their sensitive information. Through cryptographic verification mechanisms and decentralized identity frameworks, this research demonstrates how blockchain technology can transform traditional KYC models into a more cost-efficient, privacy-centric, and scalable solution (Chen et al., 2022).

The research question guiding this investigation is: Is it possible to build such an artifact that addresses both customer privacy issues as well as cost reduction for financial institutions? To answer this question, an artifact will be developed following the design science research

methodology by Hevner et al. (2004). This research question addresses the critical need for innovative solutions to overcome the inefficiencies of traditional KYC systems, particularly in the context of decentralized verification mechanisms that are pivotal to regulatory compliance for financial institutions. Additionally, the artifact is intended to enhance security within the KYC process for both financial institutions and applicants. A particular emphasis will be placed on protecting applicants' personal data, reducing the risk of identity theft, and minimizing data exposure (Grassi et al., 2019).

To follow the DSR approach, this thesis outlines several key steps: first, conducting a comprehensive review of the existing literature on the existing KYC process, Blockchain technology, blockchain-based KYC in Banks; second, developing an artifact that consists of a decentralized KYC schema utilizing these technologies to address the identified challenges and documenting the development process; finally, presenting the developed solution, assessing its contributions to the existing knowledge base, and benchmarking the artifact against predefined scalability, efficiency, and compliance metrics. Through these objectives, this research aims to contribute a novel artifact to the field blockchain-based KYC onboarding schema that leverages the power of identity management through SBTs to enhance security, scalability, decentralization, and regulatory compliance.

By addressing the scalability and security challenges in decentralized KYC processes through the innovative use of Soulbound Tokens, this thesis aims to contribute the following to the current research landscape:

- An artifact design that effectively addresses the challenges of the KYC process for both customers and financial institutions.
- Demonstration of the usability of Soulbound Tokens in a blockchain-based KYC process to ensure non-transferable, verifiable identity attestations.
- A structured, decentralized verification mechanism that enhances regulatory compliance while protecting user privacy and reducing redundancy in financial institutions' KYC processes.

2. LITERATURE REVIEW

This part of the thesis focuses on the literature research and is divided into four parts. To demonstrate the relevance of the research, firstly the traditional KYC process will be analyzed. Afterwards there will be an introduction into the technical background of blockchain. Following in the third part of the literature review, the focus will shift on blockchain-based KYC projects in banks. In the last section of this thesis, a summary is provided and the research gap as well as the research question

2.1. KNOW-YOUR-CUSTOMER PRINCIPLE

Know Your Customer (KYC) is a fundamental process in the financial sector, aimed at verifying the identity of customers, assessing their risk profiles, and ensuring compliance with anti-money laundering (AML) and counter-terrorism financing (CTF) regulations (Hannan et al., 2023). The implementation of KYC procedures enables financial institutions to mitigate fraudulent activities, prevent illicit transactions, and uphold regulatory standards. Although indispensable, the KYC process is burdened with substantial costs, procedural inefficiencies, and regulatory complexities, necessitating continuous advancements (Schlatt et al., 2021).

Traditional KYC-Process

Figure 0.1 - The traditional KYC Process (Schlatt et al., 2021)

The KYC process as illustrated in figure 1 comprises three primary components: Customer Identification (CIP), Customer Due Diligence (CDD), and Ongoing Monitoring (OM) (Bluemel, 2024). During CIP, financial institutions collect personal identification documents such as government-issued IDs, passports, or driver's licenses to establish customer identity (Mugarura, 2014). Additionally, proof of residence and supplementary documentation may be required for validation (Arasa, 2015). Following this step, CDD mandates a risk assessment where banks evaluate customer profiles against lists of politically exposed persons (PEPs), sanctioned individuals, and known financial criminals (Rajyashree et al., 2019). Based on these assessments, banks either conduct Simplified Due Diligence (SDD) for low-risk customers or Enhanced Due Diligence (EDD) for high-risk individuals (Bluemel, 2024). Lastly, ongoing monitoring requires continuous surveillance of customer transactions to detect suspicious activity and prevent financial misconduct, with any irregularities reported to regulatory

authorities (Hanbar et al., 2019; Schlatt et al., 2021). This process of initial verification and continuous monitoring must be repeated for each customer and is required every time a customer opens a new account with another bank (Fig.2) (Schlatt et al., 2021).

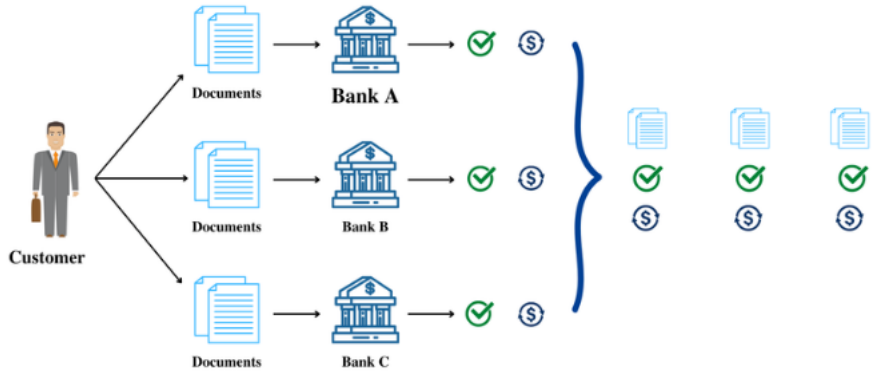


Figure 0.2 – Current process and cost structure of KYC (Hannan et al., 2023)

Regulatory Significance

Regulatory bodies impose stringent compliance requirements on financial institutions to ensure adherence to AML and CTF regulations. The Financial Action Task Force (FATF) establishes global AML standards, which have been incorporated into the legislative frameworks of over 130 countries (Hanbar et al., 2019). In the European Union (EU), the Anti-Money Laundering Directive (AMLD) governs financial institutions' KYC responsibilities, while in the United States (U.S.), the Bank Secrecy Act (BSA) and the USA PATRIOT Act stipulate KYC compliance measures (Sanction Scanner, 2023). Failure to comply with these regulations exposes financial institutions to significant financial penalties, legal actions, and reputational damage (Hannan et al., 2023). High-profile cases exemplify these risks, such as HSBC's $1.92 billion fine for facilitating money laundering by Mexican and Colombian cartels (Viswanatha & Wolf, 2012) and ING Bank's $619 million penalty for violating international sanctions (ING, 2024). These instances underscore the necessity of robust KYC compliance to prevent financial misconduct and regulatory breaches.

KYC-costs

Despite its regulatory significance, the KYC process imposes considerable financial burdens on banks. A study conducted by LexisNexis Risk Solutions (2017) across five European financial markets estimated that KYC compliance costs amount to approximately $83.5 billion annually, with labor expenses constituting 74% of the total expenditure. The per-bank compliance cost can reach as high as $60 million per year (Schlatt et al., 2021). Additionally, non-compliance with KYC obligations can result in severe financial repercussions. A 2023 IBM report found that

the average cost of a data breach in the financial sector stands at $5.9 million, making it one of the most financially detrimental industries in terms of cybersecurity risks (IBM, 2023). As digitalization of financial services accelerates, concerns regarding data protection and customer privacy continue to grow (Yadav et al., 2020). Financial institutions must safeguard sensitive client information to prevent identity theft, unauthorized data access, and financial fraud. Furthermore, banks that experience data breaches risk eroding customer trust and sustaining long-term reputational harm (Bluemel, 2024).

Traditional vs. EKYC Onboarding

There are currently two options for beacons/financial institutions to onboard their customers. A distinction is made between classic onboarding and EKYC (Hartsink, 2018).

Traditional KYC procedures rely on an in-person visit to the bank, where the customer submits original identification documents required for verification. A bank representative assesses these documents to confirm their authenticity, ensure they belong to the individual (by matching the photo on an official ID such as a passport), and verify that all necessary documentation has been provided. Once these initial checks are completed, copies of the documents are made, and the customer is required to sign a registration form along with a service agreement (Soltani et al., 2018).

The copied documents are then forwarded to either an internal compliance team or an external KYC verification provider for further evaluation. This additional verification step is conducted to assess the customer's eligibility and determine whether they meet the institution’s due diligence requirements. Upon successful completion of this process, the customer’s account is approved and activated, granting them access to the bank’s financial services (Monadal et al., 2016).

Shbair and Steichen (2018) identified the following problems within the current traditional KYC-Processes:

1. Errors may arise when users fill out KYC forms, particularly for individuals with multiple accounts. In such cases, the KYC process becomes more time-consuming, complicating the verification of details for a single account. These challenges are mainly due to the lack of an automated system that can efficiently capture account holder information and automatically identify and correct inaccuracies.

2. A shortage of knowledgeable and skilled personnel to provide guidance in the KYC process exists.

3. Presently, individuals are required to complete separate KYC processes for each bank or institution, resulting in increased overhead costs (averaging $60 million

annually) for each institution. Additionally, if an organization mishandles the KYC process, additional charges may be incurred.

4. The traditional KYC process, due to its time-consuming nature, causes delays in the overall customer enrollment process in banks and financial institutions.

E-KYC is a digital alternative to traditional KYC, allowing customers to complete the onboarding process online without the need for physical visits or manual document verification (Mansoor et al., 2022). Customers upload their identification documents via a bank's online portal or mobile app, and various advanced authentication methods, such as facial recognition, voice recognition, and multi-factor authentication, are employed to verify their identity (Schlatt et al., 2021). E-KYC is widely adopted by both traditional banks as an efficient alternative and neobanks as their primary onboarding method, given their lack of physical branches. Although E-KYC offers efficiency, cost savings, and convenience, it also presents fraud risks, including the misuse of fake or stolen documents and the potential for digital identity manipulation through deepfakes (Baum et al., 2023).

Three key advantages of E-KYC include its speed, as document verification can be completed within seconds regardless of business hours, cost-effectiveness, since banks reduce expenses related to physical branches and manual verification, and enhanced accessibility, as customers can complete onboarding remotely without geographical constraints (Elinzano & Ching, 2022).

Existing Inefficiencies

The operational inefficiencies of the traditional KYC framework further exacerbate compliance challenges. Financial institutions require customers to undergo KYC verification separately for each bank, leading to duplicative efforts, administrative strain, and customer dissatisfaction (Hannan et al., 2023). A survey revealed that 89% of customers reported frustration with the onboarding process due to its extensive documentation requirements and prolonged processing times (Schlatt et al., 2021). Additionally, financial institutions frequently encounter a shortage of skilled personnel equipped to handle KYC procedures, contributing to inefficiencies and increased operational costs (Shbair & Steichen, 2018). The reliance on manual verification methods rather than automated or digital solutions compounds these inefficiencies, making the KYC process time-intensive and costly (Colladon & Remondi, 2017).

Technological advancements, particularly in the realm of eKYC and blockchain-based identity verification, present potential solutions to streamline the KYC process. The integration of digital identity verification and machine learning-driven fraud detection can enhance efficiency while ensuring regulatory compliance (Soni & Duggal, 2014). The implementation of a sector-wide eKYC utility, similar to India's Aadhaar system, has demonstrated

improvements in reducing onboarding time and fraud-related losses (Schlatt et al., 2022). However, concerns regarding data privacy, centralization risks, and potential monopolistic control of identity verification remain critical considerations in the adoption of digital KYC solutions (Yadav et al., 2020). Given the complexities associated with KYC compliance, financial institutions must strike a balance between regulatory adherence, operational efficiency, and customer data protection to ensure sustainable financial governance.

2.2 Blockchain

2.2.1 Blockchain Technology

In the final decade of the 20th century, Dai's seminal work unveiled 'B-money'—a nascent form of digital currency characterized by its anonymity and decentralization within a network that defied tracking (Dai, 1998). Though B-money did not evolve beyond its conceptual stage, it established the foundational concepts that would later inform the development of Bitcoin and the underlying blockchain technology. Subsequently, in the following decade, Bitcoin emerged as the pioneering decentralized cryptocurrency, conceived to enable direct transactions between peers, without the intermediation of trusted entities, by employing a proof-of-work mechanism to independently record transactions (Yli-Huumo et al., 2016). The ascendancy of blockchain applications in recent years has catalyzed a surge in public interest, marked by an increasing proliferation of novel cryptocurrencies and blockchain-driven innovations (Werbach, 2018).

In examining "blockchain," it becomes evident that it entails the aggregation of multiple transactions into sequentially timestamped blocks (Cong & He, 2016), with each block securely linked to its predecessor, thereby forming an uninterrupted, chronological chain (Watanabe et al., 2016). As an advanced form of distributed ledger technology (Kakavand et al., 2017), blockchain functions as a distinct type of ledger—a cryptographically secured, sequentially ordered collection of transaction records distributed across a network (Peters & Panayi, 2015). This decentralized and distributed structure guarantees that all transactions on the blockchain are transparent to network participants, including regulatory authorities, and that any modifications are uniformly reflected without reliance on a central authority (Werbach, 2018; Cong & He, 2016).

In terms of its operational functionality, blockchain technology enables direct asset transfers between individuals without the need for centralized verification, thereby fostering a peer-to-peer framework. (Malinova & Park, 2017). Its defining features, immutability, and transparency are evidenced by the public availability of many blockchains and the permanent nature of the data they store, which is impervious to modification, interference, or erasure (Peters & Panayi, 2015).

The above-mentioned functionalities of blockchain emphasize different benefits for KYC. In their 2018 paper (Kolychev & Solovov, 2018), Kolychev and Solovov mentioned the following advantages if KYC data could be stored secure on a platform that is using blockchain (DLT):

1. Faster Onboarding Processes: Leveraging Blockchain technology enables quicker re-verification for existing customers by accessing previously stored details, leading to reduced onboarding duration.

2. Enhanced Cost Efficiency: Shared services within the Blockchain framework contribute to a marked reduction in the expenses associated with client verification.

3. Minimized Fraud Risks: The unalterable nature of Blockchain significantly lowers the potential for fraudulent customer information.

4. Optimized Customer Experience: With Blockchain, only necessary customer information is shared with new banks upon the customer's approval, streamlining the enrollment process.

5. Effortless Audit Trails: Blockchain's capability to log every update made to customer data provides a straightforward method for identifying and tracking data discrepancies.

6. Boosted Operational Security and Reliability: The anonymity provided by Blockchain operations ensures a high level of safety and dependability in transactions and data management.

It can therefore be concluded that the technical possibilities of blockchain presented provide various starting points that will be addressed in this paper. Blockchain enables the immutability of data, which would make it possible in our system not to change KYC verifications once they have been recorded. Furthermore, blockchain technology enables transparency about the status of the respective transactions, which enables greater trust among all participants in the onboarding process. The advantages that arise around security will be discussed in more detail later in this thesis.

2.2.2 Types of Blockchain

Various classifications exist for categorizing blockchain systems. In this chapter, our primary focus will be on the classification centered around the permission model of blockchain networks. These networks can fall into one of two categories: permissionless, allowing anyone to contribute a block (Yaga et al., 2018) and engage in the verification process (Peters & Panayi, 2015), or permissioned, where network access is tightly regulated, and verification nodes are predetermined by a central authority or a consortium (Peters & Panayi, 2015).

Permissionless Blockchains

In the case of permissionless blockchain networks, characterized by their public accessibility, these platforms are open to all users on the internet (Pilkington, 2015). Within this framework, every user possesses the ability not only to serve as a verifier but also to exercise rights in publishing blocks, accessing ledgers, and executing transactions on the blockchain (Yaga et al., 2018). It's worth noting that in a permissionless network, the identity of each user is often pseudonymous or even entirely anonymous (Swanson, 2015).

Beyond the technical framework, permissionless blockchain-based digital assets have entered the market, offering services within the financial sector. Depending on the intended service objectives, public blockchains may utilize either monetary or utility tokens, which is a crucial aspect from a business perspective (Dob, 2018). These networks are generally referred to as "fully decentralized blockchains" (Buterin, 2015).

Permissioned Blockchains

In contrast to permissionless blockchains, permissioned blockchains are regarded as purpose-built systems (Peters & Panayi, 2015). They incorporate an additional layer of privilege to determine and select authorized users (Kakavand et al., 2017). Authorized users are granted access to run nodes on the network, validate transaction blocks, execute transactions, and implement smart contracts in the permissioned blockchain (Dob, 2018). Verification in these ledgers is carried out by a consortium of trusted parties (Malinova & Park, 2017). This concept is akin to the traditional financial industry, where Know Your Customer (KYC) and Know Your Business (KYB) procedures are implemented to identify users permitted to conduct transactions under specific conditions (Peters & Panayi, 2015). Additionally, visibility in the ledger for these trusted parties could be controlled and restricted (Malinova & Park, 2017).

In contemporary times, financial institutions actively embraced permissioned blockchains to enhance payment transaction systems. An illustrative success story is 'Ripple,' which has been adopted by over 200 financial institutions worldwide. Ripple is a real-time settlement infrastructure technology for global transactions and cross-border payments (Cong & He, 2018). Consensus is achieved through the Ripple transaction protocol 'RTXP,' where transactions are repeatedly broadcast in the validation network until agreement is reached (Cong & He, 2018). This not only automates real-time digital transfers but also provides cost-saving, reliable transaction services. The smaller network size contributes to increased efficiency, making it easier for participants to collaborate, adjust rules, or revert transactions within the same network (Peters & Panayi, 2015).

2.2.3 Smart Contracts

The idea behind Smart Contracts were revealed by Szabo (1994) in the early 1990´s, when he phrased the following:
“Smart contracts are the computerized transaction protocols that execute the terms of contracts. On the one hand, such transaction protocols aim to achieve contractual conditions such as payment terms, lines, confidentiality or even enforcement. On the other hand, they also have objectives of eliminating malicious and accidental issues and minimizing the need for trusted intermediaries."

Considering the recent groundbreaking developments in blockchain technology and Distributed Ledger Technology (DLT), the practical utilization of smart contracts has emerged

as a prominent and viable business application within the blockchain landscape. Smart contracts, by definition, represent encoded contractual rules encapsulated in computer code and securely stored on the blockchain (Sklaroff, 2017). These encoded contractual rules can be duplicated and executed across the blockchain's distributed nodes (Peters & Panayi, 2015). Smart contracts exhibit a range of noteworthy characteristics. Firstly, they inherit the immutability feature inherent to blockchain technology, rendering the stored contractual rules unalterable once established (Sklaroff, 2017). Secondly, they possess enduring permanence, enabling their reuse for the creation of more advanced services (Peters & Panayi, 2015). Moreover, from an automation perspective, smart contracts are capable of being self-enforcing, monitoring external inputs from trusted sources to facilitate settlement in accordance with encoded terms and conditions (Peters & Panayi, 2015).

In the field of smart contracts, correctness and security are critical to their applicability in specific scenarios. Although some research has addressed security, formal methods and practical implementations remain limited. Writing secure smart contracts is challenging, especially given the complex semantics of the Ethereum Virtual Machine (EVM) (Delmolino et al., 2016). Researchers have developed frameworks to analyze and verify the runtime safety and correctness of Solidity contracts using F*, a language designed for program verification. Additionally, common security pitfalls have been documented, offering guidelines and best practices for avoiding vulnerabilities, supported by online educational resources for smart contract programming (Bai et al, 2018). Furthermore, the deployment of smart contracts creates additional challenges, like the awareness of the contract’s interaction patterns to reduce potential losses caused by fraud for example (Zheng et al., 2020).

2.2.4 Ethereum

Invented by Vitalik Buterin in 2014, Ethereum stands out as both a permissionless blockchain and a software development platform with the goal of providing access to smart contracts and facilitating the development of decentralized applications (Peters & Panayi, 2015). Ethereum empowers individuals to establish their unique rules for ownership, transaction formats, and state transition functions within their decentralized applications (Buterin, 2014).
The Ethereum Virtual Machine (EVM) serves as the runtime environment for executing smart contracts and DApps. It's a Turing-complete virtual machine that enables developers to create complex applications by writing code that runs on the Ethereum network. The EVM processes transactions and executes smart contracts across the decentralized network, facilitating trustless and tamper-resistant interactions (Buterin, 2014).

To ensure the efficient operation of Ethereum, the cryptocurrency Ether is employed. Ether serves the dual purpose of compensating miners and facilitating transaction payments across applications constructed on the platform (Garlichs & Dosch, 2017). Additionally, Ethereum's state is structured around "accounts," as defined by Buterin (2014). These accounts are categorized into two types, primarily influenced by the presence of smart contracts (Garlichs & Dosch, 2017):

• External Owned Account: These accounts are controlled by a private key and do not contain any associated code, meaning they are not connected to any smart contract. Messages can be sent from externally owned accounts through the creation and signing of transactions.

• Contract Account: In contrast, contract accounts are governed by code, representing the smart contract. Upon receiving a message, the activation of code enables the account to read and write to internal storage, thereby becoming a part of the state. This functionality empowers the contract to manage multi-state operations.

Gas costs associated with Ethereum transactions are designed to ensure efficient network usage and to prevent denial-of-service attacks. Users can set the gas price for their transactions, which, in turn, influences the transaction's priority on the network. Miners are incentivized to process transactions with higher gas fees first, encouraging users to competitively bid for faster transaction confirmations. This pricing mechanism helps balance the network and encourages efficient use of computational resources (Garlichs & Dosch, 2017).

In addition to all the possibilities that Ethereum offers, however, it should be mentioned that the blockchain faces a scalability problem due to its limited transaction throughput, which is constrained by the fixed block size and the time interval between blocks (Chauhan et al., 2018). As the number of users and transactions increases, the network experiences congestion, leading to higher transaction fees and slower confirmation times. This bottleneck arises from the need for every node in the network to process and validate all transactions, ensuring security and decentralization but limiting scalability (Bez et al., 2019). Consequently, Ethereum struggles to efficiently handle large-scale applications and a high volume of transactions, highlighting the need for scalable solutions like sharding and layer-2 protocols (Khan et al., 2021).

2.2.5 Soulbound Token

Soulbound Tokens (SBTs) have emerged as a novel mechanism within blockchain ecosystems, offering non-transferable digital assets that encode personal credentials, commitments, and affiliations. Introduced by Buterin, Weyl, and Ohlhaver (2022), SBTs represent an innovative approach to digital identity by ensuring that credentials remain bound to their original holder, preventing unauthorized transfers or sales (Buterin et al., 2022). Unlike conventional NFTs,

which are transferable and often financialized, SBTs are inherently non-transferable, making them particularly suitable for applications requiring identity verification, reputation building, and trust networks (Ohlhaver et al., 2022).

A defining feature of SBTs is their non-transferability and identity binding, which enhances the security of digital identity management. SBTs function as unique certificates issued by institutions or individuals, ensuring that an individual's identity and credentials remain immutable within a decentralized system (Hildebrandt, 2023). This property is particularly valuable in the Know Your Customer (KYC) onboarding process in financial institutions, where a one-time verification process can be recorded and referenced without redundant verification steps (Maranhão and Seigneur, 2022). Compared to traditional digital identity frameworks, which often rely on centralized verification authorities, SBTs offer an immutable, blockchain-based verification layer, reducing fraud risks and increasing operational efficiency (Hildebrandt, 2023).

Beyond their technical features, SBTs also enhance privacy and security through selective disclosure mechanisms. A privacy-preserving SBT framework enables users to reveal only specific credential attributes when verifying identity, rather than disclosing complete personal data (Reddy and Kushwaha, 2023). This feature aligns with the principles of Self-Sovereign Identity (SSI), allowing individuals to control their own digital identity while minimizing exposure to third parties (Goldston et al., 2023). Moreover, SBTs contribute to secure digital inheritance frameworks, where credentials and ownership rights can be inherited through pre-defined recovery mechanisms, ensuring continuity while protecting against fraud (Goldston et al., 2023).

Despite their advantages, the adoption of SBTs is not without challenges. One potential risk is wallet compromise, where the loss of access to an SBT-bound wallet could lead to permanent credential loss (Maranhão and Seigneur, 2022). Proposed solutions include community recovery mechanisms, where a predefined network of trusted entities can collectively authorize credential restoration, reducing reliance on centralized intermediaries (Reddy and Kushwaha, 2023).

By integrating SBTs into KYC onboarding, this research explores a blockchain-based artifact that addresses cost inefficiencies in identity verification while reinforcing privacy through decentralized identity frameworks (Buterin et al., 2022). Through cryptographic security, self-sovereign identity management, and selective disclosure mechanisms, SBTs offer a robust alternative to existing KYC processes, ensuring efficiency and regulatory compliance in financial institutions (Goldston et al., 2023).

2.3 Blockchain-Based KYC in Banks

The Know Your Customer (KYC) process remains a cornerstone of regulatory compliance in the banking sector, ensuring financial institutions can verify customer identities and prevent fraud. While existing research has explored blockchain's role in optimizing KYC, significant gaps remain, particularly in self-sovereign identity (SSI), interoperability, privacy, and incentivization. This review critically examines key papers on blockchain-based KYC, discussing their contributions and how the proposed artifact enhances and extends their findings.

In their research, Malhotra et al. (2021) provide a systematic review on how blockchain can automate KYC. They stated that the traditional KYC process is time consuming and inefficient and therefore needs a transformation. Furthermore Malhotra et al. mention that blockchain with its attributes anonymous and secure could decrease the onboarding time for customers, as well as cost and risks for both customers and financial institutions. In addition, the paper proposes a blockchain network that support financial institutions within administering customer data (Malhotra et al., 2021). These findings indicate an increased need and interest in the topic, both on the part of customers and on the part of financial institutions.

Schlatt et al. (2021) propose a self-sovereign identity (SSI) framework for KYC, leveraging decentralized identity management to enhance privacy and security. Their approach ensures that users retain control over their identity while banks verify customer details without redundant processes (Schlatt et al., 2021). However, the paper does not introduce a structured mechanism to enforce the immutability and verifiability of these identity attestations on-chain. The proposed artifact builds on this work by integrating Soulbound Tokens (SBTs) as an on-chain verification mechanism, ensuring that identity attestations cannot be transferred or forged. Additionally, while Schlatt et al. focus on the conceptual framework, the new artifact implements Solidity smart contracts for automated verification and introduces an incentive structure for banks, ensuring that financial institutions are rewarded for participating in the KYC verification process. Furthermore, the proposed artifact expands upon their work by incorporating a structured payment mechanism, addressing the economic feasibility of cross-institutional verification systems .

Moyano and Ross (2017) discuss how blockchain-based KYC can reduce verification costs and streamline identity verification across multiple banks (Moyano & Ross, 2017). Their model utilizes cryptographic hashes stored on a distributed ledger, allowing banks to verify previous KYC attestations. Moreover, their work introduces an incentive structure where banks verifying identities receive compensation for their efforts. However, their approach relies on manually triggered payments, requiring third-party intermediaries to facilitate transactions. The proposed artifact extends this concept by integrating fully automated payments via Solidity smart contracts, eliminating third-party dependencies. Additionally, instead of merely storing document hashes, the artifact introduces a verifiable credential mechanism using

Soulbound Tokens (SBTs), enhancing security and efficiency while preventing fraud. The new model ensures that banks are instantly compensated upon verifying a customer's identity, thus increasing adoption and reducing onboarding time.

Hannan et al. (2023) present a systematic review of blockchain-based KYC solutions, identifying common challenges such as lack of standardization, privacy concerns, and limited interoperability. Their study provides a comprehensive landscape of existing technologies but lacks an implementation framework that addresses these concerns practically (Hannan et al., 2023).. The proposed artifact builds on this literature by defining an 11-step process that ensures regulatory compliance, particularly with GDPR and AML directives, while integrating on-chain verification mechanisms to improve efficiency and reduce redundant verifications. Unlike the theoretical discussions in the paper, the new artifact operationalizes these findings by structuring a technically feasible model for blockchain-based KYC .

A study published in Procedia Computer Science proposes a decentralized KYC framework using Ethereum smart contracts for identity verification (Procedia Computer Science, 2022). While their approach improves transparency and data integrity, it does not explicitly address privacy concerns related to storing user data on-chain. The new artifact ensures compliance by keeping personal documents off-chain while storing only cryptographic proofs on the blockchain. Additionally, it enhances interoperability by enabling multi-bank verifications without requiring centralized control, thus increasing the adaptability of blockchain-based KYC in different financial ecosystems. Unlike the procedural framework presented in this study, the proposed artifact introduces a structured reward model that ensures financial institutions remain incentivized to participate in the verification network.

Thommandru and Chakka (2023) explore the role of blockchain in addressing anti-money laundering (AML) compliance in banking. Their study focuses primarily on the policy implications of blockchain-based KYC rather than on technical implementations (Thommandru & Chakka, 2023). While they highlight the necessity of immutable verification mechanisms, they do not propose a concrete model for how this should be achieved. The proposed artifact operationalizes these policy recommendations by integrating a cryptographic proof system using Keccak-256 hashing and Solidity smart contracts for verifiable attestations, ensuring compliance with global financial regulations. Moreover, the artifact's automated smart contract implementation makes it significantly more scalable than the policy-based recommendations provided by the authors.

Kinyua emphasizes the inefficiencies of traditional KYC onboarding, outlining how blockchain could streamline identity verification. The study presents a conceptual design but lacks a detailed technical implementation (Kinyua, 2020). The proposed artifact extends this work by developing Solidity smart contracts that facilitate cross-bank KYC verification, reducing duplication efforts while maintaining security and privacy. Furthermore, the artifact provides

an on-chain verification mechanism that banks can query without compromising user privacy, ensuring a more secure and efficient verification process. While Kinyua provides a high-level discussion, the artifact enhances this by implementing an Ethereum-based trust layer to ensure robust identity management.

Kihara et al. provide a proof-of-concept study on blockchain-based KYC, validating its feasibility but not addressing interoperability challenges between different financial institutions (Kihara et al., 2020). The proposed artifact introduces a standardized verification process using ERC-721-based SBTs, ensuring that banks can trust existing verifications without repeated manual checks. Additionally, the new artifact incorporates an incentive mechanism that rewards banks for their verification efforts, encouraging wider adoption of blockchain-based KYC. Unlike the study's proof-of-concept, the artifact presents a deployable model that directly integrates with existing banking infrastructures.

Bhaskaran et al. propose a double-blind data-sharing model where KYC information is securely exchanged between banks. While this enhances privacy, their solution does not incentivize KYC data sharing (Bhaskaran et al., 2020). The proposed artifact addresses this by rewarding banks with ETH transfers via smart contracts, ensuring that institutions actively participate in a collaborative verification ecosystem while maintaining security and compliance.

Various findings can be derived from the paper presented, which can be adapted for the design of the artifact aimed at in this thesis. Firstly, decentralized KYC processes offer significant advantages by leveraging blockchain technology, cryptographic proofs, and user-centric data management. These systems enhance data privacy and control, allowing users to manage access to their personal information securely. Blockchain’s immutability ensures transparency and trust, while reducing redundancy by enabling institutions to share pre-verified data, streamlining the KYC process and cutting operational costs. The final adaptations from the presented papers are discussed in sections 3.5 and 4.2.

2.4 Summary and Research GAP

The preceding literature research has revealed the theoretical background to the components that are crucial in the design and development of a new artifact. Research has revealed that the current KYC process in banks shows some inefficiencies, such as high costs or legal risks. One way to address these problems is attributed to blockchain technology. Over the past 8 years, researchers have begun to explain various options for the role blockchain can play in an adapted KYC process to address or, at best, eliminate the problems described. Some of this research has already resulted in successful adaptations of the KYC onboarding process.
While existing literature provides valuable insights into blockchain-based KYC, significant gaps remain in practical implementation, incentive structures, and privacy compliance. A particular limitation in previous studies is the lack of practical applications that incorporate Soulbound

Tokens (SBTs) to enhance both security and interoperability in a decentralized financial ecosystem for the customers identity management. Existing research also fails to propose a fully automated, blockchain-driven incentive system that encourages financial institutions to participate in the verification process. The proposed artifact bridges this gap by integrating SBTs for verifiable credentials, and introducing automated smart contract-driven payments, ensuring a decentralized and economically viable KYC process. By addressing these deficiencies, this research contributes a novel approach to regulatory-compliant identity verification that enhances security, reduces costs, and prioritizes user privacy.

RQ1: Is it possible to build such an artifact that addresses both customer privacy issues as well as cost reduction for financial institutions?

3. METHODOLOGY

The following section of the thesis is dedicated to the methodology on which this work was based. First, the Design Science Research Methodology (DSR) will be explained. Afterwards, the several steps performed due to this methodology will be presented. To start, the problem identification through the Literature Review will be explained. Afterwards the focus will be on the objectives of the thesis and how the novel artifact can add to the existing knowledge base. Next, the Design & Development part of the thesis is explained. In this part, the technical requirements are discussed and the tools to evaluate the artifact. The last part of this section will cover the demonstration of the novel artifact within a relevant environment.

3.1 Design Science Research Methodology

The aim of design science research is to address a problem through the creation of an artifact, ensuring a rigorous design process and substantiating the utility of the artifact with evidence (Hevner et al., 2004). In contrast to conventional design practices, the DSR approach is meticulous and results in the generation of novel knowledge, while routine design relies on pre-existing knowledge (Hevner et al., 2004, Baskerville, 2008, Gregor & Hevner, 2013). The knowledge derived from DSR can subsequently find application in routine design across a variety of fields, encompassing disciplines such as architecture, engineering, education, healthcare, computer science, and management (March & Vogus, 2010, Baskerville, 2008, Vaishnavi et al., 2019).

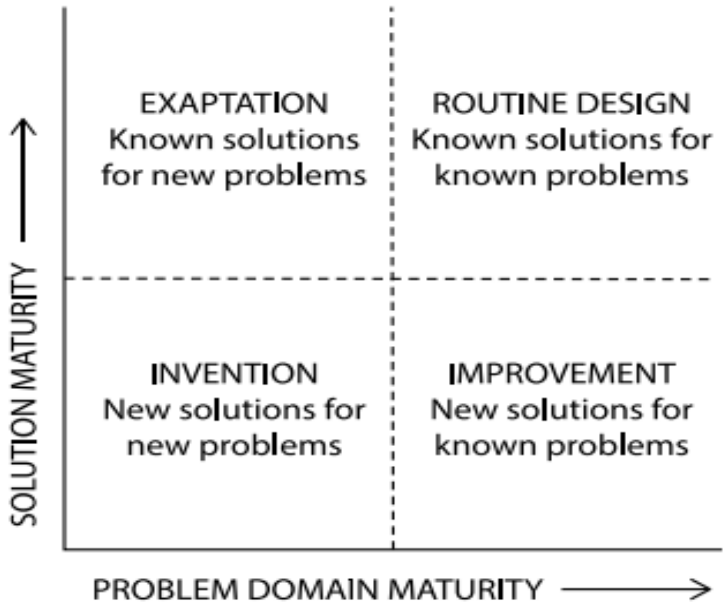


Figure 0.3 - DSR knowledge contribution framework. (Gregor & Hevner, 2013).

In general, DSR yields four distinct types of knowledge contributions, as illustrated in figure 3: routine design, exaptation, improvement, and innovation (Gregor & Hevner, 2013). Routine design, characterized by low knowledge contribution, typically falls outside the realm of design science research. This thesis aims for an improvement of the existing KYC process, based on the foundation of a DSR-approach.

DSR artifacts are expected to exhibit a certain degree of novelty in the form of enhancements, adaptations, and innovations (Gregor & Hevner, 2013). Additionally, DSR results are expected to possess a level of generality, as artifacts exclusively applicable to a specific problem offer limited value to the research community (Johannesson & Perjons, 2014, Winter, 2008, Engström et al., 2019). The significance of DSR hinges significantly on the utility of the produced artifacts (Winter, 2008).

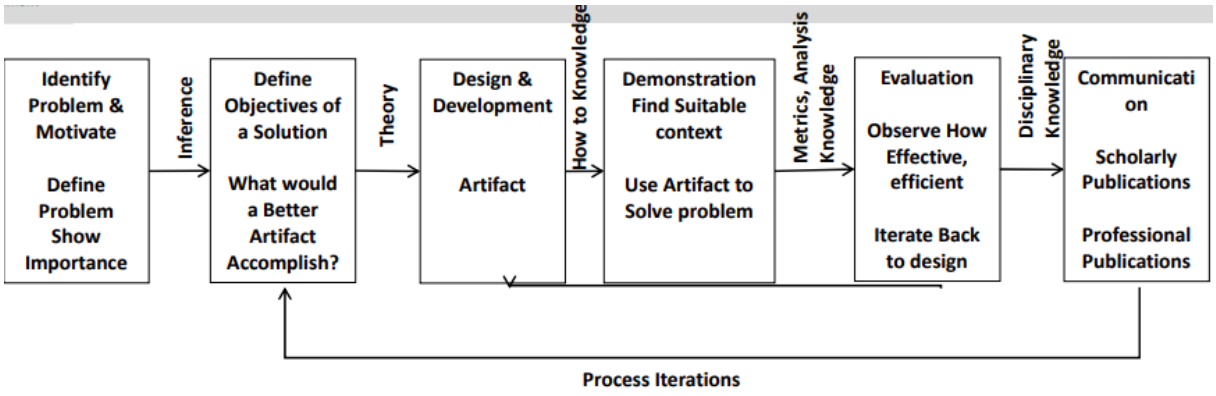


Figure 0.4 - Design Science Research Process Model, adapted from Peffers et al., 2017.

Numerous efforts have been made to conceptualize Design Science Research (DSR). This thesis employs the Design Science Research Methodology (DSRM) process, developed by Peffers, Tuunanen, Rothenberger, and Chatterjee (Peffers et al., 2007). DSRM delineates six distinct stages within DSR: problem identification and motivation, objective definition, design and development, demonstration, evaluation, and communication (Figure 4). It's important to note that the order of these steps is flexible. For instance, research may commence with the evaluation of an existing artifact rather than problem identification (Peffers et al., 2007). Generally, DSR is an iterative process (Hevner et al., 2004, Peffers et al., 2007), where insights gained during one cycle inform the next. Figure 4 illustrates the DSRM process with the incorporation of a knowledge base flow. This knowledge base encompasses existing DSR knowledge, research methods (Hevner et al., 2004), and insights from various disciplines relevant to the problem at hand (Wieringa, 2014). Effective DSR draws upon the knowledge base to ensure appropriate specification of artifact requirements and rigor in the DSR process (Hevner et al., 2004, Peffers et al. 2018, Wieringa, 2014). In contrast, routine design entails intellectual risks due to decisions made based on inadequate knowledge (Vaishnavi et al., 2019). Lastly, when DSR results are communicated, new knowledge enriches the knowledge base for future research.

The following paragraphs deal with the implementation of the individual steps of the DSR method in the context of this thesis.

3.2 Problem Identification

As described above, the process of the DSR methodology starts with the problem identification. The purpose of this is to identify a problem in the subject area under consideration based on existing literature or the exchange with practice partners. (Peffers et al., 2007).

Literature research was used to identify the problem in the context of this thesis, which was illustrated in section 2. The initial focus here was on the existing KYC process to gain an understanding of how it works and is currently mapped (Schlatt et al., 2021). The focus was to identify the costs, regulatory requirements and the existing onboarding procedures. In addition, initial inefficiencies were identified, as revealed in the paper by Shbair and Steinchen (2018).

The individual aspects of blockchain technology were then discussed in order to understand their functionality and at the same time determine whether and in what form they are suitable for use in the intended certificate. Blockchain was identified as a capable technology (Kolychev & Solovov, 2018).

Building on this theoretical knowledge, the search for existing applications was intensified as part of the literature research. The aim here was to determine the current state of research and to identify existing blockchain solutions that could be used in the further course of the work to design the artifact. The systematic literature review by Malhotra et al. (2021), which explores the use of blockchain for automating KYC processes, emerged as a prominent focus of attention. Building on the insights gained from this paper, the research further dived into the usage of blockchain in KYC or decentralized KYC approaches. The papers of Moyano et al. (2017, 2019), Schlatt et al. (2021) and Patel et al. (2021) will be conducted to scale the novel artifact. It was noticeable in all the papers reviewed that the problems of scalability, trust and user data privacy occurred several times.

The insights gained from the three literature reviews on the suitability of blockchain for eliminating inefficiencies in the current KYC process and the identification of existing blockchain solutions that should serve as the basis for the new, targeted artifact allow the following research question to be formulated: Is it possible to build such an artifact that addresses both, customer privacy issues as well as cost reducing for financial institutions?

Based on the problems identified through the literature review and the research question derived from it, the following section will discuss the definition of the objectives on which the desired artifact should be based to be able to answer the previously defined question.

3.3 Objectives of the designed Artifact

The next step of the DSR focuses on the definition of the objectives, the new artifact should be able to fulfill. The objectives on which the work is to be based in order to comprehensively address the KYC process were defined from various sources and are already reflected to a certain extent in the research question. Firstly, the objectives were derived from the literature research, as well as from the regulatory requirements for KYC. This approach should make it possible to combine previous research results and real business requirements in the objectives in line with the DSR (Schlatt et al., 2021). In this way, we have defined objectives that will be briefly explained below; a detailed explanation will be provided in Part 4 of this thesis.

Objective 1: Regulatory Compliance

To reach legally compliance with all regulatory is a key factor for every KYC process, against the background that one of the main targets is the fight against money laundering (Ostern & Riedel, 2021). The objective is driven by the Anti-Money-Laundering Act as well as the GDPR in the European Union. To reach this objective, blockhchain´s inherent auditability and transparency features should be leveraged (Grassi et al., 2019).

Objective 2: Scalability

The literature research discloses that the existing decentralized KYC process reaches its limits once it reaches a certain size (Patel et al., 2021). This is usually at the expense of transactions per second (TPS) and the gas costs incurred for a single transaction (Dhiman & Bose, 2022). To enhance the scalability in comparison to existing solutions, the proof of verification will be submitted straight to the customers wallet, while on-chain there will only be a proof that the bank verified and signed the documents. This procedure will reduce the blocksize and enhance the transaction speed for further onboardings with additional banks (Capko et al., 2022).

Objective 3: Privacy/Trust

A blockchain based KYC process prioritizes customer privacy, a key concern as data breaches become increasingly frequent and customers grow more aware of risks associated with personal data exposure (Schlatt et al., 2022). Literature highlights that privacy and trust are major concerns in traditional KYC systems, particularly due to the rising number of data leaks (Moyano et al., 2019). Providing a solution that enhances privacy protection could significantly improve customer acceptance (Jessel et al., 2018). A fundamental principle in achieving this is the "need to know" rule, which ensures that only the customer and relevant entities in the KYC process have access to personal data, aligning with widely recommended security practices for information systems (Moor, 1997, Schlatt et al., 2022). To address these concerns effectively, a survey will be conducted among customers as part of the system's design

process, ensuring that the decentralized KYC model aligns with user expectations and strengthens trust in digital identity verification.

Objective 4: Efficiency

The high costs caused by KYC pose problems for banks worldwide as well as the time-consuming process (Moyano et al., 2019). Since these problems affect the entire financial services industry, this objective was defined to ensure the real-world usability of the artifact based on the DSR method (Gregor & Hevner, 2013). To achieve the following objective, the novel artifact aims to reduce redundant KYC processes times and minimize the operational and compliance costs associated with traditional KYC.

3.4 Design & Development of the novel Artifact

The main contribution of this thesis is to develop a novel artifact and present the result of this process. To align with the design science research approach, this development has been seen as an iterative process (Peffers et al., 2007). The feedback during the development stages was gained through experts interviews, so that both, formal and informal collaborations supported the development. One main principle of the DSR methodology is the application of rigor design (Dresch et al., 2015). To fulfill that principle, the work will rely on the existing literature identified within section two and the given blockchain development frameworks (Scott et al., 2023). Firstly, the framework of Casino et al. (2021) has been used to identify the suitability of blockchain for this project and helped to decide whether to use a public or private blockchain. Based on that decision, the artifact was designed and presented to the different experts. Based on the feedback, different adaptations have been applied to the artifact. Also, during the design & development phase, the artifact adapted from existing solutions that been described in the literature review.

Based on this theoretical design the Truffle & Ganache development tools were used to develop the KYC-process. These tools were chosen based on the decision to use Solidity to write the mandatory smart contracts. Both these tools provide useful frameworks to develop smart contracts, deploy and manage them. In addition, both support EVM, an essential criteria for the selection. Truffle is a development environment and testing framework for blockchains using the EVM, which offers several features (Advanced Debugging, Built in Smart Contract compilation) that simplify the creation of the novel artifact. Besides been used in the development section, Truffle will also be used to track the gas costs of the novel artifact once the development is fulfilled (Truffle.com, 2024). In addition, Ganache will be used due to two different reasons. The first reason is to debug & monitor smart contracts after the first development phase in Truffle. Furthermore, Ganache is used to simulate network conditions to track the gas cost, by deploying a local ethereum network, where the test scripts executed through Truffle can be simulated on.

The following section of this thesis (3.5) will go more into detail about the demonstration of the artifact within the named networks.

3.5 Demonstration of the novel Artifact

In the previous section of this thesis, we described in detail how the novel artifact was designed and developed, and which steps were determined as part of this process. The following section is intended to show the ways in which the functionality of the artifact will be demonstrated to illustrate how it can simplify the KYC process. Different tools were used for the development and the measurement of the predefined metrics (part 3.6).

As already mentioned in the previous section, both Truffle and Ganache will be used to develop and monitor the smart contracts. Furthermore, a different testing environment was required to demonstrate the functionalities of the integrated smart contracts and measure their performance (TPS). To measure the transactions per second (TPS) to evaluate the novel artifact this thesis is going to rely on Hardhat. Hardhat offers the possibility to interact with smart contracts, what offers a more sophisticated testing and benchmarking setup. This environment will provide insights into how the system performs under different loads, reflecting the system's overall capability to handle the complete KYC process in various scenarios.

With the combination of these different development environments and testing networks, it should be highlighted how it would be possible to implement the artifact into a real-world scenario as well as showing the functionality of the combined parts of the KYC-process. Finally, these demonstrations should help to make it easier to evaluate the artifact in the last part of this thesis. It should also help to make the results more comprehensible to the existing knowledge base.

3.6 Evaluation and assessment of the utility of the novel artifact

The purpose of the DSR methodology is to encourage an iterative development process (Peffers et al., 2007). This iterative development tends for ongoing assessment through the whole development process (Scott et al., 2023). The following assessments were conducted through the development of the thesis to reach the highest possible utility of the novel artifact and to match the objectives defined in the previous section.

• After the design & development of the artifact there was an exchange with a Blockchain Developer and a KYC expert. Both experts were interviewed to gather feedback on the novel artifact. Further information about both interview partners can be found in appendix C. The feedback gained could be split into the sub-categories:

1. Compliance with Existing KYC and AML Regulations

2. Data Privacy and GDPR Compliance

3. Regulatory Barriers and Challenges

4. Future Regulatory Adaptation

This feedback was considered into the whole process to reach the pre-defined objective of the artifact (compare part 3.3) regulatory compliance.

• After the development of the artifact a survey was conducted to evaluate the pre-defined objective privacy/trust. This survey pursues the goal, to find out whether the generated artifact is consumer facing. At this stage, a short description as well as a picture of the general process was generated. Subsequently, both of this information were uploaded to Qualtrics (qualtrics.com) to conduct a survey with 50 randomly picked participants. Based on predefined characteristics the aim was to get feedback on the artifact from a demographically representative random sample of the customer base of financial institutions. The survey had been developed based on the DeLone and McLean Model of Information Systems Success (DeLone & McLean, 1992). This model, updated in 2003, provides a comprehensive framework for understanding the success of information systems. The model identifies six dimensions of success: system quality, information quality, service quality, intention to use, user satisfaction, and net benefits. The six dimensions of the model needed to be adapted to the context of our survey (Appendix D). This feedback was necessary to check if the customer itself would be satisfied with the developed solution & trust the developed artifact. The survey has been overviewed by the Commission Board of Nova IMS and reached ethical approval, which can be found in appendix A.

• To evaluate the pre-defined objective efficiency, this thesis will rely on different methods. The process time analysis is used to determine efficiently the blockchain-based KYC artifact processes identity verification compared to traditional KYC systems. Since one of the key objectives is efficiency, measuring the total time required for user onboarding helps assess whether the artifact improves or slows down the process. Evaluating the gas fees associated with smart contract transactions allows for an objective comparison between blockchain-based KYC costs and the operational costs of traditional KYC systems.

• Finally, the artifact will be benchmarked against the metric Transactions per second (TPS) This metric directly refer to the key requirements the novel artifacts need to reach if the objective scalability should be fulfilled. This metric should help to compare the artifact against

existing solutions within future research. Based on these steps, the final solution will be the result of a long iterative development process, where experts, customers and industrial institutions participated.

3.7 Communication of the addition to the knowledge base

The final part of the methodology section will be focused on the communication of the results. First, the goal is to add to the existing knowledge base through this thesis. Furthermore, it will be considered to publish a research paper with the objective of reaching both IS researchers and practitioners. The aim of this work is to create a basis for further research into the optimization of the KYC onboarding process.

It will be considered to present the artifact during academic, public or industry events.

The third chapter of this thesis has been used to describe the methodology this work is based on. The aim was to describe how we came up with the solution and which thoughts/influences have been considered during that process. Chapter 4 of this thesis is going to describe the developed artifact.

4. RESULTS

The following part of the thesis explains the results of the design & development of the novel artifact. Firstly, problem identification will be discussed. Subsequently the design of the novel will be presented with a description of the crucial steps taken through the KYC-onboarding process. In section 4.3, the assessment of the existing blockchain technologies as well as the soulbound tokens will be discussed to identify the solution with the suitability for the novel artifact. Afterwards, the development framework and development will be highlighted. In the final step of section for, the artifact will be evaluated against the pre-defined metrics.

4.1 Problem Identification

The Know Your Customer (KYC) process remains a fundamental requirement for financial institutions to comply with Anti-Money Laundering (AML) and data protection regulations. However, traditional KYC onboarding presents significant challenges, including high costs, inefficiencies, privacy concerns, and a lack of cross-bank interoperability. The cost burden of KYC compliance is substantial, with financial institutions incurring an average expense of $2,598 per corporate client verification, leading to redundant verification processes across multiple banks (Fenergo, 2023). Furthermore, current KYC mechanisms rely heavily on centralized databases, making them susceptible to data breaches and non-compliance with privacy regulations such as GDPR (Moyano & Ross, 2017). Customers also experience frustration due to the repetitive submission of sensitive documents, which raises trust concerns regarding data handling by financial institutions (Al Mamun et al., 2020).

Existing blockchain-based identity solutions have attempted to address these challenges, but they remain fragmented and lack widespread adoption. Self-Sovereign Identity (SSI) frameworks, for instance, allow individuals to control their digital identities, but their implementation is hindered by interoperability issues and the reluctance of financial institutions to embrace decentralized models (Schlatt et al., 2021). Moreover, while cryptographic hashing of KYC documents enhances security, it does not eliminate the inefficiencies of repeated verification across banks, as institutions must still manually authenticate customer data (Hildebrandt, 2023). The absence of standardized mechanisms to link verified identities across financial institutions further exacerbates the inefficiencies in KYC processes.

In addition to inefficiencies, privacy remains a core issue in digital identity verification. Customers are increasingly concerned about the centralized storage of their personal data, as it exposes them to risks of identity theft and unauthorized access (Hannan et al., 2023).

Current blockchain solutions do not fully address privacy concerns, as they often store cryptographic hashes of KYC documents on-chain, which, while immutable, do not provide a trustless mechanism for selective disclosure (Maranhão & Seigneur, 2022). The challenge is to develop a system where customers maintain control over their personal data while allowing financial institutions to verify identity credentials without breaching privacy regulations.

Another critical issue is the security of digital identity verification. Fraudulent activities such as identity spoofing and document forgery continue to pose risks to KYC processes, particularly when verification mechanisms lack tamper-proof attestations (Bhaskaran et al., 2020). While decentralized identity verification models using blockchain improve security, they do not fully prevent fraudulent reuse of credentials in different financial institutions (Goldston et al., 2023). Soulbound Tokens (SBTs), a non-transferable credentialing mechanism, have emerged as a promising solution to mitigate these risks by binding identity attestations to an immutable, verifiable digital identity (Buterin et al., 2022). However, their application in financial KYC processes remains underexplored.

Based on these identified problems, the following objectives have been defined for the novel artifact proposed in this research. First, the artifact must ensure regulatory compliance by aligning with AML, GDPR, and financial industry requirements to support legally sound identity verification. Second, it must enhance privacy and trust by empowering individuals with control over their digital identity while minimizing data exposure. Third, the artifact must ensure scalability, allowing interoperability between multiple financial institutions while reducing redundant verification efforts. Finally, it must improve efficiency by leveraging blockchain and smart contract automation to streamline identity verification and reduce costs. These objectives guide the development of the blockchain-based KYC solution, integrating SBTs to provide a secure, decentralized, and privacy-preserving identity verification mechanism.

4.2 Novel Designed Artifact

Based on the identified problems and the pre-defined objectives, a new artifact has been designed, as shown in Fig. 5. For the artifact to be fully functional, the following assumptions in table 1 are considered to be given:

Role	Technical Requirements
Customer	Ethereum Wallet, Ability to receive Soulbound Tokens
Bank A	Institutional wallet, smart contract deployment, ability to sign verification proofs
Bank B	Institutional wallet, ability to query smart contracts & verify signatures

Table 0.1 – Technical Requirements

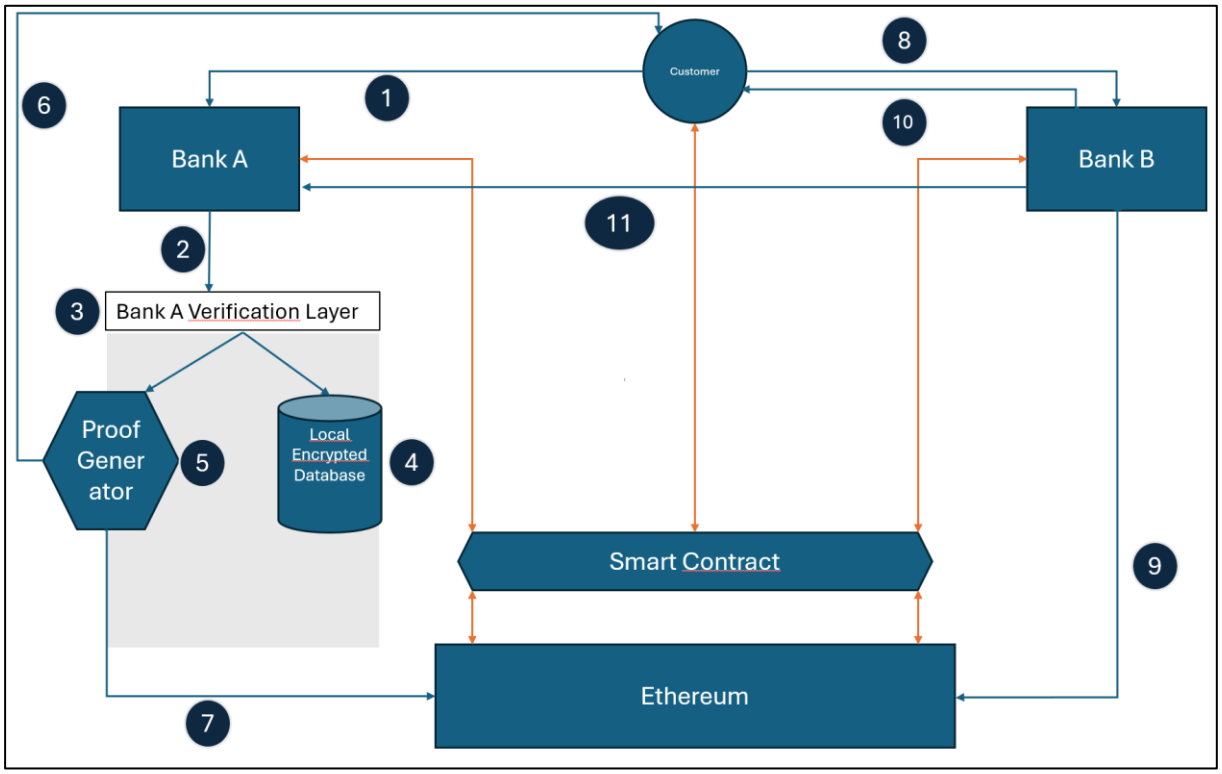


Figure 0.5 - Novel KYC-Onboarding Process

The novel designed artifact includes the following eleven steps:

1. The customer submits their personal identification documents to Bank A through an off-chain system, ensuring that their sensitive information remains private and does not get stored on the blockchain. This step is essential to comply with data protection

regulations such as GDPR and AML directives, preventing unauthorized exposure of personal data (Bluemel, 2024). This submission takes place through traditional banking channels or secure digital platforms, allowing Bank A to collect the necessary information before proceeding with the verification (Hannan et al., 2023).

2. Bank A reviews the submitted documents to check for completeness and accuracy, ensuring that all required identity proofs are included before proceeding with deeper verification. Since this process involves manual or automated document checks against specific regulatory standards, it happens off-chain, where compliance officers or AI-driven KYC solutions assess the validity of passports, IDs, and proof of address (Mugarura, 2014).
3. To comply with financial regulations, Bank A verifies the submitted documents against government databases, sanctions lists, and AML registries, ensuring that the customer is not associated with financial crimes or illicit activities. This verification occurs off-chain as it requires interactions with external data sources that Ethereum smart contracts cannot directly access. Bank A conducts these checks to assess whether the customer meets the necessary regulatory requirements before being approved for services (Hanbar et al., 2019).
4. Once the verification is complete, Bank A securely stores the validated documents in an encrypted local database rather than on-chain, protecting the customer's personal information from public exposure. Since blockchain is immutable and cannot accommodate data deletion requests, storing full documents on-chain would violate privacy laws, making off-chain storage the only viable solution. Instead of storing the documents directly, Bank A prepares for the next step by generating a cryptographic proof that serves as an immutable verification of the completed KYC process (Moyano & Ross, 2017).
5. To create a verifiable attestation of the KYC process, Bank A generates a cryptographic proof by hashing the verified documents using Keccak-256 and signing the proof with its private key. This proof, which acts as a unique fingerprint of the customer's verification, is stored on the Ethereum blockchain through a Solidity smart contract. Solidity is required here to handle the generation and verification of cryptographic signatures, ensuring that other banks can later confirm the authenticity of Bank A’s verification without accessing the actual documents (Thommandru & Chakka, 2023).
6. After the proof has been created, Bank A transmits it directly to the customer’s Ethereum wallet in the form of a Soulbound Token (SBT), a non-transferable digital credential that represents their verified KYC status. Solidity is necessary for deploying an ERC-721 smart contract with transfer restrictions, ensuring that once the SBT is issued, it remains permanently linked to the customer’s wallet. This mechanism enables the customer to prove their identity without repeatedly undergoing verification, enhancing security and convenience (Goldston et al., 2023).
7. To make the verification publicly accessible without compromising privacy, Bank A submits a transaction to the Ethereum mainnet, storing an immutable record of the

KYC verification. This Solidity smart contract logs the customer's wallet address, the issuing bank, the cryptographic proof, and a timestamp, allowing other institutions to later verify the authenticity of the KYC process. Since the actual documents are never stored on-chain, this method ensures privacy while maintaining an auditable record that cannot be altered or forged (Kinyua, 2020).

8. When the customer applies for services at Bank B, they share their KYC proof manually through their Ethereum wallet, presenting the Soulbound Token they received from Bank A. This step does not require Solidity since Ethereum's existing wallet infrastructure allows users to send their verification credentials directly. By enabling self-sovereign identity management, this step reduces dependency on centralized KYC systems and gives customers control over their verified identity (Schlatt et al., 2021)
9. Before approving the customer, Bank B queries the Ethereum blockchain to check if the KYC proof was indeed issued by Bank A. Solidity is essential in this step as the smart contract allows Bank B to verify the cryptographic signature using Ethereum's ecrecover() function, confirming that the proof was generated by a trusted entity and has not been altered. This verification ensures that Bank B can rely on the KYC process without needing to redo the entire verification, streamlining compliance while maintaining security (Moyano et al., 2019).
10. Once the verification has been confirmed, Bank B approves the customer of its services, officially accepting the KYC proof provided by Bank A. Since the decision-making process may involve additional compliance checks and risk assessments, this step occurs off-chain, where Bank B finalizes its internal review before granting full access to financial services (Kihara et al., 2020).
11. To incentivize cooperation between banks and reduce redundant KYC verification efforts, Bank B rewards Bank A with a predefined payment for verifying the customer's identity. This smart contract automates the transaction by checking whether Bank A originally issued the KYC proof, ensuring that the verification was valid before executing an on-chain transfer in ETH. This reward mechanism fosters collaboration within the financial ecosystem, encouraging banks to share trusted KYC attestations while maintaining regulatory compliance (Moyano et al., 2019).

4.3 Assessment of existing Technologies

The following part of the thesis evaluates the existing technologies to identify whether they are suitable for the development of the novel artifact.

4.3.1 Evaluation Framework for Blockchain Suitability

The blockchain suitability evaluation framework assesses whether blockchain is the optimal solution for a given application by analyzing trust assumptions, context requirements, performance characteristics, and consensus mechanisms (Casino et al., 2019). It helps determine if blockchain offers advantages over centralized databases, particularly when multiple distrusting entities require a tamper-proof, decentralized ledger, while also considering constraints such as scalability, latency, and regulatory compliance (Hildebrandt, 2023).

The adoption of blockchain technology in the Know Your Customer (KYC) onboarding process is justified by its ability to address key inefficiencies in traditional identity verification systems. Casino, Dasaklis, and Patsakis (2019) provide a comprehensive review of blockchain applications and highlight its strengths in enhancing security, transparency, and decentralization across various industries, including finance. They emphasize that blockchain is particularly effective in scenarios requiring tamper-proof data storage, trustless verification mechanisms, and efficient identity management, making it a suitable candidate for KYC onboarding in financial institutions (Casino et al., 2019). By leveraging the Ethereum blockchain, financial institutions can mitigate redundant verification efforts, minimize fraudulent identity claims, and streamline compliance with AML and GDPR regulations (Moyano & Ross, 2017).

A key argument for integrating Ethereum into KYC onboarding lies in its ability to establish a decentralized and verifiable identity system. Traditional KYC frameworks require customers to undergo repeated verification processes across multiple banks, leading to inefficiencies and increased operational costs (Malhotra et al., 2021). Ethereum provides an alternative approach by enabling single-instance verification, where once a customer's identity is verified, it is recorded on an immutable ledger and made accessible to authorized financial institutions (Schlatt et al., 2021). This approach aligns with the principles of Self-Sovereign Identity (SSI), allowing customers to retain control over their digital identity while reducing data redundancy and compliance costs (Hildebrandt, 2023). Furthermore, the use of Soulbound Tokens (SBTs) on Ethereum ensures that identity attestations remain non-transferable and immutable, providing a trustworthy verification mechanism without exposing sensitive personal data (Buterin et al., 2022).

Privacy and security are fundamental considerations in KYC processes, and Ethereum's cryptographic capabilities provide enhanced protection against identity theft and unauthorized data access (Hannan et al., 2023). Existing research highlights the vulnerabilities of centralized KYC databases, which are frequently targeted by cyberattacks, leading to large-scale data breaches (Al Mamun et al., 2020). Ethereum mitigates these risks by distributing verification records across a secure, decentralized ledger, ensuring tamper-resistant storage and reducing reliance on centralized repositories (Bhaskaran et al., 2020). Additionally, Ethereum enables zero-knowledge proofs and selective disclosure mechanisms, allowing individuals to verify their credentials without revealing unnecessary personal information, thereby enhancing privacy compliance (Reddy & Kushwaha, 2023).

Furthermore, the blockchain suitability evaluation framework introduced by Casino et al. (2019) supports the selection of Ethereum in KYC applications by assessing trust assumptions, context requirements, performance considerations, and consensus mechanisms. Given that financial institutions often operate in a mutually distrusting environment, Ethereum provides a verifiable, tamper-proof system that enhances cross-institutional trust and reduces fraud (Casino et al., 2019). Unlike permissioned blockchains, which restrict access and require central oversight, Ethereum offers a fully decentralized infrastructure that maintains public transparency while ensuring compliance through cryptographic verification (Hildebrandt, 2023).

By integrating Soulbound Tokens (SBTs) and decentralized identity solutions on Ethereum, this thesis develops an artifact that significantly improves efficiency, security, and privacy in KYC onboarding. The proposed approach enables single-instance verification, enhances data integrity through immutability, and lowers compliance costs by eliminating redundant verification steps (Moyano & Ross, 2017). Given these benefits, Ethereum represents a highly suitable blockchain infrastructure for transforming KYC onboarding in financial institutions, ensuring that compliance, trust, and efficiency are optimized within a secure and privacy-preserving framework.

4.3.2 Soulbound Tokens vs. NFT´s

The use of blockchain-based tokens in the Know Your Customer (KYC) onboarding process is necessary to ensure verifiable, tamper-proof identity attestations while maintaining decentralization and security. By leveraging tokens, financial institutions can store proof of identity verification on-chain without exposing sensitive personal data, enabling seamless, trustless identity verification across multiple institutions (Buterin et al., 2022).

While Non-Fungible Tokens (NFTs) have been widely adopted for digital ownership and verification, they are not suitable for identity management due to their transferability and marketability. NFTs, by design, are meant to be traded, bought, or sold, which introduce risks

such as identity fraud, unauthorized transfers, and misrepresentation in the context of KYC (Goldston et al., 2023). Because identity verification is inherently non-transferable, it requires a mechanism that ensures binding ownership to a single entity. Soulbound Tokens (SBTs) address this limitation by introducing non-transferable credentials, ensuring that verified identity attestations remain permanently associated with a specific individual or institution (Hildebrandt, 2023). This makes SBTs a superior choice for KYC applications, as they provide an immutable, cryptographically verifiable record of identity without the risk of ownership changes (Reddy & Kushwaha, 2023).

Another key advantage of SBTs over NFTs is their alignment with Self-Sovereign Identity (SSI) principles. Unlike NFTs, which can be lost, stolen, or transferred, SBTs remain bound to the original owner, preventing unauthorized access or fraudulent claims of identity verification (Maranhão & Seigneur, 2022). This enhances trust in the KYC process, ensuring that financial institutions can rely on immutable, decentralized verification without the risk of an identity token being sold or manipulated on the secondary market (Goldston et al., 2023). Additionally, SBTs can incorporate revocation mechanisms through community recovery models, ensuring that identity attestations remain up-to-date and trustworthy while minimizing fraud risks (Buterin et al., 2022).

Furthermore, SBTs enhance privacy and regulatory compliance compared to NFTs. Given that financial regulations such as GDPR and AML require stringent data protection mechanisms, the use of non-transferable, encrypted attestations aligns with compliance requirements by minimizing data exposure (Reddy & Kushwaha, 2023). NFTs, in contrast, do not provide built-in privacy safeguards and may expose transaction history, which poses additional privacy risks in sensitive identity applications (Hildebrandt, 2023).

4.4 Development of the novel Artifact

After identifying the problems of the current KYC onboarding process, designing the novel artifact and discussing the available technologies, this step of the thesis describes the development of the novel artifact. First, the steps described in Part 4.2 were analyzed to determine which of these steps can be represented by a smart contract. The results of this evaluation can be seen in table 2. The steps

Step	Solidity Feasibility
Step 1-4	No, Involve document collection, verification, and off-chain storage
Step 5	Can be handled by Solidity – stores a cryptographic hash of the KYC verification on-chain for future validation.

Step 6	Can be handled by Solidity – ERC-721 smart contract ensures that the SBT remains non-transferable and verifiable.
Step 7	Can be handled by Solidity – logs the cryptographic proof, issuing bank, and timestamp in an immutable smart contract.
Step 8	Cannot be handled by Solidity – user manually provides proof through their Ethereum wallet.
Step 9	Can be handled by Solidity – uses smart contract logic to validate cryptographic signatures and verify issuer authenticity.
Step 10	Cannot be handled by Solidity – involves off-chain compliance checks and risk assessments before granting full access.
Step 11	Can be handled by Solidity – smart contract automates ETH payment if KYC verification is valid.

Table 0.2 – Evaluation of Smart Contract/Solidity Feasibility

The individual steps of the artifact, the process during its development are shown below, the full Code written in Solidity can be found in Appendix B:

Step 5: Generate and Store Cryptographic Proof

In this step, Bank A, after verifying the customer's KYC documents, needs to create a tamper-proof record on the blockchain. Since privacy regulations such as GDPR prohibit storing personal data on a public ledger, the bank generates a cryptographic proof instead. The verified documents are hashed using keccak256(), creating a unique fingerprint that cannot be reversed to reveal the original information. This hash is then stored on-chain alongside the customer's wallet address, the issuing bank's address, and a timestamp.

Storing only the cryptographic proof ensures that no personal information is exposed while still allowing other banks to verify that a KYC check was performed. The contract includes a security mechanism ensuring that a KYC record cannot be stored twice for the same customer, which prevents duplicate entries and unnecessary blockchain storage costs. Additionally, only verified banks are permitted to store KYC proofs, ensuring that only trusted institutions participate in the system. Emitting an event upon storing a KYC proof allows off-chain services to track new verifications without querying the blockchain repeatedly, reducing gas costs and enhancing efficiency.

Step 6: Issue a Soulbound Token:
Once the KYC verification is successfully recorded, Bank A issues a Soulbound Token (SBT) to the customer's Ethereum wallet. The purpose of this token is to serve as permanent proof of identity verification without allowing transferability. Unlike regular NFTs, which can be traded, an SBT remains tied to the original owner, preventing misuse by third parties.

By utilizing the ERC-721 standard, the contract ensures seamless integration with existing Ethereum wallets and identity management solutions. The unique token ID is generated from the cryptographic proof, ensuring that each customer receives only one verification token. A security check is implemented to prevent issuing duplicate SBTs, maintaining integrity within the system. Additionally, the _safeMint function is used to ensure that the smart contract correctly mints the token and does not get stuck in an unusable state.

Step 7: Submit Verification Record to Ethereum
After issuing the SBT, Bank A needs to log a public, immutable verification record on the Ethereum blockchain. This step allows other banks to verify that the KYC process was completed without redoing the entire verification. The contract records the customer's address, issuing bank, cryptographic proof, and timestamp. This ensures transparency while maintaining the customer's privacy since only a cryptographic hash is stored instead of raw data.

A key security measure in this step is ensuring that only verified banks can submit KYC verification records. The event-driven architecture is used to make blockchain queries more efficient, allowing external services to track the verification process without incurring additional gas costs. The contract also prevents duplicate entries, ensuring that a customer cannot have multiple records stored unnecessarily (see Appendix B).

Step 9: Verify KYC Proof on Blockchain
Once the verification record is stored, other banks, such as Bank B, can check whether a customer has already completed the KYC process. This prevents the need for customers to repeatedly submit identification documents and undergo redundant verification steps. Instead, Bank B queries the blockchain to check if a valid KYC proof exists for the given customer.
This function is optimized for efficiency by using a view function, which does not require gas fees. Since the verification only requires reading the state of the contract and does not modify it, this approach significantly reduces costs for participating institutions. The function simply checks whether a timestamp exists for the customer in the stored records, returning true if verification is confirmed and false otherwise (see Appendix B).

Step 11: Reward Bank A for Verification

To incentivize banks to perform KYC verification and share their records, the smart contract enables automated reward payments. When Bank B successfully verifies a KYC record issued by Bank A, it sends an ETH payment to compensate for the verification effort. This is handled via a payable function, which allows Bank B to send funds directly through the contract.

The function includes multiple security checks to ensure fairness. It first verifies that the receiving bank is a trusted entity, preventing fraudulent claims. It also ensures that the reward amount is greater than zero, avoiding accidental transactions with no value. Once validated, the contract transfers the ETH payment to Bank A and emits an event to provide a transparent transaction log.

The functionality of the KYC verification system was tested using a structured approach with Truffle and Ganache. The process began by setting up the development environment, where Truffle was installed to manage smart contracts, and Ganache was used to create a local Ethereum blockchain for testing transactions without real money or network delays. A new Truffle project was initialized, providing the necessary structure for writing, compiling, and deploying smart contracts.

After the setup, the smart contract was added to the project, including all key functions for storing KYC proof, issuing a soulbound token, verifying records, and rewarding banks. OpenZeppelin dependencies were installed to ensure secure token implementation. Truffle was then configured to connect with Ganache, allowing the contract to be deployed and interacted with in a controlled environment.

Once the configuration was completed, the contract was compiled successfully, transforming the Solidity code into a format readable by the Ethereum Virtual Machine. The deployment process followed, successfully deploying the contract to the local Ganache blockchain. At this point, the contract was fully accessible and ready for testing.

Automated tests were written using JavaScript and Mocha to confirm the correct functionality of each feature. The first test validated that storing KYC proofs worked correctly. A test proof was submitted, and upon retrieval, the stored hash matched the input, confirming that the storage mechanism operated as expected. The next test checked the issuance of the soulbound token. After calling the issueSBT function, the token was successfully minted to the designated wallet, and an additional check verified that it could not be transferred, ensuring its non-transferability. The KYC verification function was tested next, with a different bank attempting to verify the stored proof. The function correctly returned a positive verification result, confirming that the data on the blockchain could be trusted. Finally, the reward mechanism was tested by sending a payment from a verifying bank to the original issuer. The

transaction was completed, and the receiving bank's balance increased, confirming that the reward system functioned correctly.

After automated testing, manual interaction was conducted using the Truffle console. Transactions were manually sent to test the contract in a real-world scenario. A KYC proof was stored, verified, and successfully linked to a soulbound token. A separate wallet addresses attempted verification, and the contract returned the expected result. The reward mechanism was also executed manually, confirming that payments were processed correctly on the blockchain (see Fig. 9).

With all tests passing and manual verification confirming expected behavior, the KYC system was deemed fully functional. The contract was successfully validated in a controlled environment, confirming its ability to store verification records securely, issue identity tokens, and facilitate trustless verification between banks.

```
let instance = await KYCSmartContract.deployed();
let accounts = await web3.eth.getAccounts();
let bankA = accounts[0];
let customer = accounts[1];
let proof = web3.utils.soliditySha3("KYC_PROOF");

// Add a verified bank
await instance.addVerifiedBank(bankA, { from: bankA });

// Store KYC Proof
await instance.storeKYCProof(customer, proof, { from: bankA });

// Verify KYC
let isVerified = await instance.verifyKYC(customer);
console.log("KYC Verified:", isVerified);

// Issue SBT
await instance.issueSBT(customer, proof, { from: bankA });

// Reward Bank A
await instance.rewardIssuer(bankA, { from: accounts[2], value: web3.utils.toWei("1", "ether")
```

Figure 0.6 – Smart Contract Testing in Ganache

A verification that the system runs can be found in Appendix E.

4.5 Evaluation

In order to evaluate the newly created artifact, the objectives described in Part 3.3 are taken up and assessed according to the evaluation matrices defined in Part 3.6. of this thesis.

Regulatory Compliance

To discuss the regulatory compliance of the novel artifact, interviews been conducted with two KYC experts. The interview questionnaires and an overview of the expert's profiles can be found in Appendix C. Regarding compliance with existing KYC and AML regulations, both experts agreed that the Soulbound Token (SBT)-based verification system aligns well with current compliance requirements by ensuring tamper-proof, verifiable identity attestations while minimizing redundant identity checks. The ability to conduct one-time verification and store immutable proofs on the Ethereum blockchain without exposing sensitive customer data was seen as an advantage. However, Expert A noted that while the system supports regulatory efficiency, further legal validation would be needed to ensure acceptance by financial authorities in different jurisdictions. Expert B stressed that while the model meets fundamental AML and KYC requirements, the practical adoption by financial institutions will depend on regulatory bodies recognizing blockchain-based identity verification as a legally valid process.
Regarding compliance with GDPR, the experts expressed mixed opinions about the use of blockchain for identity management. Expert A pointed out that the system's approach of minimizing on-chain personal data storage aligns with GDPR's data minimization and privacy-by-design principles. However, both experts acknowledged that hashed or encrypted identity attestations could still fall under GDPR's right to erasure clause, which requires further legal clarification. Public keys and blockchain identifiers, if classified as personal data, could pose additional compliance challenges (Expert B). Nevertheless, by storing only non-personal cryptographic proofs on-chain and enabling off-chain verification, the artifact's design inherently reduces the risk of violating GDPR regulations. Expert A suggested that integrating zero-knowledge proofs (ZKPs) could further enhance privacy compliance while maintaining verifiable integrity.

In terms of potential regulatory barriers, both experts emphasized that uncertainties in blockchain regulation remain a challenge for broad industry adoption. Expert B highlighted that while the EU and other global regulators are exploring blockchain governance models, there is currently no standardized framework for decentralized identity verification. This regulatory uncertainty could slow adoption, especially if financial institutions require explicit legal clarity before integrating the system into their compliance workflows. Both experts agreed that the biggest regulatory hurdles include ensuring cross-border compliance and harmonizing blockchain-based KYC solutions with existing financial policies.

Despite these concerns, the experts viewed the long-term regulatory outlook for decentralized identity verification as positive. Expert A noted that governments and regulators are increasingly recognizing the potential of blockchain for secure identity management. They pointed out that the European eIDAS regulation, which seeks to establish a trusted digital identity infrastructure, could be a key driver for the adoption of SBT-based identity verification in financial services. Expert B agreed, stating that regulatory initiatives such as the EU's Digital

Identity Framework could eventually integrate decentralized identity solutions into mainstream financial compliance structures.

Overall, while the proposed system aligns with fundamental KYC, AML, and GDPR requirements, further regulatory validation is necessary to ensure full compliance. Future work should explore legal assessments and regulatory partnerships to bridge the gap between blockchain-based KYC and existing financial laws. The experts emphasized that, despite regulatory uncertainties, the non-transferable, privacy-preserving, and verifiable nature of SBTs provides a strong foundation for modernizing identity verification within financial institutions.

Privacy/Trust

The objective of Privacy and Trust was evaluated through a survey (Appendix D) conducted after the first design phase of the artifact. The goal was to determine whether the Soulbound Token (SBT)-based decentralized KYC system fosters trust among customers, given that identity verification requires the sharing of sensitive personal data. A total of 50 participants took part in the survey, with a diverse demographic composition in terms of age and gender. Participants were introduced to the concept of the artifact through an explanatory description and an accompanying image of the process before answering three key questions regarding system security, trustworthiness, and transparency.

The survey results indicate a strong perception of trust in the designed artifact. When asked about the quality and security of the decentralized KYC system (Question A), 80% of participants rated it as either Excellent (25 participants) or Good (15 participants), suggesting that the decentralized verification model was perceived as secure and reliable. Only five participants remained neutral, and a very small minority expressed concerns, with only five responses in the lower categories (Poor or Very Poor). This suggests that the security guarantees of blockchain-based identity verification were well received by potential users.

In response to the trustworthiness of the identity verification and authentication process using SBTs (Question B), 26 participants rated it as Very Trustworthy and 14 as Trustworthy, amounting to 80% of respondents perceiving the system as reliable. Only a small fraction of participants (4%) viewed the process as untrustworthy. These results demonstrate that the concept of non-transferable, immutable identity attestations contributes to a high level of perceived trustworthiness. The ability of users to retain control over their identity proofs without repeated data sharing aligns with privacy expectations, reinforcing confidence in the system.

Regarding service quality and transparency (Question C), 72% of respondents agreed or strongly agreed that Ethereum blockchain and smart contracts improve the transparency and

quality of the KYC process. However, a minority (18%) expressed neutrality, and a smaller portion (10%) disagreed with the statement. This suggests that while most participants acknowledge the transparency advantages of blockchain, further refinements in user education and system transparency measures may enhance broader acceptance.

Overall, the results demonstrate that the artifact effectively fosters trust and confidence in decentralized identity verification, validating its alignment with privacy-enhancing principles. The survey findings confirm that users recognize the benefits of immutable, non-transferable identity attestations while appreciating the security and transparency improvements enabled by Ethereum-based verification. However, continued refinement based on user feedback, particularly in enhancing transparency and explaining the role of SBTs in fraud prevention—may further strengthen adoption and user confidence in the system.

Scalability

To evaluate the scalability of the new artifact, the Ethereum development framework Hardhat has been used. Hardhat is a widely used Ethereum development framework that provides a robust testing environment for deploying, debugging, and benchmarking smart contracts in a local blockchain network. Its performance measurement capabilities allow for precise evaluation of transaction throughput (TPS) under controlled conditions, ensuring that the artifact's scalability can be assessed before real-world deployment (hardhat.org, 2025). The TPS for the artifact been measured 5 times, the results are shown in the table below:

Measurement	TPS
Measurement 1	18
Measurement 2	21
Measurement 3	20
Measurement 4	18
Measurement 5	19

Table 0.3 – TPS Measurement

Scalability represents a critical determinant of the feasibility and practical implementation of the Soulbound Token (SBT)-based KYC system on the Ethereum blockchain. The TPS (transactions per second) measurements obtained through Hardhat provide an empirical basis for assessing the system's capacity to handle identity verification transactions. The recorded TPS values—18, 21, 20, 18, and 19—yield an average throughput of 19.2 TPS. These results are consistent with Ethereum's known transaction processing limitations, which typically range between 15 to 30 TPS on the base layer.

Given that the artifact operates within the constraints of the Ethereum mainnet, the observed TPS values suggest that the system is capable of handling KYC verification requests at a functional level. However, for large-scale implementation, particularly across multiple

financial institutions, transaction throughput could become a limiting factor should demand for KYC attestations increase significantly. While the current performance may be adequate for moderate adoption, higher transaction volumes may lead to network congestion and increased processing times.
To enhance scalability, further gas optimization techniques and smart contract efficiency improvements should be considered to minimize computational overhead. While this research does not propose Layer 2 scaling solutions, future iterations of the artifact could benefit from Ethereum's evolving scalability roadmap, including proto-danksharding and other performance enhancements, to improve transaction throughput while maintaining decentralization and security.

In conclusion, the TPS measurements indicate that the artifact aligns with Ethereum's baseline scalability expectations but may require further optimizations to accommodate widespread adoption. While transaction speed remains within Ethereum's operational limits, the long-term sustainability of the system will depend on continued advancements in blockchain infrastructure and strategic refinements to smart contract execution to support increasing transactional demand in financial institutions.
Efficiency

Efficiency is a key determinant in assessing the practicality of the Soulbound Token (SBT)-based KYC onboarding process on the Ethereum blockchain. A fundamental aspect of efficiency is cost-effectiveness, particularly in reducing the expenses associated with repeated identity verification. Traditional KYC procedures impose significant costs, with institutions spending an average of $2,598 per corporate client verification (Fenergo, 2023). In contrast, based on the prevailing Ethereum price ($2,676.64) and average gas price (2.129 Gwei), the estimated gas cost per transaction is $0.57 for a basic KYC verification and $1.14 for the issuance of an SBT (compare Appendix E). The stark contrast in cost demonstrates the economic advantage of blockchain-based KYC, which eliminates redundant verification steps and reduces compliance expenses. Additionally, cost efficiency is further improved through an incentivized cost-sharing model, where institutions conducting initial verifications receive automated compensation from those relying on their attestations. This collaborative structure fosters greater efficiency and lowers individual verification costs for financial institutions.

Beyond cost, processing time is another key factor. Conventional KYC frameworks involve document submission, manual review, background checks, and approvals, often requiring days or even weeks for completion. The proposed system substantially reduces verification time by enabling instant authentication of pre-verified identities through Soulbound Tokens (SBTs). Once issued, a SBT allows financial institutions to verify a customer's identity within seconds, eliminating redundant onboarding steps. This transition improves operational efficiency, granting customers faster access to financial services while reducing the administrative workload on compliance teams.

In conclusion, the blockchain-based KYC artifact significantly enhances efficiency by reducing costs, processing time, and administrative redundancy compared to conventional methods. The ability to verify identities instantly while fostering cost-sharing among financial institutions makes this approach scalable, economically viable, and operationally efficient. While network congestion and gas price fluctuations may introduce variability, the long-term benefits of decentralization, automation, and financial incentivization position this system as a superior alternative to traditional KYC models.

5. DISCUSSION

This research sets out to determine whether it is possible to develop a blockchain-based artifact that effectively addresses customer privacy concerns while simultaneously reducing KYC onboarding costs for financial institutions. The findings indicate that the proposed Soulbound Token (SBT)-based identity verification system meets these objectives in several ways. By utilizing non-transferable blockchain-based credentials, the artifact ensures that customer identities remain under their control while minimizing data exposure, thereby addressing privacy concerns raised in traditional KYC processes (Moyano et al., 2029). Additionally, the cost of verification per transaction, ranging between $0.57 and $1.14, is significantly lower than the traditional KYC process, which incurs an average cost of $2,598 per corporate client verification (Fenergo, 2023). By eliminating redundant verification steps and introducing an incentive-based cost-sharing model, the proposed system demonstrates a substantial economic advantage over conventional KYC procedures (Moyano & Ross, 2017).

Despite these positive outcomes, the research identifies several limitations and challenges. A major concern is the use of a public blockchain, which financial institutions may perceive as a privacy risk (Moyano et al., 2019). Although cryptographic proofs ensure that no personal data is directly stored on-chain, the fact that verification attestations are publicly visible may raise regulatory concerns, particularly under GDPR compliance frameworks (Hannan et al., 2023). Additionally, the artifact's reliance on a single verifying institution to issue the initial SBT could create a potential lock-in effect, restricting customers to the first verifying entity (Schlatt et al., 2021). This limitation may hinder competition and reduce interoperability between financial institutions unless a broader adoption framework is established to encourage multi-bank participation in the verification process (Hildebrandt, 2023).

The evaluation of the predefined research objectives suggests mixed results. Regulatory compliance was partially achieved through tamper-proof attestations and immutable verification records, aligning with AML and KYC requirements (Moyano & Ross, 2017). However, the uncertain legal status of blockchain-based identity verification raises concerns about full regulatory recognition, especially in cross-border financial transactions (Bhaskaran et al., 2020). Regarding privacy and trust, survey responses indicate that users perceive the system as highly trustworthy, with 80% rating the security and reliability of the artifact favorably. This supports the claim that SBTs enhance self-sovereign identity management while minimizing data exposure risks (Maranhão & Seigneur, 2022).

Scalability, however, presents significant challenges. The measured TPS values (18–21 TPS) confirm that, while the artifact functions effectively on Ethereum’s current infrastructure, its adoption at a global scale may be constrained by Ethereum’s throughput limitations. Future optimizations, such as gas-efficient smart contract designs or interoperability with emerging Ethereum scaling solutions, could address these issues (Goldston et al., 2023). Meanwhile, the

efficiency of the artifact was validated through reduced onboarding times, with identity verification occurring within seconds rather than days, eliminating the need for repeated document submissions and manual compliance checks (Hannan et al., 2023). Furthermore, the cost-sharing mechanism among banks significantly improves cost efficiency, reducing the financial burden of KYC compliance by encouraging institutions to leverage shared identity attestations (Moyano et al., 2019).

Several limitations of this study must be acknowledged. The research was conducted in a controlled testing environment, meaning that real-world factors such as Ethereum network congestion, gas fee fluctuations, and institutional adoption challenges were not fully accounted for (Reddy & Kushwaha, 2023). Moreover, while the artifact addresses privacy concerns through cryptographic proofs, further research is needed to determine how regulatory bodies will interpret blockchain-based identity attestations under GDPR (Hildebrandt, 2023). Another limitation concerns interoperability—since financial institutions operate within different regulatory jurisdictions, integrating a decentralized identity framework across multiple banking networks may require additional policy standardization efforts (Bhaskaran et al., 2020).

Given these findings, several avenues for future research emerge. First, further investigation is needed into privacy-enhancing cryptographic mechanisms, such as zero-knowledge proofs (ZKPs), to enhance selective disclosure capabilities and reduce privacy risks associated with public attestations (Buterin et al., 2022). Additionally, research should explore strategies to increase multi-bank adoption to prevent lock-in effects, ensuring that the system remains decentralized and widely accessible (Schlatt et al., 2021). Future studies should also examine the long-term economic impact of incentivized verification models, determining how financial institutions can be encouraged to participate in a shared KYC framework without monopolizing the verification process (Casino et al., 2019). Lastly, technical optimizations, such as Ethereum Layer 2 solutions or alternative consensus mechanisms, should be explored to improve scalability and processing efficiency while maintaining trust and decentralization (Goldston et al., 2023).

6. CONCLUSIONS AND FUTURE WORKS

The KYC process in its traditional form remains a significant challenge for financial institutions. The high costs associated with collecting customer data during onboarding, the continuous monitoring of transactions, and the ongoing verification of KYC data present persistent difficulties. To address these issues, both industry practitioners and academic researchers have shifted their focus toward blockchain technology and its potential to resolve existing inefficiencies.

This thesis applied the Design Science Research (DSR) methodology to develop a novel artifact that optimizes the KYC onboarding process. The artifact is designed on the Ethereum blockchain, providing a decentralized and innovative solution that can be integrated into various financial environments while ensuring security and trust between customers and financial institutions. By leveraging Ethereum's infrastructure, the proposed solution facilitates immutable, verifiable identity attestations while maintaining regulatory compliance and operational efficiency.

A thorough literature review was conducted to capture the current research landscape in blockchain-based KYC solutions. The analysis identified key challenges, leading to the research question of whether it is possible to create an artifact that balances the objectives of scalability, decentralization, regulatory compliance, and privacy. To meet these objectives, this thesis proposes an artifact that integrates these principles and utilizes Soulbound Tokens (SBTs) as non-transferable, verifiable identity attestations rather than traditional NFTs. The implementation of SBTs ensures enhanced privacy, reduced redundancy, and fraud prevention by permanently binding identity credentials to users without compromising security.

During the design and development process, iterative feedback was gathered from industry experts and users through interviews and surveys. Existing blockchain solutions and components were adapted and customized to align with the objectives of this research. To construct the artifact, blockchain decision-making criteria from the literature were applied to guide the selection of data management models, security features, consensus mechanisms, and smart contract design. The Ethereum framework, in conjunction with Solidity, Truffle, and Ganache, was employed to develop and test the prototype, ensuring a functional and scalable implementation.

The effectiveness of the proposed artifact is evaluated using key blockchain performance metrics, specifically transaction throughput (TPS) and gas costs per transaction. The results demonstrate that decentralized identity verification through SBTs provides a cost-efficient and privacy-preserving alternative to traditional KYC processes while maintaining compliance with financial regulations.

As digital transactions and online financial services continue to expand, the need for modernized, scalable, and privacy-focused KYC solutions will become increasingly critical. Future research should explore additional improvements, such as the integration of zero-knowledge proofs for enhanced privacy, cross-chain interoperability for wider financial adoption, and further regulatory considerations. This thesis lays the groundwork for future studies in decentralized KYC solutions, offering a foundation for advancing blockchain-based identity verification models in financial institutions.

BIBLIOGRAPHICAL REFERENCES

Al Mamun, M. A., Azad, M. A. K., Das, S., & Rahman, M. A. (2020). Secure and transparent KYC for banking system using IPFS and blockchain technology. *2020 IEEE Region 10 Symposium (TENSYMP)*. IEEE. https://doi.org/10.1109/TENSYMP50017.2020.9230987

Arasa, R. (2015). Determinants of Know Your Customer (KYC) compliance among commercial banks in Kenya. *Journal of Economics and Behavioral Studies, 7*(2(J)), 162-175. https://doi.org/10.22610/jebs.v7i2(J).574

Arner, D. W., Zetzsche, D. A., Buckley, R. P., & Barberis, J. N. (2019). The identity challenge in finance: From analogue identity to digitized identification to digital KYC utilities. *European Business Organization Law Review, 20*(1), 55–80.

Bai, X., Cheng, Z., Duan, Z., & Hu, K. (2018). Formal modeling and verification of smart contracts. *Proceedings of the 2018 7th International Conference on Software and Computer Applications*, 322–326. https://doi.org/10.1145/3185089.3185138

Baskerville, R. (2008). What design science is not. *European Journal of Information Systems, 17*(5), 441-443. https://doi.org/10.1057/ejis.2008.45

Baum, C., Chiang, J. H., David, B., & Frederiksen, T. K. (2023). SoK: Privacy-enhancing technologies in finance. *282*(12), 12:1-12:0. https://doi.org/10.4230/LIPIcs.AFT.2023.12

Ben-Sasson, E., Bentov, I., Horesh, Y., & Riabzev, M. (2018). Scalable, transparent, and post-quantum secure computational integrity. *Cryptology ePrint Archive*, Paper 2018/046. https://eprint.iacr.org/2018/046.pdf

Ben-Sasson, E., Chiesa, A., Tromer, E., & Virza, M. (2017). Scalable zero knowledge via cycles of elliptic curves. Algorithmica, 79(4), 1102–1160. https://doi.org/10.1007/s00453-016-0221-0

Bez, M., Fornari, G., & Vardanega, T. (2019). The scalability challenge of Ethereum: An initial quantitative analysis. *2019 IEEE International Conference on Service-Oriented System Engineering (SOSE)*, 167-176. IEEE. https://doi.org/10.1109/SOSE.2019.00031

Biel, P., Zhang, S., & Jacobsen, H. (2021). A zero-knowledge proof system for OpenLibra. *Proceedings of the 22nd International Middleware Conference: Demos and Posters.* https://doi.org/10.1145/3491086.3492469

Bitansky, N., Chiesa, A., Ishai, Y., Ostrovsky, R., & Paneth, O. (2013). Succinct non-interactive arguments via linear interactive proofs. *Proceedings of the TCC, 2013*, 7785, 315–333. Springer, Berlin/Heidelberg.

Bluemel, J. (2024). 3 KYC components every financial institution must follow. *IDnow*. Retrieved from https://www.idnow.io/blog/financial-institution-kyc-components/

Buterin, V. (2015). On public and private blockchains. *Ethereum Blog*. Retrieved from https://blog.ethereum.org/2015/08/07/onpublic-and-private-blockchains/

Buterin, V., Weyl, E. G., & Ohlhaver, P. (2022). Decentralized society: Finding Web3's soul. *SSRN*. https://dx.doi.org/10.2139/ssrn.4105763

Capgemini Consulting. (2017). Smart contracts in financial services: Getting from hype to reality. Retrieved from https://www.capgemini.com/consulting-de/wp-content/uploads/sites/32/2017/08/smart_contracts_paper_long_0.pdf

Capko, D., Vukmirovic, S., & Nedic, N. (2022). State of the art of zero-knowledge proofs in blockchain. *2022 30th Telecommunications Forum (TELFOR)*, 1-4. https://doi.org/10.1109/TELFOR56187.2022.9983760

Castellon, C., Roy, S., Kreidl, P., Dutta, A., & Bölöni, L. (2021). Energy-efficient Merkle trees for blockchains. *2021 IEEE 20th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, 1093-1099.

Chauhan, A., Malviya, O. P., Verma, M., & Mor, T. S. (2018). Blockchain and scalability. *2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C)*, 122-128. IEEE. https://doi.org/10.1109/QRS-C.2018.00034

Chen, T., Lu, H., Kunpittaya, T., & Luo, A. (2022). A review of zk-SNARKs. arXiv. https://doi.org/10.48550/arXiv.2202.06877

Chen, Y.-C., Chou, Y.-P., & Chou, Y.-C. (2019). An image authentication scheme using Merkle tree mechanisms. Future Internet, 11(7), 149. https://doi.org/10.3390/fi11070149

Colladon, A. F., & Remondi, E. (2017). Using social network analysis to prevent money laundering. *Expert Systems with Applications, 67*, 49-58. https://doi.org/10.1016/j.eswa.2016.09.029

Cong, L. W., & He, Z. G. (2018). Blockchain disruption and smart contracts. *Booth School of Business, University of Chicago and NBER*.

Dai, W. (1998). B-Money. Retrieved from http://www.weidai.com/bmoney.txt

Dedeoglu, V., Jurdak, R., Dorri, A., Lunardi, R., Michelin, R., Zorzo, A., & Kanhere, S. (2020). Blockchain technologies for IoT. In *Advanced Applications of Blockchain Technology* (pp. 55–89). Springer, Singapore.

Delmolino, K., Arnett, M., & Kosba, A. (2016). Step by step towards creating a safe smart contract: Lessons and insights from a cryptocurrency lab. *International Conference on Financial Cryptography and Data Security*. https://doi.org/10.1007/978-3-662-53357-4_6

Dhiman, B., & Bose, R. (2022). A reliable, secure and efficient decentralized conditional KYC verification system: A blockchain approach. In Proceedings of the 2022 International Conference on Edge Computing and Applications (ICECAA) (pp. 564–570). IEEE. https://doi.org/10.1109/ICECAA55415.2022.9936486

Dob, D. (2018). Permissioned vs permissionless blockchains: Understanding the differences. Retrieved from https://blockonomi.com/permissioned-vspermissionless-

Doe, J. (2021, May 5). Ethereum development tools. *Ethereum.org*. Retrieved from https://ethereum.org/en/developers/docs/development-tools/

Donno, L. (2022). Optimistic and validity rollups: Analysis and comparison between Optimism and StarkNet. *ArXiv*, abs/2210.16610. https://doi.org/10.48550/arXiv.2210.16610

Elinzano, G. B. O., & Ching, M. R. D. (2022). Factors that lead to adoption and use of online bank account opening through e-KYC using UTAUT and its extensions. *RSF Conference Series: Engineering and Technology, 2*(1), 85–94. https://doi.org/10.31098/cset.v2i1.508

Engström, E., Storey, M.-A., Runeson, P., Höst, M., & Baldassarre, M. T. (2020). How software engineering research aligns with design science: A review. Empirical Software Engineering, 25(4), 2630–2660. https://doi.org/10.1007/s10664-020-09818-7

Efanov, D., & Roschin, P. (2018). The all-pervasiveness of the blockchain technology. *Procedia Computer Science, 123*, 116-121. https://doi.org/10.1016/j.procs.2018.01.019

Fuchsbauer, G. (2018). Subversion-zero-knowledge SNARKs. *315-347*. https://doi.org/10.1007/978-3-319-76578-5_11

Fenergo. (2023). KYC in 2023 – Tackling amid heightened global challenges. *Fenergo*. Retrieved from https://www.fenergo.com/de/kyc-trends

Gailly, N., Maller, M., & Nitulescu, A. (2021). SnarkPack: Practical SNARK aggregation. *203-229*. https://doi.org/10.1007/978-3-031-18283-9_10

Garlichs, I., & Dosch, S. (2017). First steps with Ethereum – Concept & implementation of DApp.

Garewal, K. S. (2020). Merkle trees. In Practical blockchains and cryptocurrencies: Speed up your application development process and develop distributed applications with confidence (pp. 137–148). Apress. https://doi.org/10.1007/978-1-4842-5893-4_10

Geetha, R., Padmavathy, T., & Srikanth, G. U. (2021). A scalable blockchain framework for user identity management in a decentralized network. Wireless Personal Communications, 121(1), 1–17. https://doi.org/10.1007/s11277-021-08628-3

Goldston, J., Chaffer, T. J., Osowska, J., & Von Goins, C. A. (2023). Digital inheritance in Web3: A case study of Soulbound Tokens and the Social Recovery Pallet within the Polkadot and Kusama ecosystems. arXiv preprint arXiv:2301.11074. https://doi.org/10.48550/arXiv.2301.11074

Gong, Y., Jin, Y., Li, Y., Liu, Z., & Zhu, Z. (2022). Analysis and comparison of the main zero-knowledge proof scheme. *2022 International Conference on Big Data, Information and Computer Network (BDICN)*, 366-372. https://doi.org/10.1109/BDICN55575.2022.00074

Grassi, L., Kales, D., Khovratovich, D., Roy, A., Rechberger, C., & Schofnegger, M. (2019). Starkad and Poseidon: New hash functions for zero-knowledge proof systems. IACR Cryptology ePrint Archive, 2019, 458. https://doi.org/10.46586/tches.v2021.i2.59-111

Gregor, S., & Hevner, A. R. (2013). Positioning and presenting design science research for maximum impact. MIS Quarterly, 37(2), 337–355. https://doi.org/10.25300/MISQ/2013/37.2.01

Gupta, A., Dwivedi, D. N., & Shah, J. (2023). Financial crimes management and control in financial institutions. In *Artificial Intelligence Applications in Banking and Financial Services* (pp. 29-45). Springer, Singapore. https://doi.org/10.1007/978-981-99-2571-1_2

Gupta, A., & Gurkan, K. (2022). An ECDSA nullifier scheme for unique pseudonymity within zero-knowledge proofs. *IACR Cryptology ePrint Archive, 2022*, 1255.

Hanbar, H., Shukla, V., Modi, C., & Vyjayanthi, C. (2019). Optimizing e-KYC process using distributed ledger technology and smart contracts. In A. Saha, N. Kar, & S. Deb (Eds.), Advances in Computational Intelligence, Security and Internet of Things (pp. 132–145). Springer. https://doi.org/10.1007/978-981-15-3666-3_12

Hannan, M. A., Shahriar, M. A., Ferdous, M. S., Chowdhury, M. J. M., & Rahman, M. S. (2023). A systematic literature review of blockchain-based e-KYC systems. *Computing, 105*, 2089–2118. https://doi.org/10.1007/s00607-023-01176-8

Hartsink, G. (2018). The digital identity of legal entities: Current status and the way forward. *Journal of Payments Strategy & Systems, 12*(1), 1–7.

Hardhat.org. (2025). Hardhat Runner: Getting started. Retrieved from https://hardhat.org/hardhat-runner/docs/getting-started#overview

Hassija, V., Zeadally, S., Jain, I., Tahiliani, A., Chamola, V., & Gupta, S. (2021). Framework for determining the suitability of blockchain: Criteria and issues to consider. *Transactions on Emerging Telecommunications Technologies, 32*. https://doi.org/10.1002/ett.4334

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS Quarterly, 28*(1), 75-105. https://doi.org/10.2307/25148625

Hildebrandt, F. (2022). The future of soulbound tokens and their blockchain accounts. Konferenzband zum Scientific Track der Blockchain Autumn School 2022, 2, 18–24. https://doi.org/10.48446/opus-13450

Holzenthal, F. (2017). Five trends shaping the fight against financial crime. *Computer Fraud & Security, 2017*(3), 5-9. https://doi.org/10.1016/S1361-3723(17)30022-2

IBM. (2023). Cost of a data breach report 2023. *IBM Security*. Retrieved from https://www.ibm.com/reports/data-breach

ING Bank. (2024). Our influence in the distributed ledger technology ecosystem. Retrieved from https://www.ingwb.com/en/insights/distributed-ledger-technology/our-influence-in-the-distributed-ledger-technology-ecosystem

Iivari, J. (2010). Twelve theses on design science research in information systems. In A. Hevner & S. Chatterjee (Eds.), Design research in information systems: Theory and practice (pp. 43–62). Springer. https://doi.org/10.1007/978-1-4419-5653-8_5

Jain, H., Agrawal, S., Khandelwal, H., & Sawant, V. (2020). Financial investment recommendation and decentralized account management. In Proceedings of the 2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT) (pp. 1–6). IEEE. https://doi.org/10.1109/ICCCNT49239.2020.9225326

Jessel, B., Lowmaster, K., Hughes, N., et al. (2018). Digital identity: The foundation for trusted transactions in financial services. *Journal of Financial Transformation, 47*, 143–150.

Moor, J. H. (1997). Towards a theory of privacy in the information age. ACM SIGCAS Computers and Society, 27(3), 27–32. https://doi.org/10.1145/270858.270866

Jing, S., Zheng, X., & Chen, Z. (2021). Review and investigation of Merkle tree's technical principles and related application fields. In Proceedings of the 2021 International Conference on Artificial Intelligence, Big Data and Algorithms (CAIBDA) (pp. 86–90). IEEE. https://doi.org/10.1109/CAIBDA53561.2021.00026

Johannesson, P., & Perjons, E. (2014). An introduction to design science. Springer. https://doi.org/10.1007/978-3-319-10632-8

Kakavand, H., Kost De Sevres, N., & Chilton, B. (2017). The blockchain revolution: An analysis of regulation and technology related to distributed ledger technologies. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.2849251

Kapsoulis, N., Psychas, A., Palaiokrassas, G., Marinakis, A., Litke, A., & Varvarigou, T. (2020). Know your customer (KYC) implementation with smart contracts on a privacy-oriented decentralized architecture. *Future Internet, 12*(2), 41. https://doi.org/10.3390/fi12020041

Kerber, T., Kiayias, A., & Kohlweiss, M. (2020). Mining for privacy: How to bootstrap a snarky blockchain. *497-514*. https://doi.org/10.1007/978-3-662-64322-8_24

Khan, D., Jung, L. T., & Hashmani, M. A. (2021). Systematic literature review of challenges in blockchain scalability. *Applied Sciences, 11*(20), 9372. https://doi.org/10.3390/app11209372

KPMG. (2020). Blockchain coming to the fore. Retrieved from https://kpmg.com/ae/en/home/insights/2020/04/uae-banking-perspectives-2020.html

KPMG International. (2018). Could blockchain be the foundation of a viable KYC utility? Retrieved from https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2018/03/kpmg-blockchain-kyc-utility.pdf

Kuperberg, M., Kemper, S., & Durak, C. (2019). Blockchain usage for government-issued electronic IDs: A survey. In H. A. Proper & J. Stirna (Eds.), The Practice of Enterprise Modeling: Proceedings of the 12th IFIP Working Conference, PoEM 2019 (pp. 319–328). Springer. https://doi.org/10.1007/978-3-030-35151-5_21

Lavaur, T., Lacan, J., & Chanel, C. P. C. (2022). Enabling blockchain services for IoE with Zk-Rollups. *Sensors, 22*(17), 6493. https://doi.org/10.3390/s22176493

LexisNexis Risk Solutions. (2017). The true cost of anti-money laundering compliance. Retrieved from https://risk.lexisnexis.com/global/en/insights-resources/research/the-true-cost-of-aml-compliance-european-survey

Li, Q., & Xue, Z. (2021). A privacy-protecting authorization system based on blockchain and zk-SNARK. *Proceedings of the 2020 International Conference on Cyberspace*

Innovation of Advanced Technologies, 439–444. https://doi.org/10.1145/3444370.3444610

Lin, X., Zhang, Y., Huang, C., Xing, B., Chen, L., Hu, D., & Chen, Y. (2023). An access control system based on blockchain with zero-knowledge rollups in high-traffic IoT environments. *Sensors, 23*(7), 3443. https://doi.org/10.3390/s23073443

Liu, H., Luo, X., Liu, H., & Xia, X. (2021). Merkle tree: A fundamental component of blockchains. In Proceedings of the 2021 International Conference on Electronic Information Engineering and Computer Science (EIECS) (pp. 556–561). IEEE. https://doi.org/10.1109/EIECS53707.2021.9588047

L. Perlman, N. Gurung. (2019). Focus note: The use of eKYC for customer identity and verification and AML. Retrieved from https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID3370665_code505438.pdf?abstractid=3370665

Malhotra, D., Saini, P., & Singh, A. (2021). How blockchain can automate KYC: Systematic review. *Wireless Personal Communications, 122*, 1987-2021. https://doi.org/10.1007/s11277-021-08977-0

Malinova, K., & Park, A. (2017). Market design with blockchain technology. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2785626

Maranhão, S. M. B., & Seigneur, J. M. (2022). Enabling KYC and AML verification in DeFi services. *Crypto Valley Association.*

March, S. T., & Smith, G. F. (1995). Design and natural science research on information technology. *Decision Support Systems, 15*(4), 251-266. https://doi.org/10.1016/0167-9236(94)00041-2

March, S. T., & Vogus, T. J. (2010). Design science in the management disciplines. In A. Hevner & S. Chatterjee (Eds.), *Design research in information systems: Theory and practice* (pp. 195–208). Springer. https://doi.org/10.1007/978-1-4419-5653-8_14

Mizrahi, A., Koren, N., & Rottenstreich, O. (2021). Optimizing Merkle proof size for blockchain transactions. In *Proceedings of the 2021 International Conference on COMmunication Systems & NETworkS (COMSNETS)* (pp. 299–307). IEEE. https://doi.org/10.1109/COMSNETS51098.2021.9352820

Morana, S., et al. (2018). Tool support for design science research—Towards a software ecosystem: A report from a DESRIST 2017 Workshop. *Communications of the Association for Information Systems, 43*(1), 237-256. https://doi.org/10.17705/1CAIS.04317

Mugarura, N. (2014). Customer due diligence (CDD) mandate and the propensity of its application as a global AML paradigm. *Journal of Money Laundering Control, 17*(1), 75–96.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Retrieved from www.bitcoin.org

Norvill, R., Hilger, J., Awan, I., Cullen, A., & State, R. (2020). Decentralised compliant data trading for banks. *Proceedings of the 2nd International Electronics Communication Conference.* https://doi.org/10.1145/3409934.3409947

Ostern, N. K., & Riedel, J. (2021). Know-your-customer (KYC) requirements for initial coin offerings: Toward designing a compliant-by-design KYC-system based on blockchain technology. *Business Information Systems Engineering, 63*(5), 551-567. https://doi.org/10.1007/s12599-020-00677-6

Ostrowski, Ł., & Helfert, M. (2011). Commonality in various design science methodologies. In *Proceedings of the Federated Conference on Computer Science and Information Systems* (pp. 317–320). IEEE Computer Society Press. https://doi.org/10.15439/2011F324

Parno, B., Howell, J., Gentry, C., & Raykova, M. (2013). Pinocchio: Nearly practical verifiable computation. In *Proceedings of the 2013 IEEE Symposium on Security and Privacy* (pp. 238–252). IEEE. https://doi.org/10.1109/SP.2013.47

Parra Moyano, J., & Ross, O. (2017). KYC optimization using distributed ledger technology. *Business & Information Systems Engineering, 59*(6), 411–423. https://doi.org/10.1007/s12599-017-0504-2

Parra-Moyano, J., Thoroddsen, T., & Ross, O. (2019). Optimized and dynamic KYC system based on blockchain technology. *International Journal of Blockchains and Cryptocurrencies, 1*(1), 85–106. https://doi.org/10.1504/IJBC.2019.10021398

Partala, J., Nguyen, T. H., & Pirttikangas, S. (2020). Non-interactive zero-knowledge for blockchain: A survey. *IEEE Access, 8*, 227945-227961. https://doi.org/10.1109/ACCESS.2020.3039824

Patel, D., Suslade, H., Rane, J., Prabhu, P., Saluja, S., & Busnel, Y. (2020). KYC as a service (KASE) – A blockchain approach. In D. Bhattacharyya, H. Sasaki, & M. Elhoseny (Eds.), *Advances in machine learning and computational intelligence* (pp. 869–877). Springer. https://doi.org/10.1007/978-981-15-5243-4_76

Patil, S., Pitchai, R., Madhubabu, C., & Gunasekaran, K. (2022). Know your customer (KYC) as a service for business process management (BPM) using cloud computing. In *Proceedings of the 2022 International Conference on Innovative Computing, Intelligent*

Communication and Smart Electrical Systems (ICSES) (pp. 733–738). IEEE. https://doi.org/10.1109/ICSES55317.2022.9914162

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of Management Information Systems, 24*(3), 45-77. https://doi.org/10.2753/MIS0742-1222240302

Peffers, K., Tuunanen, T., & Niehaves, B. (2018). Design science research genres: Introduction to the special issue on exemplars and criteria for applicable design science research. *European Journal of Information Systems, 27*(2), 129-139. https://doi.org/10.1080/0960085X.2018.1458066

Peters, G. W., & Panayi, E. (2016). Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money. In P. Tasca, T. Aste, L. Pelizzon, & N. Perony (Eds.), *Banking beyond banks and money: A guide to banking services in the twenty-first century* (pp. 239–278). Springer. https://doi.org/10.1007/978-3-319-42448-4_13

Pilkington, M. (2016). Blockchain technology: Principles and applications. In F. X. Olleros & M. Zhegu (Eds.), *Research handbook on digital transformations* (pp. 225–253). Edward Elgar Publishing. https://doi.org/10.4337/9781784717766.00019

Pauwels, P., Pirovich, J., Braunz, P., & Deeb, J. (2022). zkKYC in DeFi: An approach for implementing the zkKYC solution concept in decentralized finance. *IACR Cryptology ePrint Archive, 2022*, 321.

Rajyashree, U. A., Doulani, S., & Pareek, S. (2019). Blockchain-enabled e-KYC system. *International Research Journal of Computer Science, 6*, 137–143.

Reddy, S., & Kushwaha, D. S. (2023). Framework for privacy-preserving credential issuance and verification using Soulbound Tokens. *Motilal Nehru National Institute of Technology*.

Sanction Scanner. (2023). Changes in anti-money laundering over time. Retrieved from https://www.sanctionscanner.com/blog/anti-money-laundering-changed-over-time-451

Sanka, A. I., & Cheung, R. C. C. (2021). A systematic review of blockchain scalability: Issues, solutions, analysis and future research. *Journal of Network and Computer Applications, 195*, 103232. https://doi.org/10.1016/j.jnca.2021.103232

Schlatt, V., Sedlmeir, J., Feulner, S., & Urbach, N. (2021). Designing a framework for digital KYC processes built on blockchain-based self-sovereign identity. *Information & Management, 59*(1), Article 103553. https://doi.org/10.1016/j.im.2021.103553

Scott, I. J., de Castro Neto, M., & Pinheiro, F. L. (2023). Bringing trust and transparency to the opaque world of waste management with blockchain: A Polkadot parathread application. *Computers & Industrial Engineering, 182*, 109347. https://doi.org/10.1016/j.cie.2023.109347

Sguanci, C., Spatafora, R., & Vergani, A. M. (2021). Layer 2 blockchain scaling: A survey. *arXiv preprint arXiv:2107.10881*. https://doi.org/10.48550/arXiv.2107.10881

Sklaroff, J. (2017). Smart contracts and the cost of inflexibility. *University of Pennsylvania Law Review, 166.*

Soltani, R., Nguyen, U. T., & An, A. (2018). A new approach to client onboarding using self-sovereign identity and distributed ledger. *2018 IEEE International Conference on Internet of Things (iThings), Green Computing and Communications (GreenCom), Cyber, Physical and Social Computing (CPSCom), and Smart Data (SmartData)* (pp. 1129-1136). IEEE. https://doi.org/10.1109/Cybermatics_2018.2018.00205

Soni, A., & Duggal, R. (2014). Reducing risk in KYC (Know Your Customer) for large Indian banks using big data analytics. *International Journal of Computer Applications, 97*(9), 49–53. https://doi.org/10.5120/17049-7439

Sundareswaran, N., Sasirekha, S., Paul, I. J. L., Balakrishnan, S., & Swaminathan, G. (2020). Optimised KYC blockchain system. In *Proceedings of the 2020 International Conference on Innovative Trends in Information Technology (ICITIIT)* (pp. 1–6). IEEE. https://doi.org/10.1109/ICITIIT49094.2020.9071533

Szabo, N. (1996). Smart contracts: Building blocks for digital markets. Retrieved from http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html

Tanksali, A. (2021). XipCOIN: A proposal for decentralized offline payments using Ethereum. *2021 IEEE 2nd International Conference on Technology, Engineering, Management for Societal Impact using Marketing, Entrepreneurship and Talent (TEMSMET)* (pp. 1-6). IEEE. https://doi.org/10.1109/TEMSMET53515.2021.9768705

Theadore, I., & Sitoh, P. (2022). Decentralising personal credit score. *Handbook of Research on Social Impacts of E-Payment and Blockchain Technology*. https://doi.org/10.4018/978-1-7998-9035-5.ch003

Thibault, L. T., Sarry, T., & Hafid, A. S. (2022). Blockchain scaling using rollups: A comprehensive survey. *IEEE Access, 10*, 93039-93054. https://doi.org/10.1109/ACCESS.2022.3200051

Tran, A. C., Thanh, V. V., Tran, N. C., & Nguyen, H. T. (2023). An implementation and evaluation of Layer 2 for Ethereum with zk-Rollup. *Lecture Notes in Computer Science (LNCS), 13831.* https://doi.org/10.48550/arXiv.2210.16610

Truffle Suite. (n.d.). Documentation. *Truffle Suite*. Retrieved March 28, 2024, from https://www.trufflesuite.com/docs

Vaishnavi, V., Kuechler, B., & Petter, S. (2019). *Design science research in information systems.* Retrieved from http://www.desrist.org/design-research-in-information-systems/

Venable, J., Pries-Heje, J., & Baskerville, R. (2016). FEDS: A framework for evaluation in design science research. *European Journal of Information Systems, 25*(1), 77-89. https://doi.org/10.1057/ejis.2014.36

V, S. (2022). KYC verification using blockchain. International Journal for Research in Applied Science and Engineering Technology. https://doi.org/10.22214/ijraset.2022.45156

Viswanatha, A., & Wolf, B. (2012, December 11). HSBC to pay $1.9 billion U.S. fine in money-laundering case. Reuters. Retrieved July 13, 2019, from https://www.reuters.com/article/us-hsbc-probe/hsbc-to-pay-1-9-billion-u-s-fine-in-money-laundering-case-idUSBRE8BA05M20121211

Watanabe, H., Fujimura, S., Nakadaira, A., Miyazaki, Y., Akutsu, A., & Kishigami, J. (2016). Blockchain contract: Securing a blockchain applied to smart contracts. 2016 IEEE International Conference on Consumer Electronics (ICCE), 467-468. Las Vegas, NV, USA. https://doi.org/10.1109/ICCE.2016.7430693

Werbach, K. (2018). *The blockchain and the new architecture of trust*. MIT Press. https://doi.org/10.7551/mitpress/11449.001.0001

Wieringa, R. J. (2014). *Design science methodology for information systems and software engineering*. Springer. https://doi.org/10.1007/978-3-662-43839-8

Winter, R. (2008). Design science research in Europe. European Journal of Information Systems, 17(5), 470-475. https://doi.org/10.1057/ejis.2008.44

Yadav, P., & Chandak, R. (2019). Transforming the Know Your Customer (KYC) process using blockchain. 2019 International Conference on Advances in Computing, Communication and Control (ICAC3), 1–5. IEEE. https://doi.org/10.1109/icac347590.2019.9036811

Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2018). Blockchain technology overview. National Institute of Standards and Technology (NIST).

Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where is current research on blockchain technology?—A systematic review. PLOS ONE, 11(10), e0163477. https://doi.org/10.1371/journal.pone.0163477

Yu, M., Sahraei, S., Li, S., Avestimehr, A. S., Kannan, S., & Viswanath, P. (2019). Coded Merkle Tree: Solving data availability attacks in blockchains. *IACR Cryptology ePrint Archive, 2019*, 1139. https://doi.org/10.1007/978-3-030-51280-4_8

Zheng, Z., Xie, S., Dai, H.-N., Chen, W., Chen, X., Weng, J., & Imran, M. (2020). An overview on smart contracts: Challenges, advances, and platforms. Future Generation Computer Systems, 105, 475–491. https://doi.org/10.1016/j.future.2019.12.019

APPENDIX A

This is to certify that
Project No.: **INFSYS2024-5-219462**
Project Title: **Enhancing KYC Compliance on Blockchain: A Smart Contract-Based Approach with zk-Rollups for Privacy and Scalability**
Principal Researcher: **Louis-Vincent Philipp-Messerschmidt**

according to the regulations of the Ethics Committee of NOVA IMS and MagIC Research Center this project was considered to meet the requirements of the NOVA IMS Internal Review Board, being considered **APPROVED** on 5/21/2024.

It is the Principal Researcher's responsibility to ensure that all researchers and stakeholders associated with this project are aware of the conditions of approval and which documents have been approved.

The Principal Researcher is required to notify the Ethics Committee, via amendment or progress report, of
- Any significant change to the project and the reason for that change;
- Any unforeseen events or unexpected developments that merit notification;
- The inability of the Principal Researcher to continue in that role or any other change in research personnel involved in the project.

Lisbon, 5/21/2024

NOVA IMS Ethics Committee
ethicscommittee@novaims.unl.pt

Appendix B

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.19;

import "@openzeppelin/contracts/token/ERC721/extensions/ERC721URIStorage.sol";
import "@openzeppelin/contracts/access/Ownable.sol";

contract KYCSmartContract is ERC721URIStorage, Ownable {

   struct KYCRecord {
      address customer;
      address bank;
      bytes32 proof;
      uint256 timestamp;
   }

   mapping(address => KYCRecord) public kycRecords;
   mapping(address => bool) public verifiedBanks;
   mapping(address => bool) public hasSBT;

   event KYCStored(address indexed customer, address indexed bank, bytes32 proof, uint256
timestamp);
   event SBTIssued(address indexed customer, bytes32 proof);
   event KYCVerified(address indexed customer, bool verified);
   event RewardPaid(address indexed bank, uint256 amount);

   constructor() ERC721("KYC Verification Token", "KYC-SBT") {}

   modifier onlyVerifiedBank() {
      require(verifiedBanks[msg.sender], "Only verified banks can perform this action");
      _;
   }

   function storeKYCProof(address _customer, bytes32 _proof) external onlyVerifiedBank {
      require(kycRecords[_customer].timestamp == 0, "KYC already exists");

      kycRecords[_customer] = KYCRecord({
         customer: _customer,
         bank: msg.sender,
         proof: _proof,
         timestamp: block.timestamp
      });

      emit KYCStored(_customer, msg.sender, _proof, block.timestamp);
   }
```

```
    function issueSBT(address _customer, bytes32 _proof) external onlyVerifiedBank {
        require(!hasSBT[_customer], "SBT already issued");

        uint256 tokenId = uint256(_proof);
        _safeMint(_customer, tokenId);
        hasSBT[_customer] = true;

        emit SBTIssued(_customer, _proof);
    }

    function logKYCVerification(address _customer, bytes32 _proof) external onlyVerifiedBank
{
        require(kycRecords[_customer].timestamp != 0, "KYC proof not found");

        emit KYCStored(_customer, msg.sender, _proof, block.timestamp);
    }

    function verifyKYC(address _customer) external view returns (bool) {
        return kycRecords[_customer].timestamp != 0;
    }

    function rewardIssuer(address _bank) external payable {
        require(verifiedBanks[_bank], "Bank is not verified");
        require(msg.value > 0, "Reward must be greater than 0");

        payable(_bank).transfer(msg.value);

        emit RewardPaid(_bank, msg.value);
    }

    function addVerifiedBank(address _bank) external onlyOwner {
        verifiedBanks[_bank] = true;
    }
}
```

Appendix C

This appendix shares information over the interviews conducted with the two KYC-experts to gather feedback on the regulatory compliance of the novel artifact. The Experts were provided an illustration of the artefact (compare Fig. 5) as well as the description of the 11 steps taken in the artifact (compare Part 4.2). Afterwards they were provided 4 Questions to answer. The questions, the answers possibilities and a short overview of the experts are provided below.

Expert Number	Profile	Experts position	Industry Sector	Region of operations	Blockchain Experience
1	Industry	Project Manager	Banking	Europe	Yes
2	Industry	Business Analyst	Banking	Europe	Yes

Survey Questions

1. Compliance with Existing KYC and AML Regulations: How do you assess the alignment of Soulbound Tokens (SBTs) with existing KYC and AML compliance requirements? What are the potential advantages or concerns that financial institutions might encounter when adopting this blockchain-based system?

2. Data Privacy and GDPR Compliance: In your view, does the proposed system, which minimizes the on-chain storage of personal data while using cryptographic verification methods, adequately address GDPR's privacy and data protection requirements? Are there any aspects that could pose compliance risks?

3. Regulatory Barriers and Challenges: What are the main regulatory challenges or uncertainties that financial institutions might face when integrating blockchain-based KYC verification? How do you think regulators might perceive the use of decentralized identity verification methods?

4. Future Regulatory Adaptation: How likely do you think regulatory bodies are to accept and integrate a decentralized identity verification system like this into their existing frameworks? What steps do you believe are necessary to facilitate regulatory acceptance and compliance for such a system?

Final Comments (Optional)

If you have any additional thoughts or suggestions regarding the regulatory compliance of this system, please share them below

Appendix D

This Appendix is used to present the survey that has been conducted after the first design phase of the presented artifact in section 4.2 of this thesis. The survey took place via Qualtrics and had 50 participants. The participants were handed a picture (compare Fig.5) of the designed artifact as well as an explanation of the steps that take place in an application process for a single customer. After looking at the artifact as well as reading the explanation, the participants were handed 3 questions. The questions and the options given for the answers are presented in the following as well as the study demographics. The goal of this survey was to identify, whether the designed artifact is capable to create trust among customers. Thrust worthiness is important for an application that interacts with customers given the fact, that they need to share their most important data (Passport-ID or else) when participating in the KYC-process. In addition, the survey was conducted to reach the guidelines of the DSR methodology that aims for an iterative process. Conducting the feedback provided through the survey the design of the artifact was customized to reach the highest possible output.

Description handed to the participants:

This study introduces a new way to verify identity when opening an account with a bank or financial institution. Traditionally, every time you sign up for a new financial service, you need to submit personal documents, which can be time-consuming and repetitive. This new process is designed to make onboarding simpler, faster, and more secure while also giving you more control over your personal information. Instead of submitting your documents multiple times, you will only need to complete the KYC verification once with a trusted institution. After this verification, you will receive a digital proof of verification in the form of a Soulbound Token (SBT). This token is securely stored in your digital wallet and cannot be transferred or changed by anyone, ensuring that only you can use it to verify your identity. When you need to open an account or access services at another financial institution, you simply share your digital proof instead of resubmitting your personal documents. The institution can then instantly verify that your identity has already been confirmed, making the process quicker and more convenient for you. This system is designed to increase security, reduce the risk of fraud, and give you more control over your personal data by minimizing how often sensitive information is shared. It also helps financial institutions work more efficiently while ensuring compliance with identity verification regulations.

Survey Questions:

A) System Quality and Security

Question: How would you rate the quality and security of the decentralized KYC system when submitting your documents?

1) Excellent

2) Good

3) Neutral
4) Poor
5) Very Poor

B) Information Quality and Trustworthiness
Question: How trustworthy do you perceive the identity verification and authentication process facilitated by Soulbound Tokens (SBTs) in the decentralized KYC onboarding system on the Ethereum blockchain?
1) Very Trustworthy
2) Trustworthy
3) Neutral
4) Untrustworthy
5) Very Untrustworthy

C) Service Quality and Transparency
Question: To what extent do you agree that the use of Ethereum blockchain and smart contracts improves the transparency and overall service quality of the KYC process?
1) Strongly Agree
2) Agree
3) Neutral
4) Disagree
5) Strongly Disagree

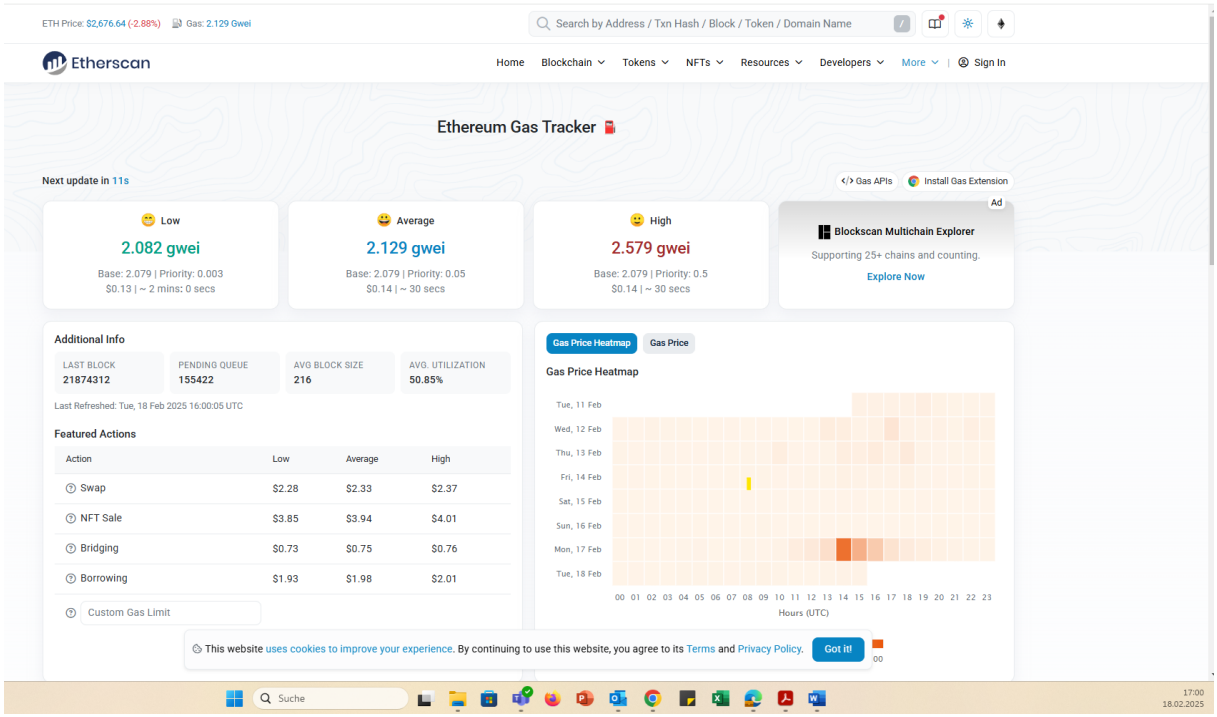
Study demographics:
-Male/Female: 35 Male / 15 Female
-Age Group:
18-30: 25 (50%)
31-50: 15 (30%)
50-70: 10 (20%)

-Evaluation of the single questions

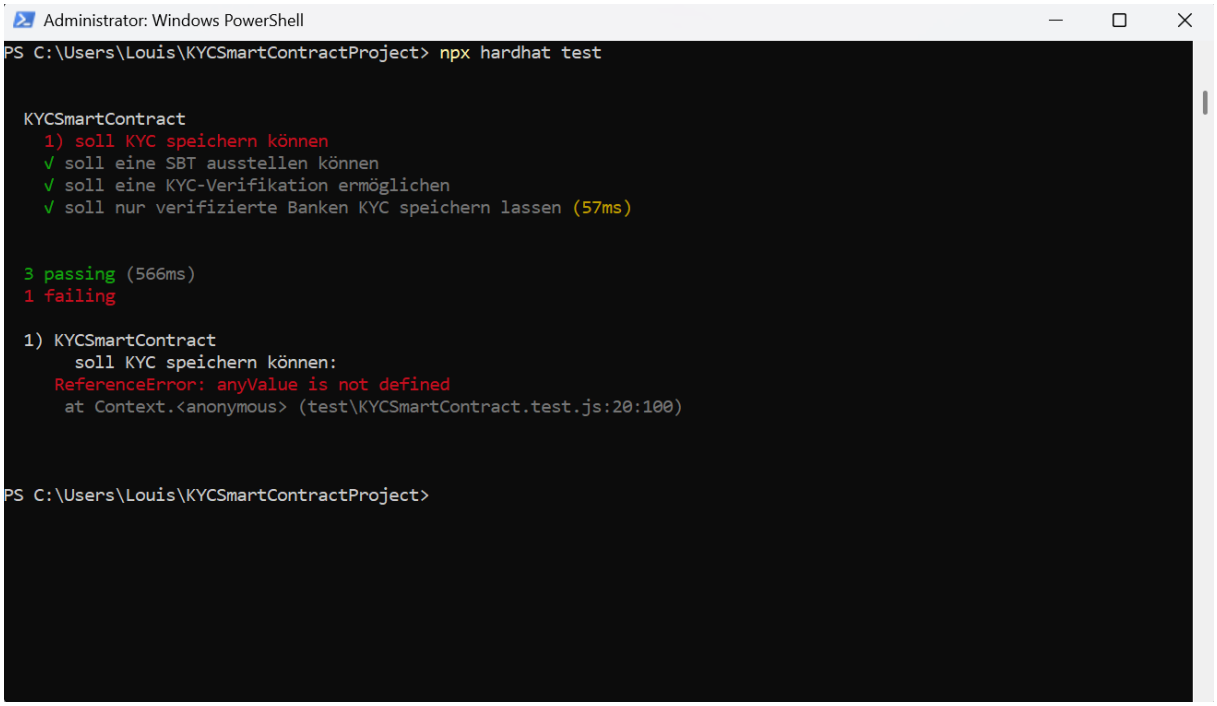
Question	Answer 1	Answer 2	Answer 3	Answer 4	Answer 5
A	25	15	5	3	2
B	26	14	8	1	1
C	23	13	5	4	5

Appendix E

Screenshot of the Ethereum and Gas Tracker Webpage: https://etherscan.io/gastracker



Appendix F


Administrator: Windows PowerShell
PS C:\Users\Louis\KYCSmartContractProject> npx hardhat test
KYCSmartContract
1) soll KYC speichern können
✓ soll eine SBT ausstellen können
✓ soll eine KYC-Verifikation ermöglichen
✓ soll nur verifizierte Banken KYC speichern lassen (57ms)
3 passing (566ms)
1 failing
1) KYCSmartContract
soll KYC speichern können:
ReferenceError: anyValue is not defined
at Context.<anonymous> (test\KYCSmartContract.test.js:20:100)
PS C:\Users\Louis\KYCSmartContractProject>

NOVA Information Management School
Instituto Superior de Estatística e Gestão de Informação

Universidade Nova de Lisboa