Non Fungible Tokens as Core Component of Event MarketPlace: Blockchain based application

Siham Lamssaoui [*]

[*]Ibn Tofail University, Faculty of Sciences Kenitra, Morocco

January 2021

We conduct experiment on decentralized applications based blockchain that enable untrusted parties to interact and share goods and services. Unlike traditional systems that relies on central entities that validate, control and manage all system transactions. We aim on this work to present a fully decentralized event market based non fungible tokens for tickets purchasing. Non fungible tokens is a form of unique and indivisible tokens introduced in late 2017, where our event organizers create NFT for a targeted and unique event using ERC721 standard offered by Ethereum ecosystem for representing non-fungible digital assets, where they are conducted to precise the event details that controlled by the only the smart contract, Furthermore, organizers cannot be a trusted entities and so we implement a smart contract that enable event holders to authenticate to the system based on a unique identifier and a generated pair of keys, combined with an incentive system in order to encourage users to act properly.

1 Introduction

Blockchain [6] is breaking down technology, creating radical innovative systems with the potential to change the way we are living and exchanging goods and services. Traditional systems are based central entities that are allowed to manage the entire system which is a point of failure that can be altered hacked any time, However, programmers and researchers sacrified immense energy and time to build secure system based cryptographic methods, authentication restrictions, migrate the data storage to cloud servers, butt still facing many attacks.
Blockchain comes up with a very secure based system enabling different entities to participate to the system without revealing previous transactions details or the ability to alter data into the chain. The robustness of the blockchain remain on the consensus protocol, a well as data storage into the block of the

[*]siham.lamssaoui@uit.ac.ma

chain. with the appearance of cryptocurrencies, the term of tokens appeared as well in the known notion of fungible that represent a digital assets built so that each individual token (or fraction of a token) is equivalent to the next, e.g., fiat money is fungible as $20 notes are interchangeable with all other (real) $20 notes. Similarly, one Bitcoin is equal to one Bitcoin, and it's equal to all other Bitcoins which makes fungibility completely essential to the concept of currency, whether they be crypto or otherwise.
In contrast, non-fungible tokens differ from fungible tokens in two major aspects uniqueness and interchangeable, this new form of token was introduced in late 2017 in form of ERC721. ERC721 is an inheritable Solidity smart contract standard, meaning that developers can easily create new ERC721-compliant contracts by importing it from the OpenZeppelin library.
However, a detailed explanation of NFT technology and its utility is mandatory, first, we describe different NFT characteristics and the differences from Fungible token, Second, a detailed process of designing and simulating an application based NFT, Third, the benefits it brings for both developers and front end users as well as describing some of its advantages and disadvantages and how it affect application domain and financial field and the facilities it brings with.
We respond to the question by developing a new decentralized application based NFT for event tickets issuing where we target athletes, media, photographers, musicians, influencers and so on, in order to bring together event organizers and entire world attendees, allowing organizers get direct profits from the events they organize online, with certain protection for front end users to prevent frauds or attacks that can affect the system trust badly, by the mean of an implement smart contract protocol for event organizers authentication consisting of a user ID and a pair of keys.1

2 Related Works

Tickets are a sort of code demonstrating the legitimate to attend certain event, they come in many form, ranging from physical papers to electronically readable codes embedded in smart cards, Tickets can be sold from the primary market by event organizers or secondary market where the price can be cheated and the event can lost its value and its viability, secondary market sellers cannot be a trusted entities as they can duplicate a bar code that cannot be instantly validated by a buyer wishing to attend the event and so sellers end up with a fake version of ticket which won't allow them to participate on targeted event with the tickets they own.
[7] is a decentralized application based NFT for event tokenization, we commonly share some kind of backend concepts, they designed and implemented a system based NFT to issue tickets for event organizers, with certain methods to manage primary market and secondary market, the secondary market inherent some properties set during the smart contract creation by the event organizers, to answer some real world issues such as purchasing fake tickets, selling tickets with higher prices etc. they interactively involved some experts in the field to

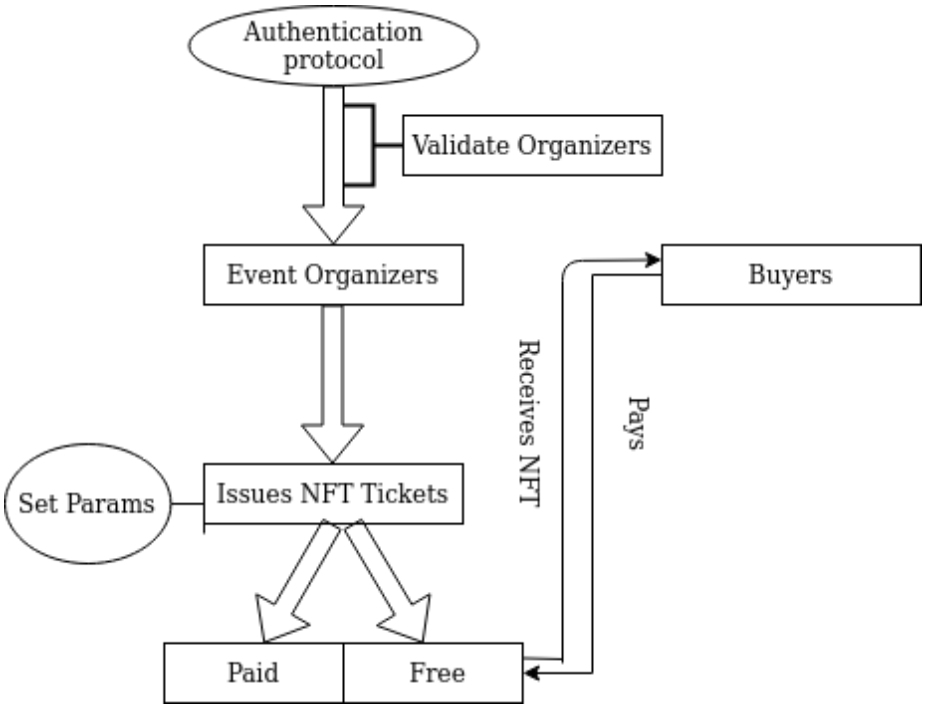

Figure 1: smart contracts architecture

evaluate there system according to scientific standards in order to improve the way it works. They addresses the purpose of NFT in the system showing up some benefits and high financial perspective and security issues it overcome.

[5] Treats the authentication issue and present many authentication ways that been developed during the years where most of the proposed solutions rely on central entities that manage the sensitive share data and face many legislation issues to exchange them or save them, and move to decentralized solution implementing Blockchain identity management and authentication solution based distributed, decentralized and fault- tolerant system by design which decreases the deployment and maintenance cost.

[3] design a attacker model in which attackers can retrieve some/all of the object's secrets such as private keys, starting from this model and developed a bubbles of trust bubbles of trust, which ensures a robust identification and authentication of devices it will be prone to numerous security risks such as information theft, data alteration and identity usurpation. But still on its early stage of development as it does not cover yet real time applications and an initialization phase.

[4] is an authentication protocol based blockchain system, evolving an algorithm based Proof of Importance where nodes are important as their activities on the network. Nodes that are active on the network will be rewarded. Each address is given a trust score, and activities on network gets higher, the more chance a node will be rewarded based on loyalty and effort. as well as a security pattern based VA of keys and identities, distinguishing three basic types of VA: Local VA with additional information, global VA with additional information and global VA without any additional information. The most convenient category is a local VA with additional information where participants had additional knowledge about the other entity such as personal (old) information (name, parents, current/former address, date of birth, etc.) or even an existing side-channel for exchanging information. Therefore, it is relatively easy to construct a personalized challenge-based on shared experiences or information which is (in a best case) only known to both entities.

3 Traditional payments through central entities

Traditional payments been improved by years if not month upon the time, in order to ensure security traceability, transferability between internet users or services. And this progress has involved many utilities and methods to empower and secure online payment. [8] has presented the internet as a marketplace that involve users allover the world to interact between eachother and exchange good that makes it more quick easy and secure because because it carries a risk of non-payment which was overcomed in order to avoid the necessity of

guarantees of credit worthiness for sellers, thus allows every participant to be both buyer and seller of information on the internet, and build a system for cardholders to seperate personal information from the account and email as well as the user interface. [1] presents a new secure electronic payments structure that address both the personal privacy and criminal use of payments that are generally caused in the third party level, and so a cryptography method is developed to bind signature and unable intermediaries to determine time or amount made by a user, ability to stop payments if claimed as stolen, and gives the ability to provide a proof of payment if needed. [2] provides a new way of financial operations allowing holders to safely carry out electronic transactions over an open communication network consisting of information and files, referred as "cyber wallet"

which is an electronic wallet in the form of stored and protected account information that can be hold or owned on a tamper resistant portable electronic storage medium. Cyber Wallet aims to attend some objectives, enabling a merchant to collect account information from remote purchasers through an untrusted public network communication. Furthermore, the transaction using central mean to perform an online payment requires a security generally approved through "Secure Electronic Transaction" protocol published by Visa INternational and MasterCard in 1996. This process perfoms some online check that are time consuming and inefficient when the value of transaction is low. Morever, TRaditional payment systems are mostly relying on acentral entity validation in every transaction which result high fees cut from participants attend to transact to the central entity that represent an entity of trust, personal could be critical information are accessible from the central entity and so internet participant privacy is revealed at least from the central party, which itself represent a point of failure in any time, could be hacked and so result personal inforations revealed to attacker who could use them for some criminal acts and so. Therefore, a Decentralised distributed system is needed to store save personal data without revealing them to the public, furthermore, Personal information is not needed while intract or attending to transact in peer to peer network as digital exchanges works with addresses representing wallets holding funds, this decentralized distributed ledger know as Blockchain and appeared in 2008,brings together network untrusted parties to interact, this interaction is ensured by a consensus protocol to validate transactions. Blockchain ecosystem is based encrypted ledger and merkle Tree wherein every single transaction is encrypted then transmitted which makes it difficult if not impossible for an attacker to reveal transaction data or tamper its content which will result uncoherent hash pointer for the previous block and then a tamper or change is revealed which causes an uncompatibility between other distributed ladgers stored in other peer to peer network partcipants and so cannot be validated and tamper is detected. Blockchain technology changed the way we are working for a central trusted entity to a decentralized trusted system that can be applicable in any field and implement any need through smart contracts, which are self executed program implementing different policies to interact and protect users upon the network or onused decentralized application.

4 NFT Payment Environment overview

In 2013 Vitalik Buterin expanded Nakamoto whitepaper to publish the " A Next Generation Smart Contract and Decentralized Application Platform " presenting new blockchain called Ethereum based turing-complete language, that enable complex code to leverage the computing power and introduce a decentralized world-scale computer.
Ethereum Blockchain ecosystem enable users to create new types of currencies known as "Tokens" built on top of ethereum blockchain that enable interaction between users, instead of creating new blockchain and its cryptocurrency from scratch. Developers have created a service based on a token issued on blockchain and will issue them through a process called " Initial Coin Offering (ICO)" the online sale of the created tokens. A token is not only a representation of digital or crypto asset, it could be rather an Utility Token that allows access to a company's service for instance, Security Token that derives its value from an already-existing asset, that could be a property, financial product, a stock etc, Commodity Token which s the most known token that is used as virtual currency, gold. This tokens are known as fungible tokens that has a value or can be represented as an amount of crypto-asset with common representation represented in Ethereum by ERC20 standard. In another hand Non-Fungible Tokens appread in July 2017, attracted interested percent of developers, users and investors known as Cryptocollectibles with its scarcity and unicity which makes ownership more desirable and it is represented as ERC721 standard **??**, there exists other NFT standard that has been proposed for Ethereum, the ERC821 standard (Ordano, 2018). There are, however, other NFT standards for other blockchains, such as NEO and EOS. NFTS are implemented as an interface and allow intraction with NFT via multiple functions such as: verifying ownership of an ERC721 token, an address can receive ERC721 token only if it has been approved before even initiating the transfer, Approved address of an ERC721 token can be checked as well, last and not least ERC721 token transfer. Non fungible Tokens has been applied and will be applied in many use cases relevant to follows:
- Gaming: in games items can be expressed as a unique set of properties powering up the owner.
- VR Real Estate: its a VR real estate simulations composed with unique components that can be used in both gaming and non-gaming enthusiasts that own those represented assets to speculate on marketplace.
- Collectibles: NFT fits perfectly collectible items such as CryptoKitties allowing users users to buy, breed and exchange digital cats with unique traits randomly generated by the original smart contract.

Fungible Tokens	Non-Fungible Tokens
Interchangeable: A token can be exchanged for any other token of the same type e.g. a dollar bill may be exchanged with another dollar bill with no effect to the holder.	**Not Interchangeable**: A Non-fungible token cannot be replaced with another non-fungible token of the same type e.g. a non-fungible token is akin to a birth certificate it cannot be exchanged with another individual's birth certificate.
Uniform: All tokens of the same type are identical in specification, each token is identical to another	**Unique**: Each token is different from all other tokens bacause of its unicity and scarcity
Divisible: Fungible tokens are divisible into smaller units and it doesn't matter which units one obtains as long as the value is the same e.g. The value remains the same if one holds a single $10billorten1$ bills.	**Non-Divisible**: Non-fungible tokens cannot be divided. The elementary unit is one token and one token only. of the same type.

Our Protocol is based Three main core smart contracts aiming to manage all the tokenization process, starting with a controller contract playing role of a router that link users with authentication contract if first interaction, this contract aims to authenticate users based chosen username for login, it allows users to recover their data if lost or set them if desired as well as drop the account if willing to leave the application. Controller link logged users to main smart contract that handle all the logic of ticketing ecosystem in order to create NFT if event organizer set its parameters and withdraw funds, while attendees can check ownership, a target token state, or buy ticket. 2

5 Pf lost set them if rotocol design

DoToken is new decentralized event ticketing innovative idea bringing together organizers and participants and ease the communication and the marketplace exchanges, based three main core protocols to strength the way they communicate and interfere. An Authentication protocol which map to every new user its login username with an unique address. An NFT smart contract allow only authentified users to interact with it via a controller that manage the transactions flux, enable users to create unique NFT tickets for a specific event. An Incentive Protocol rewarding users based on there good behavior and number of issued transactions, users rated badly and issued fake events to spam users will not be able to use the application and some sanctions will be applied depends

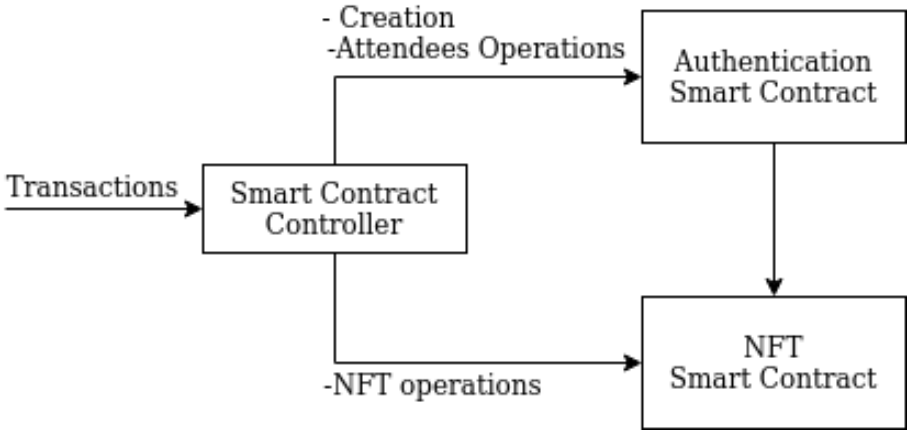

Figure 2: smart contracts architecture

on actions.3

5.1 Authentication

Our decentralized application evolve an authentication protocol to allow users authenticate to system with a user name of there choose and we map a unique address refer to that specific user that will allow him to interact with further app components. we were inspired from EtherAuth authentication protocol that was presented in one of the latest Ethereum hackathons [1], the smart contract create a wallet for the user, with set of events executed when desired or needed. Users are able to set their address and get it back if needed for other transfers using function authAddress with one argument which is the user username login, users can set their recovery address that takes two arguments login and address finally account drop that takes login username as argument delete the account and its recovery address. Authentication protocol is mandatory in a decentralized system to keep track in some way or allow you to have a unique wallet address you can use to interact with and username makes it easy to login into the system which is easy to remember and to write rather then passing full address in every intraction with the system.

5.2 Application smart contract core

Our main application logic is concentrated in this part where event organizers are able to create tickets allowing attendees to participate based non-fungible tokens where a bunch of token properties should be set such as:
- Name: which is a string refering to the token name or event name to makes it

[1] https://www.coinbureau.com/smart-contracts/creating-authentication-mechanism-blockchain/

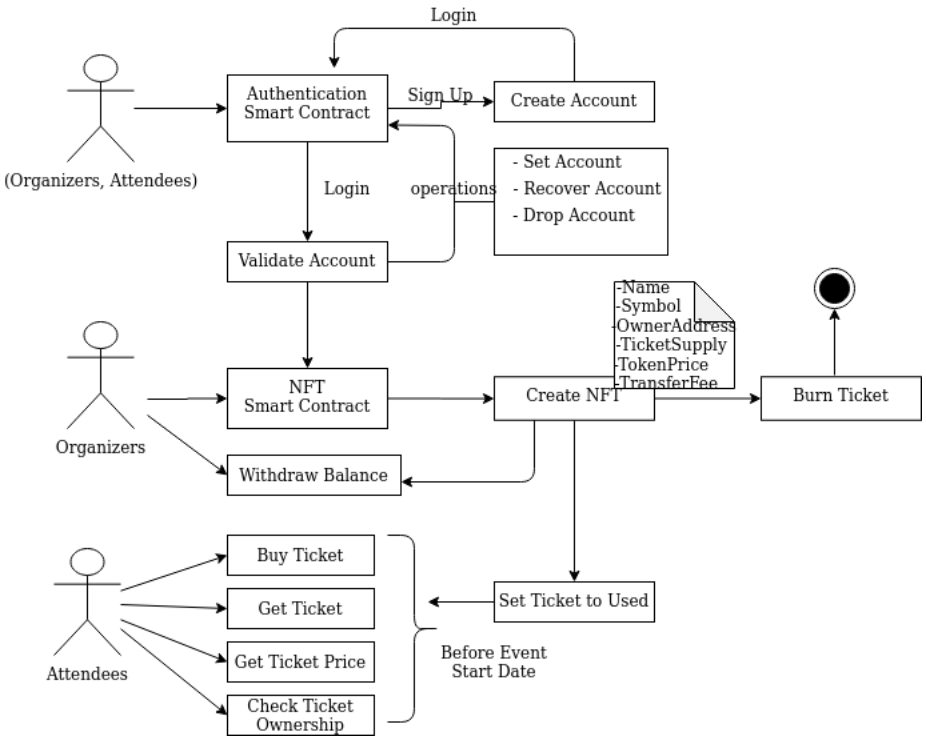

Figure 3: Detailed Protocol Design

more meaningful.
- Symbol: is a string describing the token
- OwnerAddress: is a payable address refering to the user address
- EventStartDate: is a uint64 refering to a specific event starting date
- TokenSupply: is a uint64 refering to number of supplied tickets willing to sold.
- InitialTokenPrice: in a uint256 describing the initial price an event wanna start with in its early time of issuing
- MaxPriceFactor: is uint64 refering to max price the ticket can be sold by, this mitigate from selling tikets with higher price after you been bought it in its early stage of issuing for instance.
- TransferFees: refers to amount of gas to be spend when a a transaction is issued.

Our smart contract contain different component to manage interaction with front end users represented in form of getters and setters, modifiers and events to be invoked when an action is triggered. Token is running in life cycle it gets created first then sold then destroyed, first an initialisation of the token into the structure which generate a unique event identifier, that represents a key to enter/access other following core components:
- GetToken: takes token ID as parameter and returns all relevant information about a specific event Token/Tickcet.
- GetTokenPrice: takes token ID as parameter and returns the price of specific event token which is vital for attendees/users.
- GetTokenTransferFee: takes token ID as parameter and returns the transfer fee of a specific event token/ticket.
- GetTokenStatus: takes token ID as parameter and returns event Ticket/Token status that is a boolean true for used and false for not used.
- CheckTokenOwnership: takes token ID as parameter and returns a boolean True if the transaction sender is the Token owner otherwise a false value is returned.
- setTokenToUsed: takes token ID as parameter and set individual token status to true and can be accessed by only owner.
- setEventStartDate: takes token ID as parameter and set even starting date and can only be modified by event owner.
- isAvailable: is a modifier checking if an event token supply is not yet exceeded.
- isTokenOwner: is a modifier checking if the function caller is the token owner.

Functions are called by users depending on ownership and accessiblity and utility of the returned information.

5.3 Incentive protocol

In decentralized system, third party fees are removed and so users are always winners as they don't spend more the event price in our use case example and transaction fees, and so system is more vulnerable to attackers where the utility

of an authentication protocol that is not enough to encourage users and attract their attention to use our application where the idea of adding an incentive protocol to reward honest and correct users which will encourage them to be a good member of the network, In authentication part a deposit should be provided from event organizers, this deposit value increment in synchronize way with number of token supply in order to prevent spam users to fake events and steal our users and attendees funds, after an event is finished attendees have the right to rank/report it and based on number of bad ranks and reports event organizers can risk to lose its deposit and his account wallet will be deleted and its balance can be used to reward other honest users.
Attendees can also be rewarded based on number of bought tickets and it is good behavior that could be mentioned or ranked from an event organizer.

6 Design Objectives

We aim in this project to overcome some current problems in the event ticketing, that can be manifest as lack of trust related to third party willing to sell tickets to particulars or professional with high percent of risk of purchasing fraudulent or invalid tickets, thus risks to be canceled or counterfeits, Attendees are not able or cannot easily verify the validity of purchased ticket. Furtheremore, tickcets owner could resell their tickets at highest possible price, which lead event organizers to lose control over what we called secondary market, Furthermore, Event organizers does not receive direct funds from their attendees as intermediaries always cut their profit. Thus, our solution is developed to overcome these problems with high efficiency and transparency and less fees based blockchain solution.

- Digitization: Tickets data and information are digitally stored and safely exchanged in a purely digital way.
- fully market control: Event organizers have a fully control over market, by managing the prices caps, the issued transaction and approving tickets buyers, as well as charging transaction fees that makes event organizers profits high among attendees.
- Independence: No centralized broker or authority has the right to sell tickets. Event organizers are the only conducters and managers among business independent of intermediary parties.
- Security: Our protocol ensure a secure environment by enabling accessibility to resources (availability), data authenticity (integrity), and the prevention of access to illegitimate users (privacy).
- Validation: To increase trust in the integrity of the system, we are allowing ticket ownership check in order to ease verification process.

- Transparency: Our protocol offer fully transparency of token/ticket details from the creation to the end of its lifecycle, through implemented methods to check ownership status and Ticket/Token state change.
- Cost Efficiency: The fixed and variable costs of the system should be economical from the event organizers point of view.

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. 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. 4 depicts an UML diagram that outlines the main functions of the prototype.

6.1 Authentication

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 authenticate to the system in order to create a wallet to interact with the smart contract. The sequence of interactions is numbered with 1-3 as depicted in the diagram.

(1) Authentication phase: First event organizers and attendees has to login into the system, then an wallet address is mapping to its choosed username to ease future connections with the system, the users set their login and get a unique address, users are able to set their addresses, recover its data if lost or drop their account from system.
(2) 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, 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. 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.
(3) MarketPLace: After contract deployment, event attendees can buy tickets until the supply limit is reached, by sending a transaction containing funds to the payable function buyToken(). The function first checks if the amount transferred is sufficient and then calls the internal function createToken() 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 checkTokenOwnership(id). The total number of tickets owned can be obtained by calling balanceOf().

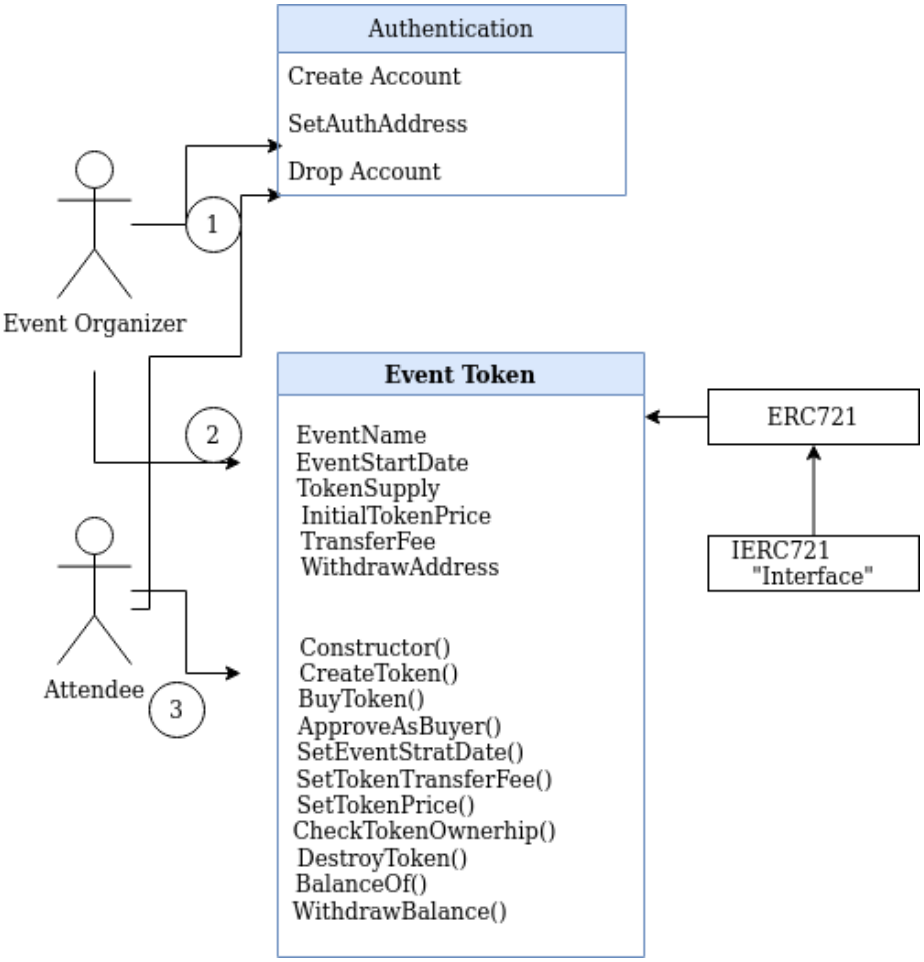

Figure 4: UML Diagram

7 Discussion and Conclusion

Aside from our findings related to the use case of event ticketing, our literature research revealed further benefits and challenges for NFTs in general. A key benefit of NFTs is representing uniqueness better than any blockchain-based instruments before, enable programmable assets 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. 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, 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, NFTs are ideally suited to represent physical assets in the digital sphere. Yet, using NFTs poses several challenges as they are software code executed on a blockchain, they are highly dependent on the properties of the underlying blockchain protocol "anything we can do with NFTs is enabled by the blockchain system, and everything we cannot do is not enabled by the blockchain system".
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 three fold: 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. Third, we elaborate on the consequences of its use and highlight practical challenges. 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 developments.

References

[1] David Chaum. Blind signatures for untraceable payments. In *Advances in cryptology*, pages 199–203. Springer, 1983.

[2] James F Chen and Jieh-Shan Wang. Electronic payment system and method, December 31 1996. US Patent 5,590,197.

[3] Mohamed Tahar Hammi, Badis Hammi, Patrick Bellot, and Ahmed Serhrouchni. Bubbles of trust: A decentralized blockchain-based authentication system for iot. *Computers & Security*, 78:126–142, 2018.

[4] Benjamin Leiding, Clemens H Cap, Thomas Mundt, and Samaneh Rashidibajgan. Authcoin: validation and authentication in decentralized networks. *arXiv preprint arXiv:1609.04955*, 2016.

[5] Shu Yun Lim, Pascal Tankam Fotsing, Abdullah Almasri, Omar Musa, Miss Laiha Mat Kiah, Tan Fong Ang, and Reza Ismail. Blockchain technology the identity management and authentication service disruptor: a survey. *International Journal on Advanced Science, Engineering and Information Technology*, 8(4-2):1735–1745, 2018.

[6] Michael Nofer, Peter Gomber, Oliver Hinz, and Dirk Schiereck. Blockchain. *Business & Information Systems Engineering*, 59(3):183–187, 2017.

[7] Ferdinand Regner, Nils Urbach, and André Schweizer. Nfts in practice–non-fungible tokens as core component of a blockchain-based event ticketing application. 2019.

[8] Lee H Stein, Einar A Stefferud, Nathaniel S Borenstein, and Marshall T Rose. Computerized system for making payments and authenticating transactions over the internet, October 20 1998. US Patent 5,826,241.