# NFTs in Practice – Non-Fungible Tokens as Core Component of a Blockchain-based Event Ticketing Application

*Completed Research Paper*

**Ferdinand Regner**
FIM Research Center
University of Augsburg
86159 Augsburg, Germany
ferdinand.regner@tum.de

**André Schweizer**
FIM Research Center
University of Bayreuth
95447 Bayreuth, Germany
andre.schweizer@fim-rc.de

**Nils Urbach**
Project Group BISE of Fraunhofer FIT
University of Bayreuth
95447 Bayreuth, Germany
nils.urbach@fim-rc.de

## Abstract

*Non-fungible tokens (NFTs) are a new type of unique and indivisible blockchain-based tokens introduced in late 2017. While fungible tokens have enabled new use cases such as Initial Coin Offerings, the potential of NFTs as a valuable component remains unclear. This paper addresses this gap in theoretical and practical knowledge and demonstrates the efficacy of NFTs in the domain of event ticketing. We follow a rigorous design science research approach of designing, building and thoroughly evaluating a prototype of an event ticketing system based on NFTs. Thereby, we demonstrate the usefulness of NFTs to tokenize digital goods, prevent fraud and improve control over secondary market transactions. Further, we contribute generalizable knowledge of the benefits and challenges of NFTs and derive implications for both researchers and practitioners. Finally, this paper proposes managerial recommendations for building applications utilizing NFTs and enables other researchers to draw on its findings and design principles.*

**Keywords:** Blockchain, Tokenization, Smart Contract, Non-Fungible Token, Ticketing

## Introduction

Blockchain technology is a radical innovation with the potential to challenge or even replace existing business models relying on third parties for trust (Beck and Müller-Bloch, 2017). The concept of blockchain was introduced in 2008 through the release of the Bitcoin whitepaper (Nakamoto, 2008) and primarily used as the technology behind cryptocurrencies during its first years. In 2014, a second generation of blockchains (e.g. Ethereum) was introduced, which allows to program and execute software – so-called smart contracts – on all participating blockchain nodes. Consequently, any user is enabled to create and deploy programs on a shared global infrastructure (Buterin, 2014; Wood, 2014). This has led to the realization of new concepts designed to simplify human interaction and collaboration on a large scale across several industries (e.g. supply chain management, international payments, international trade finance, energy markets, and notary services) (Christidis and Devetsikiotis, 2016; Morabito, 2017; Wüst and Gervais, 2017). Particularly, the use cases of Initial Coin Offerings (ICOs) that re-invent crowdfunding through the use of blockchain and its ability to tokenize assets, is drawing public attention (Fridgen, Regner, Schweizer and Urbach, 2018). The spectacular success of ICOs, where globally an estimated 12 billion USD has been collected, has been enabled by the ERC-20 standard (AutonomousNEXT, 2018). This standard, which specifies a common interface for fungible tokens that are divisible and not distinguishable, was mutually agreed on by the developer community to ensure interoperability (Vogelsteller, 2015).

In contrast, non-fungible tokens (NFTs) differ from fungible tokens in two important aspects. Every NFT is unique and it cannot be divided or merged (Voshmgir, 2018). This new form of token was first introduced with the ERC-721 standard in late 2017 (Entriken, Shirley, Evans and Sachs, 2018). ERC-721 variates significantly from the ERC-20 standard as it extends the common interface for tokens by additional functions to ensure that tokens based on it are distinctly non-fungible and thus unique (Entriken et al., 2018). For practitioners, these distinct properties of NFTs enable a variety of new use cases. It particularly improves the tokenization of individual assets which is not feasible with fungible tokens, as they cannot digitally represent uniqueness. Thus, practitioners have conducted a multitude of experiments in the past months using NFTs to represent both digital goods such as virtual gaming assets, digital artwork and software licenses as well as physical assets such as luxury goods and cars (Butcher, 2018; Griffin, 2018). NFTs are seen as key to unlock the market for collectibles which has an estimated global market size of USD 200 billion (Fenech, 2018).

However, aside from the existence of first experimental use cases, a deeper understanding of NFTs would be beneficial from the viewpoint of IS research in three main aspects. First, solidified descriptive knowledge about the general characteristics of NFTs and the differences from fungible tokens enables a better understanding of the benefits and resulting opportunities. Second, improved prescriptive knowledge about the process of designing and evaluating applications based on NFTs benefits both researchers and practitioners. Third, increased awareness of practical challenges enables future researchers to better focus on solving remaining challenges. Unfortunately, in-depth investigations of NFTs by academic researchers touching these aspects are still missing. Further, the current body of knowledge lacks best practices, development project experience, and insights to blockchain-based software development (Delmolino et al., 2016). Thus, we conclude that a clear research gap exists. We aim to bridge that gap by demonstrating the applicability of non-fungible tokens in a specific domain and answering the following research question: *What are the benefits and challenges of practical use of NFTs?*

We answer the question by following a design science research (DSR) approach and developing the use case of an event ticketing system. Doing so we present a new way to create, manage, transfer, and track the ownership and usage rights involved. We have chosen tickets as persuasive example because 1) current solutions typically face problems such as fraud, counterfeiting and limited control over secondary transactions (Waterson, 2016), 2) due to heavy reliance on third parties for trust there is a potential for disruption through blockchain technology (Beck and Müller-Bloch, 2017), and 3) the use case is limited in scope and thus suited for DSR prototype building. Therefore, we design and implement a prototype based on NFTs for a decentralized, blockchain-based event ticketing system that aims to replace the existing centralized ticket applications. By evaluating the prototype and its use, we gain valuable insights, discover challenges and draw conclusions that enable both a technical-oriented and management-oriented audience to benefit from it. The creation and evaluation of a prototype are central activities of the DSR approach we follow, which has been taken several times by IS researchers when dealing with blockchain use cases (Beck et al., 2016; Notheisen et al., 2017; Schweizer et al., 2017). Further, building an instantiation in a specific domain is a well-recognized practice when confronted with new technology (Hevner et al., 2004). Lindman et al. (2017) specifically propose the development and analysis of blockchain-based prototypes using a DSR approach. As thorough evaluation is key to prove the correctness and applicability of the resulting prototype, we follow an iterative build and evaluate approach (Hevner, 2007; Gregor and Hevner, 2013). Further, we draw on extant literature and expert interviews to assess the suitability of the artifact to its intended purpose and to gain insights into the benefits and challenges of NFTs. This approach has proven its suitability and is in line with various recent publications in the blockchain and DSR domain.

Our theoretical contributions and practical implications are threefold: First, through creating a working prototype as resulting artifact, we demonstrate the feasibility of a blockchain-based solution with NFTs as a core component for the domain of event ticketing systems. Thereby, we illustrate that many existing problems in the ticketing industry such as fraud, lack of trust and limited control over secondary grey markets can be overcome by switching to a blockchain-based solution that utilizes NFTs. Second, by exploring NFTs from a technological and economic perspective, we generate generalizable knowledge and insights. Thus, we contribute both descriptive and prescriptive knowledge to the young research domain concerning NFTs. Given that theoretic knowledge about opportunities and challenges in the area is scarce and best-practice approaches are lacking, we lay ground for further research and higher-theory (Gregor, 2006; Glaser, 2017). Third, we enable practitioners to gain insight into an efficient building process and enhance their understanding of NFTs and associated consequences of its use including potential benefits and challenges.

The remainder of this paper is structured as follows: The next section provides a brief introduction into NFTs as a novel building block in the blockchain space and the current problems in the domain of ticketing. Subsequently, we outline the DSR methodology the paper adheres to in order to address the research question and lay out the application step by step. Thereafter, we describe the resulting artifact and present its software architecture and design. The second last section deals with the evaluation and discussion of the obtained results before we present our conclusion in the final chapter.

# Background

## *Blockchain and Non-Fungible Tokens (NFT)*

Blockchain is a fairly new technology and first gained popularity as the protocol behind the cryptocurrency Bitcoin, which was introduced in 2009 at the peak of the financial crisis (Nakamoto, 2008; Zohar, 2015). Aside from this first instantiation and the use case of cryptocurrencies, a broader range of applications emerged – a development that is mainly attributed to the possibility to run pieces of software code on a blockchain (Beck et al., 2016). These so-called smart contracts, a term coined by Nick Szabo in 1994, allow parties that do neither know nor trust each other to securely perform transactions. The correct execution is ensured by a consensus protocol that runs on all participating nodes of the underlying blockchain and provides consistency (Szabo, 1994; Glaser, 2017; Sillaber and Waltl, 2017).

The first and most popular blockchain protocol, that supports a virtual machine with which Turing-complete scripting languages can be executed is Ethereum, which was first introduced in 2014 (Buterin, 2014). As Ethereum is a public, permissionless blockchain protocol, it allows any user to create and deploy programs on its shared global infrastructure (Wood, 2014). A vibrant community has evolved that runs a multitude of pieces of software code (smart contracts) on the Ethereum blockchain. To foster interoperability, the community agreed on multiple application-level standards – so-called Ethereum Requests for Comments (ERCs) (Ethereum Foundation, 2018). The most well-known standard, called ERC-20, specifies a standardized interface for fungible tokens which have been widely used to provide holders with certain access or governance rights, and to facilitate ICOs, a novel form of crowdfunding (Vogelsteller, 2015; Rohr and Wright, 2017). The spectacular popularity of ICOs, which raised over USD 7 billion in 2017 and more than USD 12 billion in 2018, has contributed to the global popularity of tokens in general (AutonomousNEXT, 2018; Pichler, 2018). A search on Etherscan, a popular Ethereum blockchain explorer, returns over 140,000 token contracts deployed on the public Ethereum main chain (Etherscan, 2018), indicating that tokens represent an important component for blockchain use cases. While fungible tokens, such as tokens based on the ERC-20 standard, have been widely used, a new class of tokens was introduced in late 2017 with the ERC-721 standard. The ERC-721 standard specifies a standardized interface for so-called *non-fungible tokens* (Entriken et al., 2018). The motivation behind the creation of this new standard was that a crucial difference between fungible tokens and non-fungibility tokens exists. The term *fungible* refers to the interchangeability of each unit of a commodity with other units of the same commodity, i.e. two parties could swap the same amount without any gain or loss. While fungibility – the ability to be substituted in place of one another – is an essential feature of any currency, non-fungibility is the opposite as every token is distinguishable and thus also cannot be divided or merged (Merriam-Webster, 2018; Voshmgir, 2018). This also has implications for tracking the ownership of tokens as each NFT needs to be tracked separately. The ERC-721 standard specifies that every NFT has a globally unique id, is transferable, and can optionally include metadata. NFTs were created for a specific purpose – to represent ownership over digital or physical assets (Entriken et al., 2018). While the concept of "colored coins" as a representation of real-world assets on the Bitcoin blockchain has been discussed before the advent of Ethereum, with the creation of the ERC-721 standard this idea has first been realized (Wang, 2017).

The first application based on NFTs to reach widespread adoption was a virtual online game called CryptoKitties. The game took up more than 70% of the transaction capacity of the Ethereum network at one point and the most expensive NFT that represents ownership of such a cat was sold for over USD 100,000 in late 2017 (Tepper, 2017; AutonomousNEXT, 2018; Muzzy, 2018). Over 100 similar digital collectibles such as virtual card games or unique original digital art have been created by the community in the past year and the number is expected to grow further (Tomaino, 2018). However, while digital items arguably only have value in the context of their ecosystem, NFTs also can help to facilitate the tokenization of real-world assets, such as artwork (Voshmgir, 2018). Multiple experiments on tokenizing software licenses, luxury goods and even cars through the use of NFTs have been conducted in the past months (Butcher, 2018; Griffin, 2018). The accounting firm EY has stated in a press release that they use NFTs to facilitate private equity transactions (Khatri, 2018). NFTs also play a key role in scaling the ability of Ethereum to process a high number of transactions using state channels (Coleman, Horne and Xuanji, 2018). Yet, despite the existence of a multitude of ideas and experiments to use NFTs for a variety of additional use cases such as tokenizing educational certificates like academic degrees, copyright enforcement, supply chain tracking, or Know-Your-Customer (KYC) procedures, peer-reviewed studies dealing with the topic remain scarce (Voshmgir, 2018). As no empirical study of the use of NFTs is available so far, the benefits and challenges remain largely unexplored. While NFTs on their own do not have any value per se, they might enable new use cases that were not possible so far and create utility for users (Sparango, 2018). Thus, we treat NFTs as a potentially valuable building blocks and utilize a specific use case to check if this assumption is valid and to gain theoretical and practical insight on usage, benefits and challenges.

### *Event Ticketing systems*

Tickets represent a mechanism to demonstrate entitlement to access to any event such as sports or culture. They come in many forms, ranging from physical paper to electronically readable codes on paper or chips embedded in smart cards or wristbands (Waterson, 2016). Tickets can be bought on the primary market directly from the event organizer or from authorized sellers such as appointed agents, mostly for a fixed price. Secondary markets also exist, with the notable difference that any price can be charged and buyers and sellers often directly engage in business or rely on secondary ticket sale platforms, which typically take 25-30 percent of secondary sales in fees (Waterson, 2016). Ticket resale is a growing business globally, totaling 8 billion USD in revenue per annum (Courty, 2017). However, while platforms and third parties do well, the status quo is not satisfactory for the two central stakeholders – the event organizer and the customer – as multiple complaints at consumer protection agencies show (McMillan, 2016; Courty, 2017; NZ Herald, 2017). Consumers have to trust third parties when buying tickets on secondary markets and thus face the risk of purchasing fraudulent or invalidated tickets, which are counterfeits or might be cancelled (The Australian Government the Treasury, 2017). Using QR-codes or barcodes, which encode information, but do not encrypt it, is not sufficient to make tickets truly tamper-proof. Further, consumers lack the possibility to validate if the barcode on their ticket is valid. In various cases, the same barcodes have been sold multiple times or been obtained by extracting it from pictures of a ticket posted online (Tackmann, 2017). The problem of ticket fraud is not exactly small: An estimated 12% of ticket buyers get scammed, which amounts to an estimated yearly damage of USD 2 bn (Waterson, 2016; Leonhart, 2018).

Ticket prices on secondary markets are taken to extremes, partially through the use of bots which automatically drive up prices to earn a profit by reselling them at the highest possible markups (Courty, 2017). Thus, multiple governments are considering bans of ticket resale for profit altogether, however, economists remain skeptical about outright resale bans (Courty, 2017). From the event organizer's point of view, a major problem is the limited control over secondary transactions. Neither does the use of static codes on a ticket permit to link a ticket to the owner if it is resold, nor is it desirable to strictly bind a ticket to a person and prohibit reselling completely as costly and time-consuming entry checks must be performed (Waterson, 2016). Summing up, a clear lack of transparency and trust is evident, and stakeholders are currently in search of efficient and effective solutions to tackle this problem (Waterson, 2016; Tackmann, 2017).

Searching for current projects in the area of event ticketing systems, we found some idea proposals and early-stage projects involving blockchain technology from companies like aventus, GET Foundation and IBM (GET, 2017; Tackmann, 2017; aventus, 2018). However, a first analysis of these proposed solutions revealed that each of them relies on fungible tokens at the core and the core features are not build on an immutable ledger but rather off-chain by the company. This means that tickets are not truly represented by unique identifiers on a trust-free blockchain and the potential improvement using NFTs as a core component has yet to be assessed. The problems in secondary markets in the domain of ticketing are prototypical and apply to many other industries. Current literature suggests that industries with heavy reliance on third parties for trust are a potential target for disruption through blockchain technology (Beck and Müller-Bloch, 2017).

# Research Method

To design, implement and evaluate a blockchain event ticketing system prototype, we follow a DSR approach. DSR, which historically originated from engineering, involves the creation of an artifact which has not existed previously and serves a meaningful human purpose (March and Smith, 1995). Typical characteristics of such research efforts are strong reliance on creativity and trial-and-error search (Hevner et al., 2004). In the DSR context, the creation of a prototype depicts an instantiation of a blockchain-based IT artifact (March and Smith, 1995). Through artifact instantiation, we demonstrate both feasibility of the design process and the designed product and enable researchers to learn about the effect of the artifact on the real world and appropriate use (Hevner et al., 2004). This approach has been taken several times by IS researchers when dealing with new aspects of blockchain technology (Beck et al., 2016; Notheisen et al., 2017; Schweizer et al., 2017).

Hevner et al. (2004) list seven guidelines for applying DSR in the IS space: It requires the creation of an innovative artifact that fulfills a specific purpose (1) for a specified problem domain (2). It is crucial to thoroughly evaluate the artifact with respect to providing a solution to the specified problem (3). A clear and verifiable contribution such as solving an unsolved problem or solving a known problem in a more effective or efficient manner is also mandatory (4). It requires rigorous definition, formal representation, coherence, and internal consistency of the artifact (5). Through the creation of the artifact, we construct a problem space along the process and a method to find an effective solution for it (6). Finally, we must communicate the results effectively (7). In Table 1, we map our approach to meet these seven guidelines.

| Guideline | Contribution |
|---|---|
| Design as an artifact | The prototype we build during our research instantiates an NFT-based artifact that allows trust-free creation, management and transactions of event tickets. |
| Problem relevance | We address a research gap in scientific literature regarding the question whether NFTs are suited to represent scarce digital assets (such as event tickets) and additionally try to gain insight into the benefits and challenges of the use of NFTs, which are yet to be determined by researchers. Regarding the use case of event tickets, we aim to address the problems of fraud, lack of trust, lack of control over secondary market transactions, low transparency and high dependence on intermediaries. |
| Design evaluation | To evaluate the prototype in terms of functionality, formal completeness, consistency, accuracy, reliability and efficiency, we follow the approach of Hevner et al., 2004, who state that the first and foremost aim is to show that (1) the solution works (proof by construction) and (2) characterize the environments in which it works (illustrative scenarios). |
| Research contributions | Our contribution is to demonstrate the usefulness of NFTs in the domain of event tickets in scientific rigor. Through artifact instantiation, we demonstrate both feasibility of the design process and the designed product and enable researchers to learn about the effect of the artifact on the real world and appropriate use (Hevner et al., 2004). Additionally, we aim to lay ground for further research and higher-theory in the area of NFTs and blockchain-based application development (Gregor, 2006; Glaser, 2017). |
| Research rigor | As this table shows, we closely follow the guidelines by Hevner et al., 2004 regarding the DSR process in IS. Additionally, we draw on best practices by other IS researchers that have dealt with similar approaches when evaluating new aspects of blockchain technology (Beck et al., 2016; Notheisen et al., 2017; Schweizer et al., 2017). To determine if our artifact design is complete, we follow a strategy of satisficing, meaning the solution is satisfactory regarding solving the requirements and constraints of the problem we state for the selected use case (Hevner et al., 2004). |

| | |
|---|---|
| Design as search process | We follow an iterative build and evaluate approach. To further assess suitability of the artifact to its intended purpose and gain insights into the benefits and challenges, we additionally draw on extant literature on both the application and solution domain as suggested by Hevner et al. (2004) and perform semi-structured expert interviews (Schultze and Avital, 2011). As peer-reviewed literature is scarce in this new area of research, we also make use of publicly accessible Internet sources such as open-source code repositories, whitepapers and blog articles, which strengthens our domain knowledge and ensures the recency of this paper. |
| Communication of research | We aim to provide clear information to both the management-oriented and technically-oriented audiences. The former benefits by the schematic UML diagram and theoretical reasoning about benefits and challenges, while for the latter we publish the entire source code of the project on GitHub, including all formal tests. This enables technical researchers and practitioners to replicate our work and/or build on it. |

**Table 1. Mapping of DSR Guidelines by Hevner et al. (2004) and our Contributions**

## Prototype Design and Development

In this section, we present the design and development of our blockchain-based event ticketing system according to the DSR guidelines by Hevner et al. (2004). First, we briefly outline the verified problem statement and the design objectives for the prototype. Second, we elaborate the fundamental design decision that led to the choice of the Ethereum blockchain and NFTs as core component of the prototype. Finally, we present an overview of the resulting prototype design and briefly explain its application.

### *Problem Statement and Derivation of Design Objectives*

Our literature analysis revealed the current problems in the event ticketing industry. To recap our findings, the status quo is not satisfactory for the two central stakeholders – the event organizer and the attendee, as multiple complaints at consumer protection agencies show (McMillan, 2016; Courty, 2017; NZ Herald, 2017). Following the relevance cycle laid out by Hevner (2007), we additionally validated our findings by interviewing the CEO of a ticketing firm, who contributed valuable expert knowledge. He largely confirmed our preliminary findings and added that it would be desirable for event organizers to directly interact with event attendees rather than the need to rely on intermediaries for trust and that an open protocol would be preferable over the opaque status quo. Table 2 gives a brief summary of the identified main problem areas.

| Problem area | Description |
|---|---|
| Lack of Trust | Consumers have to trust third parties when buying tickets on secondary markets and thus face the risk of purchasing fraudulent or invalidated tickets, that face the risk of being cancelled or are counterfeits (The Australian Government the Treasury, 2017). |
| No control over secondary market prices | Consumers ticket prices on secondary markets are taken to extremes, partially through the use of bots which automatically drive up prices to earn a profit by reselling them at the highest possible markups (Courty, 2017). From the event organizer's point of view, a major problem is the limited control over secondary transactions. |
| Dependence on intermediaries | Event organizers are dependent on intermediaries and bear financial risks while being cut off from windfall profits and direct relations with event attendees. |
| No immediate validation | Attendees cannot easily verify if their tickets are valid (Tackmann, 2017). |
| Lack of Transparency | A lack of transparency in the secondary market is evident in the event ticketing industry (Waterson, 2016) |

**Table 2. Overview of Identified Problem Areas**

Based on these findings and additional literature, we derived the desired design objectives for the prototype. Compliant to the relevance cycle proposed by Hevner (2007), we defined our design objectives and subsequent acceptance criteria for the evaluation of the research results based on Hevner et al. (2004). Table 3 lists the design objectives and the proposed evaluation criteria and methods.

| Design Objective | Description | Evaluation |
|---|---|---|
| **1. Digitization**<br>1.1. Digital storage of all data<br>1.2. Digital exchange of all data | Portability for tickets independent from a physical medium should be achieved (Fujimura et al., 1999). All data has to be stored and exchanged in a purely digital way (Nærland, Müller-bloch, Beck and Palmund, 2017). | Validation of efficacy and completeness though simulation and descriptive methods. |
| **2. Control over secondary market transactions**<br>2.1. Managing transactions<br>2.2. Prices caps<br>2.3. Charging transaction fees | The event organizer should be able to manage ticket transaction and earn transaction fees from any paid ticket transfer among attendees. Management policies should be determined by the ticket issuer (Fujimura et al., 1999). This includes pausing all transactions and capping ticket prices for secondary market transactions. | Functional analysis of the prototype to assess efficacy and reliability through testing and simulation. |
| **3. Independence**<br>3.1. Decentralization<br>3.2. Trustfulness | No centralized broker or authority should be assumed to sell tickets (Fujimura et al., 1999). Event organizers should be able to conduct business independent of intermediary parties. | Assessment of efficacy and validity through testing and descriptive evaluation. |
| **4. Security**<br>4.1. Availability<br>4.2. Integrity<br>4.3. Privacy | A secure environment is characterized by the accessibility of resources (availability), the authenticity of data (integrity), and the prevention of access to illegitimate users (privacy) (Vacca, 2013). | Consistency and reliability should be verified using testing, simulation and descriptive evaluation. |
| **5. Validation**<br>5.1. Verifiability of ownership | To increase trust in the integrity of the system, ticket ownership should be verifiable in a simple way at any time. | Functional testing and simulation to assess the reliability. |
| **6. Transparency**<br>6.1. View current ticket ownership<br>6.2. Access to transaction history | Ticket transaction history should be fully transparent. Current ownership status and any state change, from the creation and transfers between attendees to end of its lifecycle, should be publicly viewable. | Analysis of accuracy and completeness through simulation and descriptive methods. |
| **7. Automation**<br>7.1. No manual interaction required after setup | The event organizer should not be required to perform any manual action after an initial setup. Any policies set by the organizer should be enforced automatically. | Functionality and reliability should be assessed through testing and simulation. |
| **8. Cost Efficiency**<br>8.1. Efficient cost structure | The fixed and variable costs of the system should be economical from the event organizers point of view. | Assessment of efficiency through simulation. |

**Table 3. Design Objectives**

## *Fundamental Design Decisions*

A well-designed system architecture provides the roadmap for the subsequent development process (Nunamaker, Chen and Purdin, 1990). Before trying to apply a blockchain-based solution right away, we first ensured that our fundamental design decisions are well grounded. Thus, we followed the decision model by Wüst and Gervais (2017), which helps to decide if the use of blockchain technology is useful for a specific scenario. It guides the user through sequential decision criteria in form of questions. As the key question if all interacting parties can inherently be trusted was clearly answered with no, a blockchain solution is advisable according to the model. Since we positively answered the follow-up question if publicly available verification is necessary, the model advised making use of a public permissionless blockchain. Our design objectives provided a valuable guideline to select a blockchain with desired features. The Ethereum blockchain is a public and permissionless blockchain that supports smart contracts, and has the largest community of developers and rests on more than 60.000 nodes that run the network without a central point of failure (Beck et al., 2016). These properties enabled us to build an automated application that inherits the key features of the underlying blockchain such as decentralized trust, integrity, transparency, non-repudiation, and availability. Ethereum developed its own high-level programming languages which compile into bytecode that can be run on the Ethereum virtual machine; its most popular being *Solidity* which features a JavaScript-like syntax (Tikhomirov, 2018). Thus, we chose to develop the smart contract code for the prototype in Solidity. We relied on the development framework *Truffle*, which contains tools for the deployment of contracts and the testing library *Mocha* as well as *ganache-cli,* which provides a local Ethereum blockchain for testing (Truffle, 2019). Additionally, *Infura* provides access to public Ethereum test networks such as *Ropsten* without requiring us to set up our own full Ethereum node (Consensys, 2019). This toolkit proofed essential for efficient development, which is characterized by being test-driven and quick iterations (Janzen and Saiedian, 2005). Each of these choices is well-recognized and well-tested in the blockchain community, with more than 1 million users each (Mougayar, 2018). We used NFTs as the fundamental core component of our prototype, as they contribute to fulfilling our design goals thanks to their properties of uniqueness, indivisibility and transferability (Entriken et al., 2018). We reused the well-tested, audited and community-reviewed implementation of the ERC-721 standard by *OpenZeppelin*, which we extend by additional functions needed for our specific use case (OpenZeppelin, 2019).

### *Resulting Prototype*

Adhering to the design objectives and design choices we had specified, we built a prototype that addresses the concerns of both the event organizer and the attendees. Following the DSR cycle laid out in the previous section, we took to an interactive approach and started with a very basic design to resolve a highly simplified and abstracted problem. After evaluation of the preliminary results and performance of unit tests, we refined the requirements and the design needed to solve it respectively. The resulting prototype should be viewed as a basic implementation that focuses on core features necessary to meet the design goals we specified. Figure 1 depicts an UML diagram that outlines the main functions of the prototype.

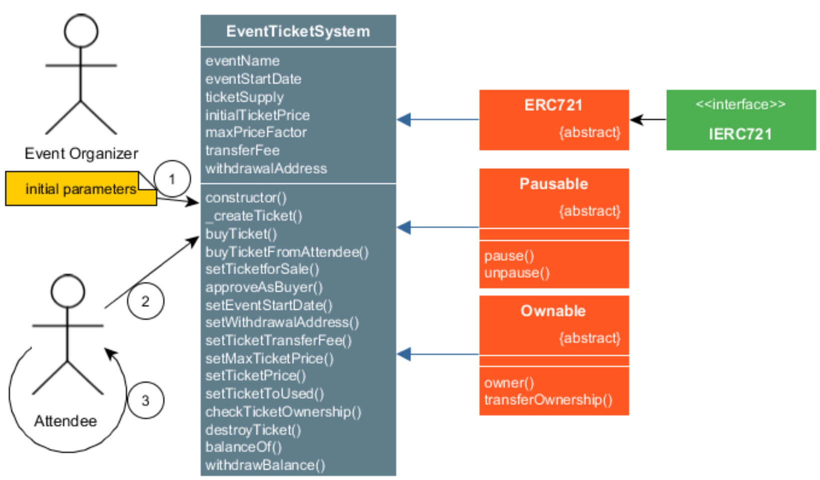


**Figure 1. UML Diagram (simplified)**

As the UML diagram shows, the only two entities participating in the simplified process are the event organizer and the event attendees. They conduct business solely by interacting with the smart contract – the need for a middleman is eliminated completely. The only requirement for the two parties is to own an account on the Ethereum blockchain, funded with some of its native cryptocurrency Ether, to interact with the smart contract. The sequence of interactions is numbered with 1-3 as depicted in the diagram.

**(1) Setup phase:** First, event organizers deploy a smart contract for a specific event. Initial parameters, such as the name of the specific event, an initial ticket price, a maximum price factor for tickets, the event start datetime, the maximum amount of tickets available and an initial transaction fee for secondary ticket transactions are provided to the *constructor()* as specified in the contract deployment script. A screenshot of the console log during the deployment of a sample event is pictured in Figure 2. The event organizer is the owner of the smart contract and thus can change these parameters later by interacting with the smart contract, in addition to withdrawing its balance and pausing transactions of tickets at any time.

```
2_deploy_contracts.js
=====================
Deploying contract for event  MyConcert ( MC ) on  7/7/2020
A maximum of 100 tickets are available
The initial ticket price is 1 ETH
Ticket prices are only allowed to be a factor of 2 of the initial ticket price
The ticket transfer fee between attendees is set to  20 % of the ticket price

   Deploying 'EventTicketSystem'
   ----------------------------
   > transaction hash:    0xd9ec4c3fa95851bc342f92bf6bd9b86f1c34859cb32b514594de7b6089b6cf1b
   > Blocks: 1            Seconds: 9
   > contract address:    0x672D4930a2425B94553843a057a2f3b14681C8E3
```

**Figure 2. Console Log of Contract Deployment on the Ropsten Test Network**

**(2) Primary market:** After contract deployment, event attendees can buy tickets until the supply limit is reached, by sending a transaction containing Ether to the payable function *buyTicket()*. The function first checks if the amount transferred is sufficient and then calls the internal function *_createTicket()* which "mints" a new NFT that acts as the virtual representation of a ticket. Each ticket is unique as its id can only exist once per contract and its ownership can be verified at any time by calling the function *checkTicketOwnership(id)*. The total number of tickets owned can be obtained by calling *balanceOf()*.

**(3) Secondary market:** Ticket owners can offer their tickets for resale by calling the function *setTicketForSale()*. They can use the function *setTicketPrice()* to charge any price that does not exceed the maximum price as defined by the event organizer. Any user with access to a blockchain-enabled web browser can purchase tickets from current ticket owners once approval has been set by the ticket owner through the call of *approvedAsBuyer()*. The buyer can now transfer the required amount of cryptocurrency to the payable function *buyTicketFromAttendee()*, which finally transfers the ticket to the buyer. The transaction fee set by the event organizer is automatically deducted and kept by the contract, where it can be withdrawn only by the contract owner. Once the event has started, the modifier *EventNotStarted()* will prohibit the use of any setter functions. Thus, no more tickets can be created or transferred after the time specified in *eventStartDate*. The organizer can call *setTicketToUsed()* to validate a ticket at the venue.

While the scope of this prototype does not feature a front-end for retail users, its full compatibility with the ERC-721 standard enables users to use any compatible wallet or NFT-marketplaces like OpenSea to facilitate peer-to-peer transactions in an easy manner (OpenSea, 2019). The prototype is deployed on the Ethereum test network *Ropsten* and thus allows any user with access to an Ethereum node to invoke the smart contract and use it. The source code of the implemented prototype including instructions for deployment is publicly available on GitHub[1].

## Evaluation and Discussion

For the evaluation, we linked back our resulting prototype to the design objectives and the evaluation criteria (see Table 3). Our evaluation is not limited to a single activity conducted at the end of the build phase, but rather represents an iterative process and encompasses multiple methods and perspectives (Pries-Heje, Baskerville and Venable, 2008).

### *Testing and Experimental Evaluation*

For a thorough analysis of our prototype's functionality, structure, formal completeness, consistency and quality, we relied on algorithmic white box testing, such as unit tests (Hevner et al., 2004). To refine and optimize our prototype, we followed a test-driven approach and iterated between testing and improving (Janzen and Saiedian, 2005). We utilized the Truffle framework containing the Mocha testing library and

[1] https://github.com/ratio91/NFT-event-tickets

Chai assertion library for structural testing, unit tests and functional tests (Truffle, 2019). To ensure the consistency and quality of each public function and all modifiers our prototype contains, we wrote several unit tests. Additionally, we created a series of integration tests to simulate the complete workflow, allowing us to test the formal completeness and functionality of our prototype. In total, we created 33 tests within 289 lines of JavaScript code to ensure that our prototype behaves correctly during state changes. A successful test run with artificial data, simulating the fully automated completion of the entire process as laid out in the previous section, thus serves as proof of construction and shows that our solution works (Nunamaker et al., 1990). Further, the simulation of the realistic test scenario yielded an estimated cost of 5 million gas for the deployment of the system. In addition to running tests and performing simulation, we also used the code linter *Solhint* and fixed all reported issues (Protofire, 2019). To avoid security holes and potential defects in our code, we searched recent literature covering security issues for smart contracts such as Atzei et al. (2017) and Fröwis et al. (2017) and amended our code where necessary (e.g. setting some public functions to private). To allow other researchers or practitioners to verify our prototype and to enhance it further, we open sourced the entire project.

### *Expert Evaluation*

Aside from simulation and testing, we relied on additional sources such as relevant literature and expert interviews to make informed arguments (Hevner et al., 2004). To assess our artifact and discuss different scenarios regarding implications for our prototype and NFTs in general, we selected nine experts with different backgrounds based on their previous knowledge of NFTs and event ticketing as shown in Table 4.

| Id | Short Description | Current Position |
|---|---|---|
| 1 | Blockchain consultant specialized in asset tokenization | Managing Partner, Consulting firm |
| 2 | Subject matter expert in mobile ticket applications | CEO, Ticketing software company |
| 3 | Deep tech analyst specialized in the blockchain industry | Analyst, Venture capital firm |
| 4 | Blockchain researcher specializing in token ecosystems | PhD Candidate, University |
| 5 | IS researcher focused on blockchain-based identity research | Researcher, Research Institute |
| 6 | Behavioral economics researcher with blockchain focus | PhD Candidate, University |
| 7 | Technical advisor specialized in blockchain prototypes | Senior Consultant, Consulting firm |
| 8 | Blockchain programmer specialized in asset tokenization | Developer, Blockchain startup |
| 9 | Venture capital fund manager with a focus on blockchain | MP, Venture capital firm |

**Table 4. Expert Interviews**

We introduced all experts to our research beforehand and followed a semi-structured interview guide (Holstein and Gubrium, 1995). We digitally recorded the interviews and analyzed them afterwards according to scientific standards (Schultze and Avital, 2011). Our interviews consisted of two main parts and typically lasted about 30 minutes. First, we focused on the recommended descriptive evaluation approach of assessing an artifacts efficacy and utility through the creation of illustrative scenarios around it (Hevner et al., 2004; Akoka, Comyn-Wattiau, Prat and Storey, 2017). We discussed the suitability of our prototype regarding our specified design objectives and invited the interview partners to come up with realistic scenarios and explore implications on our prototype. Second, we also asked open questions to allow for an open discussion of the general aspects of NFTs. Exemplary questions were:

- How can the implications NFTs have on the use case discussed be generalized in your opinion?
- What do you see as the main benefits of NFTs?
- In your perspective, what disadvantages does the use of NFTs have?
- What challenges remain and how could they be addressed in the future?

Depending on the technical background of the interviewee, we also included analytic questions regarding the perceived fit of our prototype into existing technical IS architecture (Hevner et al., 2004).

## *Evaluation Results and Discussion*

**DO1 – Digitization**: Our simulation reveals that the whole workflow can be processed without the need for any physical representation of the data. Full digitization is achievable in principle, especially for the process of buying and selling tickets [expert #5]. However, fallback mechanisms are advisable to include less sophisticated users such as generating QR-codes that encode the id of the ticket. The user could then decide whether to print out the ticket or show it digitally on the phone [expert #1].

**DO2 – Secondary Markets:** NFTs enable us to embed logic in digital assets such as event tickets themselves, rather than embedding logic in the applications that control assets. The prototype shows that embedding business rules for transfer on event tickets works and enables event organizers to stay in control of the process, set price limits and charge ticket sellers a defined fee. A hard-coded logic is superior to governance or regulation that requires the monitoring of actual user behavior and enforcement of rules by human actors (Waltl, Sillaber, Gallersdörfer and Matthes, 2019). It is much easier to collect a fee from the seller of a ticket if it is automatically deducted or to prevent transactions altogether, rather than requiring the seller by law to obey certain rules (Davidson, Novak and Potts, 2018). Thus, we consider the prototype as both more effective and more efficient than currently existing ways to control secondary market transactions. The only weakness we discovered is a scenario, where users circumvent the system altogether by transferring the private key of an Ethereum account that owns an event ticket itself, rather than exchanging the ticket within the system [expert #6, #7]. This could be prevented by the implementation of KYC measures, which verify the identity of a user of a blockchain address [expert #6, #7]. KYC itself is a hot topic among practitioners and researchers at the moment and could also be realized using a blockchain-based system (Parra Moyano and Ross, 2017).

**DO3 – Independence:** To become independent of intermediaries, event organizers and event attendees require a system that operates in a trust-free way. Using blockchain technology, users can trust the rules which are enforced automatically and cannot be manipulated (Beck et al., 2016). As every Ethereum node processes and validates transactions independently, the only trust required is in the underlying blockchain protocol (Glaser, 2017). However, trustlessness is not only a property of the platform but also of every individual smart contract (Fröwis and Böhme, 2017). Our interview partners generally agreed that independence from intermediaries can be achieved and the design objective is met. However, several experts highlighted that the most realistic use case for our NFT-based prototype would be the integration with existing platforms to benefit from the aggregation of users. Existing dependencies on intermediaries are replaced with a new dependence on technical intermediaries such as smart contract developers [expert #5].

**DO4 – Security:** Our literature research revealed that security of a blockchain-based system is dependent on the general security of the underlying blockchain protocol and the security of individual smart contracts. The former faces security risks such as a 51% attack, where a single entity holds the majority of computing power (Choi et al., 2016). Operational risks include forks, that can happen if the developer community disagrees over important issues. This can result in several competing versions of the code base and could compromise the integrity of a blockchain protocol (Lindman et al., 2017). The latter faces security risks that origin from coding errors, a fact that we acknowledged at the beginning of our process and tried to mitigate as far as possible. The use of well-audited code from OpenZeppelin as a basis for our implementation is an effective measure to reduce the attack surface of our smart contracts [expert #4]. Despite these measures, it cannot be ruled out that the application is vulnerable. Penetration tests by security professionals would be a valuable contribution (Vacca, 2013). Operational errors, such as the redeployment of new smart contract versions open further possibilities for human error. Yet, a scenario where users are misled to interact with an outdated or even a fraudulent version of the smart contract, instead of the valid one, could be imagined and poses a problem. Additionally, the account security of the event organizer could be compromised in case the private key securing it is obtained by a malicious party [expert #1]. Thus, trust in the security measures taken by the event organizer is critical for the overall security of the system. We tried to limit the potential damage of such a scenario by effectively restricting the options of the owner to change parameters and pause transactions. Ownership of tickets itself would still be protected in such a case, thanks to the use of NFTs, which embed rules to only give current owners certain permission (Entriken et al., 2018). NFTs also help to ensure the integrity as they guarantee uniqueness of tickets by design [expert #4]. The prototype does not provide a high level of privacy for users, as the Ethereum blockchain is public and uses pseudonymous identities. Researchers have shown that with limited effort, privacy based solely on pseudonymity can be overcome (Tschorsch and Scheuermann, 2016). Several interviewed experts indicated potential legal issues as data privacy laws might be breached. Aside from integrity and privacy, availability is a key factor of a secure system (Vacca, 2013). The Ethereum blockchain which is the protocol used as the basis for our prototype ensures virtually no downtime (Vermeulen, Fenwick and Kaal, 2018).

**DO5 – Validation:** Verifying the ownership of tickets worked fine in our simulations. Due to the transparency of all transactions conducted with the smart contract, users are able to verify the correctness of their actions at any time (Beck et al., 2016). The only prerequisites are internet access and the possession of the cryptocurrency Ether, as function calls are not free from transaction costs. If not enough gas is provided, which has to be paid for using the cryptocurrency Ether, interactions with the smart contract will fail (Delmolino et al., 2016). However, as a recent proposal shows, it is also possible to set up a network of smart contracts to pay the gas costs instead of the user (Weiss, Tirosh and Forshtat, 2018). Additionally, the propagation time for the use of access control at the event location of takes time which might not suffice for scenarios where low latency is required (Cai et al., 2018). As reading all ticket permissions directly from the blockchain might not be feasible, caching of data just before the start of an event could be a workaround.

**DO6 – Transparency**: As the transaction data is immutably stored on the blockchain, a record of ticket ownership is maintained. The open nature of the Ethereum blockchain allows anyone to view and thus verify the current owner of a ticket at any given time. However, viewing ownership only returns the Ethereum account or smart contract owning a ticket. Due to the pseudonymous nature of the blockchain, no details on user identity are known, unless effort is taken to uncover the true identity behind the account or perform KYC to identify users beforehand (Cai et al., 2018). To achieve full transparency KYC is necessary as any entity can own multiple Ethereum addresses [expert #3]. Higher transparency would be met with resistance by many event organizers due to fear of uncovering illegal side deals, such as withholding special contingents of tickets not visible for the public that are dealt behind the back for special favors [expert #2].

**DO7 – Automation:** As our simulation successfully showed, the event organizer is free from the need to take any manual action after the initial deployment of the smart contract. However, in case of errors being made in the setup phase, the event organizer can only correct these by sending transactions to the smart contracts which cost transaction fees. Thus, the organizer needs to properly fund the account in advance.

**DO8 – Cost efficiency:** Simulating the deployment of the prototype showed that the expected gas amount required of 5 million gas costs about 0.01 Ether. The corresponding amount in fiat currency such as USD or EUR depends on the current exchange rate, which is highly volatile (Rimba et al., 2018). At the time of our simulation, it corresponded to about 1 USD (EthGasStation, 2019). Rising Ether prices could increase the costs substantially and lower cost efficiency [expert #6]. For event attendees, transaction fees for each interaction with the smart contract are substantially lower. However, despite lower costs, the fact that users are constantly reminded that any interaction with the prototype comes with a small fee might lead some users to prefer a centralized solution, where prices are more hidden instead (Beck et al., 2016).

## *Discussion of General Benefits and Challenges*

Aside from our findings related to the use case of event ticketing, our literature research and expert interviews revealed further benefits and challenges for NFTs in general. We briefly discuss these discoveries here and present potential ways to overcome each of the problems we discovered.

A key benefit of NFTs is **representing uniqueness** better than any blockchain-based instruments before [expert #3]. They can help to make assets programmable and enhance liquidity and security. Even for assets with certain fungible aspects, a better differentiation can be achieved if NFTs are used rather than fungible tokens [expert #3]. Thanks to these benefits, **NFTs enable new use cases** for blockchain technology and have the potential to improve existing blockchain systems by simplifying it [expert #1]. Two main use cases can be distinguished. First, **tokenization of digital goods** is a perfect fit for NFTs as they can guarantee authenticity and uniqueness [expert #4]. Tickets could be considered as a bundle of rights and thus the tokenization of rights in general could be considered a viable use case for blockchain-based systems and specifically NFTs as well [expert #3, #5]. During research of grey literature, we found several use cases that provide further evidence that NFTs are useful such as the enablement of new business models for software licenses and new form of ownership in digital art (0xcert, 2018; Griffin, 2018). Second, NFTs are ideally suited to **represent physical assets** in the digital sphere [expert #4, #7, #9]. A resulting increase in the transparency of ownership benefits regulators [expert #6]. However, to bridge the gap between the physical and the digital world, additional components such as intelligent sensors are necessary [expert #7, #8].

Yet, using **NFTs poses several challenges**. As they are nothing more than a standardized piece of software code executed on a blockchain, they are highly dependent on the properties of the underlying blockchain protocol. As one expert explained, "*anything you can do with NFTs is enabled by Ethereum, and everything you cannot do is not enabled by Ethereum*" [expert #1]. One of the most notable challenges of Ethereum is its **limited scalability** (Eberhardt and Tai, 2018). However, we found that solutions that overcome this challenge already exist, such as using state channels (Coleman et al., 2018). If this issue is resolved, NFTs should be extremely scalable, as tests revealed that a single contract can handle $2^{128}$ NFTs without problems (Entriken et al., 2018). Another challenge is the design dilemma of **privacy** vs. permissionless blockchain (Corten, 2017). Multiple researchers have shown that privacy is not guaranteed as it is possible to make sense out of pseudonymous data on public blockchains, where transparency and public access is a key feature (Tschorsch and Scheuermann, 2016). Yet, development of new promising technologies such as zero-knowledge proofs (ZKP) is ongoing and will solve this issue in the future (Koens, Ramaekers and Van Wijk, 2018). ZKP is a cryptographic method allowing to proof to another party certain properties without revealing them (e.g. proving that you're of a certain age, without revealing your actual age) (Koens et al., 2018). Early proof that privacy is feasible for NFTs has been achieved by a dedicated team of the firm EY, which used ZKPs in combinations with NFTs to facility private equity transactions (Khatri, 2018). Further, NFTs **lack easy accessibility for retail users** as they are a backend component and do not provide a user-friendly interface [expert #1]. The requirement of paying gas for each function call, which is priced in Ether complicates the use of blockchain-based systems even for experienced users (Rimba et al., 2018). Thus, users are required to purchase cryptocurrency upfront to pay transaction fees, even in case the business model would generally not charge the retail users (Cai et al., 2018). However, a recent EIP (Ethereum Improvement Proposal) called "Gas Stations Network", enabling smart contracts to pay the gas costs instead of the user, shows that this problem can be resolved (Weiss et al., 2018). Not only the price of gas fluctuates but also the price of the cryptocurrency Ether is highly volatile (Rimba et al., 2018). This makes it very hard for retail users to calculate costs based on fiat currencies such as USD. A potential way to overcome this challenge is to use decentralized stablecoins such as Dai, that try to resemble the value of fiat currency and thus free users from the currency risk and mental effort of fluctuating exchange rates (Ito and O'Dair, 2019). Another important challenge for the use of blockchain-based systems in general is **limited legal enforceability** (Christidis and Devetsikiotis, 2016). While token owner can rely on authenticity, legal ownership and consumption of the rights represented by NFTs are a different matter [expert #3, #7]. For a blockchain-based system to be truly trustless, legal correctness and legitimacy within the current institutional environment are required (Hawlitschek, Notheisen and Teubner, 2018). Further, as NFTs are a very young phenomenon, people who understand NFTs are very scarce and the language used in the blockchain space is very technical and generally not well understood by the public [expert #1, #5, #9].

During the construction of the artifact, we revealed a typical issue for NFTs regarding the **creation of tokens**. Unlike for fungible tokens, for NFTs it is not possible to create many tokens right away. Minting NFTs one by one is cumbersome and inefficient since it requires lots of computational power and thus high gas costs occur. One solution we found and applied is to create the tokens only when demanded and paid for by buyers. This strategy is called "user-mintable" tokens (Stehlik and Vogelsang, 2018). Another challenge is the two-stepped process of **approving transactions** before the actual transaction can happen (Entriken et al., 2018). While a solution that is commonly used is to transfer NFTs temporarily to a marketplace contract that takes care of the transactions, this approach has some disadvantages. The fact that token ownership is temporarily transferred away from the owner poses a problem for some use cases and security can be negatively affected. What is more, every additional transfer costs gas and reduces efficiency. Further, the nature of smart contracts generally makes it easy to extend the system with new features. However, **upgrading** existing smart contracts bears multiple technical and operational risks and costs money. Relying on development frameworks like OpenZeppelin and Truffle significantly simplifies upgrade procedures and reduces risks.

Summing up, NFTs enable new beneficial ways to digitally represent digital and physical assets. Yet, many challenges remain to be solved. NFTs are based on blockchain technology which is still in its infancy and not yet ready for a mass market of retail users, who demand simplicity, user-friendly interfaces and legal clarity. These demands cannot be solved by NFTs but need to be addressed on the level of the underlying blockchain protocols and legal institutions. Further, public knowledge about NFTs is still scarce. For these challenges, we expect its role to be restricted to a backend component rather than being directly visible for retail users. Nonetheless, we consider NFTs a highly valuable component for blockchain-based systems with the potential to enable many more practical use cases apart from the one discussed in this paper.

## Conclusion

We have investigated NFTs as an emerging phenomenon and evaluated NFTs as a core building block for a blockchain-based event ticketing system. We followed a design science approach based on the guidelines by Hevner et al. (2004) and iteratively developed a prototype. Through the process of designing, building, and evaluating the NFT-based prototype, we were able to generate several relevant findings regarding benefits and challenges of the new token type. We found that NFTs can help to overcome the current weaknesses of existing non-blockchain event ticketing systems, such as susceptibility to fraud, lack of control over secondary market transactions and validation of ownership. Further, our findings indicate that the use of NFTs currently poses several challenges, mostly inherited from the underlying blockchain protocol. Since we have shown that work on solutions to overcome these challenges is currently in progress, we propose further research to re-assess the state of these challenges in the near future.

Before highlighting the contributions of our research, we must consider its limitations. First, by considering a specific use case in detail and following a rigorous research process to draw generalizable implications from it, we may have missed on certain insights that might have been discovered in different use cases. The use case itself is limited to a strongly simplified model of requirements for an event ticketing system and does not capture the role of other stakeholders and related processes in detail. Our architectural choices may narrow down the generalizability further (Koens and Poll, 2018). Second, despite our attempt to address the issues of user experience, legal implications as well as technical and operational risks, we acknowledge its limited role in this study (Governatori et al., 2018). To reveal more insight into user acceptance of a system based on NFTs, we thus suggest complementary studies on other use cases of NFTs, including extensive field experiments with retail users and legal experts as key parts. Therefore, our findings should merely be perceived as a preliminary step towards a better theoretical and practical understanding of NFTs.

Despite these limitations, our research is one of the first scientific attempts to address the questions if NFTs are useful in practice and how they can help to improve existing systems in real-world domains. The valuable insights we generate for practitioners are threefold: First, we highlight the differences between NFTs and fungible tokens and provide best practices for the development and evaluation of systems using NFTs. Second, we demonstrate the usefulness of NFTs for the use case of event tickets and provided proof by construction through a successful implementation of a working prototype (Hevner et al., 2004). Third, we elaborate on the consequences of its use and highlight practical challenges. In addition to these practical insights, we add descriptive knowledge to an emerging field of research where scientific studies are scarce. We extend and complement existing studies in the literature on blockchain technology by adding new best practice approaches on how to build and evaluate a blockchain-based system using DSR (Glaser, 2017). Finally, our research serves as a foundation for future theoretical and practical research on NFTs, enable other researchers to draw on its findings and design principles and lay ground to higher-theory development (Gregor, 2006).

## References

0xcert. (2018). "NFT Spotlight #3 - KnownOrigin, the non-fungible art platform." Retrieved from https://0xcert.org/news/nft-spotlight-3-knownorigin/

Akoka, J., I. Comyn-Wattiau, N. Prat and V. C. Storey. (2017). "Evaluating knowledge types in design science research: An integrated framework." *Lecture Notes in Computer Science*.

Atzei, N., M. Bartoletti and T. Cimoli. (2017). "A Survey of Attacks on Ethereum Smart Contracts (SoK)." In: M. Maffei & M. Ryan (Eds.), *Principles of Security and Trust* (pp. 164–186). Springer.

AutonomousNEXT. (2018). "Crypto Utopia." Retrieved from https://t.co/QsFhfc8MSl

aventus. (2018). *A Blockchain-Based Event Ticketing Protocol*. Retrieved from https://aventus.io/doc/whitepaper.pdf

Avital, M., J. L. King, R. Beck, M. Rossi and R. Teigland. (2016). “Jumping on the Blockchain Bandwagon: Lessons of the Past and Outlook to the Future Panel.” In: *ICIS 2016 Proceedings* (pp. 1–6).

Beck, R. and C. Müller-Bloch. (2017). “Blockchain as Radical Innovation: A Framework for Engaging with Distributed Ledgers as Incumbent Organization.” In: *Proceedings of the 50th Hawaii International Conference on System Sciences (2017)* (pp. 5390–5399).

Beck, R., J. Stenum Czepluch, N. Lollike and S. Malone. (2016). “Blockchain – The Gateway to Trust-Free Cryptographic Transactions.” In: *Twenty-Fourth European Conference on Information Systems (ECIS), İstanbul,Turkey, 2016*. (pp. 1–14). Springer Publishing Company.

Butcher, M. (2018). “What next? Oh yes, turning a luxury car into a non-fungible token.” Retrieved from https://tcrn.ch/2uPJuIf

Buterin, V. (2014). “A next-generation smart contract and decentralized application platform.” Retrieved from http://buyxpr.com/build/pdfs/EthereumWhitePaper.pdf

Cai, W., Z. Wang, J. B. Ernst, Z. Hong, C. Feng and V. C. M. Leung. (2018). “Decentralized Applications: The Blockchain-Empowered Software System.” *IEEE Access*, *6*, 53019–53033.

Choi, S., K. Smolander, S. Park, J. Yli-Huumo and D. Ko. (2016). “Where Is Current Research on Blockchain Technology?—A Systematic Review.” *PLOS ONE*, *11*(10), 1–27.

Christidis, K. and M. Devetsikiotis. (2016). “Blockchains and Smart Contracts for the Internet of Things.” *IEEE Access*, *4*, 2292–2303.

Coleman, J., L. Horne and L. L. Xuanji. (2018). *Counterfactual: Generalized State Channels*. Retrieved from https://l4.ventures/papers/statechannels.pdf

Consensys. (2019). “Infura - Scalable Blockchain Infrastructure.” Retrieved from https://infura.io/

Corten, P. A. (2017). *Blockchain Technology for Governmental Services : Dilemmas in the Application of Design Principles*.

Courty, P. (2017). *Ticket resale, bots, and the fair price ticketing curse*. Retrieved from http://web.uvic.ca/~pcourty/FPT1005.pdf

Davidson, S., M. Novak and J. Potts. (2018). *The Cost of Trust: A Pilot Study*. Retrieved from https://ssrn.com/abstract=3218761

Delmolino, K., M. Arnett, A. E. Kosba, A. Miller and E. Shi. (2016). “Step by Step Towards Creating a Safe Smart Contract: Lessons and Insights from a Cryptocurrency Lab.” In: J. Clark, S. Meiklejohn, P. Y. A. Ryan, D. S. Wallach, M. Brenner, & K. Rohloff (Eds.), *Financial Cryptography and Data Security, Christ Church, Barbados, February 26, 2016* (Vol. 9604, pp. 79–94). Springer.

Eberhardt, J. and S. Tai. (2018). *ZoKrates-Scalable Privacy-Preserving Off-Chain Computations*. Retrieved from https://github.com/JacobEberhardt/ZoKrates

Entriken, W., D. Shirley, J. Evans and N. Sachs. (2018). “ERC-721 Non-Fungible Token Standard.” Retrieved from https://eips.ethereum.org/EIPS/eip-721

Ethereum Foundation. (2018). “Ethereum Improvement Proposals.” Retrieved from https://eips.ethereum.org/

Etherscan. (2018). “Token Tracker.” Retrieved from https://etherscan.io/tokens

EthGasStation. (2019). “ETH Gas Station.” Retrieved from https://ethgasstation.info/calculatorTxV.php

Fenech, G. (2018). “Unlocking a $200 Billion Dollar Collectibles Market on the Blockchain.” Retrieved from https://www.forbes.com/sites/geraldfenech/2018/11/08/unlocking-a-200-billion-dollar-collectibles-market-on-the-blockchain/#4e2a60cf5554

Fridgen, G., F. Regner, A. Schweizer and N. Urbach. (2018). “Don’t Slip on the Initial Coin Offering (ICO) - A Taxonomy for a Blockchain-enabled Form of Crowdfunding.” In: *ECIS 2018*.

Fröwis, M. and R. Böhme. (2017). “In Code We Trust?” In: J. Garcia-Alfaro, G. Navarro-Arribas, H. Hartenstein, & J. Herrera-Joancomartí (Eds.), *Data Privacy Management, Cryptocurrencies and Blockchain Technology* (pp. 357–372). Cham: Springer International Publishing.

Fujimura, K., H. Kuno, M. Terada, K. Matsuyama, Y. Mizuno and J. Sekine. (1999). “Digital-ticket-controlled Digital Ticket Circulation.” In: *Proceedings of the 8th Conference on USENIX Security Symposium - Volume 8* (p. 18). Berkeley, CA, USA: USENIX Association.

GET. (2017). *Guaranteed Entrance Token - Smart Event Ticketing Protocol*. Retrieved from https://get-protocol.io/files/GET-Whitepaper-GUTS-Tickets-latest.pdf

Glaser, F. (2017). “Pervasive Decentralisation of Digital Infrastructures: A Framework for Blockchain enabled System and Use Case Analysis.” In: *50th Hawaii International Conference on System Sciences (HICSS-50), Waikoloa Village, Hawaii, January 4 - 7, 2017* (pp. 1543–1552).

Governatori, G., F. Idelberger, Z. Milosevic, R. Riveret, G. Sartor and X. Xu. (2018). “On legal contracts, imperative and declarative smart contracts, and blockchain systems.” *AI and Law*, *26*(4), 377–409.

Gregor, S. (2006). "The Nature of Theory in Information Systems." *MIS Quaterly*, *30*(3), 611–642.

Gregor, S. and A. R. Hevner. (2013). "Positioning and presenting design science research for maximum impact." *MIS Quaterly*, *37*(2), 337–355.

Griffin, J. (2018). "Software licences as non-fungible tokens." Retrieved from https://medium.com/collabs-io/software-licences-as-non-fungible-tokens-1f0635913e41

Hawlitschek, F., B. Notheisen and T. Teubner. (2018). "The limits of trust-free systems: A literature review on blockchain technology and trust in the sharing economy." *Electronic Commerce Research and Applications*, *29*, 50–63.

Hevner, A. R. (2007). "A three cycle view of design science research." *Scandinavian Journal of Information Systems.*, *19*(2), 87–92.

Hevner, A. R., S. T. March, J. Park and S. Ram. (2004). "Design Science in Information Systems Research." *MIS Quarterly*, *28*(1), 75–105.

Holstein, J. A. and J. F. Gubrium. (1995). *The Active Interview*. SAGE Publications.

Ito, K. and M. O'Dair. (2019). "A Critical Examination of the Application of Blockchain Technology to Intellectual Property Management." In: H. Treiblmaier & R. Beck (Eds.), *Business Transformation through Blockchain: Volume II* (pp. 317–335). Cham: Springer International Publishing.

Janzen, D. and H. Saiedian. (2005). "Test-driven development concepts, taxonomy, and future direction." *Computer*, *38*(9), 43–50.

Khatri, Y. (2018). "EY Reveals Zero-Knowledge Proof Privacy Solution for Ethereum." Retrieved from https://www.coindesk.com/ey-reveals-zero-knowledge-proof-privacy-solution-for-ethereum/

Koens, T. and E. Poll. (2018). "What Blockchain Alternative Do You Need? BT - Data Privacy Management, Cryptocurrencies and Blockchain Technology." In: J. Garcia-Alfaro, J. Herrera-Joancomartí, G. Livraga, & R. Rios (Eds.), (pp. 113–129). Cham: Springer International Publishing.

Koens, T., C. Ramaekers and C. Van Wijk. (2018). *Efficient Zero-Knowledge Range Proofs in Ethereum*. Retrieved from https://t.co/RDwESNOvjR?amp=1

Leonhart, M. (2018). "About 12 percent of people buying concert tickets get scammed." Retrieved from https://www.cnbc.com/2018/09/13/about-12-percent-of-people-buying-concert-ticketsget-scammed-.html

Lindman, J., V. K. Tuunainen and M. Rossi. (2017). "Opportunities and Risks of Blockchain Technologies - A Research Agenda." In: *Proceedings of the 50th Hawaii International Conference on System Sciences* (pp. 1533–1542). Waikoloa, United States.

March, S. T. and G. F. Smith. (1995). "Design and natural science research on information technology." *Decision Support Systems*, *15*(4), 251–266.

McMillan, C. (2016). "Secondary ticketing: the problem and possible solutions, explained." Retrieved from https://inews.co.uk/culture/music/secondary-ticketing-problems-solutions/

Merriam-Webster. (2018). "Fungible Synonyms, Fungible Antonyms." Retrieved from https://www.merriam-webster.com/thesaurus/fungible

Morabito, V. (2017). *Business Innovation Through Blockchain*. Springer International Publishing.

Mougayar, W. (2018). "The Blockchain's Magical Million Users Club." Retrieved from http://startupmanagement.org/2018/11/20/the-blockchains-magical-million-users-club/

Muzzy, E. (2018). "CryptoKitties Isn't About the Cats." Retrieved from https://medium.com/@everett.muzzy/cryptokitties-isnt-about-the-cats-aef47bcde92d

Nærland, K., C. Müller-bloch, R. Beck and S. Palmund. (2017). "Blockchain to Rule the Waves - Nascent Design Principles for Reducing Risk and Uncertainty in Decentralized Environments Abstract." In: *Thirty Eighth International Conference on Information Systems, South Korea 2017*.

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Retrieved from https://bitcoin.org/bitcoin.pdf

Notheisen, B., J. B. Cholewa and A. P. Shanmugam. (2017). "Trading Real-World Assets on Blockchain." *Business & Information Systems Engineering*, *59*(6), 425–440.

Nunamaker, J. F., M. Chen and T. D. M. Purdin. (1990). "Systems development in information systems research." *Journal of Management Information Systems*, *6*(4), 89–106.

NZ Herald. (2017). "The great ticket mark-up - how fans are paying through the nose." Retrieved from https://www.nzherald.co.nz/entertainment/news/article.cfm?c_id=1501119&objectid=11833817

OpenSea. (2019). "OpenSea." Retrieved from https://opensea.io/

OpenZeppelin. (2019). "OpenZeppelin." Retrieved from https://openzeppelin.org/

Parra Moyano, J. and O. Ross. (2017). "KYC Optimization Using Distributed Ledger Technology." *Business and Information Systems Engineering*, *59*(6), 411–423.Pichler, D. (2018). *Tokenization: The Shifting Future of Digital Assets*. Retrieved from https://riat.ac.at/pichlerd_tokenization.pdf

Pries-Heje, J., R. L. Baskerville and J. R. Venable. (2008). "Strategies for Design Science Research Evaluation." *European Conference on Information Systems (ECIS 2008)*, Paper 87.

Protofire. (2019). "Solhint - Solidity Linter." Retrieved from https://protofire.github.io/solhint/

Rimba, P., A. B. Tran, I. Weber, M. Staples, A. Ponomarev and X. Xu. (2018). "Quantifying the Cost of Distrust: Comparing Blockchain and Cloud Services for Business Process Execution." *Information Systems Frontiers*, 1–19.

Rohr, J. and A. Wright. (2017). *Blockchain-Based Token Sales, Initial Coin Offerings, and the Democratization of Public Capital Markets* (Cardozo Legal Studies Research Paper No. 527). *SSRN*.

Schultze, U. and M. Avital. (2011). "Designing Interviews to Generate Rich Data for Information Systems Research." *Information and Organization*, *21*(1), 1–16.

Schweizer, A., V. Schlatt, N. Urbach and G. Fridgen. (2017). "Unchaining Social Businesses - Blockchain as the Basic Technology of a Crowdlending Platform." In: *38th ICIS*.

Sillaber, C. and B. Waltl. (2017). "Life Cycle of Smart Contracts in Blockchain Ecosystems." *Datenschutz Und Datensicherheit - DuD*, *41*(8), 497–500.

Sparango, B. (2018). "The Rise of Non-Fungible Token Assets." Retrieved from https://medium.com/coinmonks/the-rise-of-non-fungible-token-assets-7fdb4bbb8ad7

Stehlik, P. and L. Vogelsang. (2018). *Privacy-Enabled NFTs: User-Mintable, Non-Fungible Tokens With Private Off-Chain Data*. Retrieved from https://eips.ethereum.org/EIPS/eip-721

Szabo, N. (1994). "Smart Contracts." Retrieved from https://bit.ly/2rLG2Nr

Tackmann, B. (2017). "Secure event tickets on a blockchain." In: *Lecture Notes in Computer Science* (Vol. 10436 LNCS, pp. 437–444). Springer, Cham.

Tepper, F. (2017). "People have spent over $1M buying virtual cats on the Ethereum blockchain." Retrieved from https://t.co/Ea718is6M5

The Australian Government the Treasury. (2017). *Ticket Reselling in Australia*. Retrieved from www.itsanhonour.gov.au

Tikhomirov, S. (2018). "Ethereum: State of Knowledge and Research Perspectives." In: A. Imine, J. M. Fernandez, J.-Y. Marion, L. Logrippo, & J. Garcia-Alfaro (Eds.), *Foundations and Practice of Security* (pp. 206–221). Cham: Springer International Publishing.

Tomaino, N. (2018). "Digital Collectibles: A New Category of Tokens Emerging." Retrieved from https://thecontrol.co/digital-collectibles-a-new-category-of-tokens-emerging-fb991c1dff6a

Truffle. (2019). "Truffle Suite." Retrieved from https://truffleframework.com/

Tschorsch, F. and B. Scheuermann. (2016). "Bitcoin and beyond: A technical survey on decentralized digital currencies." *IEEE Communications Surveys and Tutorials*, *18*(3), 2084–2123.

Vacca, J. R. (2013). *Computer and information security handbook*. (J. R. Vacca, Ed.) (2nd ed). Waltham, Mass.: Morgan Kaufmann.

Vermeulen, E., M. Fenwick and W. Kaal. (2018). "Why Blockchain will Disrupt Corporate Organizations: What can be Learned from the "Digital Transformation."" *The Journal of the British Blockchain Association*, *1*(2), 91–100.

Vogelsteller, F. (2015). "ERC: Token standard #20." Retrieved from https://github.com/ethereum/EIPs/issues/20

Voshmgir, S. (2018). "Fungible Tokens vs. Non-Fungible Tokens." Retrieved from https://blockchainhub.net/blog/blog/nfts-fungible-tokens-vs-non-fungible-tokens/

Waltl, B., C. Sillaber, U. Gallersdörfer and F. Matthes. (2019). "Blockchains and Smart Contracts: A Threat for the Legal Industry?" In: *Business Transformation through Blockchain: Volume II* (pp. 287–315).

Wang, Y. (2017). *Designing Privacy-Preserving Blockchain Based Accounting Information Systems*. *SSRN Electronic Journal*.

Waterson, M. (2016). *Independent Review of Consumer Protection Measures concerning Online Secondary Ticketing Facilities*. Retrieved from https://bit.ly/2wLvnrB

Weiss, Y., D. Tirosh and A. Forshtat. (2018). "EIP 1613: Gas stations network." Retrieved from https://eips.ethereum.org/EIPS/eip-1613

Wood, G. (2014). "Ethereum: a secure decentralised generalised transaction ledger." *Ethereum Project Yellow Paper*, 1–32.

Wüst, K. and A. Gervais. (2017). "Do you need a Blockchain?" *IACR Cryptology EPrint Archive*, 1–7.

Zohar, A. (2015). "Bitcoin: Under the Hood." *Communications of the ACM*, *58*(9), 104–113.