МАТЕМАТИЧКИ ФАКУЛТЕТ

СЕМИНАРСКИ РАД

ИЗ ТЕХНИЧКОГ И НАУЧНОГ ПИСАЊА

NFT И КРИПТОВАЛУТЕ

Аутори:

Давид Ћурувија, Милан Манојловић**Страхиња Степановић, Вања Полак, Давид Ћурувија, Милан Манојловић**

Садржај

Глава 1

УВОД: Основне информације о NFT и криптовалутама

Шта је NFT?

Иако ће кеш и платне картице и даље бити главне у процесима плаћања производа и услуга, чињеница је да је дошло до раста популарности сасвим нове платне вредности и могућности размене добара. Реч је о (NFT) токенима, односно незаменљивим (енг. non-fungible) токенима, који заправо представљају дефиницију дигиталне имовине. NFT је вид криптовалуте која омогућава да се разна уметничка дела на различитим медијима и сајтовима "токенишу"и продају путем механизама дигиталне трговине. Власништво над NFT-ом је забележено у блок-ланцу (blockchain) и власник га може пренети, што омогућава продају и промет NFT-а.

NFT токени функционишу као криптографски токени, али за разлику од криптовалута као што је нпр. Bitcoin, NFT токени су уникатни и самим тим незаменљиви. Другим речима, док су сви биткоини једнаки, не постоје два NFT токена која су потпуно идентична, јер сваки комад садржи јединствена дигитална својства. Потврда о његовој уникатности је дигитално записана у облику blockchain-а.

NFT може бити било какав дигитални фајл (нпр. фотографија, графички дизајн, гиф, текст, видео, име домена...). Фактички, купац NFT-а не може физички да га поседује, зато што се ради о дигиталном формату. Као што је новац добио своју дигиталну форму, може се рећи да је и креативни садржај и колекционарство добило свој дигитални облик.

Шта су криптовалуте?

Криптовалута је облик дигиталне имовине која се користи као средство размене користећи криптографију као начин обезбеђивања сигурности трансакција, контроле стварања додатних новчаних јединица и ради потврде трансфера валуте. Криптовалуте обично користе децентрализовану контролу, за разлику од дигиталне валуте централне банке. Када је криптовалута издата од стране једног издавача, она се генерално сматра централизованом. Када се имплементира са децентрализованом контролом, свака криптовалута ради преко блок ланца, који служи као база података јавних финансијских трансакција.

Криптовалуте су у својој основи само скуп математички добијених дигиталних података. Запис о укупном броју овако добијених дигиталних података се назива *ledger* и у њему је дефинисан број јединица неке криптовалуте. Овакав "дигитални новац" се разликује од традиционалних валута по томе што за њега не постоје банкарске гаранције, нпр. у злату или хартијама од вредности, као ни централна банка или неки државни орган који их издаје. За разлику од стандардних банкнота, папирног или металног новца, криптовалуте може да креира свако ко поседује "опрему за рударење" (енг. mining rig) и посебне врсте хардвера за убрзање израчунавања алгоритама (graphic accelerator, GA).

Крипто Валута (Скраћеница)	Вредност валуте(USD)					
	2018. Jan	2019. Jan	2020. Jan	2021. Jan	2022. Jan	Максимална вредност
Bitcoin(BTC)	9914.47	3441.03	9545.08	34622.37	37928.58	61374.28
Ethereum(ETH)	1066.72	107.57	186.26	1385.5	2604.37	4426.74
Dogecoin(DOGE)	0.006	0.002	0.002	0.03	0.14	0.3
Ripple(XRP)	1.14	0.32	0.24	0.43	0.6	2.28
Tether(USDT)	0.98	0.99	1	1	1	1.05

Глава 2

Историја NFT-а и криптовалута

Историја NFT-а

Први NFT по имену *Quantum* креирали су Кевин Мекој и Анил Даш у мају 2014. године. Quantum се састоји од видео клипа који је направила Мекојева супруга Џенифер. Мекој и Даш су ту технологију назвали „монетизована графика“.

У октобру 2015, први NFT пројекат, *Etheria*, покренут је и демонстриран на конференцији DEVCON 1 у Лондону. Све Етеријине хексагоналне плочице тренутне и претходне верзије, продате су за укупно 1,4 милиона USD. Тржиште NFT-а је имало брз раст (нарочито 2021.) [2] све до маја 2022, када је The Wall Street Journal известио да је тржиште NFT-а "у колапсу с обзиром на то да је дневна продаја NFT токена опала за 92% од септембра 2021. године.

Историја криптовалута

1983. године, амерички криптограф Дејвид Чаум осмислио је врсту криптографског електронског новца под називом *ecash*. Касније, 1995. године, имплементирао га је преко раног облика криптографског електронског плаћања под називом *Digicash*. Digicash трансакције су биле јединствене по томе што су биле анонимне због бројних криптографских протокола које је Чаум развио.[1]

У јануару 2009. програмер Сатоши Накамото креирао је најпознатију криптовалуту *Bitcoin*. [3] Један од главних Сатошијевих циљева био је независност мреже од било ког органа власти. Дизајниран је тако да свака особа, као и свака машина која учествује у рударењу и потврдама трансакција постане део мреже. Чак иако неки део мреже падне, новац ће наставити да се креће.

Глава 3

Популарност NFT-а и криптовалута

Када је NFT постао популаран?

Тренд прављења NFT-ијева је почео 2017. са блок-ланац игрицом "Crypto-Kitties у њој играчи паре, усвајају и размењују дигиталне мачке. Највећи скок у популарности виђамо у јануару 2021.
Одлике NFT-а је оно што га чини популарним, најзначајније су:

1. NFT токени постоје на блок-ланцу, што значи да не могу бити повучени,обрисани или репродуковани.

2. Блок-ланац осигурава лакоћу проналажења оригиналног власника.

3. Пошто су NFT-ијеви ретки, што додаје на њихову вредност и популарност, корисници су жељни да их поседују.

Овај талас популарности је привукао и познате личности као што су Снуп Дог, Стеве Аоки, Џими Фелон као и многи други, што још више доприноси популарности.

Изглед једних од најпопуларнијих NFT-ијева, Bored Ape Yacht Club

Глава 4

Безбедност и трансакције NFT и криптовалута

Безбедност NFT и криптовалута

Прво се мора поменути где се NFT и криптовалуте складиште. Пошто је то дигитална слика, она се не може чувати на традиционалне начине. NFT се заједно са криптовалутама најчешће складиште на нечему што се зове дигитални блок-ланац (eng. Digital Block-Chain). Над њим се врше све трансакције као што су продаја и куповина криптовалута. Блок-ланац је поуздан начин чувања криптовалута јер се користе непроменљиве дистрибуиране књиге (или технологију дистрибуиране књиге) које свако унутар мреже може да види. Ово чини блок-чејнове веома тешким за манипулисање. Када купите NFT, добијате приватни кључ који можете да складиштите у дигиталном новчанику (све док тај новчаник подржава NFT). Овај приватни кључ је неопходан за приступ и пренос NFT на друго место и треба га чувати у тајности у сваком тренутку. Ако изгубите свој приватни кључ, више нећете моћи да приступите свом NFT, што би могло довести до значајног финансијског губитка.

Рањивост у NFT и крипто индустрији

NFT и крипто индустрије не постоје дуго, релативно су младе и звог тога су циљ огромног броја сајбер напада (eng.Cyber attacks) како би нападач покушао да преузме контролу над вашим дигиталним новчаником. Постоје две кључне информације којима ће сајбер криминалац покушати да приступи како

би украо ваше NFT или криптовалуте: ваш приватни кључ и почетну фразу. Ваш NFT/криптовалута се не може нигде преместити без коришћења приватног кључа, јер вам то омогућава да потврдите да сте ви извршили трансакцију. Поврх овога, основна фраза може дати приступ вашем дигиталном новчанику. Овим информацијама нападач може да се дочепа ваших NFT или криптовалута које се налазе у вашем дигитиалном новчанику (eng.Digital wallet) за неколико минута. Највећи губитак у историји биткоина десио се у фебруару 2014, када је MT. Гок, тржиште биткоина у Токију, изгубило 850.000 BTC, што је укупно износило 474 милиона долара у то време. У време писања овог текста,узимајући у обзир тренутну тржишну цену, губици би износили више од 7 милијарди долара.Касније, MT. Гокс објавио је да је до инцидента дошло због флексибилности трансакције. Други пример је напад на Децентрализовану аутономију Организација (ДАО),фонд ризичног капитала који је омогућио инвеститорима да директно финансираju предлоге путем паметних уговора,заснованих на платформи Етхереум.Тај напад довео до крађе чак 3,6 милиона етер кованица,у вредности од 3,1 милијарде долара на тренутној тржишној цени.Нападачи су искористили рупу која је омогућила да рекурзивно преносе средства са родитељског рачуна на дете,без ажурирање матичног биланса.

Како се одбранити од напада на NFT и крипто тржишту

1. Користите виртуелну приватну мрежу (ВПН)(eng.VPN) да шифрујете и анонимизујете свој саобраћај.
2. Избегавајте сумњиве вебсајтове и сумњиве линкове. Можда ћете завршити на сајту са злонамерним софтвером или на сајту за крађу идентитета.
3. Никада не делите своју почетну фразу или податке за пријаву ни са ким или на било ком сајту.
4. Урадите сопствено истраживање пре него што уложите у NFT пројекат.Проверите профил и позадину оснивача пројекта пре улагања.
5. Тргујте само на познатим,провереним NFT тржиштима и користите сигуран дигитални новчаник.
6. Користите двофакторну аутентификацију да додате додатни ниво сигурности свом крипто новчанику.

Литература

[1] Waleed Abrar. Untraceable electronic cash with digicash, 1900.

[2] Lennart Ante. The non-fungible token (nft) market and its relationship with bitcoin and ethereum. *FinTech*, 1(3):216–224, 2022.

[3] Björn Segendorf. What is bitcoin. *Sveri gesRiksbankEconomicReview*, 2014:2–71, 2014.