MINISTERUL EDUCAȚIEI, CULTURII ȘI CERCETĂRII AL REPUBLICII MOLDOVA

Universitatea Tehnică a Moldovei

Facultatea Calculatoare Informatică și Microelectronică

Departamentul Ingineria Software și Automatică

Programul de studii: Securitate Informațională

Admis la susținere
Șef departament:
Fiodorov Ion, dr., conf. univ.

_____

„ ___ ” _____ 2022

ANALIZA PROBLEMELOR DE SECURITATE ÎN ECOSISTEMUL NFT

Teză de master

Student: **Agapii Daniela, SI-211M**

Coordonator: **Bulai Rodica, asist. universitar**

Chișinău 2022

ADNOTARE

Prezenta lucrare de master prezintă o cercetare de ansamblu sistematică a modului în care funcționează ecosistemul NFT și indetifică trei actori majori: piețe, entități externe și utilizatori. Efectuarea unei analize aprofundate a primelor 8 piețe (clasate în funcție de volumul tranzacțiilor) pentru descoperirea potențialelor probleme, dintre care multe pot duce la pierderi financiare substanțiale. De asemenea, colectarea unei cantități mari de date despre active și evenimente referitoare la NFT-urile tranzacționate pe piețele examinate. Analizarea automata a acestor date pentru a înțelege modul în care entitățile externe blockchain-ului sunt capabile să interfereze cu piețele NFT, ceea ce duce la consecințe grave și cuantificarea comportamentele de tranzacționare rău intenționate desfășurate de utilizatori sub mantia anonimatului. Analiza soluțiilor existe și propunerea contramăsurilor corespunzătoare problemelor depistate.

Capitolul 1 caracterizează și descrie întreg ecosistemul NFT care se bazeaza pe sistemul Ethereum. Prezentarea Blockchain-ului Ethereum care este un registru public distribuit, în care tranzacțiile sunt extrase în blocuri de către Proof of Work (PoW). În acest ecosistem, un cont este o entitate reprezentată de o adresă care este capabilă să depună tranzacții. Un alt compartiment foarte important care se abordează este descrierea token-urilor și analiza desfășurată a anatomiei ecoistemului NFT. Tot aici se prezintă și componetele tehnice care sunt legate de activitățile token-urilo non-fungibile.

Capitolul 2 descrie probleme ce apar in NFTM (piețele nft). Aici este vorba despre 4 cele mai critice și des întâlnite probleme care necesită o abordare cât mai detaliată din punctul de vedere a tuturor părților participante în ecosistem. Probleme se relatează la autentificarea utilizatorului pentru validarea identității, meetingul de jetoane ce reprezintă verificabilitatea contractelor cu simboluri, lista de jetoane care indica principiul cel mai mic privilegiu și tranzacționarea cu jetoane.

Capitolul 3 Prezintă analiza înșelătoriile, malpraxisurile și problemele de securitate din ecosistemul NFT. În special, investigarea întrebărilor de cercetare legate de cele trei entități identificate în capitolul 2, adică utilizatori, piețe și entități externe. S-a folosit o abordare hibridă (atât calitativă, cât și cantitativă) pentru analiza celor mai populare 8 piețe și vulnerabilitățile lor comune.

Capitolul 4 este capitolul final în care se prezintă analiza comportamentelor frauduleente a utilizatorului atunci când obține acces și privilegii pe una dintre platformele de gestionare, cumpărare și vânzare a nft-urilor. Tot aici se analizează malpraxisurile comerciale și calcularea volumelor relative de tranzacționare de spălare pe diferite piețe, cele mai importante ținte fiind OpenSea și Rarible. Punctul final fiind evaluare securității pe 6 cele mai importante etape.

ANNOTATION

This master's thesis presents a systematic overview of how the NFT ecosystem works and identifies three major actors: markets, external entities and users. Conducting an in-depth analysis of the top 8 markets (ranked by trading volume) to uncover potential problems, many of which can lead to substantial financial losses. Also, collecting a large amount of asset and event data regarding NFTs traded in the examined markets. Automated analysis of this data to understand how entities external to the blockchain are able to interfere with NFT markets, leading to serious consequences, and quantifying malicious trading behaviors carried out by users under the cloak of anonymity. Analysis of existing solutions and the proposal of countermeasures corresponding to the identified problems.

Chapter 1 characterizes and describes the entire NFT ecosystem that is based on the Ethereum system. Introducing the Ethereum Blockchain which is a distributed public ledger where transactions are mined in blocks by Proof of Work (PoW). In this ecosystem, an account is an entity represented by an address that is capable of submitting transactions. Another very important compartment that is addressed is the description of tokens and the unfolding analysis of the anatomy of the NFT ecosystem. The technical components related to non-fungible token-urilo activities are also presented here.

Chapter 2 describes problems that belong to NFTM (nft markets). Here are 4 of my most critical and common problems that require a detailed approach from the point of view of all parties participating in the ecosystem. Issues relate to user authentication for identity validation, the token meeting representing the verifiability of token contracts, the token list indicating the principle of least privilege, and token trading.

Chapter 3 presents the analysis of scams, malpractices and security issues in the NFT ecosystem. In particular, investigating research questions related to the three entities identified in Chapter 2, i.e. users, markets and external entities. A hybrid approach (both qualitative and quantitative) was used to analyze the 8 most popular markets and their common vulnerabilities.

Chapter 4 is the final chapter in which the analysis of the fraudulent behavior of the user when gaining access and privileges on one of the platforms for managing, buying and selling nfts is presented. This is also where trading malpractice is analyzed and the calculation of relative wash trading volumes in different markets, with OpenSea and Rarible being the most important targets. The final point being security assessment on the 6 most important stages.

Cuprins

INTRODUCERE

Jetoanele non-fungibile (NFT) au apărut ca o modalitate de a colecta artă digitală, precum și un vehicul de investiții. În ciuda faptului că au fost popularizate doar recent, piețele NFT au fost martorii mai multor vânzări de active de mare profil (și de mare valoare) și o creștere extraordinară a volumelor de tranzacționare în ultimul an. Din păcate, aceste piețe nu au primit încă mult control de securitate. În schimb, majoritatea cercetărilor academice s-au concentrat asupra atacurilor împotriva protocoalelor de finanțare descentralizată (DeFi) și a tehnicilor automate pentru a detecta vulnerabilitățile contractelor inteligente.

În această lucrare, se prezintă mai întâi o privire de ansamblu sistematică a modului în care funcționează ecosistemul NFT și indetificarea a trei actori majori: piețe, entități externe și utilizatori. Apoi efectuarea unei analize aprofundate a primelor 8 piețe (clasate în funcție de volumul tranzacțiilor) pentru a descoperi potențiale probleme, dintre care multe pot duce la pierderi financiare substanțiale. De asemenea, colectarea unei cantități mari de date despre active și evenimente referitoare la NFT-urile tranzacționate pe piețele examinate. Analizarea automata a acestor date pentru a înțelegerea modul în care entitățile externe blockchain-ului sunt capabile să interfereze cu piețele NFT, ceea ce duce la consecințe grave și cuantificarea comportamentele de tranzacționare rău intenționate desfășurate de utilizatori sub mantia anonimatului.

Această lucrarea mai poate servi și ca un ghid pentru a ajutra NFTM-urile să evite greșelile în timp ce îi face pe utilizatori să conștientizeze pericolului spațiului NFT. În special contribuții cum ar fi:

a) **Anatonia ecosistemului NFT**, sistematizarea ecosistemului NFT, analiza actorilor participanți-piețe, entități externe și utilizatori plus analiza interacțiunilor lor reciproce.
b) **Colectarea cuprinzătoare de date**. Folosirea mai multor surse de date, de exemplu, Blockchain-ul Ethereum, canalele de asistență DISCORD ale NFTM-urilor induviduale, date despre active și evenimentele provenite din dApps NFTM pentru a crea o imagine holistică a modului în care funcționează ecosistemul.
c) **Identificarea neregulilor în NFTM-uri.** Analizând manual datele colectate de la diverse canale de suport discord și interacționarea cu NFTM-uri, astfel s-au identificat defecte în proiectare și implementare care au un impact de securitate, confidențialitate, utilizare sau financiar.
d) **Identificarea problemelor cu entitățile externe**, identificarea entităților externe inafara lanțului conectat la ecosistem și modul în care astfel de entități pot prezenta amenințări pentru utilizatori.
e) **Descoperirea comportamentelor rău intenționate** ale utilizatorilor.

BIBLIOGRAFIE

[1] [citat 13.10.2022]. Disponibil: https://decrypt.co/61963/now-postage-stamps-are-getting-the-nft-treatment.

[2] [citat 13.10.2022]. Disponibil :

//www.prnewswire.com/news-releases/usps-certifies-casemail-as-firstblockchain-generated-epostage-301267842.html.

[3] [citat 13.10.2022]. Disponibil: https://cointelegraph.com/news/you-can-now-buy-gold-backed-nfts-with-the-mining-carbon-footprint-offset.

[4] [citat 14.10.2022]. Disponibil: https://www.blockchainappfactory.com/real-estate-tokenization.

[5] [citat 14.10.2022]. Disponibil: https://www.flipkick.io.

[6] Mengya Zhang, Xiaokuan Zhang, Yinqian Zhang, and Zhiqiang Lin. TXSPECTOR: Uncovering attacks in ethereum from transactions. In 29th USENIX Security symposium (USENIX Security), 2020.

[7] [citat 23.11.2022]. Disponibil: https://dune.xyz/rchen8/opensea.

[8] [citat 23.11.2022]. Disponibil: https://github.com/JohannesBuchner/imagehash.
[9] [citat 27.10.2022]. Disponibil: https://dappradar.com.
[10] [citat 30.10.2022]. Disponibil: https://decrypt.co/62898/most-expensive-nfts-ever-sold.

[11] Neville Grech, Michael Kong, Anton Jurisevic, Lexi Brent, Bernhard Scholz, and Yannis Smaragdakis. Madmax: surviving out-of-gas conditions in ethereum smart contracts. In Proc. International Conference on Object-Oriented Programming, Systems, Languages, and Applications, 2018.

[12] [citat 03.12.2022]. Disponibil: https://www.bbc.com/news/technology-58399338.
[13] [citat 19.11.2022]. Disponibil: http://www.hackerfactor.com/blog/index.php?/archives/432-Looks-Like-It.html.
[14] [citat 21.11.2022]. Disponibil: https://tornado.cash.
[15] [citat 22.11.2022]. Disponibil: https://www.prnewswire.com/news-releases/usps-certifies-casemail-as-firstblockchain-generated-epostage-301267842.html.

[16] Sukrit Kalra, Seep Goel, Mohan Dhawan, and Subodh Sharma. ZEUS: analyzing safety of smart contracts. In Proc. The Network and Distributed System SecuritySymposium, 2018.

[17] Kai Li, Jiaqi Chen, Xianghong Liu, Yuzhe Tang, Xiaofeng Wang, and Xiapu Luo.As strong as its weakest link: How to break blockchain dapps at rpc service. In NDSS, 2021.

[18] Liying Zhou, Kaihua Qin, Antoine Cully, Benjamin Livshits, and Arthur Gervais. On the just-in-time discovery of profit-generating transactions in defi protocols. In IEEE SP, 2021.

[19] Liying Zhou, Kaihua Qin, C. F. Torres, D. Le, and Arthur Gervais. High-frequency trading on decentralized on-chain exchanges. In SP, 2020.

[20] [citat 12.12.2022]. Disponibil: https://github.com/crytic/echidna.
[21] https://decrypt.co/61963/now-postage-stamps-are-getting-the-nft-treatment.
[22] Neil Gandal, JT Hamrick, Tyler Moore, and Tali Oberman. Price manipulation in the bitcoin ecosystem. Journal of Monetary Economics, 95, 01 2018.

[23] Shelly Grossman, Ittai Abraham, Guy Golan-Gueta, Yan Michalevsky, Noam Rinetzky, Mooly Sagiv, and Yoni Zohar. Online detection of effectively callback free objects with applications to smart contracts. In Proc. Symposium on Principles of Programming Languages, 2018.

[24] Loi Luu, Duc-Hiep Chu, Hrishi Olickel, Prateek Saxena, and Aquinas Hobor. Making smart contracts smarter. In Proc. Conference on Computer and Communications.

[25] Kaihua Qin, Liying Zhou, B. Livshits, and Arthur Gervais. Attacking the defi ecosystem with flash loans for fun and profit. In Proc. Financial Cryptography and Data Security, 2021.

[26] Kaihua Qin, Liying Zhou, B. Livshits, and Arthur Gervais. Attacking the defi ecosystem with flash loans for fun and profit. In Proc. Financial Cryptography and Data Security, 2021.

[27] Petar Tsankov, Andrei Marian Dan, Dana Drachsler-Cohen, Arthur Gervais, Florian Bünzli, and Martin T. Vechev. Securify: Practical security analysis of smart contracts. In Proc. Conference on Computer and Communications Security, 2018.

[28] Jiahua Xu and Benjamin Livshits. The anatomy of a cryptocurrency pump-and-dump scheme. In Proc. USENIX Security Symposium, 2019.

[29] Mengya Zhang, Xiaokuan Zhang, Yinqian Zhang, and Zhiqiang Lin. TXSPECTOR: Uncovering attacks in ethereum from transactions. In 29th USENIX Security symposium (USENIX Security), 2020.

[30] Jiahua Xu and Benjamin Livshits. The anatomy of a cryptocurrency pump-and-dump scheme. In Proc. USENIX Security Symposium, 2019.

[31] William Entriken, Dieter Shirley, Jacob Evans, and Nastassia Sachs. Eip-721: Erc-721 non-fungible token standard, ethereum improvement proposals, no. 721.https://eips.ethereum.org/EIPS/eip-721.

[32] Shayan Eskandari, Seyedehmahsa Moosavi, and Jeremy Clark. Sok: Transparent dishonesty: Front-running attacks on blockchain. In Andrea Bracciali, Jeremy Clark, Federico Pintore, Peter B. Rønne, and Massimiliano Sala, editors, Proc. Financial Cryptography and Data Security, 2020.

[33] [citat 26.10.2022]. Disponibil: https://www.cryptokitties.co.
[34] Interplanetary file system (ipfs). https://ipfs.io.
[35] Now postage stamps are getting the nft treatment. [citat 28.11.2022].
Disponibil: https://decrypt.co/61963/now-postage-stamps-are-getting-the-nft-treatment.
[36] Perpetual image hash. [citat 13.12.2022].
Disponibil: http://www.hackerfactor.com/blog/index.php?/archives/432-Looks-Like-It.html .
[37] You can now buy gold-backed nfts with the mining carbon footprint offset. [citat 11.11.2022]. Disponibil: https://cointelegraph.com/news/you-can-now-buy-gold-backed-nfts-with-the-mining-carbon-footprint-offset.
[38] Real estate tokenization. [citat 13.11.2022]. Disponibil: https://www.blockchainappfactory.com/real-estate-tokenization.

[39] Signing and verifying ethereum signatures. [citat 13.11.2022].

Disponibil: https://yos.io/2018/11/16/ethereum-signatures.

[40] Mengya Zhang, Xiaokuan Zhang, Yinqian Zhang, and Zhiqiang Lin. TXSPECTOR: Uncovering attacks in ethereum from transactions. In 29th USENIX Security.

[41] Dune analytics—opensea. [citat 10.12.2022]. Disponibil: https://dune.xyz/rchen8/opensea.

[42] Imagehash. [citat 13.10.2022]. Disponibil: https://github.com/JohannesBuchner/imagehash.

[43] Dappradar. [citat 17.12.2022]. Disponibil: https://dappradar.com.

[44] The 15 most expensive nfts ever sold. [citat 13.10.2022]. Disponibil: https://decrypt.co/62898/most-expensive-nfts-ever-sold.

[45] Neville Grech, Michael Kong, Anton Jurisevic, Lexi Brent, Bernhard Scholz, andYannis Smaragdakis. Madmax: surviving out-of-gas conditions in ethereum smartcontracts. In Proc. International Conference on Object-Oriented Programming,Systems, Languages, and Applications, 2018.

[46] Fake banksy nft sold through artist's website for £244k. [citat 15.10.2022]. Disponibil: https://www.bbc.com/news/technology-58399338.

[47] Perpetual image hash. [citat 18.11.2022]. Disponibil:

http://www.hackerfactor.com/blog/index.php?/archives/432-Looks-Like-It.html.

[48] Tornado cash. [citat 15.11.2022]. Disponibil: https://tornado.cash.

[49] Usps certifies casemail as first blockchain generated epostage. [citat 18.10.2022]. Disponibil: https://www.prnewswire.com/news-releases/usps-certifies-casemail-as-first-blockchain-generated-epostage-301267842.html.

[50] Sukrit Kalra, Seep Goel, Mohan Dhawan, and Subodh Sharma. ZEUS: analyzing safety of smart contracts. In Proc. The Network and Distributed System SecuritySymposium, 2018.

[51] Kai Li, Jiaqi Chen, Xianghong Liu, Yuzhe Tang, Xiaofeng Wang, and Xiapu Luo. As strong as its weakest link: How to break blockchain dapps at rpc service. InNDSS, 2021.

[52] Liying Zhou, Kaihua Qin, Antoine Cully, Benjamin Livshits, and Arthur Gervais. On the just-in-time discovery of profit-generating transactions in defi protocols.In IEEE SP, 2021.

[53] Liying Zhou, Kaihua Qin, C. F. Torres, D. Le, and Arthur Gervais. High-frequency trading on decentralized on-chain exchanges. In SP, 2020.

[54] Echidna. [citat 17.11.2022]. Disponibil: https://github.com/crytic/echidna.

[55] Joel Frank, Cornelius Aschermann, and Thorsten Holz. ETHBMC: A bounded model checker for smart contracts. In 29th USENIX Security Symposium (USENIX Security), 2020.

[56] Neil Gandal, JT Hamrick, Tyler Moore, and Tali Oberman. Price manipulation in the bitcoin ecosystem. Journal of Monetary Economics, 95, 01 2018.

[57] Shelly Grossman, Ittai Abraham, Guy Golan-Gueta, Yan Michalevsky, Noam Rinetzky, Mooly Sagiv, and Yoni Zohar. Online detection of effectively callback free objects with applications to smart contracts. In Proc. Symposium on Principlesof Programming Languages, 2018.

[58] Loi Luu, Duc-Hiep Chu, Hrishi Olickel, Prateek Saxena, and Aquinas Hobor. Mak-ing smart contracts smarter. In Proc. Conference on Computer and Communications Security, 2016.

[59] Kaihua Qin, Liying Zhou, and Arthur Gervais. Quantifying blockchain extractable value: How dark is the forest? ArXiv, abs/2101.05511, 2021.

[60] Kaihua Qin, Liying Zhou, B. Livshits, and Arthur Gervais. Attacking the defi ecosystem with flash loans for fun and profit. In Proc. Financial Cryptography and Data Security, 2021.

[61] Petar Tsankov, Andrei Marian Dan, Dana Drachsler-Cohen, Arthur Gervais, Florian Bünzli, and Martin T. Vechev. Securify: Practical security analysis of smart contracts. In Proc. Conference on Computer and Communications Security, 2018.

[62] Jiahua Xu and Benjamin Livshits. The anatomy of a cryptocurrency pump-and- dump scheme. In Proc. USENIX Security Symposium, 2019.

[63] Mengya Zhang, Xiaokuan Zhang, Yinqian Zhang, and Zhiqiang Lin. TXSPECTOR: Uncovering attacks in ethereum from transactions. In 29th USENIX Security.

[64] Tai Nguyen, Long Pham, Jun Sun, Yun Lin, and Minh Quang Tran. sfuzz: An efficient adaptive fuzzer for solidity smart contracts. In Proc. International Conference on Software Engineering, 2020.

[65] William Entriken, Dieter Shirley, Jacob Evans, and Nastassia Sachs. Eip-721: Erc-721 non-fungible token standard, ethereum improvement proposals, no. 721. [citat 03.12.2022]. Disponibil:

https://eips.ethereum.org/EIPS/eip-721.

[66] Shayan Eskandari, Seyedehmahsa Moosavi, and Jeremy Clark. Sok: Transparent dishonesty: Front-running attacks on blockchain. In Andrea Bracciali, Jeremy Clark, Federico Pintore, Peter B. Rønne, and Massimiliano Sala, editors, Proc. Financial Cryptography and Data Security, 2020.

[67] Cryptokitties. [citat 13.12.2022]. Disponibil: https://www.cryptokitties.co.

[68] Interplanetary file system (ipfs). [citat 17.12.2022]. Disponibil: https:/ipfs.io.

[69] Nakamoto, S.: Bitcoin: A peer-to-peer electronic cash system. Tech. rep., Manubot (2019).

[70] Gervais, A., Karame, G.O., Wust, K., Glykantzis, V., Ritzdorf, H., Capkun, S.: On the security and performance of proof of work blockchains. In: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security.pp. 3–16. ACM (2016).

[71] Garay, J., Kiayias, A., Leonardos, N.: The bitcoin backbone protocol with chains of variable difficulty. In: CRYPTO. pp. 291–323. Springer (2017).

[72] Flow. [citat 23.11.2022]. Disponibil: https://www.onflow.org/.

[73] Wax:worldwide asset exchange. [citat 05.11.2022]. Disponibil:

https://github.com/world-exchange/whitepaper.

[74] Hong, S., Noh, Y., Park, C.: Design of extensible non-fungible token model in hyperledger fabric. In: Proceedings of the 3rd Workshop on Scalable and Resilient Infrastructures for Distributed Ledgers. pp. 1–2 (2019).

[75] Fast box. [citat 05.12.2022]. Disponibil: https://www.fastbox.cc/.

[76] Szabo, N.: Smart contracts: building blocks for digital markets. EXTROPY: The Journal of Transhumanist Thought,(16) 18(2) (1996).

[77] Jacques, D., Jordi, B., Thomas, S.: Eip-777: Erc-777 token standard. [citat 19.12.2022]. Disponibil: https://eips.ethereum.org/EIPS/eip-777 .

[78] Shostack, A.: Experiences threat modeling at microsoft. MODSEC@ MoDELS 2008 (2008).

[80] [citat 05.10.2022]. Disponibil:

https://www.researchgate.net/publication/361312316_A_Formal_Verification_Model_for_Security_Vulnerability_in_Non-Fungible_Tokens_NFTs_Platform.

[81] [citat 05.10.2022]. Disponibil: https://medium.com/alwaysnft/when-good-nfts-go-bad-bd4ab48b0a9f.

[82] [citat 07.10.2022]. Disponibil: https://leftasexercise.com/2021/09/26/non-fungible-token-nft-and-the-erc-721-standard/.