Journal of Advances in Mathematical & Computational Sciences
An International Pan-African Multidisciplinary Journal of the SMART Research Group
International Centre for IT & Development (ICITD) USA
© Creative Research Publishers
Available online at https://www.isteams.net/ mathematics-computationaljournal.info
DOI: dx.doi.org/10.22624/AIMS/MATHS/V10N1P7
CrossREF Member Listing - https://www.crossref.org/06members/50go-live.html

A Formal Verification Model for Security Vulnerability in Non-Fungible Tokens (NFTS) Platform.

[1]Ahubele, B.O. & [2]Okolai, B.D.
[1]Department of Computer Science, University of Port Harcourt, Port Harcourt, Nigeria
[2]Department of Computer Science, Niger Delta University, Bayelsa State, Nigeria.
E-mails: [1]betty_ahubele@uniport.edu.ng; [2]okolaibiriyai@gmail.com
Phones: [1]+2348087473122; [2]+2348038996396.

ABSTRACT

Non-fungible tokens have been a unique transformation in the implementation of the concept of distributed ledger technology in digital assets. NFTs are said to be non-interchangeable, which distinguishes its value from fungible tokens like Bitcoin (Btc). Scammers are utilizing the open source nature of the blockchain to victimize users and steal their NFTs, leaving NFT collectors with infringed artwork. In a bid to eliminate security vulnerability and attack in NFT platform, we implemented a smart contract verification model. Our verification model is a 2-pronged approach that utilized F*, functional programming language. We presented two tools that translated solidity source code and EVM bytecode to solidity* and EVM* respectively. The EVM decompiler analyzes contracts in which the solidity source codes are unavailable as well as low level properties of contracts. The EVM* and Solidity* tools helped to check the equivalence between a solidity program and the bytecode output from the solidity compiler in order to avoid bugs and preserve verified properties at the source level. In this paper, Etherscan token tracker was used to verify and authenticate NFT token before buying or minting such NFT.

Keywords: Non-Fungible Tokens (NFTs), The NFT- marketplace (NFTM), Ethereum

Ahubele, B.O. & Okolai, B.D. (2022): A Formal Verification Model for Security Vulnerability in Non-Fungible Tokens (NFTs) Platform.. Journal of Advances in Mathematical & Computational Sciences. Vol. 9, No. 2. Pp 61-74. DOI: dx.doi.org/10.22624/AIMS/MATHS/V10N1P7
Available online at www.isteams.net/mathematics-computationaljournal.

1. INTRODUCTION

The invention of disruptive technologies and pandemic has broadened digital environments with tremendous transformation in terms of digital investments, digital currencies and intellectual property owners. Crypto currencies have consequently developed into a large sector, resulting in global participation of investors in digital assets and crypto-currencies. In recent years, the attention towards non-fungible token (NFT) have greatly increased stemming from both industrial and scientific communities. Although, digital creators are left with a fiction of their work due to insecurity, ownership etc., but NFTs were designed to fix these issues as they reflect ownership of the digital asset link to a token on the blockchain. The market for NFT is experiencing progressive growth reaching a population of over 340 million dollars of sales in February, 2021, as against 1 million in December, 2020 [6]. Such increased in market sales makes NFT to be highly rated as the future of digital assets by crypto users and developers. Individuals participate in various types of NFT-related trades or games with enthusiasm. Besides games and collectibles, NFTs promotes the development of art, ticketing event, value, IoT and finance. Despite the potential benefits of these non-fungible tokens (NFTs); security becomes a major challenge in the NFT ecosystem as the digital assets were presented as exploitable surface for easy access by an attacker.

Denial-of-Service (DoS) can be used to attack the centralized web applications or off-chain data, resulting in DoS to NFT service [2]. Similarly, an attacker may steal the private key of the user and exploit authentication to transfer the ownership of NFTs when a user interacts to mint or sell NFTs [2]. Since all transactions occur online where information related to each transaction is vulnerable to unauthorized access, privacy and security becomes the most well-known factors of the several use cases of NFTs. Third parties can access blockchain-based web wallets when online since they are vulnerable to scam, outdated security patches, and malware attacks, which cyber hackers can manipulate to their benefit [1]. The attacker can also execute a spoofing attack since he's able to pose as another entity on the system. Therefore, digital collectors and investors with huge amounts of non-fungible tokens are advised to use a hardware wallet in addition to a web wallet. In this paper, we implemented a formal verification model for the non-fungible token smart contract and utilized a Trezor wallet to prevent unauthorized access to the private key.

2. NON-FUNGIBLE TOKENs (NFTs)

Decentralized computing systems and blockchain applications have provided a platform to link real world items to digital records that can prove ownership and trading rights [6]. According to Vitalik Buterin (Ethereum founder), ethereum was invented to extend the usability of blockchain from a mere financial transaction to a platform where other applications can run as smart contracts [8]. Consequently, the fundamental difference between Ethereum and the Bitcoin blockchain network is that an Ethereum (Turing complete programming) facilitates programming on the blockchain and financial transactions while Bitcoin only allow financial transactions on the digital ledger due to its non-turing nature.

Buterin further described smart contracts as "programs which automatically move digital assets according to some predefined set of rules" [9]. In other words, a smart contract can be defined as a contract between two parties that can self-execute and self-enforce lines of program code when contractual agreements are met. Ethereum was the first turing complete and public blockchain whose protocol can allow any user to create and deploy programs on its shared infrastructure. To promote interoperability, the Ethereum community agreed on so-called Ethereum-Requests-for-Comments (ERCs).

The first and well known standard was ERC-20, which satisfies the standard interface for fungible tokens to facilitate Initial Coin Offerings and afford holders with certain access or governance rights. However, with the invention of NFTs as colored coins in 2012 [10], a new class of token was introduced in 2017 with the ERC-721 standard for NFTs. Non-Fungible Tokens (NFTs) can arguably be construed as an expansion of the underlying principles of scarcity that have been fueling the digital asset economy since inception as well as a key building block in the development of a new blockchain-powered asset class. The main difference between NFTs and crypto-currencies is that crypto-currencies can be exchange for another as they represent equal value while NFTs are unique and un-interchangeable. NFTs are unique [1], un-interchangeable [3] and indivisible blockchain-based tokens initiated in the ERC-721 standard in late 2017 [1]. The ERC-721 clearly demonstrates the global uniqueness and un-interchangeable nature of every existing non-fungible tokens. Nevertheless, NFTs were created to represent authenticity over digital or physical assets [4] and facilitate the tokenization of real word assets such as artwork [5].

2.1 How Non-Fungible Token (NFT) Works

Non-Fungible Token protocols represent an underlying decentralized ledger for tokens and other transactions which makes them un-exchangeable on a Peer-to-Peer network. These tokens can be purchased, traded and sold as digital assets. However, NFTs run on the blockchain to prove the validity of the ownership of an asset and ensure that all transactions between records and the actual object are recorded. Typically, the NFT process is made up of two actors; NFT owner and the NFT buyer. Figure 1 shows the NFT process and functions performed by each actor. An NFT owner converts the raw data into a digital form and stores it on an eternal blockchain-based database. Finally, the owner signs the transaction with a hash and sends the data to a blockchain-based smart contract. The smart contract processes the data, mint or trades it as a transactional data on the blockchain. Once confirmation is approved through a consensus mechanism, the NFT is permanently linked to its unique hash address and broadcasted to other immutable nodes on the blockchain.

2.2 Potentials of Non-Fungible Tokens (NFTs)

NFTs can perform a plethora of diverse roles and functionality in any field. Presently, it has become difficult for artiste and musicians to generate revenue due to its over-saturated market and unfair hierarchical structure within the industry. Streaming as a whole is only profitable to artiste with a large and established audience and most musicians get paid fractions of a token per stream. Although, digital art marks the most common and expensive form of non-fungible token, due to the fact that some of the most valuable NFTs in the space are with an artistic element like Lava Lab's Crypto Punks, Yuga Lab's Bored Yacht Club and American generative artist Tyler Hobbses Fedenas etc. Since 2021, a number of top tier sporting corporations, team and athletes embraced NFT technology, creating unique game moments and immortalize game play on-blockchain.

For instance, Dapper Lab's NBA Top shot, which is an NFT marketplace developed in partnership with the National Basketball Association (NBA); focused on acquitting fans with some iconic moments in basketball. The designers of the NFTs platform generate revenue from the release of new NFT bundles and earn percentages from every peer-to-peer token transaction executed on the blockchain [12]. Every video clip on NBA top shop was represented on Dapper's own proprietary blockchain as an NFT, which can be bought, sold and traded on the Top shot's marketplace. Besides the NBA, other sporting behemoths like MBL and UFC have now embraced NFT.

However, when COVID-19 created restrictions on live sports and entertainment, which resulted in over $18B lost in global sports revenue, digital technologies paved way for fans to connect to their brands, teams, and personalities [23]. Consequently, NFT has emerged as a promising medium for fan engagement, allowing musical artiste to create direct artiste-to-fan interaction as well as benefitting financially from the tokenization of their assets in exchange for real world economic value. Businesses have lost huge sum of money to counterfeit brands, the effects of which can be prevented or completely eliminated with the use of NFTs. Nevertheless, the use of NFTs in fashion is still a relatively new concept. However, after the surge of pandemic which resulted to the closure of physical stores that lasted for about a year, the fashion industry has made attempts to broaden their prospects by venturing into fashion tech.

In the same perspective, companies have started embedding digital NFTs in physical articles to distinguish ownership and retain exclusivity [1]. NFT fashion provides a new revenue stream for designers, designing exclusive bags, video games, couture and more to be sold on NFT marketplaces. Some of the most well-known designers and brands that have ventured into the world of NFTs include Louis Vuitton, Yves Saint Laurent, Alexander Wang and Prada [17]. The gaming community as well as NFTs developers have gained significantly by utilizing NFTs to provide ownership data for in-game objects, fueling in-game eco-systems and other perks to facilitate players [14]. Many standardized game players buy different items and objects for inventory but if the purchased item is no longer needed, the player can recover his/her money by selling off the item. Consequently, players can possibly generate revenue as the value of the said item increases over time [15]. Developers are embracing non-fungible tokens to construct their virtual land ecosystems (Metaverse), thereby opening up a new and innovative market for investors.

2.3 Current Challenges / Attacks on NFTs

As the NFT space exploded with multi-million-dollar sales, cyber criminals and scammers have flocked the markets (OpenSea, Rarible, and Axie), making spontaneous profits and defrauding unsuspected users. Impersonation poses a major challenge where an imposter can tokenize and sell someone's art, keeping the creator unconscious of the fraud. In August 2021, a popular graffiti artist named Banksy was impersonated [16]. The perpetrator created a fake art piece by the artist and sold the NFT for about $336k in an online auction. In [32], a scammer infiltrated the implemented RARIBLE'S verification process and faked an account with the renowned artiste 'Derek Laufman' verified. NFT clones, counterfeit, copycat or parody projects exist to mimic reputable collections by reputable sources. The popular CRYPTOPUNKS have numerous clones where scammers can create illegal customer support channels and social media accounts that pretend to be linked with NFT in order to compromise account to steal user's information [24].

Another challenge is rug pulls, where the owner of an NFT hypes an asset unscrupulously to inflate the value. Considering the incident of the famous rapper 'Lil Uzi Vrt' with over 8m followers who made a tweet on the EXTERNAL BEINGS collection that attracted investment from buyers eventually deleted all his tweets leading to a drop in the token value [14]. Similarly, hackers can hack into account of the user to steal crypto from digital wallets after a user clicked on a fraudulent link to be gifted NFT on Opensea. Scammers also organize NFT airdrops and ask users to transfer Crypto for transaction charges which are usually higher than it actually is. Recently, with the boom and rise in value of NFT, many people uploaded their personal works to the NFT platform for investment and auction.

As a result, cyber-criminals utilize various methods to attack weaknesses in the ecosystem in order to steal other people's NFT assets or cryptocurrencies. Furthermore, the famous NFT project "Monkey Kingdom" was hacked in the instant messaging platform (Discord) in late December 2021 [18]. The hacker posed himself as the group administrator and sent a fake link where the users ignorantly clicked the link without verifying the URL. The crypto-currency in the crypto wallet worth about 1.3m US Dollars was stolen. In February 2022, a hacker impersonated one of the biggest NFT trading platforms (OpenSea) and launched an attack by sending a malicious link to users, tricking them to sign the problematic smart contract and transfer crypto-assets to the hacker's wallet [19]. Consequently, about 1.7m US Dollars was stolen from affected users. The transparencies of distributed ledgers open up the possibility of launching economic attacks by manipulating the market. Relatively, NFT attacks are classified into Phishing, security vulnerability in the NFT platform and Counterfeit or infringement of NFTs as shown in figure 1.

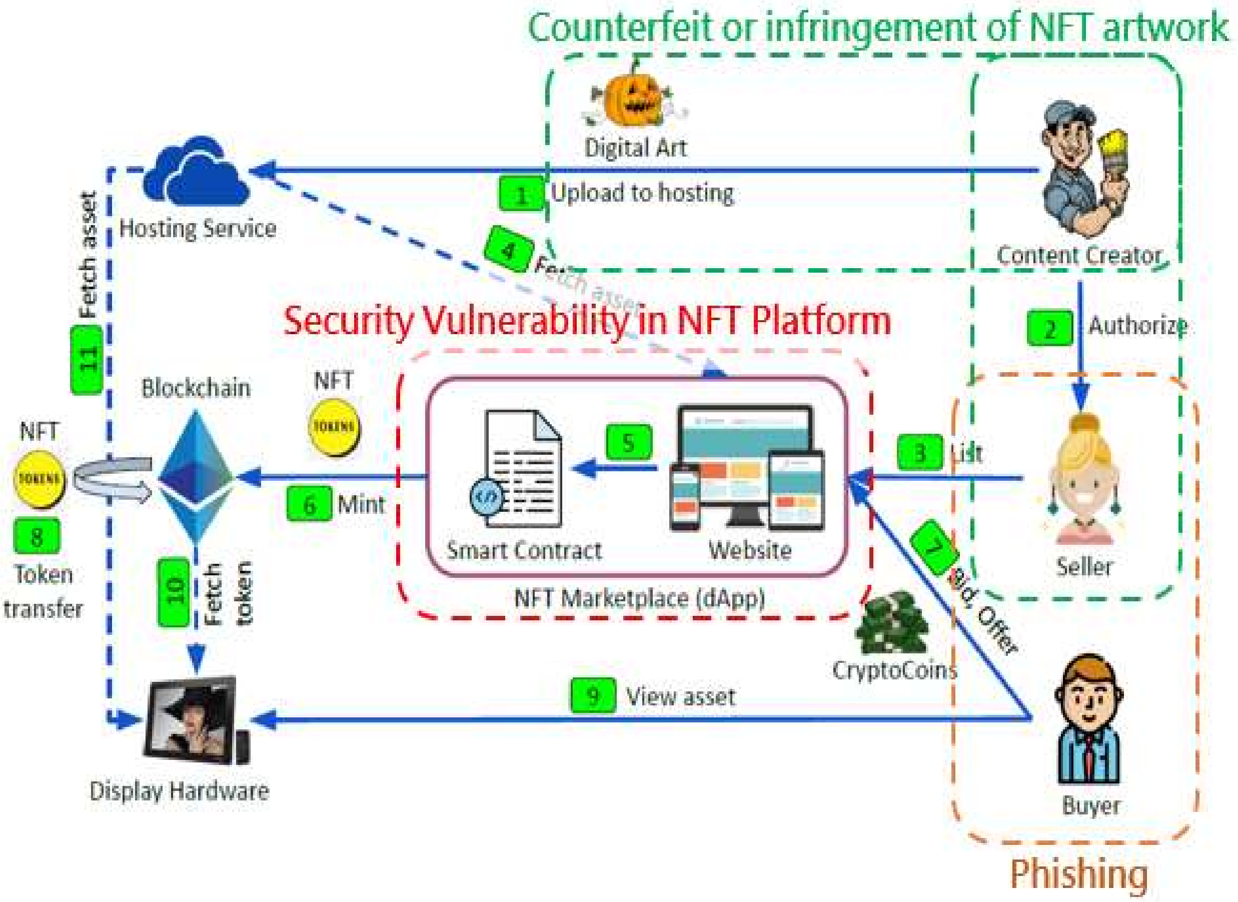


Figure 1: Classes of NFT Attacks [20]

2.4 Related Works

The advancement of distributed ledger technology does not only allow for greater efficiency in the trade of digital assets (NFTs), but also introduces challenges, especially in the area of cyber security. [2] presented an overview, evaluation, opportunities and challenges of NFTs. The NFT ecosystem was explored beginning with an overview of NFT, NFT solutions, components, standard protocols and desirable properties. NFT represents a type of cryptographic token unique asset, either within the real world or in digital context, which function as verifiable proof of authenticity and ownership within a blockchain. In [1], a detailed overview of NFT and its underlying ethereum-based blockchain was carried out. The authors also presented the various platforms for buying and selling NFTs, applications of NFTs in education, fashion, sports and digital art and the key challenges in adaptation of NFT technology from the perspective of security, privacy, environmental impact, ownership, governance, and property rights.

Despite an increasing sales and tremendous growth in trading volumes of NFTs, no much security scrutiny have been given to the emerging technology. However, various academic researches centered on attacks against decentralized finance protocols and automated procedure to detect smart contract vulnerabilities. [25] presented a workflow of the NFT ecosystem and detailed analysis of the top eight(8) marketplaces to discover potential issues which in most cases led to substantial financial loses. The authors automatically analyzed the asset data collected in the examined marketplaces in order to quantify fraudulent trading behaviors exhibited by users under the coverage of ‘anonymity’ [25].

3. EXISTING NFTs ARCHITECTURE

The present NFTs ecosystem comprises actors and the various components they interact with (see figure 2). The core components of the existing NFT ecosystem is broken down into:

Users

The users are categorized into content creator, seller and buyer. The content creator is responsible for creating and uploading digital assets to an external entity for public accessibility. Although, some content creators lack technical capability to convert their artwork into an NFT but they can authorize sellers to mint NFTs and place them on marketplaces. Buyer’s places bid, if the bids are accepted or auction completed, the NFT will be transferred to the buyer as the new owner of the NFT. Users perform activities such as authentication, minting, token listing and token trading by interacting with a Web App.

NFT Marketplaces (NFTM)

NFT Marketplaces (NFTM) is DApps platform where NFTs (digital assets) are traded. This is further broken down into smart contract and user Web App. The user interacts with the web app and sends transactions to the smart contract. NFT contracts consists of two contracts; marketplace contract; which enforces the NFT protocols (On-chain or Off-chain protocols) that interacts with the blockchain and token contracts; which manages NFTs. They allow users to carry out their token related activities.

External Entities

These are off-chain services and devices that provides necessary infrastructure for the NFT ecosystem to function properly. For instance, creators can store digital artwork on web servers or storage services like Amazon S3 or IPFS. When buyers make any NFT, they're exercising their bragging right by displaying the art on a photo book-format or digital NFT photo frames. Websites, photo-frames and NFTMs fetches token from the blockchain and the respective artwork from those services.

3.1 Disadvantages of the Existing Architecture

The following are limitations of the existing system:

i. The smart contract in the NFT Market place lack verification model which is necessary to meet functional requirement and eliminate any loophole which an attacker may explore to his benefits.

ii. The buyer places an order and submits to the NFTM App without proper verification to identify genuine order.

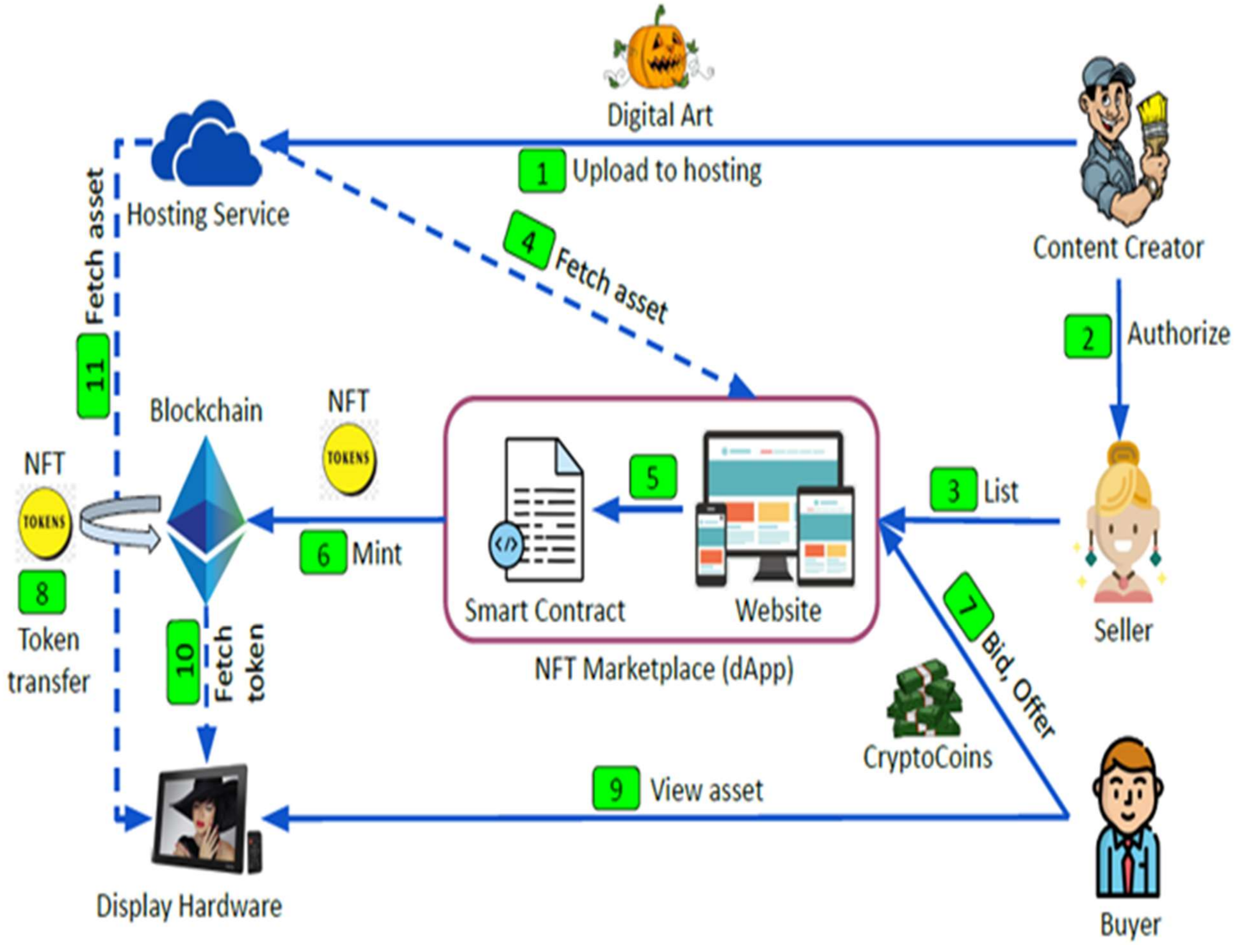


Figure 2: Existing NFT Architecture [1]

3.2 The Proposed NFTs Architecture

In the entire NFTs ecosystem, security concern will continue to thrive as transactions stored on blockchain are transparent, creating room for hackers to exploit vulnerability and transfer token or funds from victimized users' accounts. Crypto-assets and crypto-currencies face vulnerability to cyber-attacks at diverse stages; firstly, NFTs face risks on the platform where the smart contracts run; next, exchanges that facilitate NFTs trading have their vulnerabilities. Finally, cyber-criminals can hack user's wallet where NFTs are stored. Cyber-attacks are targeted against NFT exchanges and wallets. Existing NFT Marketplace, smart contract model lack formal specification which is needed for establishing correctness. In this paper, we implore a security measure to detect vulnerability on NFT Marketplace smart contracts and also utilize a cold wallet (Trezor) where NFTs are stored in order to disconnect the private key from the internet, so hackers cannot access them.

Our smart contract verification model implemented a framework to analyze and verify the smart contract using F* (a functional programming language for program verification). F* makes use of applied, dependent, refinement and monadic effects to generate automated queries, necessary for verifying properties in order to obtain the solidity source code and EVM byte-code of a target smart contract. Although, separate tools were provided for decompiling EVM bytecode (EVM*) and analyzing Solidity* (Solidity source code) but a language-based approach is required for smart contracts verification in order to detect solidity compiler loophole. EVM takes the bytecode of a contract source code, translates it into a representation in F* and then performs a stack analysis by the decompiler to detect stack under/overflows and identify jump destinations in the program. The result is an equivalent F* program which operates on a machine with infinite single-assignment registers. Two tools based on F* were presented:

a. Solidity*: which translates source program to embedded F* program and verifying at the source level for functional correctness (Contract invariant) as well as removing runtime error.
b. EVM*: The EVM decompiler which produces an equivalent F* program that works on a simpler non-stack machine.

The verification framework also checks the correctness of the output of the solidity compiler one step at a time using relational reasoning. Smart contract verification provides the functional correctness and runtime safety of solidity smart contract before deployment on the blockchain. In addition to verification of NFT marketplace smart-contract, our proposed model also provided a framework for verifying the bid order placed by the buyer before including the order on the NFT Marketplace DApp. In this paper, we used etherscan block explorer to track and verify NFT transactions bought or traded. The buyer utilized the Etherscan Token Tracker to verify NFTs before placing a bid order on the website.

3.3 Translation of Solidity Code to F*

A shallow translation of Solidity source code to F* was performed as follows:

1. smart contracts are translated to functional module, F* mod;
2. translating type-to-type declarations: nums to sums of data constructors, structs translated to records, and mappings to F* maps;
3. all contract properties are packaged together within a state record, such that each property determines a reference;

4. translating each method to the function, thereby eliminating de-functionalization since Solidity is 1st- order only;
5. if statements that have a continuation will be re-written only when one branch ends in return or throw (i.e moving the continuation on the other branch), else (proceeding with duplicating the continuation in each branch).
6. to translate assignments, an environment of local, state, and ambient global variable names are kept: local variable declarations and assignments are required to be translated to let bindings; replacing global with library calls and state properties with update on the state type; the built-in method calls like address.send() are replaced by library calls.

1.

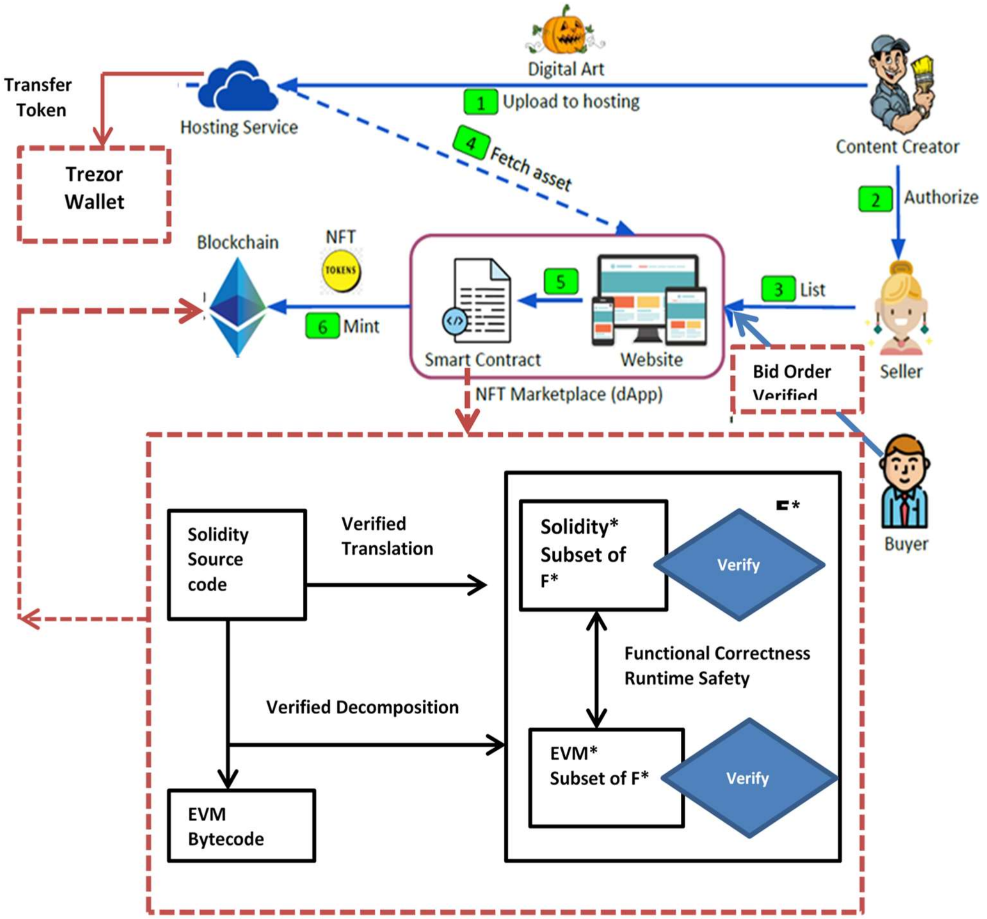


Figure 3: The Proposed Architecture

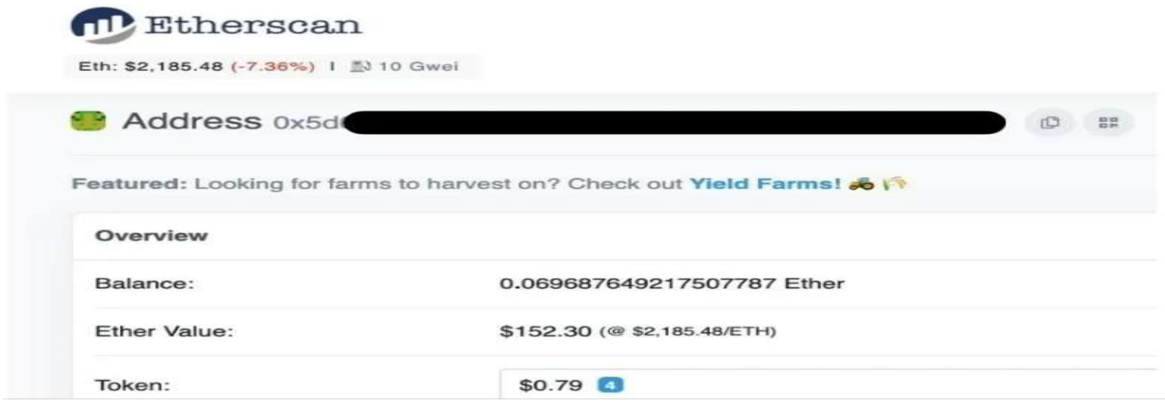
3.4 Advantages Of The Proposed System

NFTs have made it possible for artists and creators to make money from their artwork on the internet without dependence on art galleries or art shows. Hence, the advantages of the added components include:

a) The smart contract verification model using functional programming language (F*), helps to ensure the functional specification of contract correctness and runtime safety of EVM bytecode.
b) Buyers bid order is verified using an Ethereum-based and easy-to-use token tracker to identify genuine order on the NFT. The Etherscan Token Tracker provides support for all ERC-721 tokens.
c) The verified NFT model will allow buyers to know exactly what he/she is buying, who he/she is transacting with, and the time the transaction is completed successfully.
d) Trezor wallet is utilized to protect the user's private key off the chain and guide against financial loss in digital assets.

4. RESULTS AND DISCUSSION

In the past, ethereum-smart-contract had experienced vulnerability which resulted in loss of ethers worth over $50million dollars (DAO attack). However, implementing an error or bug free smart contract can be strenuous due to its complex semantics and transparency. A digital asset contract is not an exception to security vulnerability that could occur on a non-fungible platform, phishing attack and infringement of NFT artwork. Our proposed model developed a framework where the non-fungible contract source code and EVM byte-code are translated to equivalent codes (Solidity* and EVM*) using functional programming language (F*). Also, before an order is placed for a particular NFT, the user is expected to login to "Etherscan.io" with his wallet address on the search bar. Then select the tokens to be verified (Figure 4a). To check a specific NFT's transaction data, a drop-down arrow on the blockchain explorer page is selected and the token transactions viewed. This will display a historical list of transaction for the specific token type viewable by the user in its wallet (Figure 4b).



Etherscan

Eth: $2,185.48 (-7.36%) | 10 Gwei

Address 0x5d[redacted]

Featured: Looking for farms to harvest on? Check out Yield Farms!

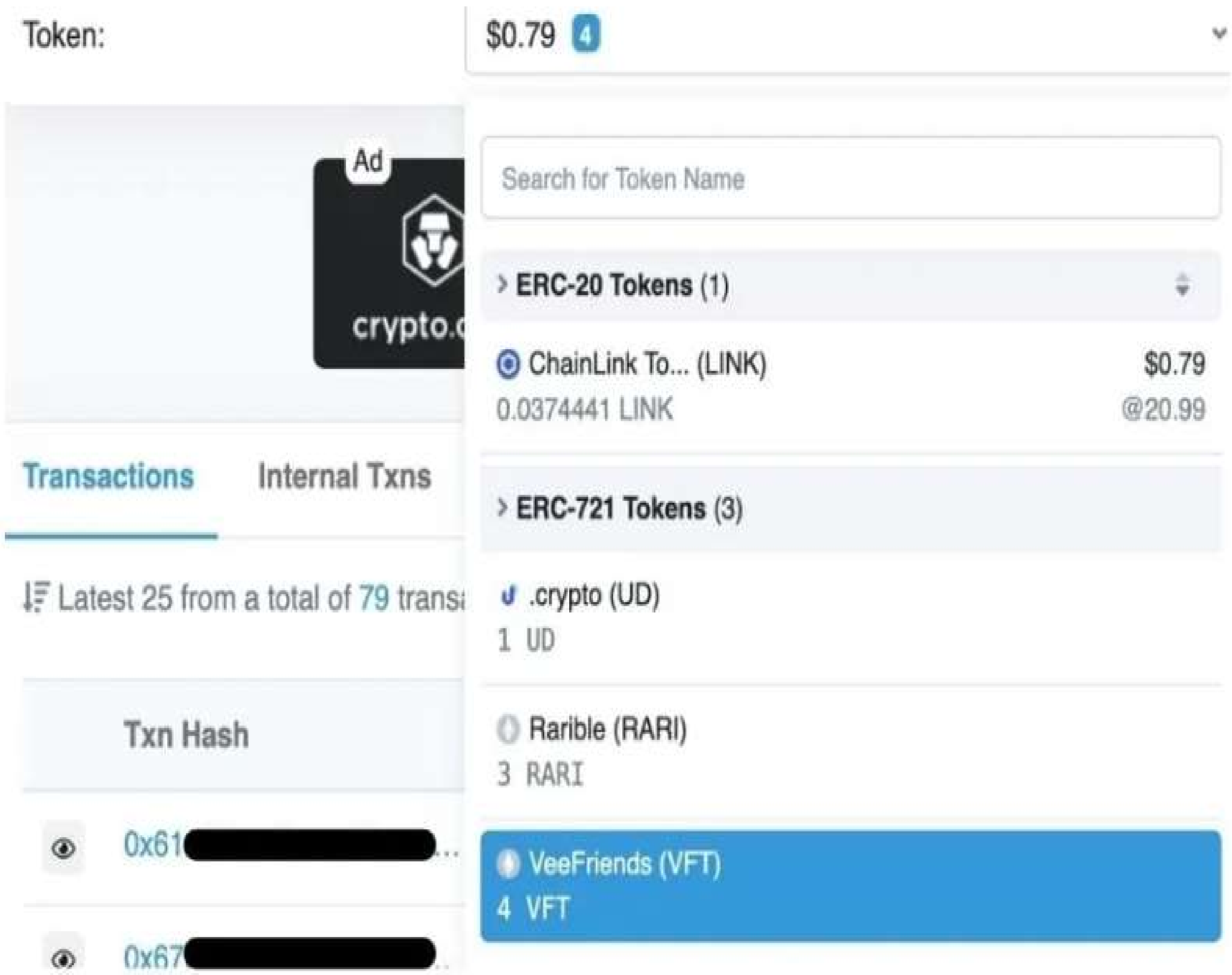
Overview

Balance: 0.069687649217507787 Ether

Ether Value: $152.30 (@ $2,185.48/ETH)

Token: $0.79 4

Figure 4a: NFT Verification model



Token: $0.79 4

Search for Token Name

› ERC-20 Tokens (1)

ChainLink To... (LINK) $0.79
0.0374441 LINK @20.99

› ERC-721 Tokens (3)

.crypto (UD)
1 UD

Rarible (RARI)
3 RARI

VeeFriends (VFT)
4 VFT

Transactions Internal Txns

Latest 25 from a total of 79 transa

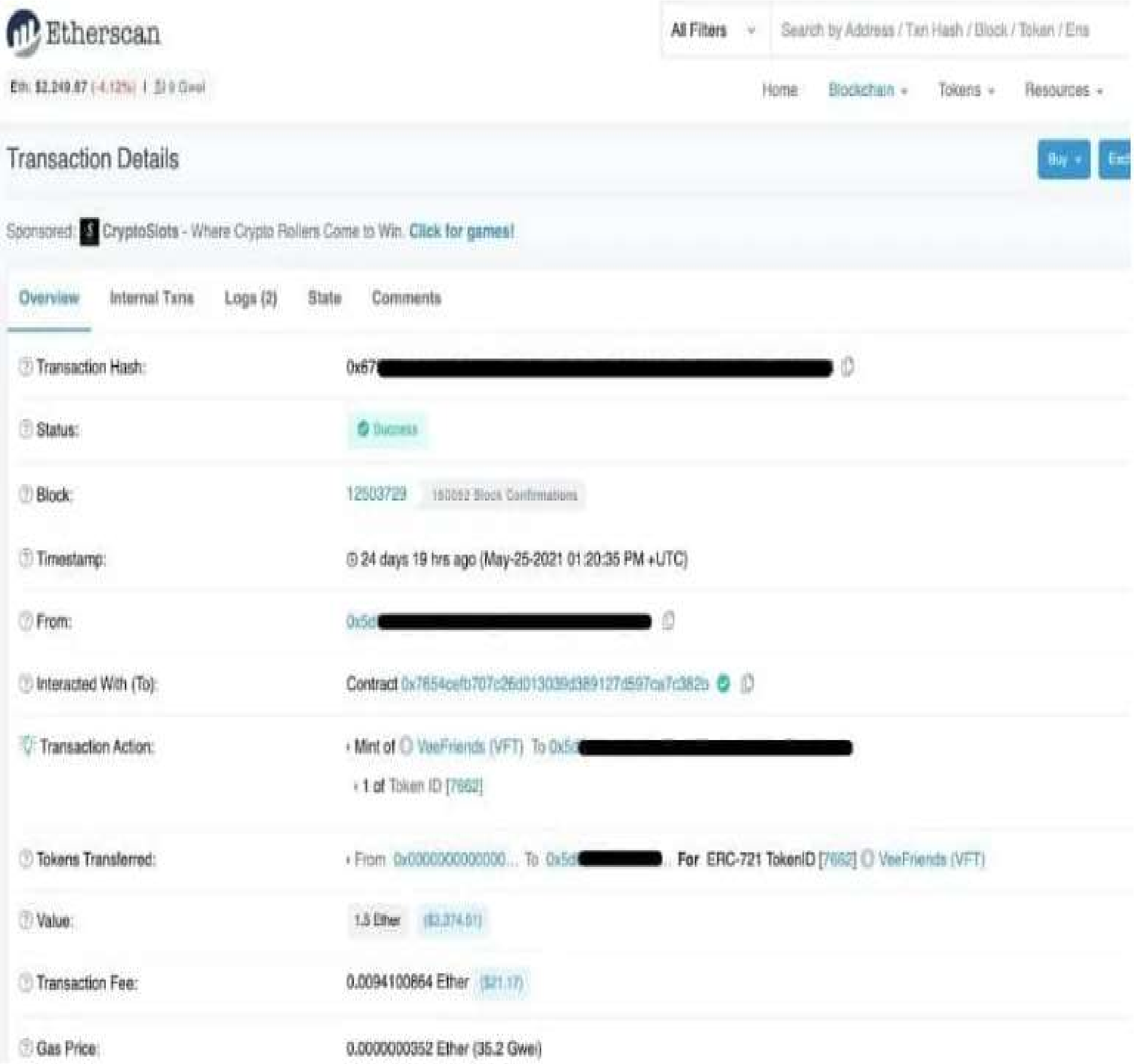
Txn Hash

0x61[redacted]...

0x67[redacted]...

Figure 4b: Tracking Pax Dollar NFT using Etherscan

Multiple transactions are displayed to choose from depending on the user's available token balance. The user can select the Txn Hash to view the exact details of a specific transaction. After the user has selected the NFT transaction to verify, a page is displayed which contain details such as Transaction Hash, Status, Block confirmation, Timestamp, Transaction Action, Current and purchase value, Gas fee, Gas cost per transaction, Ether Price, Gas Limit etc. Finally, the user verifies the status and tokens Transferred for a completed transaction and disperse to a proper wallet (Figure 5).



Etherscan

Eth: $2,249.87 (-4.12%) | 9 Gwei

Transaction Details

Transaction Hash: 0x67[redacted]

Status: Success

Block: 12503729 150052 Block Confirmations

Timestamp: 24 days 19 hrs ago (May-25-2021 01:20:35 PM +UTC)

From: 0x5d[redacted]

Interacted With (To): Contract 0x7654cefb707c26d013039d389127d597ca7c382b

Transaction Action: › Mint of VeeFriends (VFT) To 0x5d[redacted]
› 1 of Token ID [7662]

Tokens Transferred: › From 0x0000000000000... To 0x5d[redacted]... For ERC-721 TokenID [7662] VeeFriends (VFT)

Value: 1.5 Ether ($3,374.51)

Transaction Fee: 0.0094100864 Ether ($21.17)

Gas Price: 0.0000000352 Ether (35.2 Gwei)

Figure 5: NFT verified and transferred.

4. CONCLUSION

The NFT market is experiencing spontaneous growth exceeding 23 billion US Dollars in 2021. As at February, 2022, over 38 billion US Dollars NFTs have been recorded both in sales and market value. Consequently, the U.S. multinational investment bank and financial services company estimated that in 2030, the NFT market value could reach 240 billion US Dollars. This accelerated growth in the NFT market value has generated diverse opportunities for investors as well as hackers and cyber-criminals.

As a result, the victims of such acts include content creators or owners, investors in NFT projects, sellers and buyers of NFTs. However, perpetrators use techniques such as hacking, social engineering scams and malware to gain unauthorized access to victims' digital wallets where the NFTs are stored and convince victims to invest in fake schemes in order to divulge sensitive information. Consequently, NFTs are vulnerable to breaches, bugs, attacks, scams, and frauds on the digital assets' platform. Although creators or owners of NFTs can create high-value NFTs but consumers, buyers, and investors must be abreast of a wide variety of crimes and scams taking place in an NFT marketplaces in order to implement adequate security precautions. Proper watch and effective measures must be taken by owners of digital assets that can be minted into NFTs to ensure that their assets are not misapplied. Our proposed model implemented a functional programming language (F*) to detect smart contract vulnerability in NFT platform. The implemented model also expounds the Trezor wallet for digital storage and secure transfer of non-fungible tokens against unauthorized access to private key.

REFERENCES

1. Regner, F, A. Schweizer and N. Urbach. NFTs in practice-Non-fungible tokens as core component of a blockchain-based event tracking application.*40th International Conferenc on Information systems.* Munich, 2019.
2. Wang, Q.,R. Li,. Qi & S. Chen. Non-Fungible Token (NFTs) Overview, Evaluation. https://doi.org/10.48550/arXiv.2105.07447.
3. Ardit, A., O. Garimidi, D. Hirsch nd I. Milionis. An Initial framework for NFT Auction Mechanism design; Impossibility, Results & solutions. COMS 6998-006 Foundations of Blockchains, Columbia University. 1-24. 2020.
4. Entricken, W., D. Shirley, J. Evans & N. Sachs.NFT Standard.2018. https://eips.ethereum.org/EIPS/eips-721
5. Voshmgir, S. Fungible TokensVs NFTs. 2018. https:// https://blockainhub.net/blog/blog/nfts-fungible-tokens-vs-nonfungible-tokens/
6. Cornelius,K. Betraying BC: Accountability, Transparency and Document Standards for Non-FungibleTokens (NFTs). Information 2021. 12,358. https://www.mdpi.com/journal/information.
7. Rafti, P.A.D. NFT Become a copy right solution. *Journal of digital Law & Policy.* 1(2). ISSN 2808-3652.
8. Buterin, V. A Next-Generation Smart Contract and Decentralized Application Platform. Available online: http://buyxpr.com/build/pdfs/EthereumWhitePaper.pdf (accessed on 1 September 2021).
9. Vujicic, D.; Jagodi´c, D.; Randi´c, S. Blockchain technology, bitcoin, and Ethereum: A brief overview. In Proceedings of the 2018. 17th International Symposium on INFOTEH-JAHORINA, INFOTEH 2018—Proceedings, East Sarajevo, Bosnia and Herzegovina, 21–23 March 2018; pp. 1–6.
10. Valeonti, F., Antonis Bikakis, Melissa Terras, Chris Speed, Andrew Hudson-Smith and Konstantinos Chalkias. 2021. Crypto Collectibles, Museum Funding and OpenGLAM: Challenges, Opportunities and the Potential of Non-Fungible Tokens (NFTs). Appl. Sc2021, 11, 9931. https://doi.org/10.3390/app11219931. https://www.mdpi.com/journal/applsci

11. Pinto-Gutiérrez, C., S. Gaitán, D. Jaramillo and S. Velasquez. The NFT Hype: What Draws Attention to Non-Fungible Tokens? Mathematics 2022, 10, 335. https://doi.org/10.3390/math10030335 https://www.mdpi.com/journal/mathematics
12. Rattan, C. NFTs: The Digital Assets Capable of Restructuring Media Industries. April 21, 2021. https://com.miami.edu/wp-content/uploads/2021/06/mma_2021_secondplace.pdf. [https://usa.visa.com/content/dam/VCOM/regional/na/us/Solutions/documents/visa-nft-whitepaper.pdf] .
13. Rehman, W., H. Zainab, J. Imran, N. Z. Bawany. NFTs: Applications and Challenges. Center for Computing Research, Department of Computer Science and Software Engineering, Jinnah University for Women. Conference Paper · December 2021. DOI: 10.1109/ACIT53391.2021.9677260
14. Popescu, A. "Non-Fungible Tokens (NFT) - Innovation Beyond the Craze", in 5th International Conference on Innovation in Business, Economics and Marketing Research, 2021.
15. Goldberg, M., P. Kugler and F. Schär, "The Economics of Blockchain-Based Virtual Worlds: A Hedonic Regression Model for Virtual Land", SSRN Electronic Journal, 2021. Available:10.2139/ssrn.3932189.
16. Fake banksy nft sold through artist's website for £244k. https://www.bbc.com/news/technology-58399338.
17. Gupta, A. From music and art to video games and more—here's our round-up of the top five NFT types. 2021.https://www.jumpstartmag.com/top-5-nft-types-of-2022/
18. MonkeyKingdom. https://www.hkcert.org/blog/what-you-know-about-the-cyber-security-of-nft
19. Phishing attack. https://twitter.com/opensea/status/1495625768713469954
20. HKCERT. What You Know about the Cyber Security of NFT. Release Date: 11 Mar 2022 4443 Views. https://www.hkcert.org/blog/what-you-know-about-the-cyber-security-of-nft.
21. Digital scarcity. https://policyreview.info/glossary/digital-scarcity.
22. Hackers stole nfts from nifty gateway users. https://www.theverge.com/2021/3/15/22331818/nifty-gateway-hack-steal-nfts-credit-card.
23. Nft mania is here, so are the scammers. https://www.theverge.com/2021/3/20/22334527/nft-scams-artists-opensea-rarible-marble-cards-fraud-art.
24. Social engineering nft users through unauthorized support channel. https://www.theverge.com/22683766/nft-scams-theft-social-engineeringopensea-community-recovery.
25. Dipanjan Das, Priyanka Bose, Nicola Ruaro, Christopher Kruegel, and Giovanni Vigna. Understanding Security Issues in the NFT Ecosystem {dipanjan, priyanka, ruaronicola, chris, vigna}@cs.ucsb.edu. University of California, Santa Barbara. 2022