

NFT ID

Development of a prototype for a blockchain-based Remote-Ident solution and its impact on User Experience

Master Thesis

submitted on 05.07.2022

Faculty Art & Design

Study Program Visual Experience Design

Semester VED2021

Written by

Jakob Wiemer

Supervised by Prof. Dr. Peter Crnokrak and Magnus Kreisel

University of Europe for Applied Sciences

Konrad-Zuse-Ring 11, 14469 Potsdam

Abstract

Remote Identification has become highly relevant in the context of the COVID-19 pandemic and the recent trend of *online* banking, stock or crypto marketplaces and insurance companies. Due to the increasing number of new users every day, online providers such as TradeRepublic, Coinbase or N26 are faced with the challenge of offering a user-friendly way of identification. At the same time, smartphones are becoming more capable and could eventually enable technologies like real-time *Deepfakes* in the near future. This puts conventional Remote-Ident methods to the test in terms of *Security* and *User Experience*. In this context, this master's thesis examined the three most common methods of remote identification in Germany: *VideoIdent*, *PostIdent* and *eID*. It was found that PostIdent is the most secure procedure, but it costs the user a lot of time and therefore makes it impossible to register spontaneously with an online bank for instance. In terms of UX, eID is the most advanced method as it provides a fast identification experience without a third party involved. However, it is barely supported by online providers like TradeRepublic, Coinbase or N26. VideoIdent is the most commonly used Remote-Ident method as there is no prior setup required and can be processed significantly faster than PostIdent. However, it is also less secure than PostIdent, requires a third party to perform the identification within a video chat and is slower than eID. None of the established methods thus offer an ideal solution in the aspect of security and UX. In this context, a *blockchain-based* approach for remote identification was investigated. *Non-fungible Tokens* have been found to provide the technical foundation to securely represent passports and other identity documents to the Blockchain through their characteristics of uniqueness and proof of authenticity. Subsequently, a visual prototype was developed that simulates the User Experience of a blockchain-based Remote-Ident method. In particular, the disadvantages of conventional methods are being addressed and improved.

Table of contents

List of Abbreviations.....	IV
List of Figures.....	V
1. Introduction.....	1
1.1 Motivation	1
1.2 Problem Statement and Research Goal	1
1.3 Structure of the thesis and Research Methodology	2
2. Discussion of the Theoretical Background I - Blockchain and Non-fungible Tokens	3
2.1 Blockchain.....	3
2.1.1 Definition of Terms.....	4
2.1.2 Transaction Processing using the example of Bitcoin	5
2.1.3 Security	7
2.2 Non-Fungible Tokens	9
2.2.1 Definition of Terms.....	9
2.2.2 Smart Contracts.....	10
2.2.3 Transfer and Validation	11
3. Discussion of the Theoretical Background II - Usability and UX	13
3.1 Usability.....	13
3.1.1 Definition of Terms.....	13
3.1.2 Usability Heuristics according to Nielsen.....	15
3.2 User Experience Design	16
3.2.1 Definition of Terms.....	16
3.2.2 Hierarchy of User Needs according to Jordan	18
4. Methodology.....	20
4.1 Design Science Research.....	20
5. Comparative Analysis of conventional Remote-Ident Methods	24
5.1 Registration Process at TradeRepublic	24

5.2 VideoIdent.....	25
5.3 PostIdent	26
5.4 eID	27
6. Use of Non-fungible Tokens as Remote-Ident Method.....	30
6.1 Advantages of NFT ID.....	30
6.2 Feature Description.....	31
7. Conclusion	36
7.1 Summary.....	36
7.2 Critical Reflection and Outlook.....	37
Attachment	39
Bibliography.....	40
Acknowledgement.....	45

List of Abbreviations

NFT = Non-Fungible Token

PoW = Proof of Work

UX = User Experience

UI = User Interface

App = Application

2FA = Two-Factor-Authentication

List of Figures

Figure 1: Hierarchy of User Needs according to Jordan	18
Figure 2: Three-Cycle-View according to Hevner	20
Figure 3: DSRP Model according to Peffers	21
Figure 4: Registration Process of TradeRepublic	24
Figure 5: Verification with VideoIdent	25
Figure 6: Verification with PostIdent	27
Figure 7: Verification with eID	28
Figure 8: Verification with NFT ID	31
Figure 9: Selection of desired Registration Method	32
Figure 10: Help Screen	33
Figure 11: Incoming Verification Request	33
Figure 12: Pending Verification Request	34
Figure 13: Two-Factor-Authentication	34
Figure 15: Successful Biometric Matching	35
Figure 16: Completed Verification	35

1. Introduction

1.1 Motivation

The *Smartphone* has profoundly changed our world in all possible areas of life over the past 15 years. The fact that people communicate via Smartphone, order something to eat or watch movies on is nothing new anymore. However, in the past two years, an interesting trend can be seen that more and more people are investing money in the stock or crypto market through their smartphone. Apps like TradeRepublic or Coinbase have grown massively as they make the financial world accessible, especially for young people.¹ Since these are apps in which users invest their private money in order to benefit from possible share gains, it is required by law that each new user must be identified. Therefore, online providers such as TradeRepublic use remote identification methods like VideoIdent to identify users without the need of a physical appearance. During the COVID-19 pandemic crisis, the ability to identify a person without being physically present became even more important. Currently, the most widely used Remote-Ident method is VideoIdent which is still considered sufficiently safe at the current time. Here, the user is identified in a video chat by a third party which is contracted by online providers such as TradeRepublic. However, smartphones are becoming more and more performant and may in the future be able to bypass methods such as VideoIdent through technologies such as *Deepfakes*. For an attacker, it is then enough to steal someone's passport or ID to register with online banks, insurance companies or financial marketplaces under a false name. The following master thesis therefore investigates a *blockchain-based* approach that could replace conventional methods such as VideoIdent in terms of security and User Experience.

1.2 Problem Statement and Research Goal

As described in Chapter 1.1, there is a clear trend towards more and more people registering with online banks, stock exchanges or insurance companies. Remote-Ident methods such as VideoIdent or PostIdent make it possible even for those customers who are physically far away to identify themselves. At the same time, however, security

¹ Statista 2021

requirements are growing as technologies such as *Deepfakes* could bypass conventional Remote-Ident methods in the near future.

In this context, this paper aims to answer two main research questions. First, the question of whether a blockchain-based Remote-Ident method is technically possible at all is to be clarified. The second question is to identify what strengths and weaknesses traditional Remote-Ident methods have that could be solved by a blockchain-based approach. Based on the two research questions answered, the goal of this thesis is to develop a prototype that presents the User Experience of a blockchain-based Remote-Ident method. Furthermore, it will be shown how this approach is superior to conventional methods in aspects of security and User Experience.

1.3 Structure of the thesis and Research Methodology

This first chapter serves as an introduction to the topic and includes the problem statement as well as the research goals. The research process of the master thesis is based on the research methodology *Design Science Research* and is oriented to the *Design Science Research Processing Model* according to Peffers. Thus, the thesis is structured into three main major components. First, a theoretical base is laid in Chapter 2 and 3. In Chapter 2, insights gained about *Blockchain* and *Non-fungible Tokens* simultaneously answer the first research question, whether a blockchain-based Remote-Ident method is technically feasible at all. In Chapter 3, all terms relevant to this thesis are presented with regards to *Usability* and *User Experience*. These insights gained will be used in the subsequent development of the prototype to justify the design decisions made. Chapter 5 then uses a *Comparative Analysis* to answer the second research question of what strengths and weaknesses current Remote-Ident methods have that could potentially be solved by a blockchain-based approach. In the last step of this thesis, a *prototype* is presented, which illustrates what the User Experience of a potential blockchain-based Remote-Ident method could look like in the future. The final evaluation in Chapter 7 contains a conclusion that summarizes all the results obtained. In addition, the thesis is critically reflected and an outlook on future research possibilities is given.

2. Discussion of the Theoretical Background I - Blockchain and Non-fungible Tokens

In order to provide an entry point into the subject matter of this master thesis, the following chapter discusses the relevant technological aspects of *Blockchain Technology* and *Non-fungible Tokens*. Using the example of *Bitcoin* as the first and most well-known *Blockchain*, it will be explained what a Blockchain is, how it fundamentally works and why it provides a high level of data security. Subsequently it will be discussed, what *Non-fungible Token* are, how these are related to Blockchain Technology and how they work on the basis of *Smart Contracts*. Additionally, it will be explained why their characteristics make them particularly suitable for the use of remote identity authentication in online environments. In this context, the first research question will be answered, whether a blockchain-based Remote-Ident method is technically feasible.

2.1 Blockchain

Many people initially associate *Digital Banking* with traditional *Online Banking*: Transactions can be made from a smartphone or computer and it is not necessary to physically go to a bank anymore. But either way, every transaction is processed by the bank which costs money and can take several days until completion. The current finance system therefore relies on centralized instances where banks act as the man in the middle between its users.² Satoshi Nakamoto introduced an alternative approach in 2008 called *Bitcoin*, which he described as a *Peer to Peer Electronic Cash System*. The most important aspect he outlined is that the systems digital currency BTC is cryptographically validated and processed within seconds by the *Blockchain* without involving a trusted third party.³ With this whitepaper, Nakamoto laid the foundation for today's developments of cryptocurrencies and various use cases for Blockchain technology in different industries.

This chapter introduces the terminology Blockchain and provides a technical overview how transactions are processed using the example of Bitcoin. Furthermore, the security aspects of a Blockchain will be discussed. It must be noted here that the functionality of a

² cf. Meinel/Gayvoronskaya/Schnjakin 2018, p.13

³ cf. Fill/Meier 2019, p.3

blockchain is greatly simplified in the following due to its high complexity, as only a basic understanding is required for the further course of this thesis.

2.1.1 Definition of Terms

In a nutshell, the Blockchain is decentralized public ledger that chronologically lists transactions and enables secure and anonymous transfer of sensitive data such as financial assets through cryptographic encryption. In this context, the terms Blockchain and Bitcoin are commonly considered synonyms, however the *Blockchain* is a technology and *Bitcoin* a system which utilizes it to process transactions.⁴ A more detailed explanation is given in the following subchapter.

The Blockchain builds on three fundamental concepts. The first concept of a Blockchain is a **public electronic register** that records any information (e.g. orders, bonds, property deeds) of the respective system. Each system can have its own type of data that differs from others. In case of Bitcoin, it is a list of every *Transaction* that have ever been processed by the network. All transactions are chronologically grouped into *Blocks*, which form a chain by cryptographically referencing the previous block.⁵ Traditional banking relies on banks as a trusted third party to secure anonymity and manage a user's financial assets. Blockchain technology, on the other hand, is a self-managing system that provides transparency regarding its transactions: Every user can see all transactions ever processed by the Blockchain system, thus, who received how many e.g. Bitcoins from whom. In order to protect the identity of its users, Blockchain systems use anonymous addresses, which can not be traced back to a user.⁶

The second core concept is a Blockchain's **decentralization**. This means, that the electronic register is not running on a single server but distributed to all network users.⁷ Secure transactions and the decentralized management of the Blockchain are made

⁴ cf. Meinel/Gayvoronskaya/Schnjakin 2020, p.14

⁵ cf. Schlatt, Schweizer, Urbach, Fridgen 2016, p.8f

⁶ cf. Meinel/Gayvoronskaya/Schnjakin 2018, p.20f

⁷ cf. German Federal Office for Information Security 2019, p.9f

possible by cryptographic algorithms, which is the third core concept called **Mining**.⁸ There are two types of *Network Nodes* (or users) inside the Bitcoin system: *Passive Nodes* and *Mining Nodes*. *Passive Nodes* are users of the system who send Bitcoins from node A to node B. *Miners* are selected nodes of the decentralized network which provide computing power to validate, process and record these new transactions to the blockchain.⁹ This process is called *Mining*, because new blocks are added to the Blockchain for each new transaction.¹⁰

2.1.2 Transaction Processing using the example of Bitcoin

As described above, Bitcoin is a digital currency system that can process transactions and move financial assets between users without an intermediate. This subchapter breaks down this complex mechanism from a technical perspective using the following example:

Bob wants to send Alice one Bitcoin.

To interact with the Blockchain, Alice and Bob must open a *Wallet*, a software for mobile and desktop devices where Bitcoins and other crypto assets can be managed. A wallet is comparable to a bank account, but apart from a so-called *Address*, mentioned in the previous chapter, it does not contain any further details which could be used to trace back the user.¹¹

A *Miner* needs to perform two tasks to validate this transaction and accordingly add a new block to the chain. First, it needs to check whether Bob owns one Bitcoin.¹² As explained earlier, Bitcoin's Blockchain is a decentralized public register of all transactions that have ever been processed. Each block can be identified by a *Digital Signature* in form of a hash value. Hash functions transform an arbitrarily long input into a hexadecimal string of

⁸ cf. Schlatt, Schweizer, Urbach, Fridgen 2016, p.9

⁹ cf. Schlatt, Schweizer, Urbach, Fridgen 2016, p.12

¹⁰ cf. German Federal Office for Information Security 2019, p.9f

¹¹ cf. Schlatt, Schweizer, Urbach, Fridgen 2016 p.10f

¹² cf. Berentsen, Schär 2017, p.61ff

always the same length.¹³ The following example uses Bob's name and the SHA-256 algorithm, which is also used for Bitcoin¹⁴, to demonstrate how different the hash values are if only a single character changes:

Bob

cd9fb1e148ccd8442e5aa74904cc73bf6fb54d1d54d333bd596aa9bb4bb4e961

Bob1

8d0496eaa52dfb600b6fe804c3ae3403c06023f4a0ae7cd358222ba51326b654

Each wallet contains a *Private Key* and a *Public Key*. This key pair is used to generate the Digital Signature.¹⁵ To send the Bitcoin to Alice, Bob signs the transaction with his private key. Before the transaction can be processed, Alice needs to validate the authorship of Bob's Bitcoin using the public key in form of his wallet address. As this example illustrates, Digital Signatures ensure data integrity through asymmetric encryption and are used to validate the authorship of digital assets within the Blockchain system.

After it has been validated that Bob owns one Bitcoin, the second task of the Miner is to actually process the transaction and add the new block to the chain. As described above, the Blockchain is formed by referencing the previous block. Each block contains a set of important information including the hash of the previous block, which works as a pointer. Additionally, it stores the senders, receivers and the amount of Bitcoins to be transferred¹⁶ of all transactions within approximately 10 minutes.¹⁷ For the sake of clarity, this example assumes that only one transaction is created per block. In order to add a new block to the Blockchain and thus synchronize the not yet validated transaction, the miners need to find a hash value, that meets a certain requirement specified in the network

¹³ cf. Fill/Meier 2019, p.11f

¹⁴ cf. Nakamoto 2008, p.3

¹⁵ cf. Schlatt, Schweizer, Urbach, Fridgen 2016 p.10f

¹⁶ cf. Ali, Bagui 2021, p. 50

¹⁷ cf. Nakamoto 2008, p.4

protocol. In other terms, this involves finding a so-called *Nonce*, which in combination with the transaction hash does not exceed a certain value.¹⁸ The different Mining Nodes of the network compete to generate a new block and need to perform a series of highly complex cryptographic tasks to find the correct hash.¹⁹ Once a Mining Node has found the hash, the new block is added to the chain. Furthermore, it provides the hash to all other nodes with regards to synchronize the public register among the network. With that, Bob's transaction is fully processed. The winning Mining Node receives a certain portion of a Bitcoin for each block found in addition to transaction fees included in the transactions.²⁰ This mining mechanism, called **Proof of Work**, takes milliseconds but requires large amounts of computing power, which is provided by the Mining Nodes as mentioned earlier.²¹ Due to recent breakthroughs in the development of Blockchains, another mechanism has been introduced called **Proof of Stake**, which however is beyond the scope of this master thesis and therefore will not be explained further.

2.1.3 Security

One reason why Blockchain systems ensure a high level of security is its **decentralization**. As explained earlier, the register of transactions is fully synchronized with each network node. Thus, the distribution of the Blockchain on many independent computers protects against system failure or data loss. The network is not effected if single nodes can not operate. However, generally applies, the more nodes participate the more secure the network is.²²

Another reason for Blockchain's security is **anti-counterfeiting**. As shown in the previous chapter, the hashing allows unique identification of each block. The hashes preserve the order of the entered data. Once transactions are stored in the blockchain, they cannot be changed with realistic effort. Additionally, a transaction is not considered valid until it is

¹⁸ cf. Berentsen, Schär 2017, p.197ff

¹⁹ cf. Meinel/Gayvoronskaya/Schnjakin 2018, p.36f

²⁰ cf. Schlatt, Schweizer, Urbach, Fridgen 2016 p.14

²¹ cf. Berentsen, Schär 2017, p.61f

²² cf. Meinel/Gayvoronskaya/Schnjakin 2018, p.33f

included in a block that already has at least five following blocks. This number was set on the assumption that potential attackers do not have enough computing power to recalculate six blocks.²³ As explained earlier, the single blocks of a Blockchain reference each other using hash values. If an information stored in the Blockchain changes, the respective hash value would also change as the example in Chapter 2.1.2 demonstrates. This would cause the chain to break because it interrupts the referencing to the neighboring blocks. In combination with the distributed structure, a Blockchain provides a high level of security against the forgery of information.²⁴

Finally, Blockchains ensure **privacy and anonymity** while the public register is fully **transparent**. Wallet addresses for transactions are calculated from hash values of the recipient's public signature keys, whose corresponding private keys can later authenticate an onward transfer. Users therefore do not have to appear in Bitcoin with their real identity, contrary to conventional banking.²⁵ At the same time, all transactions of the network can be tracked through the public register as already described.

Although a Blockchain offers a high level of security due to its decentralized structure and cryptographic encryption, there are still potential opportunities for attack. Since a further explanation would go beyond the scope of this paper, here should be referred to further literature.

To summarize, Blockchain Technology provides secure infrastructure to send sensitive data such as financial assets instantaneously over the Internet without relying on a middleman. For this reason, the Blockchain is also called the *Internet of Values*.²⁶ In this context the Bitcoin system was presented as which is a decentralized digital finance system that builds on the Blockchain. With that, it is highly secure, independent from a third party, manages itself and reduces the costs and time of a single transaction. Therefore, a wide

²³ cf. Meinel/Gayvoronskaya/Schnjakin 2018, p.36f

²⁴ cf. Schlatt, Schweizer, Urbach, Fridgen 2016 p.45ff

²⁵ cf. German Federal Office for Information Security 2019, p.39

²⁶ cf. Meinel/Gayvoronskaya/Schnjakin 2018, p.15

variety of use cases arise in various industries. These range from *Gaming*, *Metaverse*, *Supply Chain Management*, *Real Estate*, elections to the *Internet of Things* just to name a few. The following chapter extracts one of these use cases in more detail: *Non-Fungible Tokens*, which are of essential relevance for the further course of this work.

2.2 Non-Fungible Tokens

Until now, digital works could be multiplied infinitely. The uniqueness of a thing was previously reserved for the physical world. However, with the recent rise of *Non-fungible Tokens*, or *NFTs*, a transformation in digital estates is emerging. In 2021, the NFT space was able to record an immense upswing: Digital works such as paintings, graphics, audio files or animations were sold and traded on platforms such as OpenSea.io. The NFT art project *Bored Ape Yacht Club* is one of the largest in the space and includes thousands of collectibles which generated global public interest also among celebrities. With a total trading volume of 570.000 Ethereum, which equals approx. \$1.25 Billion at a current price of \$2000 per Ethereum (May 2022), the *Bored Apes* might indicate a turnaround in the digital art industry. Although NFTs are not yet widespread in other economic sectors, development is currently being done on further use cases for the gaming, music, finance and real estate industry.²⁷ Already today, pioneer projects such as *The Sandbox* or *Axie Infinity* show the potential usage of NFTs as they serve as a basis for secure trading of digital assets in the context of online environments or the *Metaverse*. The following chapter provides a brief overview of the extensive subject of NFTs. In order to not overstretch the scope of this thesis, factual content is also explained in a simplified manner for the sake of comprehensibility.

2.2.1 Definition of Terms

NFT stands for *Non-fungible Token* which represent a unique individual value and are unchangeable and firmly anchored on the Blockchain.²⁸ On the other hand, cryptocurrencies like Bitcoin are *fungible* tokens as they can be traded and exchanged for each other. Further, fungible tokens are always equivalently valued: Each Bitcoin is always

²⁷ cf. Wang, Li, Wang, Chen 2021, p. 11

²⁸ cf. Ante 2021, p. 1

50000\$ for instance. Because each NFT is an individual token, the respective values differ.²⁹ Due to its characteristics, NFTs are particularly well suited for assets such as art or collectibles.

NFTs are linked to a digital certificate of authenticity which confirms the authorship and ownership rights.³⁰ Each Non-fungible Token contains a set of information including a unique identification, the original creator, the current owner and its transfer history.³¹ Furthermore, additional information can be stored such as a description of which asset the NFT represents. Accordingly, it is possible to store any data records in an NFT, which can be easily queried by third parties.³² An NFT can therefore be described as an **unique, digital ownership certificate** that represents a digital or even physical asset on the Blockchain. In this context, so-called *Smart Contracts* are utilized to manage the transferability and the ownership of NFTs.

2.2.2 Smart Contracts

In order to understand how NFTs work, it is important to briefly explain the underlying Blockchain *Ethereum*. In addition to Ethereum, other Blockchains like *Cardano* or *Solana* also support NFTs. However, these will not be considered further with regard to the scope of this thesis as Ethereum is currently the largest Blockchain system which implements the storing and sending of NFTs. Fundamentally, Ethereum is very comparable to Bitcoin in the way it works as it also builds on the *Proof of Work* mechanism described in Section 2.1.2. What is different, however, is that Ethereum is also able to run software on its Blockchain, so-called *Smart Contracts*.³³ Basically, as in the physical world, a Smart Contract is also about several parties agreeing on something, such as the exchange of digital financial goods or other assets. This agreement is transferred into a Smart Contract,

²⁹ cf. Regner, Schweizer, Urbach, p. 3

³⁰ cf. Ali, Bagui 2021, p. 53

³¹ cf. Basu, Basu, Austin 2022, p. 112f

³² cf. Regner, Schweizer, Urbach, p. 3

³³ cf. Ali, Bagui 2021, p. 50f

which programmatically ensures that the contractually defined conditions are met without the need for an intermediate.³⁴ The following examples illustrates this concept:

Alice invests in Bob's startup using the crowdfunding platform Kickstarter.

After enough money has been collected for the product development, the money will be send to Bob. Alice and Bob both have to trust the middleman *Kickstarter*, which handles the transaction and keeps a fee for it. A Smart Contract would replace *Kickstarter* in this scenario:

Alice invests in Bob's startup using a Smart Contract.

Investors like Alice send the money from her wallet via Blockchain to the Smart Contract, which, in the event of the budget target being reached, automatically sends the money to Bob's wallet. If the target is not met within a certain period of time, the invested money will be send back to Alice. The programmatically defined conditions determine what event will be executed on what trigger. As this example outlines, the advantage of a Smart Contract is that no trusted middleman is required. Additionally, the contract fees are very low compared to third party platforms like *Kickstarter*.³⁵ Since Smart Contracts are executed on the Blockchain, a high level of security is also ensured by decentralization and encryption as extensively described in Section 2.1. Similar to the executed transactions, the terms and conditions of a Smart Contract can also be viewed transparently.

2.2.3 Transfer and Validation

Now, that the underlying concept of *Smart Contract* has been explained, the following further elaborates how NFTs can be transferred between users of a Blockchain system and how their ownership is proven.

³⁴ cf. Regner, Schweizer, Urbach, p. 3

³⁵ cf. Regner, Schweizer, Urbach, p. 12

When an new NFT is created, the corresponding informations are stored on the Blockchain by adding a new block. This mechanism was explained in Section 2.1.2. In order to elaborate the process how an NFT is transferred, the following example is given.

Bob buys an NFT from Alice.

First, Bob needs to make sure that Alice actually currently owns the NFT. Proving if a seller owns the corresponding NFT is similar to proving if a user owns a Bitcoin. The token itself in combination with Alice public key serves as a *proof of ownership* since the token was verifiably transferred to the her wallet. The public key of the original creator serves as certificate of authenticity of the NFT.³⁶ As described earlier, this mechanism ensures that the origin and transfer history is always stored on the Blockchain. Now that the ownership has been validated, Bob sends the money, in this case a certain amount of Ethereum, to Alice' wallet address. The transaction is handled by a Smart Contract through Ethereum's *ERC-721 Non-Fungible Token Standard* which ensures the secure transfer of the NFT to Bob's wallet after Alice has received the money.³⁷ By selling the NFT, Alice loses her access since Bob's private key guarantees his sole access. Accordingly, an NFT can only have one single owner at a time.

The value of an NFT comes from its **unchanging uniqueness** and **guaranteed certainty of origin**. NFTs thus break the common paradigm that digital goods can be infinitely multiplied and copied, as they are linked to a certificate of authenticity that is verified by the blockchain. Unlike fungible tokens of a cryptocurrency like Bitcoin, the value of an NFT is unique. Although they are currently still very much associated with digital art, it is fundamentally possible to store arbitrary data sets in a non-fungible token. Smart Contracts enable secure and fast transfer of NFTs between users without the need for a third party. Because of these characteristics, NFTs are well suited for taking information currently stored on physical identity documents such as a passport and putting it into a digital and secure format.

³⁶ cf. Regner, Schweizer, Urbach, p. 3

³⁷ cf. Di Angelo, Salzer 2022, p. 3

3. Discussion of the Theoretical Background II - Usability and UX

As Chapter 2 introduced the technological fundamentals and concepts for this thesis, in the following, the topics of *Usability* and *User Experience Design* are presented as the second necessary theoretical component of this master thesis.

3.1 Usability

In this subchapter, the term *Usability* is defined and placed in the context of this thesis. Furthermore, common principles from the literature and standardized norms for good Usability are explained. These findings will be taken up in the further course of this paper to justify design decisions.

3.1.1 Definition of Terms

The term *Usability* has established itself especially in the field of software development. In the broader understanding it refers to physical products as well. Good Usability can be stated, if a software application or a product is easy and efficiently to handle within a short period of time, thus the user can quickly accomplish the intended tasks.³⁸ Jakob Nielsen, a Danish writer within the range Software Usability and UX, defines the term *Usability* as one of two aspects of the term *Usefulness* beside *Utility*. Utility focuses on the functions that are needed to complete a task. In this context, Usability means the ease of use of these functions. Furthermore, Nielsen describes Usability as a critical quality characteristic of a product. He also defined the term on the basis of five attributes:³⁹

- *Learnability*: The system should be as easy to learn as possible, so that the user can perform his tasks after a short time.
- *Efficiency*: After learning the system, the user should be able to perform his tasks as efficiently as possible.
- *Memorability*: The system should be designed in such a way that it is possible for the user to work efficiently with the system again without a new learning phase, even after a longer break.

³⁸ cf. Richter/Flückinger 2013, p. 3

³⁹ cf. Nielsen 1993, p. 25ff

- *Few errors*: The system should be designed in such a way that the user can make as few errors as possible. Simple errors should be easy to correct. Serious errors should not occur at all.
- *Satisfaction*: The system should be intuitive to use and thus trigger satisfaction.

The term Usability has been internationally standardized since 1998. Usability is defined in DIN ISO 9241 (Part 11) as follows:

*"The extent to which a product can be used by specific users in a specific context of use to achieve specific goals effectively, efficiently, and satisfactorily"*⁴⁰

Usability is measured in three levels, whereby these are considered as basic requirements for the entire system:⁴¹

- *Effectiveness*: The accuracy and completeness with which users achieve a given goal.
- *Efficiency*: The effort used in relation to accuracy and completeness for users to achieve a given goal.
- *Satisfaction*: Freedom from interference and positive attitude towards the use of the product.

The definition of DIN ISO 9241 has a complementary reference to the definition of Nielsen, but adds the approach that Usability is significantly dependent on the respective context of use. An explanatory example follows: the Usability of a hammer for hammering in nails can be good, but not if the task consists of turning a screw into the wall.⁴² In the context of user-friendly software applications, this means that it is not just a matter of optimizing the graphical *User Interface*. Thus, the future users should be identified first of all. This implies likewise the development of the respective task context. Afterwards, functions and information have to be defined, which are needed to perform the identified

⁴⁰ German Institute for Standardization 1998, Guiding principle ISO 9241-11

⁴¹ cf. German Institute for Standardization 1998, Guiding principle ISO 9241-11

⁴² cf. Richter/Flückinger 2013, p. 5

tasks. Only in the last step is it a matter of mapping these functions in a user-friendly graphical UI. Fundamentally, the result should then be able to be used effectively, efficiently and satisfactorily.⁴³

3.1.2 Usability Heuristics according to Nielsen

In the 1990s, Jakob Nielsen developed ten general heuristics for good *Interaction Design*. Interaction Design describes a relatively young discipline since 1980 of computer science, which deals with the design of interaction between people and graphical user interfaces. Although Nielsen formulated the following principles almost 30 years ago, they are still valid today:⁴⁴

- *Visibility of system status*: The system should inform the user about what is currently happening (e.g., the progress of a download) - in a timely manner and through appropriate feedback.
- *Match between system and the real world*: The communicated information of the system should follow a natural dialog logic, which is understandable for the user.
- *User control and freedom*: Users tend to perform actions unintentionally. Functions such as "Undo", "Redo" and "Exit" should be clearly recognizable.
- *Consistency and standards*: Users should not have to think about whether different words, situations, and actions mean the same thing. The interface should consistently implement a coherent design, a consistent navigation structure, and platform specifications.
- *Error prevention*: Better than error messages is a careful design that reduces errors by the user to a minimum. Error-prone situations should be avoided. The user should be made aware of errors that occur and be able to confirm actions.
- *Recognition rather than recall*: Visible objects, actions and options mean that the user has to remember less. Instructions on how to interact with the system are visible or easy to reach.

⁴³ cf. Richter/Flückinger 2013, p. 6

⁴⁴ cf. Nielsen 1994

- *Flexibility and efficiency of use:* Experienced users should be enabled to operate the system efficiently by shortcuts and other forms of personalization. These functions should initially remain hidden from newcomers, so as not to overwhelm them with the system.
- *Aesthetic and minimalist design:* Dialog boxes should mainly present relevant information and reduce unnecessary information.
- *Help users recognize, diagnose, and recover from errors:* Error messages should be formulated in clear language and support the user in correcting the error (e.g. incorrect password entry).
- *Help and documentation:* Basically, the interface should be designed in such a way that the user can interact with it largely without help. However, in certain cases it may be necessary to provide documentation that explains the execution of a specific task. This information should be easy to find and focus on the essentials.

3.2 User Experience Design

User Experience Design is thematically based on Usability and complements some approaches and concepts. In the following, the term *UX* is first defined by different perspectives being used. Then, selected models of User Experience from the literature will be elaborated.

3.2.1 Definition of Terms

The term *User Experience* was first introduced by Don Norman, a professor of cognitive science and Computer Science at the University of California. In collaboration with Jakob Nielsen, he defined User Experience as a comprehensive term for all aspects that influence the interaction between the user and a company's (digital) products or services.⁴⁵ The fundamental prerequisite is the fulfillment of the customer's needs. Only in the second step is it a matter of simplicity and aesthetics. According to Nielsen and Norman, it is important to understand that the User Experience of digital products like websites or apps is strongly dependent on the *User Interface*, but other factors also play an essential role.⁴⁶ In the

⁴⁵ cf. Norman/Nielsen 2016

⁴⁶ cf. Norman/Nielsen 2016

literature, the exact meaning of User Experience is disputed. According to Bevan, the term UX can be conceptualized in different ways. Bevan understands User Experience primarily as an extended approach to Usability to include the component of satisfaction. While Usability mainly aims at the efficiency of a system, User Experience encompasses the overall impression of a user. In addition, UX serves as a collective term for all subjective perceptions of the user, whereby Bevan refers to the Part 210 of DIN EN ISO 9241.⁴⁷ In this, User Experience is defined as follows:

*Perceptions and reactions of a user resulting from actual and/or expected use of a product, system, or service.*⁴⁸

According to the definition, UX encompasses all emotions, personal preferences, behaviors, and services that occur before, during, and after use of a (digital) product or service.⁴⁹ According to Sarodnick and Brau, UX can also depend on factors such as advertising and marketing, social media, packaging, the user's current emotional state, or the opinion of other people. In the explicit context of digital products, however, Usability is a particularly important factor for the User Experience.⁵⁰

Law differentiates UX as a partial aspect of Product Experience. In this approach, User Experience is limited exclusively to the areas in which the user interacts with the product or service by means of a User Interface.⁵¹

According to Hassenzahl, the term UX can be broken down into three parts. The first part includes the user's emotions (needs, motivation, emotional state, knowledge, expectations). The second part describes the characteristics of the system (usability, utility, complexity, purpose, etc.). As the third part, Hassenzahl considers the environment (company, free-will

⁴⁷ cf. Bevan 2009

⁴⁸ German Institute for Standardization 2010, Guiding principle ISO 9241-210

⁴⁹ cf. German Institute for Standardization 2010, Guiding principle ISO 9241-210

⁵⁰ cf. Sarodnick/Brau 2010, p. 22

⁵¹ cf. Law et al. 2009, p. 726

of use, importance of the task, etc.). According to Hassenzahl, the User Experience is the intersection of these three areas.⁵²

At this point, it can be concluded that the term User Experience is interpreted differently in the literature. Generally, UX describes all points of contact between the user and the product, service or system.

3.2.2 Hierarchy of User Needs according to Jordan

According to the British-American author Jordan, Usability is not considered a pleasure factor. Good usability is expected by users and can provide satisfaction to a certain degree. Poor usability, on the other hand, has a major impact and results in dissatisfaction. To get users excited about a product or service, Usability serves as a foundation and must be extended to include a *pleasure-based approach*. According to Jordan, the term *Pleasure* in association with products is composed of *emotional, hedonic and practical benefits*. The emotional benefits refer to how the product can affect the mood of the user. Effectively and efficiently solved tasks result in practical performances. Hedonic benefits include the sensory and aesthetic pleasure for the user, which are triggered by the associated product.⁵³ In this context, Jordan formulates a hierarchy of user needs, which has an analogy to the Kano model:

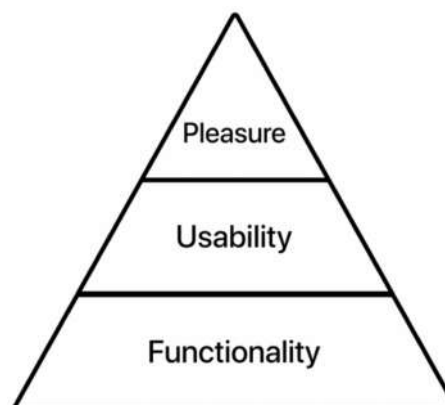


Figure 1: Hierarchy of User Needs according to Jordan⁵⁴

⁵² cf. Hassenzahl/Tractinsky 2006, p. 95

⁵³ cf. Jordan 2000, p. 6ff

⁵⁴ In: Jordan 2000

The Kano model describes customer satisfaction in the context of *basic needs, performance needs and delighters*.⁵⁵ In Jordans model, the *Functionality* of a product represents the basic needs. These are the minimum expectations a user has and cannot increase satisfaction. If a certain functionality is not given which is expected, the user is dissatisfied. Therefore, the core functions must be designed to meet the user's needs in a certain context in order to provide any value at all.⁵⁶ *Usability* represents performance needs which increase satisfaction linearly. It can lead to dissatisfaction, if the usability needs are not fulfilled. On the other hand, if the app or website can be operated intuitively, it can certainly lead to satisfaction, but does not guarantee it. *Delighters* have a strong effect on *Pleasure*, since these are not expected and surprise the user in a positive manner.⁵⁷

Digital products must provide functions which offer a clear value by solving a specific problem. This functions must be made accessible by wrapping them into an intuitive User Interface. To exponentially increase a good User Experience, measures must be taken that trigger pleasure. But if the system does not fulfill the purpose for which it was designed, it does not provide any value, even if a well-designed interface has been implemented.

Jordan adds, that the UX is not based on a single product feature, but rather encompasses the entire interaction between the user and the product. Products are perceived differently by people, based on different preferences, experiences and needs.⁵⁸ The design of a product should therefore address all three levels: It should provide appropriate functions for the task to be fulfilled (Utility), it should be simple, understandable and intuitive to use (Usability) and it should also be enjoyable and and trigger pleasure for a good user experience (Pleasure).

⁵⁵ cf. Buhl et al. 2006, p. 4

⁵⁶ cf. Bartel/Quint/Weichert 2018, p. 21

⁵⁷ cf. Bartel/Quint/Weichert 2018, p. 22

⁵⁸ cf. Jordan 2000, p. 12

4. Methodology

In the following chapter, the research methodology used in the context of the master thesis is presented.

4.1 Design Science Research

This master thesis is based on the research method *Design Science Research*. According to Hevner, Design Science Research is a problem-solving approach in which an IT artifact is developed and then evaluated. An artifact can be a model, a construct, a method or an instantiation with the goal to develop innovative ideas, practices, technical capabilities or products. Design Science research in this context includes two core activities: *Build* and *Evaluate*. In the *Build* process, the artifact is developed to serve a specific purpose. In the second core activity *Evaluate*, the constructed artifact is then evaluated and its performance checked.⁵⁹

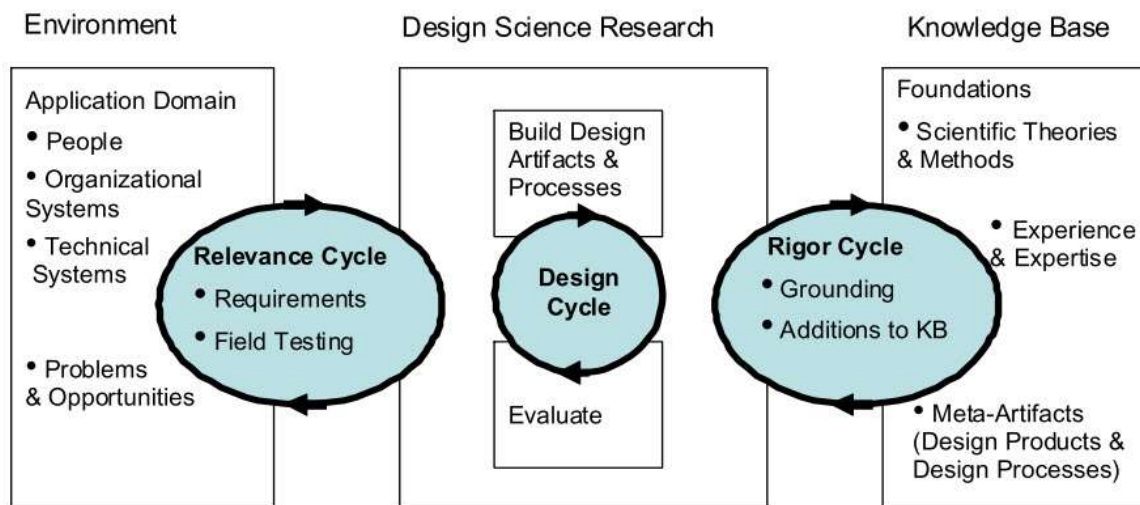


Figure 2: Three-Cycle-View according to Hevner⁶⁰

Figure 1 presents the *Three Cycle View* framework developed by Hevner, which puts the design science paradigms into context. *Environment* represents the problem for which a solution is to be found and all factors that influence the solution process. *Knowledge Base* includes methods and tools available to the researcher to solve the problem. The section

⁵⁹ cf. Hevner 2007, p. 3

⁶⁰ Hevner 2007, p. 3

Design Science Research includes the actual development of the artifact. This process is also called *Design Cycle*, because the development consists of a cycle of the already described activities *Build* and *Evaluate*. The *Rigor Cycle* is another cycle of the framework. During the development of the artifact, the researcher uses existing knowledge from the knowledge base and expands it. The *Relevance Cycle* represents the final cycle: The developed artifact serves as a solution in the intended environment.⁶¹

Since Design Science Research does not define a concrete process model, this thesis draws on the *DSRP Model* (Design Science Research Process Model) according to Peffers.

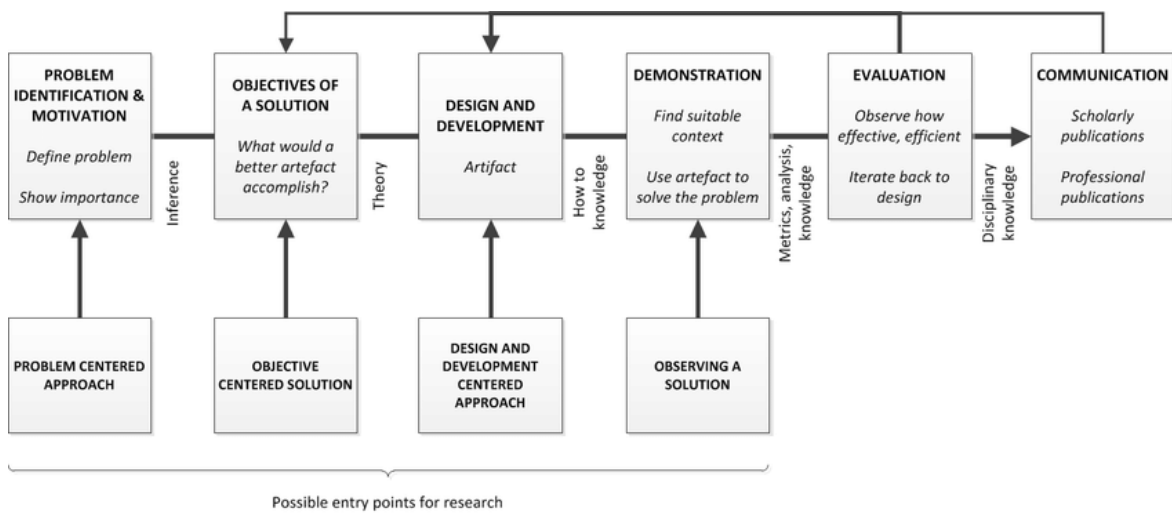


Figure 3: DSRP Model according to Peffers⁶²

The first step is to *identify the problem* and justify the added value of a possible solution. Establishing the value of a solution in advance is important because, on the one hand, it sets a clear goal and, on the other hand, it helps the reader to understand the researcher's solution and the underlying argumentation behind it. Subsequently, *objectives of a solution* are determined on the basis of the previous problem definition. This requires knowledge about existing solutions, their problems and limitations. Additionally, the researcher needs to identify possible components of a solution.

⁶¹ cf. Hevner 2007, p. 3ff

⁶² Peffers et al. 2006, p. 98

For these purposes, Chapter 1 pitches the general problem with existing online Remote-Ident solutions, the motivation why current security standards will not be sufficient in the future with regards to evolving technology and provides possible environments of operation. Afterwards, the research presented in Chapter 2 lays the theoretical groundwork of this thesis. In order to develop a blockchain-based Remote-Ident method, this technology must first be understood in technical depth. Simultaneously, the User Experiences of existing solutions are examined in Chapter 5 in the context of a comparative analysis in order to identify strengths and weaknesses which should be addressed by a blockchain-based approach.

In the next step, according to the DSRP model, the IT artifact must be developed. Since this thesis primarily focuses on the User Experience of a blockchain-based Remote-Ident solution rather than on the technical implementation behind it, no further technical detail was provided in this case. Instead, Chapter 6 presents a visual prototype that presents the UX flow of a potential solution with utilizing NFTs as the core component in the identity authentication process. It was deliberately decided not to neither demonstrate nor test this prototype, as this would go beyond the scope of this paper.

Prototyping aims at developing and evaluating an executable early version of a software product before it actually goes into development. Typically, these prototypes focus on presenting the expected user experience and interface design of the final product.⁶³ A distinction is made between *exploratory*, *experimental* and *evolutionary prototyping*. Explorative Prototyping is used when the problem is still unclear. The basic ideas are formulated into initial requirements, but exploratory prototyping is not prematurely limited to an explicit approach. The focus of the Experimental Prototyping lies on the technical implementation of a certain development goal. In the foreground software-ergonomic questions stand thereby above all. Evolutionary Prototyping makes a continuous adjustment possible in view of changing basic requirements.⁶⁴ In the context of this master

⁶³ cf. Raithel 2006, p. 71

⁶⁴ cf. Floyd 1984, p. 6ff

thesis, experimental prototyping is used, since the objective is already formulated and software-ergonomic questions are in the foreground.

Furthermore, a distinction is made between *horizontal and vertical prototyping*. Horizontal prototyping is about designing all or large parts of a system, deliberately avoiding designing every functionality in full depth, especially at the beginning of the design process. With vertical prototyping on the other hand a certain part of the entire system in all depth is designed.⁶⁵ In this case, the vertical approach is taken, as the prototype is intended to demonstrate the UX flow of a blockchain-based Remote-Ident authentication.

According to Seiden and Gothelf, the first ideas are initially sketched on paper. These sketches already give an early impression of the product right at the beginning of the process. However, this type of prototyping should mainly be used at the beginning of the design process, since the level of abstraction is very high and paper prototypes can only represent the intended user experience to a certain degree. In the later course of the process, a prototype should therefore be created that simulates the intended user experience as precise as possible. According to Seiden and Gothelf, so-called *high-fidelity prototypes* are developed in this context, which represent the look and feel of the final product in terms of user experience and visual design. High-fidelity prototypes can, for example, simulate interactions in a very high quality like animated drop-down menus, page transitions or button behaviour. Basically, the interactivity is of course not on the same level in direct comparison to natively programmed prototypes, but visual prototypes can be developed in a fraction of the time.⁶⁶

⁶⁵ cf. Kiebach 1992, p. 9

⁶⁶ cf. Seiden/Gothelf 2013, p. 59ff

5. Comparative Analysis of conventional Remote-Ident Methods

In order to better assess the efficiency of identity authentication using NFTs in the later course of this thesis, the following section demonstrates the pros and cons of established remote identification methods with regard to User Experience and Security in the context of a previously conducted comparative analysis. For this purpose, an exemplarily online registration was run through at the German online broker *TradeRepublic* using VideoIdent. In this context, the second research question will be answered, what strengths and weaknesses conventional Remote-Ident methods have that could be solved by a blockchain-based approach.

5.1 Registration Process at TradeRepublic

As can be deduced from Figure 4, the registration at TradeRepublic can be broken down into two steps before the user needs to verify their identity. First of all, the user has to **open an account**. In this context, they need to provide and verify their mobile phone number. For that, a code is sent to the user's phone which needs to be entered in the TradeRepublic app or website. After that, the user sets a PIN and e-mail address. In this case, it is not required to validate the e-mail in order to continue with the registration. This step took approximately 2 minutes in the exemplary run through.

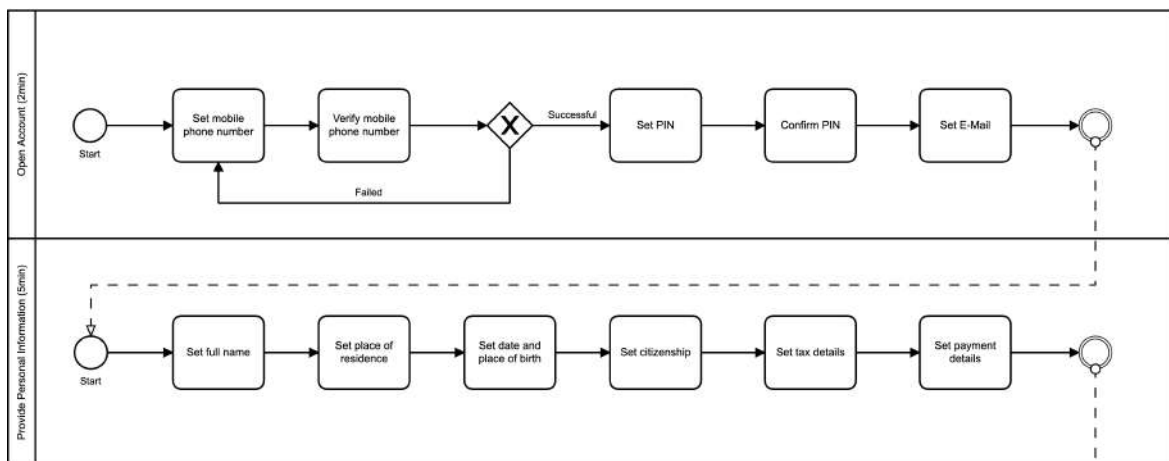


Figure 4: Registration Process of TradeRepublic

The second step is to provide a set of **personal information**. In this case, the user needs to provide the full name, current place of residence, date and place of birth, citizenship, basic

tax information and banking details. This step took approximately 5 minutes. After completing the first two steps of the registration, the user needs to **verify their identity**. In this exemplarily case at TradeRepublic, the VideoIdent method was the only available option of identify verification. The complete process can be found in the appendix. To demonstrate PostIdent and eID in the same context, VideoIdent is replaced by these in the following diagrams.

5.2 VideoIdent

VideoIdent is a remote identification method using video chats following a standardized pattern in order to authenticate users in online environments without the need of a physical appearance. VideoIdent is used by online banks or brokers like *TradeRepublik* where it is mandatory by law to verify the identity of new users. It is a service provided by third party companies contracted by the online provider where the user is registering. The process focuses on a biometric matching and the verification of authenticity of the identity document.⁶⁷

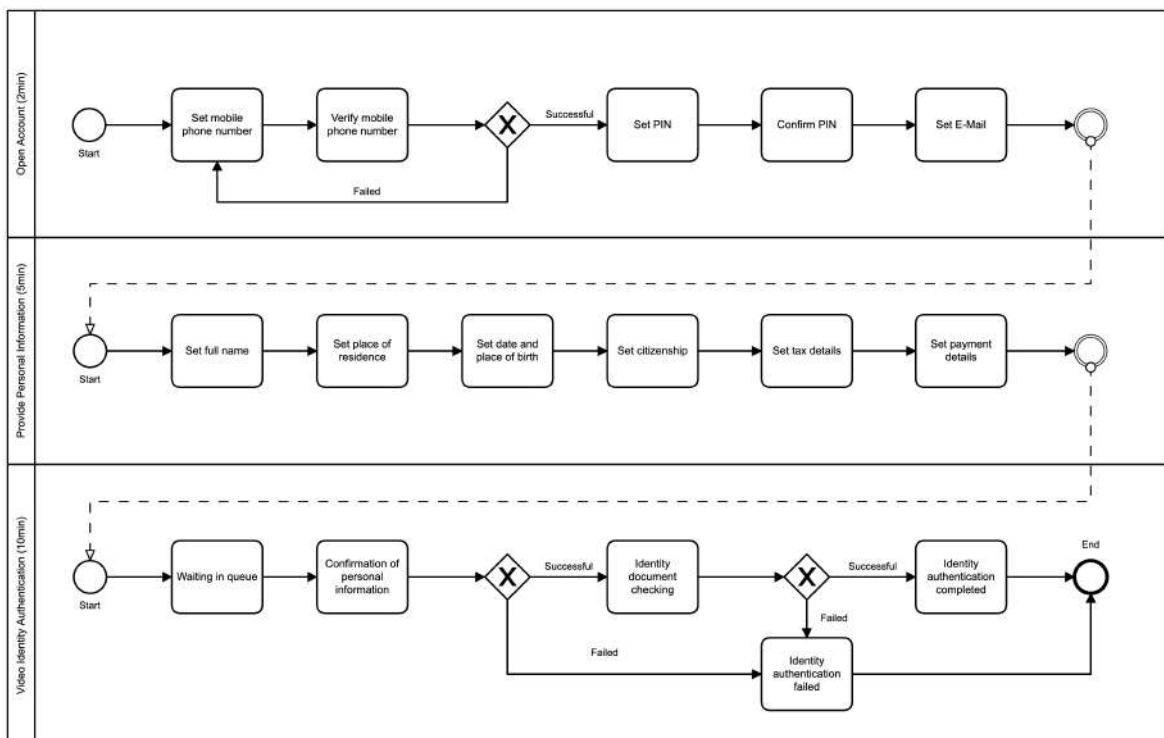


Figure 5: Verification with VideoIdent

⁶⁷ cf. Pohlmann 2017, p. 72

In the exemplary test run illustrated in Figure 5, the waiting time to be forwarded to a third party employee via video chat took about 3 minutes. Subsequently, the user is asked for the previously entered information and must verbally confirm them again which took 2 minutes in this run. The employee then checks the identification document. In this case, a passport was used. The user is asked to hold the document up to the camera in various angles so that the employee can confirm the authenticity of the document through the holograms incorporated. Depending on the lighting conditions in the environment and the camera quality, this step may have to be repeated several times. In this scenario, it took about 5 minutes. Thus, the VideoIdent verification took a total of 10 minutes which result in 17 minutes total time for registration.

The advantage of this method is that no further setup is required which enables spontaneous registration. The user needs a webcam and their ID or passport. The biometric comparison makes VideoIdent very secure at the current state. However, as computing power increases, there is a risk of real-time deepfakes that could bypass this system. From a UX perspective, VideoIdent can be an arduous process because the user needs to wait in the queue. Furthermore, the duration of the process depends strongly on the light conditions and the quality of the webcam. Therefore, the verification process itself can't be optimized. Room for improvement is to shorten the average waiting time in the queue.

5.3 PostIdent

PostIdent is an identification service in Germany provided by *Deutsche Post AG* which is an exchange-listed logistics and postal company. As can be deducted from Figure 6, after completing the former registration explained in Section 5.1, the users receives an QR code provided by Deutsche Post for verification at TradeRepublic. With that, the user must visit a post office which supports PostIdent verification. At the post office, a biometrical matching is performed. In addition, the passport or ID is scanned to read out and validate the corresponding data. If the confirmation is successful, the data is transferred to TradeRepublic.⁶⁸

⁶⁸ cf. Deutsche Post 2021

The duration of this process depends on two factors. First, it depends on how quickly the user can get to a corresponding Post Office branch that supports PostIdent. In a bigger city, this is not a problem. However, if the user lives in a far-off village, the process may take considerably longer. Secondly, it depends on how long it takes to provide the confirmation to TradeRepublic. Normally, the entire process should not exceed one day. With regard to UX, PostIdent is not very user friendly because it involves a high time investment up to two days until the whole process is completed. On the other hand, it is very secure, since the biometric matching is physically performed by another human being.

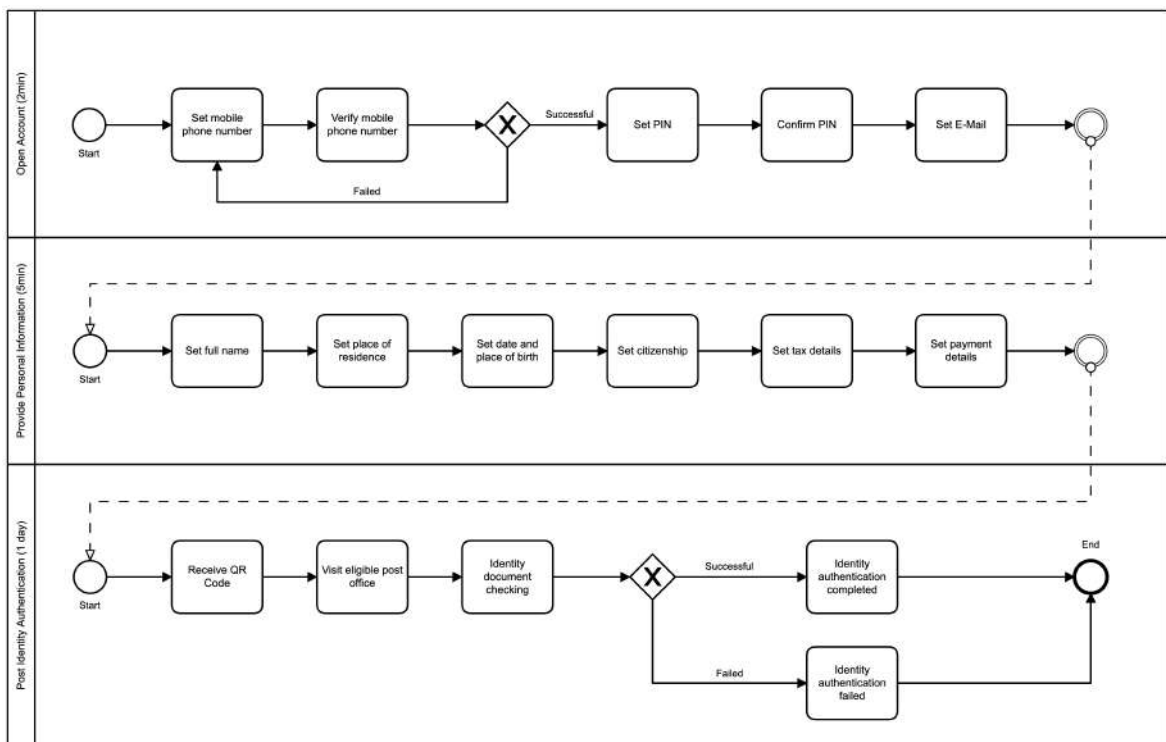


Figure 6: Verification with PostIdent

5.4 eID

eID is a remote identification service provided by the German government in collaboration with various trusted third parties.⁶⁹ The technology behind eID bases on *RFID* (Radio-Frequency-Identification), more specifically on *NFC* (Near-Field-Communication), which is specialized to enable secure data transmission over short distances.⁷⁰ Modern passports

⁶⁹ cf. German Federal Ministry of the Interior 2022

⁷⁰ cf. Alrawais 2020, p. 621

and IDs are equipped with these NFC tags and digitally store the corresponding personal information which can be read by e.g. smartphones or NFC readers at Airports. In order to use the eID service for online registrations, users need to activate the eID functionality in advance. After activation, they receive a PIN per post which is required in order to access the eID in corresponding eID apps.⁷¹

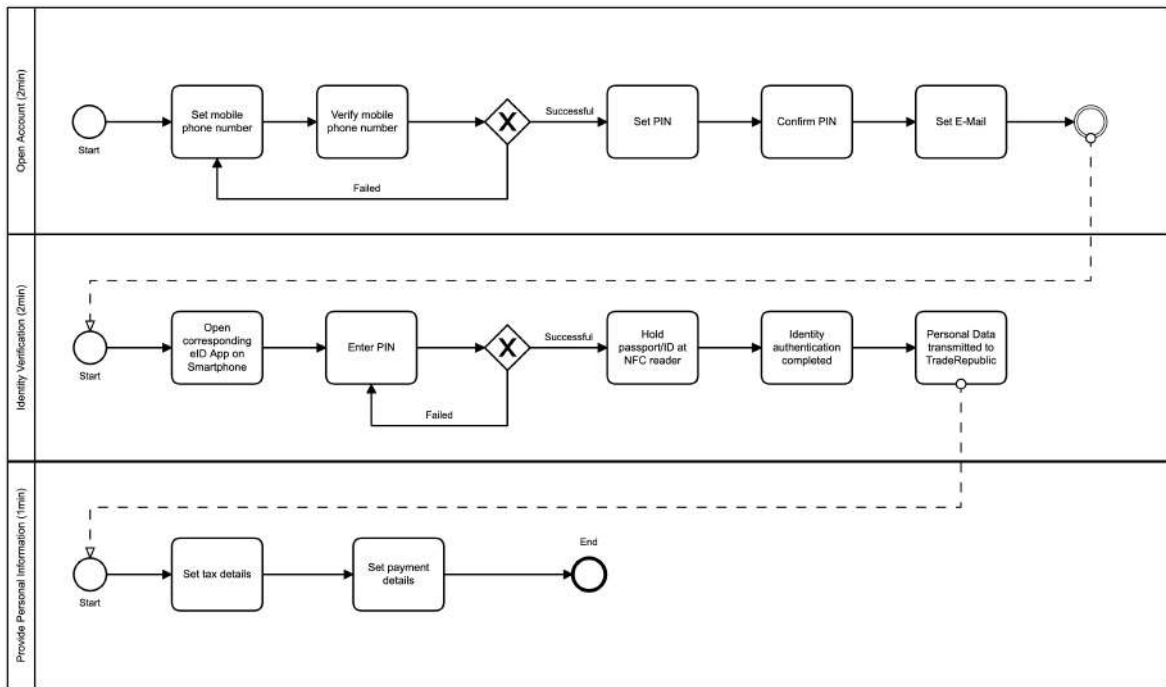


Figure 7: Verification with eID

As it is illustrated in Figure 7, the advantage of eID is that it is very fast since the user only needs to open a corresponding eID app, enter their PIN and hold their passport or ID at their smartphone. Once the NFC tag has been read, the user is identified, gets redirected to TradeRepublic and the personal information have been automatically transmitted. With regard to UX, the eID is more efficient than PostIdent or VideoIdent due to the fact that the users do not depend on a third party as they run through the verification process by themselves. Furthermore, the process is very user friendly as it is quick and easy and there is no need for manual input of personal information. In this case, the registration including verification may take up to 5 minutes which is approximately 12 minutes faster than VideoIdent.

⁷¹ cf. IDnow 2022

Nevertheless, eID is less secure in direct comparison to VideoIdent or PostIdent, because there is no biometric matching and it is sufficient for an attacker to obtain the ID or passport and the corresponding PIN. Furthermore, eID requires that the user has already activated the service in advance. Spontaneous online registration is therefore only possible if the user already has a corresponding eID app on the smartphone that is also supported by the online platform, in this case TradeRepublic. Otherwise, the user must either download a supported app or, in the worst case, activate the eID service first, which can take a few days, since an activation code is sent to the user by post beforehand. Current estimates assume that only about one third of the ID cards in Germany that support eID actually have this function activated.⁷² Additionally, the users needs a smartphone with NFC reading capability. Potential for improvement therefore lies in automatically activating the eID when requesting a new ID or passport and making an industry wide standardized solution (equivalent to SignIn with Google, Apple or Facebook) available to the user without relying on thrusted third parties.

At the present time, VideoIdent in particular has prevailed over PostIdent and the barely used eID due to its simple and fast processing without prior setup and overall good security. However, it should be noted that PostIdent still has its justification for existence in terms of security. Nevertheless, it scores poorly in terms of UX, as the process is very time-consuming and inconvenient for the user. The eID follows the approach that the users can verify themselves quickly and easily online, which is at an advantage over the other two methods in terms of UX. However, it has not yet gained widespread acceptance, as it relies on many different providers, and the functionality itself has to be activated manually in advance making spontaneous registrations difficult to realize.

⁷² Pohlmann 2017, p. 74

6. Use of Non-fungible Tokens as Remote-Ident Method

As discussed in the previous chapter, existing Remote-Ident solutions are each associated with different drawbacks. PostIdent is a very secure procedure, but it costs the user a lot of time and therefore makes it impossible to register spontaneously with an online bank, for example. In terms of UX, eID is the best method, but it barely supported as it relies on different third party providers and is less secure than PostIdent. VideoIdent can be used without any setup, but requires a third party for identification and is also comparatively less secure than PostIdent. The project elaborated within the framework of this master thesis called **NFT ID**, a blockchain-bases Remote-Ident method, takes the advantages of all presented solutions and eliminates their disadvantages. This chapter first discusses the benefits of NFT ID and presents a proposal of how they could be issued by the government. Subsequently, the functionality and UX of NFT ID is exemplified with the help of a prototype for the registration process at TradeRepublic.

6.1 Advantages of NFT ID

NFT ID ensures a high level of **security** similar to PostIdent. Comparable to conventional passports or ID cards, NFT IDs are also issued by the respective state authority. As described in Chapter 2, the original creator is always stored in an NFT. In this case, the state is the original creator, which makes it possible to prove that the respective NFT is an original ID document issued by the state. After the NFT ID has been created by the state on the Blockchain, it is transferred to the applicant's wallet. Furthermore, NFT ID also eliminates the need for a third party to identify the user, as it is the case with VideoIdent or PostIdent. A Two-Factor-Authentication app connected to the respective user's wallet is used for biometric matching via Face ID. The combination of biometric matching and the fact that the NFT ID is an identity document secured by the Blockchain ensures an enormously high level of security that cannot be overcome by deepfakes, which could well be the case with VideoIdent in the coming years.

In terms of **UX**, the NFT ID comes along with a similar experience as the eID but with higher security. Comparable to the eID, the NFT ID stores the same information that is contained in a physical passport or ID card (name, age, address, nationality, etc.), which

can be extracted from, for example, third parties like TradeRepublic. This is a great advantage for the UX, because the users do not have to provide their personal information themselves, but it is automatically taken from the NFT ID. In summary, NFT ID offers a Remote-Ident solution that guarantees high security and provides a fast and straightforward User Experience.

6.2 Feature Description

The following Chapter provides a product overview of NFT ID by explaining its UX flow in the context of TradeRepublic. Additionally, certain design decisions are justified by the findings obtained from the literature described in Chapter 3.

As previously described, NFT ID allows to automatically fill in personal information. For the registration process at TradeRepublic this results in the following UX Flow:

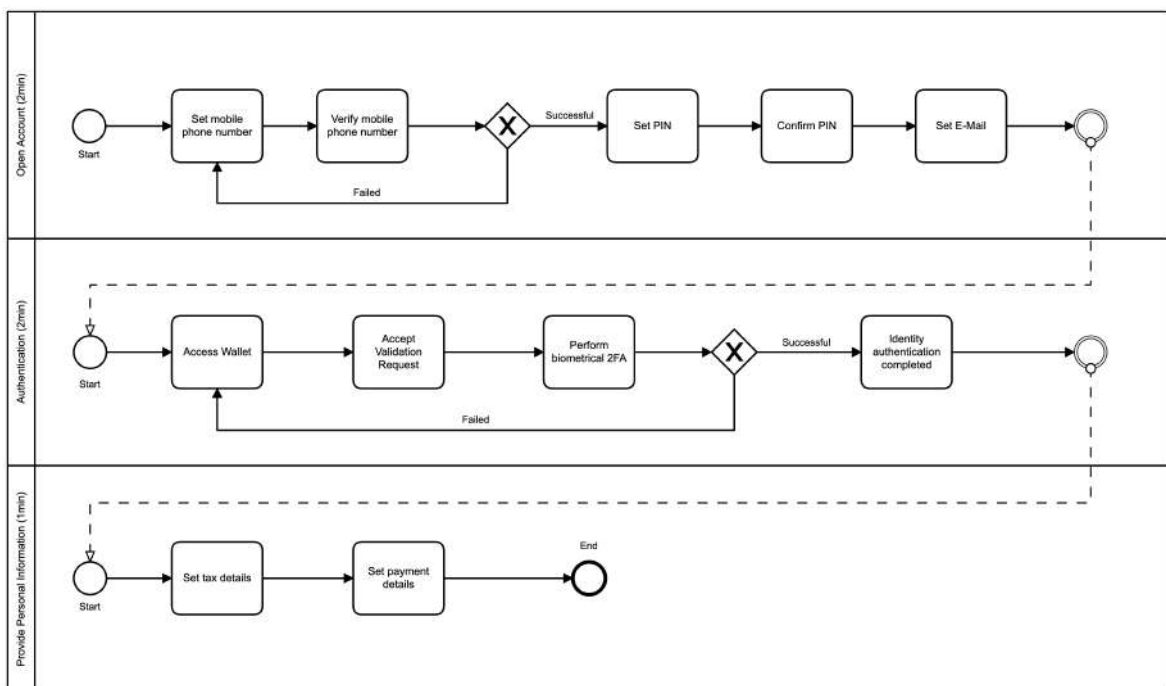


Figure 8: Verification with NFT ID

As can be seen from Figure 9, after successful verification of the mobile phone number as the initial step, the user can choose between manual registration or registration with NFT ID. The manual registration is equivalent to the actual registration process of TradeRepublic, which has been described in Section 5.1. According to Nielsen's heuristic

Help and Documentation, the UI indicates how long each registration method takes until completion, so the users know what they can expect.

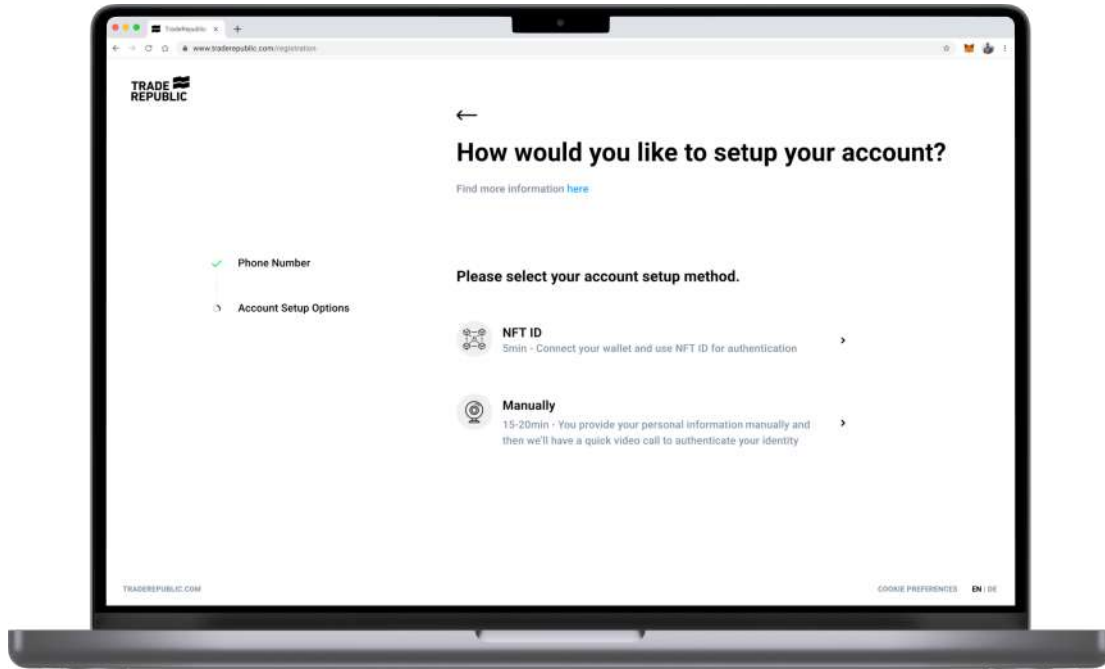


Figure 9: Selection of desired Registration Method

After choosing NFT ID as the registration method, the users will be asked to connect TradeRepublic to their wallet in order to provide their necessary personal information and to verify their identity. According to Nielsen's heuristic *Help and Documentation*, the UI shown in Figure 10 describes the required steps and provides an indication where the wallet browser extension can be found. In general, however, it can be assumed that users who choose NFT ID as registration method already know how to interact with it. If a user is totally unexperienced, they can find more information about NFT ID by clicking the highlighted URL in blue. Furthermore, according to Nielsen's heuristic *Visibility of system status*, the users can recognize where they currently are in the registration process on the left hand side. This indication can also be found in a similar way in the original registration process.

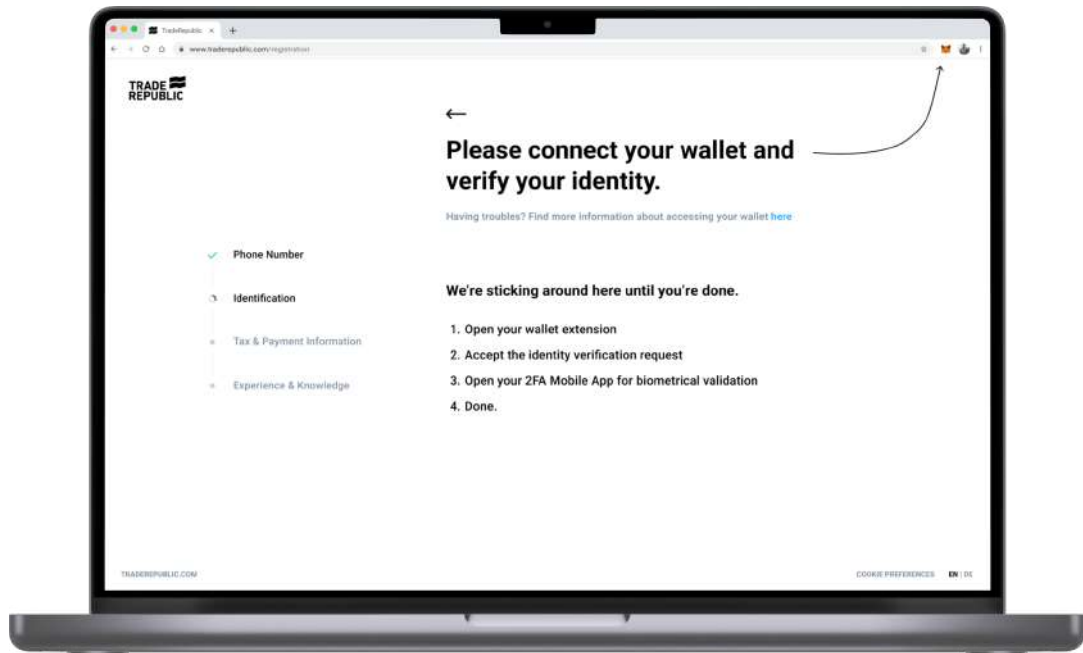


Figure 10: Help Screen

Once the wallet has been opened, users will find TradeRepublic's verification request and will be asked to either deny or confirm it as shown in Figure 11. In the first case, the wallet closes again automatically.

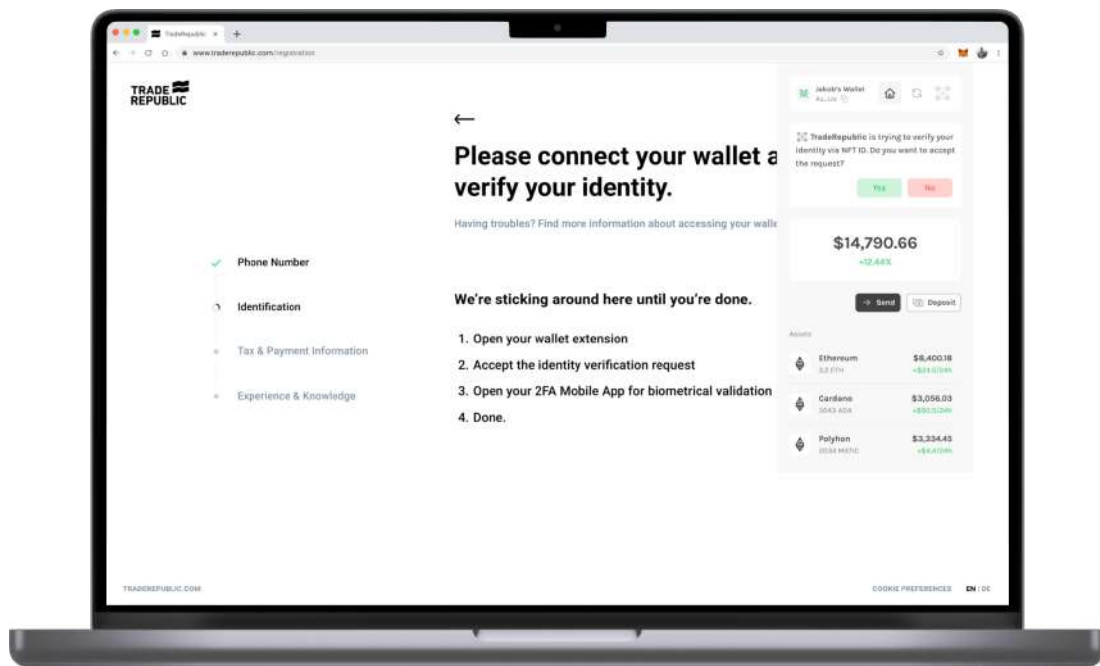


Figure 11: Incoming Verification Request

In the second case illustrated in Figure 12, the users are asked to open the Two-Factor-Authentication app associated with their wallet to confirm their identity via biometric matching with Face ID. A loading spinner is displayed during the waiting time according to Nielsen's heuristic *Visibility of system status*.

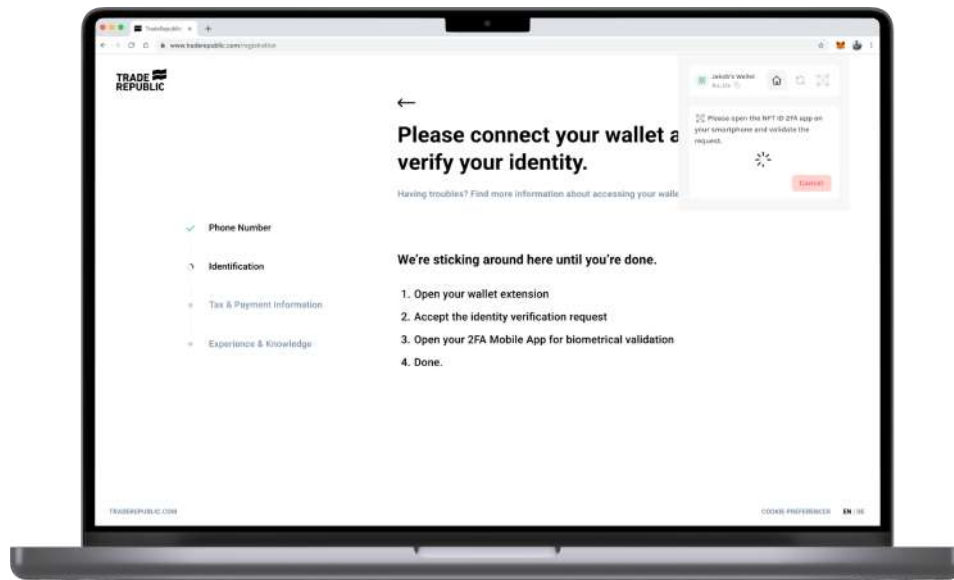


Figure 12: Pending Verification Request

The users receive a notification on their mobile device once they accept the request within their browser wallet. After opening the 2FA app, the user is asked again if the request should be accepted to avoid requests being confirmed unintentionally.

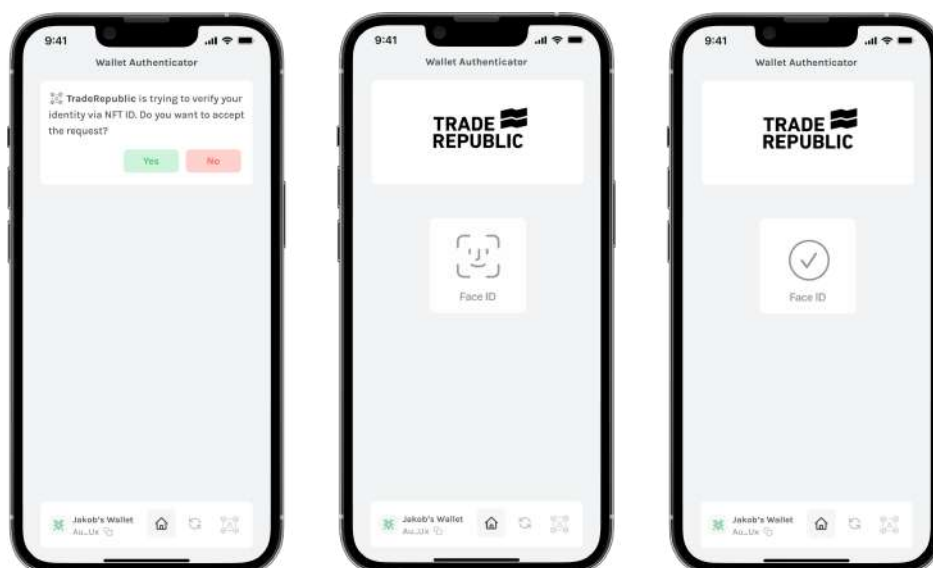


Figure 13: Two-Factor-Authentication

Once the request has been confirmed by identifying the user via Face ID, the user is simultaneously informed within the browser extension that the request has been successfully confirmed according to Nielsen's heuristic *Visibility of system status*.

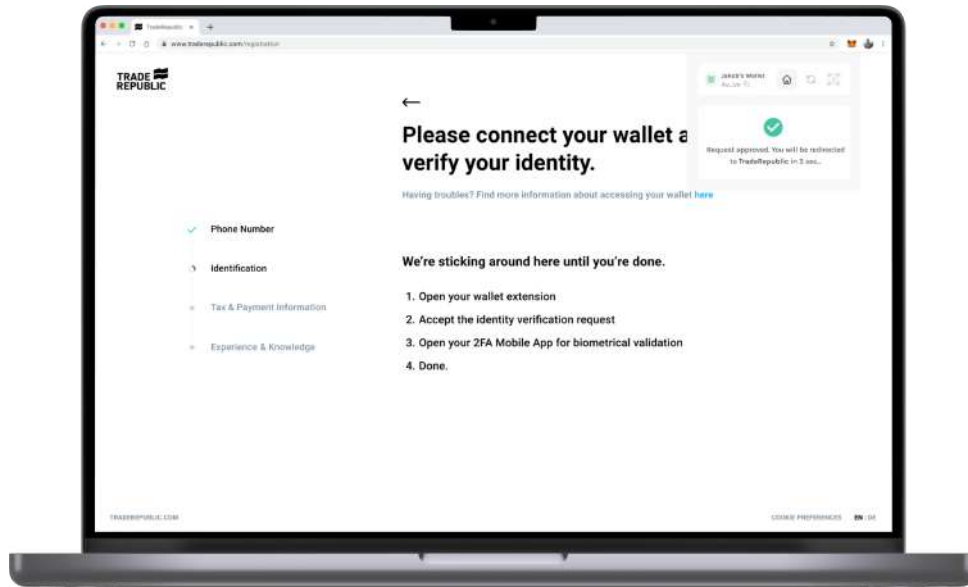


Figure 15: Successful Biometric Matching

Finally, the wallet closes automatically after 3 seconds and TradeRepublic automatically refreshes. With that, the verification is completed.

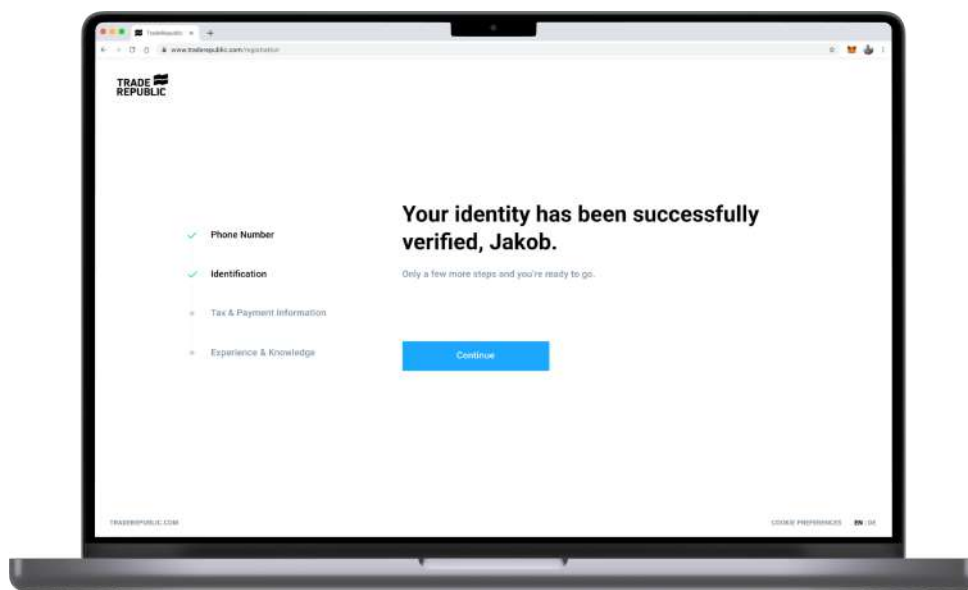


Figure 16: Completed Verification

7. Conclusion

In the following, the results of this master thesis are summarized. Furthermore, a critical reflection as well as an outlook on future research possibilities is given.

7.1 Summary

In order to answer the first research question of this master thesis, whether a blockchain-based approach would be technically feasible and what advantages would result from it, especially in terms of security, a comprehensive literature review on *Blockchain* and *Non-fungible Tokens* was conducted first. On the basis of the findings obtained, it was possible to conclude that a blockchain-based solution is technically feasible and well suited for the purpose of online authentication especially because of security through decentralization and cryptographic encryption. In the second step of the literature research, the topics of *Usability* and *User Experience* were examined in order to gain insights that would be incorporated into the later development of the prototype.

Subsequently, conventional Remote-Ident methods were examined for their strengths and weaknesses within the context of a comparative analysis. It was found that none of the established methods offer an ideal solution in the aspect of security and UX. PostIdent is a very secure, but does not offer a user-friendly approach due to the high effort involved. eID offers a good UX in itself, but is hardly widespread and less secure. Currently, VideoIdent is the most widely used method as it offers a moderate level of security, requires no prior setup like eID, and is comparatively much faster than PostIdent but slower than eID.

In the final step of this master thesis, a prototype of a blockchain-based Remote-Ident method was developed and an exemplary registration process was used to illustrate what the UX of NFT ID could look like in the future. *Non-fungible Tokens* have been found to provide the technical foundation to securely represent passports and other identity documents to the Blockchain through their characteristics of uniqueness and proof of authenticity. Blockchain technology therefore enables NFT ID to have a very high level of security while eliminating the need for a third party identification provider. Two-factor authentication and facial recognition via smartphone make it impossible to overcome NFT

ID even through deepfakes. Therefore, NFT ID offers a fast, secure and user-friendly overall solution and is outperforming conventional Remote-Ident methods.

7.2 Critical Reflection and Outlook

Although the research question has been answered and the objective of the thesis has been achieved, the results are critically reflected and any limitations that arise are presented in the following.

At this point, it can be critically reflected that this master thesis puts a strong focus on the User Experience of NFT ID as blockchain-based Remote-Ident method and neglects the technical point of view. Although an extensive literature research on Blockchain and NFT was conducted in Chapter 2, the gained insights are only sufficient to prove the technical feasibility of NFT ID. However, since Blockchain and Non-Fungible Tokens are highly complex technologies, further investigation by developers is needed for the technical implementation of NFT ID. Future studies in this context may, for example, examine how to prevent NFT IDs from being sold in NFT marketplaces. Furthermore, it could be explored how Visas could be implemented. In addition, consideration could be given to complementing NFT ID with other technologies such as RFID or NFC. Instead of storing the NFT ID only on the smartphone or desktop device, it could be investigated how it could also be stored in RFID tags implanted in the hand, for example. As NFT IDs contain personal information which allow conclusions to be drawn about the wallet owner, it should additionally be approached how it could be encrypted to preserve the core principle of anonymity of a Blockchain. First, however, the prototype presented in this thesis should be further developed and tested in the context of a usability study as it only shows a successful verification and does not present the UX flow of a failed one for instance.

In conclusion, it can be said that the research questions formulated at the beginning were answered comprehensively through the use of appropriate research methodology and logical argumentation. The results obtained in this master thesis create an outlook on how remote identification can be made more secure and efficient in the future through the use of Blockchain and Non-Fungible Tokens. Thus, a basis for NFT ID from a User Experience

point of view has been created, which should now be complemented by a further study from a technical perspective.

Attachment

	Videoident	PostIdent	eID
Concept	remote identity verification method where users are validated based on face-to-face video calls	identity verification method where users need to visit a physical post office for verification	remote identity verification method where users verify themselves by scanning their ID using NFC
Third Party	Videoident is provided by private third party services contracted by the company where the user wants to register	Post Ident is a service in Germany provided by Deutsche Post AG which is an exchange-listed logistics and postal company	eID is service provided by the German government in in collaboration with various trusted third parties
Requirements	Webcam	Physical post office which supports PostIdent	New ID with active eID functionality, smartphone with NFC reading capability
Duration without former setup	8-12min	Up to 24h	3min
Biometrical Matching	Yes	Yes	No
Security	Medium	High	Low
Automatical Input Filling	No	No	Yes

Bibliography

Alrawais, A. (2020) Security Issues in Near Field Communications (NFC). In: International Journal of Advanced Computer Science and Applications, Vol. 11, No. 11, 2020

Ali, M., Bagui, S. (2021) Introduction to NFTs: The Future of Digital Collectibles. In: International Journal of Advanced Computer Science and Applications, Vol. 12, No. 10, 2021

Ante, L. (2021). The non-fungible token (NFT) market and its relationship with Bitcoin and Ethereum

<https://deliverypdf.ssrn.com/delivery.php?ID=170124119105002019103118121005079077122024024079020086078022114005121119108105118081017021040022038009060126017096094117004025055090056092048090112098012102031121067066009020082101020072096086092120031098000086020102112001116067111012118101124064115006&EXT=pdf&INDEX=TRUE> (last accessed 08.05.2022)

Bartel, T., Quint, B., Weichert, S. (2018) Quick Guide UX Management, So verankern Usability und User Experience im Unternehmen. Wiesbaden: Springer Gabler Verlag

Basu, S., Basu, K., Austin, T. (2022) Crowdfunding Non-fungible Tokens on the Blockchain. In: Silicon Valley Cybersecurity Conference 2021

Berentsen, A., & Schär, F. (2017) Bitcoin, Blockchain und Kryptoassets: Eine umfassende Einführung. Basel: Universität Basel.

Brau, H., Sarodnick, F. (2010) Methoden der Usability Evaluation, Wissenschaftliche Grundlagen und praktische Anwendung. Vol. 2. Bern: Huber Verlag

Bevan, N. (2019) What is the difference between the purpose of usability and user experience design evaluation methods? https://www.researchgate.net/publication/238775905_What_is_the_difference_between_the_purpose_of_usability_and_user_experience_evaluation_methods (last accessed 23.04.2022)

Buhl, U., Kundisch, D., Schachmann, N., Renz, A. (2007) Spezifizierung des Kano-Modells zur Messung von Kundenzufriedenheit. Augsburg: AIS Electronic Library

Deutsche Post (2021) Einfach überall sicher identifiziert mit PostIdent, <https://www.deutschepost.de/de/p/postident.html> (last accessed 02.06.2022)

Di Angelo, M., Salzer, G. (2021) Identification of token contracts on Ethereum: standard compliance and beyond. In: International Journal of Data Science and Analytics 2021

Fill, H., Meier, A. (2019) Blockchain kompakt. Grundlagen, Anwendungsoptionen und kritische Bewertung. Wiesbaden: Springer Vieweg

Floyd, C. (1984) A systematic look at prototyping, Berlin: Institut für angewandte Informatik

Flückiger, M./Richter, M. (2013) Usability Engineering Kompakt, Vol. 3. Berlin: Springer Vieweg

German Federal Office for Information Security (2019) Blockchains sicher gestalten. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Blockchain_Analyse.pdf (last accessed 01.03.2022)

German Federal Office for the Interior (2022) eID Service <https://www.personalausweisportal.de/Webs/PA/DE/wirtschaft/technik/eID-service/eid-service-node.html#doc14620562bodyText1> (last accessed 08.05.2022)

Gothelf, J., Seiden, J. (2011) Lean UX: Applying Lean Principles to Improve User Experience

Hassenzahl, M., Tractinsky, N. (2006) User Experience – A Research Agenda, in: Behaviour & Information Technology, Vol. 25, No. 2

Hevner, A. (2007) A Three Cycle View of Design Science Research, in: Scandinavian Journal of Information Systems, Vol. 19, No 2

IDnow (2022). eID: Fast and secure identity verification with the German identity card. <https://www.idnow.io/de/produkte/idnow-eid/> (last accessed 08.05.2022)

Jordan, P. (2000) Designing Pleasurable Products, An introduction to the new human factors. London: Taylor & Francis

Kiebach, A., Licher, H., Schneider, M., Züllighofen, H. (1992) Prototyping in industriellen Software-Projekten – Erfahrungen und Analysen, in: Informatik-Spektrum, Vol. 15, No. 184

Law, C., Roto, V., Hassenzahl, M., Vermeeren, A., Kort, J. (2009) Understanding, Scoping and Defining User Experience: A survey approach. Boston: International Conference on Human Factors in Computing Systems

Meinel, C., Gayvoronskaya, T., Schnjakin (2018) Blockchain: Hype oder Innovation. Technische Berichte Nr. 113. Potsdam: Hasso Plattner Institut

Nakamoto, S. (2008) Bitcoin: A Peer-to-Peer Electronic Cash System. <https://bitcoin.org/bitcoin.pdf>, (last accessed 01.03.2022)

Nielsen, J. (1993) Usability Engineering. San Diego: Academic Press Inc.

Nielsen, J. (1994) 10 Usability Heuristics for User Interface Design, www.nngroup.com/articles/ten-usability-heuristics/ (last accessed 07.05.2022)

Nielsen, J., Norman, D. (2016) The Definition of User Experience (UX), www.nngroup.com/articles/definition-user-experience/ (last accessed 13.05.2022)

Peppers, K., Tuunanen, T., Gengler, C., Virtanen, V., Bragge, J. (2006) The design science research process: A Model for producing and presenting information systems research, Claremont: DESRIST

Pohlmann, N. (2018) eID Service

<https://norbert-pohlmann.com/app/uploads/2017/07/358-Wenn-der-Softbot-menschliche-Identit%C3%A4t-best%C3%A4tigt-%E2%80%93-VideoIdent-Verfahren-Die-Technik-Prof.-Norbert-Pohlmann.pdf> (last accessed 08.05.2022)

Raithel, J. (2008) Quantitative Forschung - Ein Praxiskurs. Berlin: Springer VS Verlag

Regner, F., Schweizer, A., Urbach, N. (2019) NFTs in Practice – Non-Fungible Tokens as Core Component of a Blockchain-based Event Ticketing Application. <https://www.fim-rc.de/Paperbibliothek/Veroeffentlicht/1045/wi-1045.pdf> (last accessed 22.05.2022)

Schlatt, V., Schweizer, A., Urbach, N., Fridgen, G. (2016) Blockchain: Grundlagen, Anwendungen und Potenziale. Augsburg: Fraunhofer-Institut für Angewandte Informationstechnik

Statista (2021) Monthly number of active users of selected leading apps that allow for online share trading in Germany. <https://www.statista.com/statistics/1259986/etrading-app-monthly-active-users-germany/> (last accessed 22.06.2022)

Wang, Q., Li, R., Wang, Q., Chen, S. (2021) Non-Fungible Token (NFT): Overview, Evaluation, Opportunities and Challenges. <https://arxiv.org/pdf/2105.07447.pdf> (last accessed 08.05.2022)

Acknowledgement

I hereby confirm that I have independently written my master thesis with the topic: *NFT ID - Development of a prototype for a blockchain-based Remote-Ident solution and its impact on User Experience*, and that I have not used any sources or aids other than those indicated. I also assure that the submitted electronic version is identical to the printed version.

EIGENSTÄNDIGKEITSERKLÄRUNG / STATEMENT OF AUTHORSHIP

Wiemer

Name | Family Name

41277458

Matrikelnummer | Student ID
Number

Jakob

Vorname | First Name

NFT ID - Development of a prototype for a blockchain-based Remote-Ident solution
and its impact on User Experience

Titel der Examsarbeit | Title of Thesis

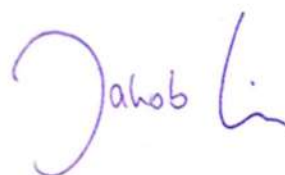
Ich versichere durch meine Unterschrift, dass ich die hier vorgelegte Arbeit selbstständig verfasst habe. Ich habe mich dazu keiner anderen als der im Anhang verzeichneten Quellen und Hilfsmittel, insbesondere keiner nicht genannten Onlinequellen, bedient. Alles aus den benutzten Quellen wörtlich oder sinngemäß übernommene Teile (gleich ob Textstellen, bildliche Darstellungen usw.) sind als solche einzeln kenntlich gemacht.

Die vorliegende Arbeit ist bislang keiner anderen Prüfungsbehörde vorgelegt worden. Sie war weder in gleicher noch in ähnlicher Weise Bestandteil einer Prüfungsleistung im bisherigen Studienverlauf und ist auch noch nicht publiziert.

Die als Druckschrift eingereichte Fassung der Arbeit ist in allen Teilen identisch mit der zeitgleich auf einem elektronischen Speichermedium eingereichten Fassung.

With my signature, I confirm to be the sole author of the thesis presented. Where the work of others has been consulted, this is duly acknowledged in the thesis' bibliography. All verbatim or referential use of the sources named in the bibliography has been specifically indicated in the text.

The thesis at hand has not been presented to another examination board. It has not been part of an assignment over my course of studies and has not been published. The paper version of this thesis is identical to the digital version handed in.



29.06.2022 Berlin

Datum, Ort | Date, Place

Unterschrift | Signature