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. During covid'19 crisis many sponsors and event organizers suffers from luck of reliable system to manage ticket issuing and pricing in a secure and transparent way, where the need of a fully decentralized event marketPlace. Where the idea of designing and implementing a fully decentralized application based non fungible tokens as a unique and indivisible tokens introduced in late 2017 for tickets purchasing enabling event organizers to create NFT for a specific event using ERC721 standard offered by Ethereum ecosystem representing non-fungible digital assets, where only the token creator own all the rights over the issued tickets, red Moreover, we propose a novel hybrid blockchain architecture that combines permissioned and permissionless blockchain to allow sensitive data to be treated on a permissioned blockchain so that only the event organizers can issue NFTs for events, and no one else. At the same time, we leverage permissionless blockchains to make the upcoming, ongoing, previous events, and payments. Furthermore, using smart contracts deployed on public blockchain, we show how to incentivize truthful behavior among the events.
Our extensive empirical results show that this architecture is efficient in terms of runtime and monetary cost compared to pure public blockchain based Event MarketPlace implementations.

Keywords— Blockchain, NFT, Event MarketPlace, Hybrid, Security

1 Introduction

Blockchain [13] is breaking down technology, creating radical innovative systems with the potential to change the way we are living and exchanging goods and services.

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

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 sacrifice immense energy and time to build secure system based cryptographic methods, authentication restrictions, migrate the data storage to cloud servers, However, many attacks continue to occurs with any new appeared technology.

In the other-hand Blockchain as a decentralized system comes up with a very secure based system enabling different trusted and untrusted 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, as well as data storage into the block of the chain. Moreover, cryptocurrencies defined as virtual/digital money which takes the form of tokens or "coins." known as well as fungible that represent a digital assets built so that each individual token equal to the next, for instance, a 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.

However, there exists another form of tokens known as non-fungible tokens that differ from the fungible ones in two major aspects uniqueness and interchangeable, this 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.

In covid'19 crisis where distanciation is mandatory and vital to keep ourselves and others safe, and so most if not all events and lectures switched from presential as traditional manner to attend/participate in an event, to remotely running lectures, conferences, events etc. Thus, new model of interaction and exchanging funds has to be estabilished, where the need of well designed and implemented architecture based blockchain is needed in order to monetize and organize online events and help sponsors and events hosts receive direct funds and so mitigate the gap between users and technology that will approach technology to users so they get familiar with it and use to exchange.

Our system is a new decentralized application based NFT for event tickets issuing where we are targeting 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 implemented smart contract for event organizers authentication consisting of a user ID and a pair of keys. 1

redIn this work, we try to address some of the challenges and limitations discussed above using a novel solution that combines public and private blockchains to enable privacy-enhancing for NFTs. Our proposed solution uses public blockchain to keep necessary information about attendees and operations are allowed to execute while private blockchain based smart contracts are used to securely issue NFT for a specific event and are pre-approved among group of nodes/participant and finally, public blockchain based smart contracts are used to show up events and punish any party that tries to cheat.

red To our knowledge, this is the first work that combines public and private blockchains to enable privacy-enhancing, Event marketPlace based NFT, The main contributions of this work can be summarized as follows:

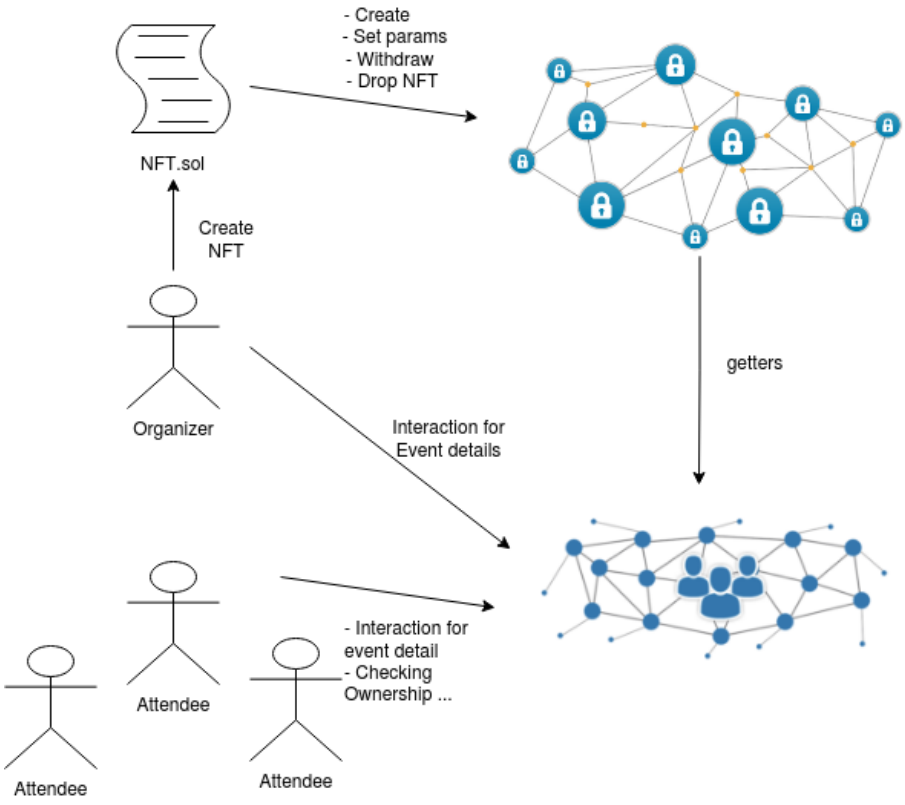

Figure 1: smart contracts architecture

- We propose a novel hybrid blockchain architecture for online Event MarketPlace based NFTs
- We show detailed designing and implmentation model
- We show why NFTs are better solution and why monetizing Online Events is advantageous for both event organizers and participants.
- We empirically show that the proposed hybrid architecture enables more computationally efficient and less expensive.
- We show that the proposed solution only discloses sensitive NFT information (issuing) to the public. This in return reduces the frauds. Furthermore, we show that any cheating party could be monetarily punished using public smart contracts.

Our paper is organized as follows, firstly a paper introduction is presented to describe the paper purpose. Secondly, a detailed explanation of NFT technology and its utility is mandatory, then presenting different NFT characteristics and there difference regarding Fungible tokens, Thirdly, a detailed process of designing, implementing, simulating and testing application based NFT, Fourthly, the benefits it brings for both developers and front end users as well as describing some of its advantages and disad-

vantages and how it affect application domain and financial field and the facilities it brings with. Finally, we conclude our paper and findings with a discussion a conclusion.

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.

[15] 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 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.

[11] 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.

[7] 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.

[10] 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 payments as one of uncounted online services. [16] has presented the internet as a marketplace that involve users all over the world to interact between eachother and exchange good that makes it more fast, easy and secure because of the risk it carries regarding non-payments, which was overcomed 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. [2] 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 cryptographic methods are developed to bind signatures and unable intermediaries to determine time or amount made by a user during a transaction, ability to stop payments if claimed as stolen, with process enabling users to provide a proof of payment if needed.
[3] 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 means to perform an online payment querying high security level generally approved through "Secure Electronic Transaction" protocol published by Visa International and MasterCard in 1996. This process performs some online checks that are time consumers and inefficient when the transaction value is low. However, Traditional payment systems are mostly relying on a central entity validation in every transaction which result high fees cutted from participants attending to transact through central entity as a trusted intermediate, Thus, the personal information/data could be critical as they can be easly 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, and could be hacked and so result personal information revealed to attackers 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.
NB: Personal information is not needed while interacting or attending to transact in peer to peer network as digital exchanges works with addresses representing wallets holding funds. A decentralized distributed ledger known as Blockchain, appeared in 2008, brings together network untrusted parties to interact, while privacy is ensured by the consensus protocol to validate transactions. Blockchain ecosystem is based en-

crypted ledger, where transactions are structed in form of merkle Tree structure that holds all encrypted transactions things that disables attackers to reveal transaction data or tamper its content because it will result uncoherent transaction hash pointers and then a tamper or change is evoked which causes uncompatibility between other distributed ledgers stored in the other nodes participating in the peer to peer network, then tamper is detected and transaction cannot be validated.
Blockchain technology changed the way the application universe works from central trusted entity to decentralized one that can be applicable in any field and implement any need through smart contracts, which are self executed programs able to implement different policies to interact and protect users upon the network.

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 enables users to create new types of currencies known as "Tokens" built on top of ethereum blockchain enabling interaction between participants, instead of creating new blockchain and its cryptocurrency from scratch which could be time consuming and more works to be set, 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 rather be an **Utility Token** allowing access to services, 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 is 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.[14] In another hand Non-Fungible Tokens appread in July 2017, and attract an interesting percent of developers, users and investors to adopt it. NFTs are also known as Cryptocollectibles and there scarcity and unicity which makes ownership more desirable, NFT is represented as ERC721 standard **??** [5], and it is not the only one representation there exists others been proposed by Ethereum, like the ERC821 standard [1], it does not end here, other NFT standards from other blockchains, such as NEO and EOS been introduced and adopted.
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 transferability between users. NFTs start being adopting and applied in many use cases relevant to follows:[12][14] [8][1]
- 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 repre-

[1] https://medium.com/decentraland/the-non-fungibles-revolution-of-2018

sented 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 $10 bill or ten $1 bills.	**Non-Divisible**: Non-fungible tokens cannot be divided. The elementary unit is one token and one token only. of the same type.

The application we are proposing is based private and public blockchains that handle different smart contracts, the private one hold the "NFT" contract that allow only approved event organizers to create unique non fungible tokens for there event, in the other hand, the public blockchain manage the public interaction, starting with a "ProxyController" controller contract playing role of a router that link users with "DoAuth" 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 ticketing operations enabling public users to check target tickets specifications. 2

5 Application design

DoToken is new decentralized event ticketing innovative idea bringing together event organizers and attendees based hybrid blockchain ecsystem, it eases the communication and the marketplace exchanges, based three main core smart contracts to strength the way the communication goes and interfere. Public Blockchain: **Authentication** a smart contract implemented in solidity language through online platform Ethereum propose to its developer Remix [2] to ease the development process that include compiler and deployment feature and many other components, the none authenticated users has to first enter a login that will allow them to interact with the application later, the

[2] https://remix.ethereum.org/

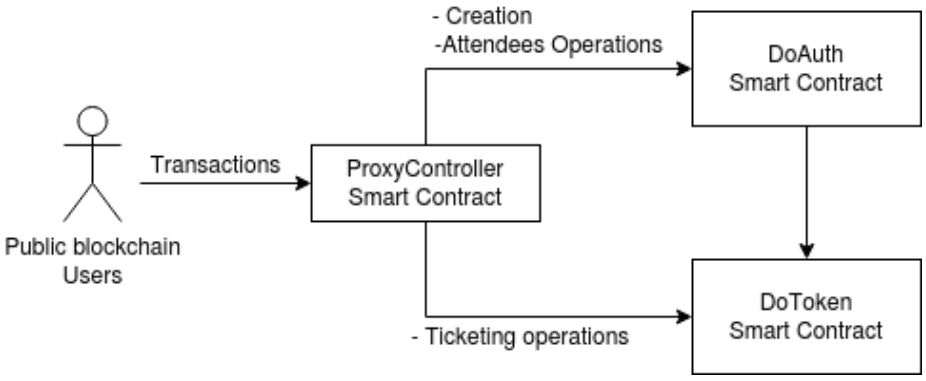

Figure 2: smart contracts architecture

purpose of using a login as a username to authenticate it is its ease to remember then after setting login username a unique address is mapped to its account that allow him to save exchange, withdraw and transfer funds. Authenticated users are able to set there username, address, recover there address if lost, set recovery address, or drop the account if not wishing to interact with application later.
Then a DoToken smart contract allows only authenticated users to interact with it via a controller that manage the transactions flux, these contract allow users event organizers and attendees to get information for a specific event. However, private blockchai manage NFT SC that enable approved organizers to create unique NFT tickets, by setting some necessary parameters that define or hold the ticket details such as name which the event name, symbol, ownerAddress, token supply which is an integer representing the limit number of how many tickets to be sold, event start date is an integer representing when the event is expected to be started, token price is an integer representing the ticket price, finally, transfer fee which is an integer specifying the gas fees the event organizers wanna charge the transactions issuers, with a set of functions using this variables to interact with front users such as setters and getters and core function such as buytoken(), approveasbuyer(), createtoken(). Then, and in order to encourage users to use our application and behave in good manner an Incentive Protocol is set to reward certain users based on there good behavior and number of issued transactions[9], users with low rate and high number of reporters are rejected from the app and there account will be dropped and some sanctions will be applied depends on the action, these mechanism has been adopted by many uses cases in order to reward active members, which in other hand push them to provide there best for the sake of the system and its good process[9] [18][4][17]. 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

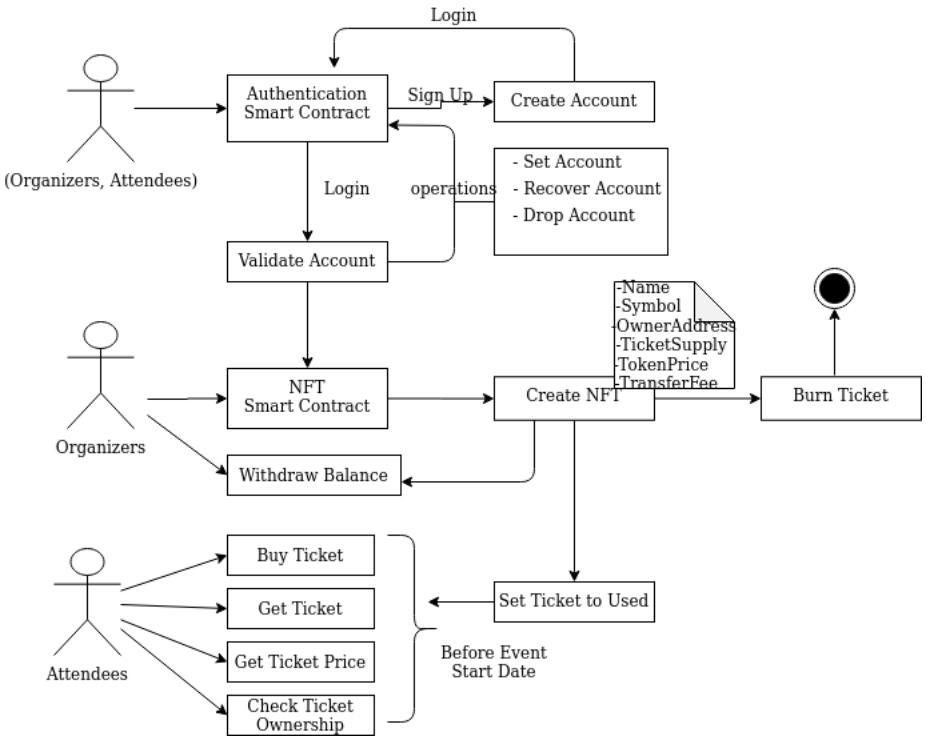

Figure 3: Detailed Protocol Design

the latest Ethereum hackathons [3], 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 NFT smart contract

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 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.
- 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.

The system handle DoToken smart contract contain different component to manage interaction with front end users represented in form of getters to be invoked when an action is triggered such as:
- 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

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

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.

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.
red

5.4 Blockchain based Application

Following the decision model by Wüst and Gervais proposed in (2017), which guide designers, project developers and researchers to decide whether blockchain technology is vital for a specific scenario, and which type of blockchain. It follows a special technique to help users and readers give rise to their need based a well defined and direct questions. One of the major key question that helps us define the blockchain ecosystem is, if all interacting parties can inherently be trusted was clearly answered with no, thus, a blockchain solution is advisable according to the model. Since we positively answered the following-up question if publicly available verification is necessary, the model advised making use of a public permissioned blockchain and so a HYBRID blockchain[6] based system is proposed for security preservation.
The private blockchain is instantiated using NFTs parameters by event organizers permitted to join the network from only a selected group of organizers, which means the used private blockchain is a quasi-permissioned blockchain where there is no trusted third party or membership service provider that allows members to join the network. Once the organizer is approved the access control list is updated and organizers are able to create new unique NFTs for there events setting required parameters for attendees and participants, allowing only the event creator to set parameters if wished after the creation in condition that parameters can only be set before event starting day, attendees are updated and notified with every change.
The attendees and network participants are interacting with the public network, where the private and public blockchains are interlinked with help of a module that opens sockets to both chains The sockets initialize connection between the chains and create

a layer of communication between them.
Since both chains are exclusive, event organizers can hold two seperate accounts to access both chains, while participants are able to hold only one address for one account in the public chain. The attendees address are saved in form of a map linking their wallet address with their login username and whenever a new member joined the chain or quite it, the corresponding map add it or delete it.
Two smart contracts have been implemented to ensure this communication, the NFT contract is deployed on the private blockchain. While the public blockchain hosts two smart contracts namely the DoTokenAuth for authentication and the DoToken for attendees willing to get or set different functionalities or check ticket ownership.

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, tickets 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

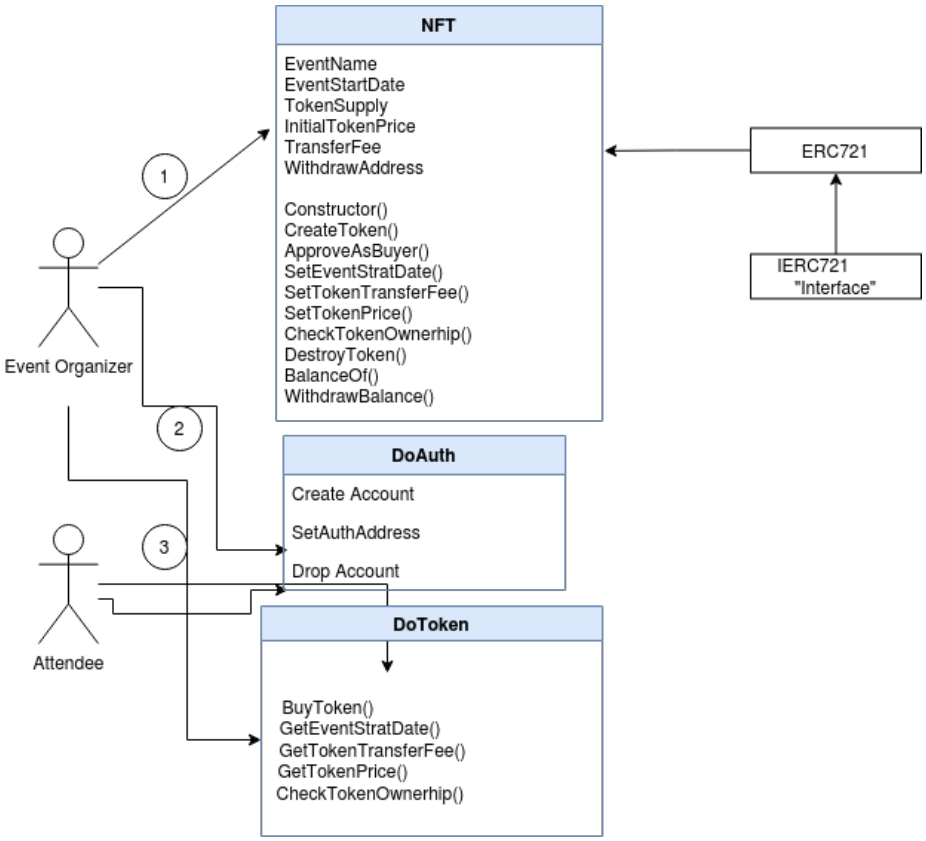

Figure 4: UML Diagram

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().

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] Mustafa Bal and Caitlin Ner. Nftracer: a non-fungible token tracking proof-of-concept using hyperledger fabric. *arXiv preprint arXiv:1905.04795*, 2019.

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

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

[4] Qian Chen, Gautam Srivastava, Reza M Parizi, Moayad Aloqaily, and Ismaeel Al Ridhawi. An incentive-aware blockchain-based solution for internet of fake media things. *Information Processing & Management*, 57(6):102370, 2020.

[5] Sylve Chevet. Blockchain technology and non-fungible tokens: Reshaping value chains in creative industries. *Available at SSRN 3212662*, 2018.

[6] Harsh Desai, Murat Kantarcioglu, and Lalana Kagal. A hybrid blockchain architecture for privacy-enabled and accountable auctions. In *2019 IEEE International Conference on Blockchain (Blockchain)*, pages 34–43. IEEE, 2019.

[7] 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.

[8] HS Jennath, S Adarsh, Nikhil V Chandran, R Ananthan, A Sabir, and S Asharaf. Parkchain: a blockchain powered parking solution for smart cities. *Frontiers in Blockchain*, 2:6, 2019.

[9] Adia Khalid, Muhammad Sohaib Iftikhar, Ahmad Almogren, Rabiya Khalid, Muhammad Khalil Afzal, and Nadeem Javaid. A blockchain based incentive provisioning scheme for traffic event validation and information storage in vanets. *Information Processing & Management*, 58(2):102464, 2021.

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

[11] 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.

[12] N Mofokeng and T Fatima. Future tourism trends: Utilizing non-fungible tokens to aid wildlife conservation. *African Journal of Hospitality, Tourism and Leisure*, 7(4), 2018.

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

[14] Luis Oliveira, Liudmila Zavolokina, Ingrid Bauer, and Gerhard Schwabe. To token or not to token: Tools for understanding blockchain tokens. 2018.

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

[16] 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.

[17] Eric Ke Wang, Zuodong Liang, Chien-Ming Chen, Saru Kumari, and Muhammad Khurram Khan. Porx: A reputation incentive scheme for blockchain consensus of iiot. *Future Generation Computer Systems*, 102:140–151, 2020.

[18] Shichang Xuan, Li Zheng, Ilyong Chung, Wei Wang, Dapeng Man, Xiaojiang Du, Wu Yang, and Mohsen Guizani. An incentive mechanism for data sharing based on blockchain with smart contracts. *Computers & Electrical Engineering*, 83:106587, 2020.