UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

MAGISTRSKO DELO

ANALIZA TEHNOLOŠKIH TVEGANJ POVEZANIH S TEHNOLOGIJO IN UPORABO KRIPTOVALUT

Ljubljana, januar 2024 NEJC KOTNIK

IZJAVA O AVTORSTVU

Podpisani Nejc Kotnik, študent Ekonomske fakultete Univerze v Ljubljani, avtor predloženega dela z naslovom Analiza tehnoloških tveganj povezanih z uporabo kriptovalut, pripravljenega v sodelovanju s svetovalcem doc. dr. Antonom Manfredo

I Z J A V L J A M

1. da sem predloženo delo pripravil samostojno;

2. da je tiskana oblika predloženega dela istovetna njegovi elektronski obliki;

3. da je besedilo predloženega dela jezikovno korektno in tehnično pripravljeno v skladu z Navodili za izdelavo zaključnih nalog Ekonomske fakultete Univerze v Ljubljani, kar pomeni, da sem poskrbel, da so dela in mnenja drugih avtorjev oziroma avtoric, ki jih uporabljam oziroma navajam v besedilu, citirana oziroma povzeta v skladu z Navodili za izdelavo zaključnih nalog Ekonomske fakultete Univerze v Ljubljani;

4. da se zavedam, da je plagiatorstvo – predstavljanje tujih del (v pisni ali grafični obliki) kot mojih lastnih – kaznivo po Kazenskem zakoniku Republike Slovenije;

5. da se zavedam posledic, ki bi jih na osnovi predloženega dela dokazano plagiatorstvo lahko predstavljalo za moj status na Ekonomski fakulteti Univerze v Ljubljani v skladu z relevantnim pravilnikom;

6. da sem pridobil vsa potrebna dovoljenja za uporabo podatkov in avtorskih del v predloženem delu in jih v njem jasno označil;

7. da sem pri pripravi predloženega dela ravnal v skladu z etičnimi načeli in, kjer je to potrebno, za raziskavo pridobil soglasje etične komisije;

8. da soglašam, da se elektronska oblika predloženega dela uporabi za preverjanje podobnosti vsebine z drugimi deli s programsko opremo za preverjanje podobnosti vsebine, ki je povezana s študijskim informacijskim sistemom članice;

9. da na Univerzo v Ljubljani neodplačno, neizključno, prostorsko in časovno neomejeno prenašam pravico shranitve predloženega dela v elektronski obliki, pravico reproduciranja ter pravico dajanja predloženega dela na voljo javnosti na svetovnem spletu preko Repozitorija Univerze v Ljubljani;

10. da hkrati z objavo predloženega dela dovoljujem objavo svojih osebnih podatkov, ki so navedeni v njem in v tej izjavi.

11. da sem preveril verodostojnost informacij, ki izhajajo iz zapisov na podlagi uporabe orodij umetne inteligence.

V Ljubljani, dne _____ Podpis študenta: _____

KAZALO

KAZALO TABEL

KAZALO SLIK

KAZALO PRILOG

SEZNAM KRATIC

angl. – angleško
ABI – (angl. Application Binary Interface): Binarni vmesnik aplikacije
AJAX – (angl. Asynchronous JavaScript and XML); Asinhroni JavaScript in XML
API – (angl. Application Programming Interface); Vmesnik za programiranje aplikacij
BSC – (angl. Binance Smart Chain); Pametna veriga Binance
CNN – (angl. Cable News Network); Omrežje kabelskih novic
CS244 – (angl. Computer Science 244); Računalniška znanost 244
DAX – (angl. Data Analysis Expressions); Izrazi za analizo podatkov
DDoS – (angl. Distributed Denial of Service); Porazdeljeno zavračanje storitve
DES – (angl. Data Encryption Standard); Standard šifriranja podatkov
DNS – (angl. Domain Name System); Sistem domenskih imen
ENS – (angl. Ethereum Name System); Sistem imen Ethereum
ERC – (angl. Ethereum Request for Comment); Ethereum zahteva za komentar
EVM – (angl. Ethereum Virtual Machine); Navidezni stroj Ethereum
FTP – (angl. File Transfer Protocol); Protokol za prenos datotek
GCHQ – (angl. Government Communications Headquarters); Sedež vladnih komunikacij
HTTPS – (angl. Hypertext Transfer Protocol Secure); Varni protokol za prenos hiperteksta
IT – Informacijska Tehnologija
NFT – (angl. Non-Fungible Token); Neizmenljiv žeton
NSA – (angl. National Security Agency); Agencija za nacionalno varnost
OFAC – (angl. Office of Foreign Assets Control); Urad za nazor tujega premoženja
PGP – (angl. Pretty Good Privacy); Precej dobra zasebnost

PIN – (angl. Personal Identification Number); Osebna identifikacijska številka
PoS – (angl. Proof of Stake); Dokazilo o deležu
PoW – (angl. Proof of Work); Dokazilo o delu
RSA – Rivest-Shamir-Adleman
SI-CERT – (angl. Slovenian Computer Emergency Response Team); Slovenska skupina za odzivanje na računalniške grožnje
SMS – (angl. Short Message Service); Storitev kratkih sporočil
SSL – (angl. Secure Sockets Layer); Varnostni vmesniški sloj
TLS – (angl. Transport Layer Securtiy); Varnost transportnega sloja
TOR – (angl. The Onion Router); Čebulni usmerjevalnik
TPS – (angl. Transactions Per Second); Transakcije na sekundo
URL – (angl. Uniform Resource Locator); Enotni iskalnik virov
USB – (angl. Universal Serial Bus); univerzalno serijsko vodilo
UTXO – (angl. Unspent Transaction Output); Neporabljen izhod transakcije
XML – (angl. Extensible Markup Language); Razširljiv označevalni jezik
WBTC – (angl. Wrapped Bitcoin); Zavit bitcoin
WETH – (angl. Wrapped Ether); Zavit eter
ZDA – Združene Države Amerike

1 UVOD

Varnost je ena temeljnih potreb po Maslowu, ki sledi fiziološkim potrebam, med katere sodijo: dostop do hrane, pitne vode, bivališča, spanja ipd. Ta potreba se je v preteklosti udejstvovala v združevanju posameznikov v večje skupine, ki so se tako lažje zavarovale pred potencialnimi napadalci in naravnimi nesrečami. Obzidja, gradovi, utrdbe in obrambni jarki so bili v preteklosti namenjeni odvračanju agresije in obrambi pred zavojevalci. Posamezniki pa pogosto niso želeli zaščititi le svojega življenja, ampak tudi svoja sredstva in drugo lastnino pred potencialnimi nezgodami. Zato so v preteklosti nastale banke in zavarovalnice, ki so imele takrat v določenih pogledih dosti drugačno vlogo kakor danes (Davis, 2013). Zaradi tehnološkega napredka so določene oblike varovanja življenja in lastnine postale manj primerne. Po izumu smodnika so kovinski oklepi in kamnita obzidja zagotavljali dosti manj varnosti kot prej. Sčasoma so jih nadomestile tehnološko naprednejše in učinkovitejše rešitve, ki uporabnikom ponujajo večjo varnost na enoto cene.

V današnjem svetu smo uporabniki digitalnih tehnologij povezani med seboj kot še nikoli doslej. Digitalizacija komunikacijskih tehnologij nam tudi omogoča veliko hitrejši prenos sporočil z manjšo verjetnostjo izgube sporočila na poti do naslovnika. To pa se lahko v praksi izkaže za dvorezen meč. Internet nam omogoča, da lahko med seboj vzpostavimo povezavo praktično ne glede na to, kje smo. Tako lahko v realnem času vzpostavimo besedilne, glasovne in video povezave z ljudmi v drugih državah ali celo na drugih celinah. Ob tem pa ne smemo zanemariti možnosti, da obstajajo tudi posamezniki, ki zlorabljajo moderne tehnologije za finančno okoriščanje na račun drugih uporabnikov. Čeprav najrazličnejše finančne in investicijske prevare niso nič novega, so v zadnjih letih zaradi razvoja digitalnih valut in kriptovalut dobile nov zagon. Digitalne valute so tip valute, ki obstaja in je hranjena v digitalni obliki. Kriptovalute obstajajo kot podmnožica digitalnih valut in se od njih razlikujejo po tem, da za svojo zaščito uporabljajo kriptografijo, zaradi česar jih je težko ponarediti (Rose, 2015). Po ekonomski krizi leta 2008 se je na spletu začela širiti ideja o bitcoinu, ki ga danes razumemo kot prvo decentralizirano finančno platformo, čeprav so ideje o decentraliziranih digitalnih plačilnih sredstvih obstajale že v 90. letih 20. stoletja (Cunha in drugi, 2021).

Še ena izmed pomembnih lastnosti decentraliziranih kriptovalut je njihova odpornost na cenzuro transakcij, ker v tem sistemu ni posamezne entitete oz. ustanove, ki bi imela nadzor nad omrežjem in transakcijami, ki se po njem prenašajo (Nakamoto, 2008). Tako lahko vsak uporabnik uporablja poljubno število naslovov za hranjenje svojih kovancev; hkrati je omrežje zasnovano tako, da je skoraj nemogoče povrniti transakcije, ki so že zabeležene v verigi blokov. Žal se je v praksi izkazalo, da ravno tisti, ki se še posebej zavedajo pomena anonimnosti, pogosto izkoriščajo to lastnost za prikrivanje svojih nečednih poslov. Zato se je bitcoin že v zgodnjih letih svojega obstoja pogosto uporabljal kot plačilno sredstvo na spletnih straneh, ki so se želele izogniti finančnim regulacijam digitalnih transakcij. To

predstavlja velik izziv oškodovanim uporabnikom, ker je izgubljena finančna sredstva zelo težko vrniti brez privoljenja tatu. Oškodovani uporabniki pogosto iščejo pomoč na družbenih omrežjih, pri vladnih agencijah ali pa kar neposredno stopajo v stik z razvijalci programske opreme. Realnost pa žal ostaja takšna, da zaradi narave tehnologije izgubljenih sredstev praviloma ni mogoče dobiti nazaj, če ne uspejo razkriti identitete storilca. Varnost je zato v svetu kriptovalut ključnega pomena, ker transakcije, ki so že vključene v verigo blokov, ni več mogoče preprečiti ali razveljaviti (Cunha in drugi, 2021). To je še eden izmed razlogov, zakaj digitalni zlikovci raje zahtevajo plačilo v kriptovalutah kot bančna nakazila. Poleg tega obstaja veliko prevar z novimi projekti, ki so oglaševani kot naslednji veliki preskok v tehnologiji, v praksi pa se v večini primerov izkaže, da to ni tako. Takšni projekti mečejo slabo luč na celotni sektor, ker najpogosteje finančno oškodujejo ravno tiste uporabnike, ki niso dovolj informirani o razlikah med tehnologijami, ki jih uporabljajo, in drugimi tveganji, povezanimi z uporabo kriptovalut (Fernando, 2015).

Zlonamerni posamezniki prežijo na neuke ali naivne uporabnike, ki jih poskušajo izkoristiti na različne načine. Naj bodo to neresnična sporočila o zapuščini premožnega daljnega sorodnika iz tujine, lažni spletni oglasi, ki ponujajo najnovejše artikle po najnižjih cenah, nenapovedani klici tehnične podpore, ki je nismo naročili, in še marsikaj drugega. Obstajajo tudi zlorabe, ki se lahko zgodijo zunaj cone našega vpliva. Programska oprema, ki jo uporabljamo, lahko vsebuje varnostne ranljivosti, ki lahko omogočajo zlorabo sistema tretji osebi brez vednosti uporabnika (Agency, 2021). Tako lahko hekerji pridobijo dostop do uporabnikovih podatkov in v nekaterih primerih celo nadzor nad njegovo napravo. Zlorabe varnostnih ranljivosti lahko postanejo še veliko bolj problematične, če se nanašajo na finančno infrastrukturo, ki omogoča takojšnji prenos finančnih sredstev. To pomeni, da lahko z enim napačnim oz. nepremišljenim klikom pošljemo sredstva s svojega bančnega računa na račun spletnega kriminalca.

Crypto.com (Wang, 2021) poroča, da je po njihovih ocenah julija 2021 število svetovnih uporabnikov kriptovalut preseglo 220 milijonov. Ta številka v praksi pomeni veliko potencialnih tarč, ker se določeni delež uporabnikov ne poglobi dovolj v podrobnosti, da bi lahko ločili legitimne projekte od prevar. Zato se je pomembno zavedati potencialnih nevarnosti ob uporabi nove tehnologije in kako lahko uporabniki minimizirajo lastno tveganje ob njihovi uporabi (Yildirim in Varol, 2019). Na podlagi lastnih izkušenj lahko potrdim, da spletni prevaranti ne prežijo zgolj na varnostne ranljivosti v strojni ali programski opremi. V praksi se pogosto izkaže, da je lažje prepričati naivnega uporabnika, da pošlje nepovratno transakcijo, kot da bi iskali varnostne ranljivosti v programski opremi. To lahko uporabniki naredijo prostovoljno misleč, da bodo v zameno dobili legitimni produkt ali žetone v višji vrednosti. Lahko pa se tudi zgodi, da jih neznanci prek socialnega inženiringa poskušajo zvabiti, da bi kliknili na okuženo povezavo, ki bi lahko ogrozila varnost uporabnikovih sredstev (Gkioulos in drugi, 2017).

Namen magistrskega dela je prispevati k zmanjšanju števila uporabnikov kriptovalut, ki bi lahko bili oškodovani zaradi pomanjkljivega razumevanja tehnoloških tveganj, povezanih s

tem področjem. Informiranost, sploh pa podučenost uporabnikov je zelo pomembna, ker ozaveščeni uporabniki redkeje nasedejo spletnim prevarantom in lahko tako uporabljajo nove tehnologije z manjšo stopnjo tveganja. Zato bom v magistrskem delu poskušal odgovoriti na vprašanje: »Katera so najpogostejša tveganja uporabnikov kriptovalut?« in predstaviti potencialne rešitve za zmanjšanje teh tveganj. Cilji magistrskega dela so:

- predstaviti ključne pojme s področja kibernetske varnosti in kriptografije,
- opisati največje digitalne vdore in najpogostejše razloge, da do njih pride,
- predstaviti praktične uporabe tehnologij veriženja blokov,
- analizirati objave, ki opisujejo ilegalne odtujitve kriptovalut,
- analizirati najpogostejša tveganja za uporabnike kriptovalut,
- predstaviti varnostne prakse, ki omogočajo zmanjšanje identificiranih tveganj.

V teoretičnem delu magistrskega dela bom predstavil osnove tehnološke varnosti, zgodovino kriptografije, prednosti, slabosti in različne lastnosti kriptovalut, največje digitalne vdore in varnostna tveganja, ki lahko ogrožajo uporabnikovo premoženje na blockchainu. Praktični del vsebuje kvantitativno analizo objav člankov o digitalnih vdorih s treh spletnih virov, ki poročajo o novicah s področja blockchaina in kriptovalut. Naslove objav sem zbral z orodjem Octoparse in jih obdelal ter prikazal z orodjem PowerBI. Poleg tega sem intervjuval strokovnjaka s področja razvoja decentraliziranih aplikacij na verigah blokov. Temu sem dodal pregled najpogostejših informacijskih tveganj, ki lahko ogrožajo sredstva uporabnikov kriptovalut in navedel varnostne prakse, ki lahko zmanjšajo uporabnikovo izpostavljenost tem tveganjem. S svojim delom želim povečati ozaveščenosti obstoječih in bodočih uporabnikov kriptovalut, ker pomanjkanje znanja na tem področju pogosto pripelje do nepotrebnih finančnih izgub. Nepovratnost transakcij na verigah blokov je problematična za oškodovanca, ker je ukradena sredstva praktično nemogoče dobiti nazaj.

2 POMEN KIBERNETSKE VARNOSTI

Dandanes se velik del našega življenja dogaja v digitalnem svetu. Morda se niti sami ne zavedamo, koliko informacij in komunikacijskih kanalov je potrebnih za nemoteno brskanje po spletu, igranje video iger, pretočno predvajanje vsebin itd. Za dostop do digitalnih storitev uporabniki najpogosteje potrebujejo uporabniški račun, do katerega lahko dostopajo prek unikatne kombinacije uporabniškega imena ali e-naslova in gesla. Ker je uporabniško ime načeloma javno in posledično vidno drugim uporabnikom, je geslo pogosto edini mehanizem, ki preprečuje drugim osebam dostop do uporabnikovega računa in upravljanja z njim. Zato je pomembno, da imajo uporabniki kompleksna in raznolika gesla, ki morajo ostati skrita pred potencialnimi zlonamernimi akterji (Furnell, 2022). Zagotavljanje varnosti uporabniških računov je eno od področij, s katerimi se ukvarja kibernetska varnost.

Kibernetska varnost je po standardu ISO/IEC 27032 definirana kot »ohranjanje zaupnosti, celovitosti in dostopnosti informacij v kibernetskem prostoru.« Slovar Merriam-Webster

definira pojem kibernetske varnosti kot »ukrepi za zaščito računalnika ali računalniškega sistema pred nepooblaščenim dostopom ali napadom.« (Cybersecurity, brez datuma) V enciklopediji Britannica je ta pojem opredeljen kot »zaščita računalniških sistemov in informacij pred poškodbami, krajo in nepooblaščeno uporabo.« (Computer security, brez datuma).

Ker so podatki, do katerih dostopamo, pogosto zaupne narave, sta upoštevanje in uporaba varnostnih praks ključnega pomena. Uporabniki lahko svoj uporabniški račun dodatno zavarujejo z uporabo večfaktorskega potrjevanja, ki naj bi zagotovilo varnost uporabnikovega računa tudi v primeru razkritja njegovega uporabniškega gesla. Žal pa to v praksi ni zagotovilo, da je uporabnikov račun popolnoma varen pred vdorom (Wolff, 2022).

Poleg tega ne smemo pozabiti, da večina spletnih komunikacij poteka prek kanalov, ki so javno dostopni. To pomeni, da lahko vsakdo, ki poseduje potrebno znanje in tehnično opremo, spremlja podatke, ki se prenašajo po internetu. Ker so ti podatki pogosto zaupne narave, potrebujemo pri takšni komunikaciji močna zagotovila, da iz javno dostopnih podatkov ni mogoče dešifrirati izhodiščnega sporočila. Zato danes večina komunikacijskih sistemov uporablja kriptografijo, da bi zagotovili anonimnost podatkov, ki se prenašajo med napravami. To dosežejo tako, da informacije zakodirajo v šifrirano besedilo z algoritmom šifriranja in javnim ključem. Če je uporabljen algoritem varen, lahko to zašifrirano sporočilo javno delijo z drugimi z močnimi zagotovili, da ga ne bodo mogli dešifrirati, če nimajo potrebnega skrivnega ključa (Kumar Sharma in drugi, 2022).

2.1 Management tveganj informacijskih tehnologij in kibernetska varnost

Management informacijsko-tehnoloških tveganj je proces upravljanja in preprečevanja tveganj s previdnim planiranjem, specializiranimi sistemi, smernicami in odločitvami v različnih sektorjih. Ukvarja se z identifikacijo potencialnih negativnih tehnoloških posledic dela na daljavo, prednostmi in slabostmi različnih oblik shrambe podatkov v podjetju, minimizacijo tehnoloških tveganj pri sodelovanju z zunanjimi izvajalci in implementacijo planov v sili, če bi prišlo do informacijsko-tehnološkega incidenta (Sukianto, 2023).

Kibernetska varnost se ukvarja z varovanjem sistemov, naprav, programov in omrežij pred kibernetskimi napadi. Varnost digitalnih podatkov v podjetjih je danes še kako pomembna. Hitre internetne povezave in dostop na daljavo omogočajo hekerjem, da z lahkoto odtujijo veliko količino zaupnih informacij, če njihovega vdora ne preprečimo oz. v najslabšem primeru ne identificiramo dovolj hitro (Sukianto, 2023).

Izraza »management tveganj informacijskih tehnologij« in »kibernetska varnost« na prvi pogled delujeta zelo podobno. Vendar med njima obstajajo velike razlike in ju ne bi smeli uporabljati kot sopomenki. Kibernetska varnost pokriva del informacijske varnosti in se osredotoča na zaščito naprav pred nepooblaščenim dostopom, zlonamerno programsko opremo in drugimi napadi. Management tveganj informacijskih tehnologij se nanaša na širše

področje, ki vključuje tudi druge tipe tveganj kot na primer napake v strojni in programski opremi, človeške napake, ki lahko pripeljejo do tehnoloških tveganj, tveganja, povezana z regulacijo, itd. (Sukianto, 2023)

2.2 Pregled velikih digitalnih vdorov

Uporabniki digitalnih tehnologij nekako predpostavljamo, da so naši podatki varno hranjeni in da do njih lahko dostopamo le mi in morda nekatere pooblaščene osebe. Žal pa to v praksi pogosto ni tako. Najrazličnejši razlogi lahko pripeljejo do nepooblaščenega dostopa do zaupnih podatkov. Seveda pa kraja podatkov ni edini način, na katerega lahko nepridipravi otežujejo življenje nič hudega slutečim posameznikom. Izkoriščanje varnostnih ranljivosti, ki prisilijo uporabnikovo napravo v neprestano ponovno zaganjanje operacijskega sistema in uporaba izsiljevalske programske opreme sta le dva primera zlorab, ki jih bom predstavil v tem poglavju.

- Citibank (1995): Vdor v Citibank mnogi razumejo za prvi bančni napad v zgodovini interneta. Ruski programer Vladimir Levin je leta 1995 oškodoval njihove stranke za $10 milijonov. Vendar pa je to dosegel na dokaj nekonvencionalen način. Vdor v telefonski sistem banke mu je omogočil prisluškovanje pogovorom med strankami in bančnimi uslužbenci in prestrezanje zaupnih informacij (predvsem številke bančnih računov in njihova gesla). Levin je podatke uporabnikov izkoristil za prenos sredstev na različne račune po svetu. Po prijetju so ga obsodili na 3 leta zapora in od njega izterjali vsa odtujena sredstva z izjemo $400 tisoč (Dteckt, brez datuma; Sundar, 2017).
- Virus Melissa (1999): Leta 1999 je programer David Lee Smith vdrl v AOL in e-pošti dodal prilogo, ki je obljubljala brezplačna gesla za plačljiva spletna mesta vključujoč strani za odrasle. Po kliku na datoteko se je aktiviral virus, ki je poslal e-poštno sporočilo prvim 50 stikom tega uporabnika s priloženo okuženo datoteko. To je virusu omogočilo izredno hitro širjenje, ki je zaradi količine poslane pošte preobremenilo e-poštne strežnike nekaterih ponudnikov, vključujoč Microsoft. Ocenjuje se, da je virus okužil približno 20 % svetovnih računalnikov. Virus sicer ni ukradel ali zaklenil uporabnikovih podatkov, vendar pa je moral njegov kreator po aretaciji plačati $ 80 milijonov odškodnine in preživeti 20 mesecev za zapahi (Dteckt, brez datuma; Sundar, 2017).
- Mafiaboy (2000): 15-letni Micharl Chalice, v hekerskih vodah poznan pod psevdonimom Mafiaboy, je 7. februarja 2000 z DDoS napadom za 1 uro onemogočil uporabo storitev platforme Yahoo!. Yahoo! je takrat spadal med največja tehnološka podjetja z vodilnim iskalnikom. Naslednji dan je nekdo drug preobremenil Buy.com, kar je Mafiaboy razumel, kot da ga je nekdo izzval. Sledil je uspešen napad na eBay in CNN, za katerega so nekateri trdili, da se bi lahko ubranil napada zaradi naprednejšega omrežja. Po nekaj dneh je izbral za naslednjo tarčo Dellovo spletno stran in kasneje še Amazon.com. Cena povzročene škode je bila ocenjena na $1,1 milijardo (Dteckt, brez datuma; Blackhat Ethical Hacking, brez datuma).

- Virus Sasser (2004): Sven Jascan je pri 17-letih ustvaril računalniški virus, ki je okužil računalnike z operacijskima sistemoma Windows 2000 in Windows XP. Virus je izkoriščal sistemske ranljivosti, prek katerih je lahko ustvaril na drugi napravi FTP strežnik, prek katerega se je širil dalje. Čeprav virus ni vseboval namerno destruktivne kode, je s svojimi procesi pogosto upočasnil delovanje sistema in ga pogosto tudi sesul, kar je povzročilo, da se je računalnik nepričakovano ponovno zagnal. Okuženi računalniki so povzročili odpovedi nekaterih čezatlantskih letov iz Amerike. V Avstraliji so zaradi nedelujočega radijskega omrežja za nekaj časa odpovedali večino vlakov. Ena izmed največjih bolnišnic v Južni Koreji je imela zamude pri obravnavi pacientov zaradi beleženja njihovih podatkov s pisalom in papirjem. Varnostni strokovnjaki ocenjujejo, da je bilo okuženih na milijone računalnikov (Dteckt, brez datuma; Elsevier Ltd., 2004).
- Iceman (2007): Max Ray Butler, ki se je na spletu predstavljal s psevdonimom Iceman, je v 90. letih prejšnjega stoletja delal kot svetovalec za računalniško varnost. Po prelomu tisočletja se je začel ukvarjati s hekanjem in odsedel 18 mesecev v zaporu zaradi nepooblaščenega dostopa do računalnikov ameriške vojske. Po izpustitvi leta 2003 je nadaljeval s programiranjem zlonamerne programske kode, ki bi se lahko izmikala protivirusnim programom. Z izkoriščanjem varnostnih ranljivosti je uspel ukrasti podatke o kreditnih karticah podjetja American Express. Naslednja tarča je bil Citibank, kjer je s pomočjo trojanskega konja ukradel identitete uporabnikov za dostop do PIN kod njihovih strank. Aretirali so ga leta 2007 in ga obtožili kraje skoraj 2 milijonov številk kreditnih kartic, na katerih je bilo skupno nekaj več kot $86 milijonov goljufivih stroškov. Obstojen je bil na 13 let zapora in $27,5 milijonov odškodnine (Dteckt, brez datuma).
- Epsilon (2011): Podjetje Epsilon je leta 2011 ponujalo storitve trženja prek e-pošte 2500 podjetjem, med katera so spadala tudi velika podjetja, kot so Barclaycard US, Citigroup, JP Morgan in Best Buy. Hekerji so med vdorom v Epsilon ukradli imena in e-poštne naslove milijonov ljudi. Drugih podatkov na srečo niso uspeli odtujiti. Mnoga podjetja, ki so poslovala z Epsilonom, so svoje stranke začela obveščati o potencialnih nevarnostih vabljivih e-poštnih sporočil, ki bi jih lahko pošiljali nepridipravi. Vdor je podjetje stal med $225 milijonov in $4 milijarde (Dteckt, brez datuma).
- WannaCry (2017): Izsiljevalska oprema WannaCry je zašifrirala podatke na uporabnikovem računalniku in v zameno za dešifrirni ključ zahtevala plačilo odkupnine z bitcoini. Odkupnina, ki je sprva znašala $300 v bitcoinu, se je po treh dneh podvojila na $600. WannaCry je izkoriščal varnostno ranljivost v operacijskemu sistemu Windows, imenovano EternalBlue, ki naj bi jo sprva odkrila ameriška agencija za nacionalno varnost. Kasneje jo je javnosti razkrila hekerska skupina Shadow Brokers. Čeprav je Microsoft izdal varnostne popravke za operacijske sisteme Windows 2 meseca pred napadom, mnogi posamezniki in organizacije niso naložili potrebnih posodobitev, ki bi jih zaščitili pred tem napadom. WannaCry je okužil približno 230 tisoč računalnikov po svetu. Med drugimi je prizadel tisoče zdravstvenih domov in kirurških ordinacij v Združenem Kraljestvu, ki so morale odpovedati 19 tisoč pregledov. Ocena

stroškov britanskega zdravstvenega sistema se giblje okrog £92 milijonov, v globalnem merilu pa je skupna škoda ocenjena na $4 milijarde (Dteckt, brez datuma).

Žal lahko na podlagi predstavljenih primerov zaključimo, da nenadzorovana uporaba zlonamerne programske opreme pogosto privede do zelo velike finančne in v določenih primerih tudi gmotne škode. Četudi poskušamo stvar obravnavati z ekonomskega vidika, bi težko zaključili, da se kratkoročna finančna korist hekerju splača, če upošteva verjetnost visoke odškodnine in relativno dolge zaporne kazni. Stranska škoda je lahko še toliko večja, če virus okuži naprave ustanov, ki so kritične narave, kot na primer porodnišnice, zdravstveni domovi in urgence.

2.3 Najpogostejši razlogi za vdore

Glede na vdore, omenjene v prejšnjem poglavju, lahko identificiramo nekatere razloge, ki so se pojavili v več primerih. Čeprav v praksi dva vdora nista popolnoma ista, je smiselno nameniti dodatno pozornost razlogom, ki pogosto pripeljejo do njih. Tako lahko uporabniki z relativno majhnim vložkom povečajo varnost svojih podatkov v digitalnem svetu. Seveda bi bilo idealno, če bi lahko zagotovili absolutno varnost, vendar pa moramo žal v praksi zaradi omejenosti dobrin (predvsem časa in denarja) najti smiseln kompromis med vloženimi sredstvi in pričakovanimi rezultati.

2.3.1 Šibka uporabniška gesla

Uporabniška gesla imajo zanimivo vlogo z varnostnega vidika, ker jih zelo pogosto uporabljamo. Hkrati predstavljajo veliko varnostno ranljivost. Uporabniki se v praksi pogosto zanašajo na lasten spomin za shrambo gesel, zato ta ne smejo biti preveč kompleksna oz. je pogosto za uporabnika lažje, če ta sledijo določenemu vzorcu. Napadalci lahko do uporabnikovih gesel poskušajo priti na različne načine (Yu in Huang, 2015):

- Razbijanje s surovo silo na podlagi verjetnosti (angl. brute-force cracking based on probability) poskuša naključno uganiti kombinacije znakov gesla. Ker je to v primeru kompleksnih gesel lahko zelo zamudno, se ta pristop zanaša na verjetnostne metode, da bi povečal verjetnost svojega uspeha. Tradicionalna verjetnostna metoda uporablja majhen niz kot testni niz, na katerem opravi frekvenčno analizo. Na koncu izbere niz znakov z visoko frekvenco kot vhodni niz. Markov model je modernejša in bolj učinkovita metoda, ki v modelu upošteva tudi verjetnost zaporedja določenih znakov.
- Razbijanje s slovarjem (angl. dictionary cracking) predpostavlja, da gesla uporabnikov niso niz naključnih znakov, ampak vsebujejo običajne besede, da bi si ga lažje zapomnili. Pri tem je ključna uporaba »dobrega« slovarja. V praksi se običajno začne z majhnim slovarjem, ki vsebuje podatke o tarči, kot so ime, rojstni dan, številka osebnega dokumenta, telefonska številka, domači naslov ipd. Na podlagi majhnega slovarja napadalci ustvarijo velik slovar s pravili za prevajanje. Ta lahko pretvarjajo velike in

male črke, zamikajo znake v besedah, pretvarjajo znake (npr. a v @) ipd. Veliki slovar se potem uporabi kot nabor potencialnih gesel, ki bi jih lahko tarča uporabljala za zaščito dostopa do svojih računov.

- Razbijanje z mavrično razpredelnico (angl. rainbow table cracking) se za razliko od razbijanja s surovo silo osredotoča na količino porabljene shrambe na račun hitrosti. Razbijanje z mavričnimi razpredelnicami poteka v dveh korakih: predizračun in spletni napad. V prvem koraku se izračuna m-verige, ki imajo po t-točk. Razpredelnica hrani le začetno in končno točko vsake verige. V drugem koraku poskuša algoritem najti čim večje ujemanje med predizračunanimi verigami z zakodirano verigo. Tako lahko na podlagi bolj skladnih verig predpostavlja vrednosti, ki bi lahko bile zakodirane.
- Razbijanje gesel z visokozmogljivimi računalniki (angl. password cracking on high performance computer) zahteva poskušanje čim večjega števila gesel z upanjem, da bo eno izmed njih sčasoma pravilno. Za takšne napade se pogosto uporablja avtomatizirana orodja in računalnike, ki vzporedno poskušajo gesla, da bi pospešili proces.

V primeru nedovoljenega dostopa do uporabnikovega računa uporabniki ne bi smeli prevzeti celotne odgovornosti, če jim je spletno mesto dovolilo uporabljati šibko geslo in jim ni predlagalo mehanizmov za ustvarjanje varnejšega gesla. Furnell (2022) ugotavlja, da so se varnostne prakse večine spletnih mest med letoma 2007 in 2022 izboljšale. Večina spletnih strani, med določanjem gesla uporabniškega računa, uporabnika ne informira o pomenu varnosti in dobrih praksah za izbiro močnega gesla. Poleg tega pogosto dajejo nejasne povratne informacije ob vnosu neustreznega gesla. Nekatere strani uporabljajo napredno prepoznavo pogostih gesel, medtem ko druge še vedno dopuščajo gesla, kot so »123456«, »qwerty« in »password« (Furnell, 2022).

Svoje račune lahko uporabniki dodatno zavarujejo z več faktorskim potrjevanjem, kjer mora uporabnik za vstop poleg gesla vnesti še naključno zaporedje znakov, ki se spremeni, ko preteče določeni časovni interval. Ta začasna gesla lahko prejmemo prek SMS-a, e-pošte ali pa jih generiramo z za to namenjeno napravo ali aplikacijo na pametni napravi. Uporaba večfaktorskega potrjevanja v teoriji ponuja večja varnostna zagotovila, ker mora heker poleg uporabniškega imena in gesla imeti tudi dostop do druge naprave, ki omogoča generacijo začasnega gesla. V praksi pa se izkaže, da sta varnost in zanesljivost večfaktorskega potrjevanja zelo odvisna od posamezne implementacije in pogosto nima tako močnih varnostnih zagotovil, kot bi pričakovali (Wolff, 2022).

2.3.2 Varnostne ranljivosti v programski opremi

Razvijalci lahko v programski opremi, ki jo razvijajo zaradi lastne nepazljivosti ali malomarnosti, pustijo nenamerne napake. Te napake lahko odkrijejo hekerji, ki jih izkoristijo za ogrožanje naprav, ki poganjajo programsko opremo z varnostnimi pomanjkljivostmi. Raziskovalci kibernetske varnosti se prav tako ukvarjajo z odkrivanjem nepravilnosti v programski opremi, vendar pa za razliko od hekerjev odkritih nepravilnosti

ne izkoristijo za ogrožanje varnosti uporabnikov, ampak o njih obvestijo razvijalce in po potrebi varnostne organe. Nagrajevanje odkrivanja hroščev v programski opremi lahko prepriča akterje v sivi coni, da raje odkrito ranljivost prijavijo podjetju, kot da bi jo razkrili na hekerskih forumih ali prodali na »deep-webu«.

Težava lahko nastane tudi s pretiranim zanašanjem na obstoječe programske knjižnice. Mnogih njihovi razvijalci ne vzdržujejo več in zato ne vsebujejo vseh popravkov za nedavno identificirane varnostne ranljivosti. Ker mnoga podjetja niso pretirano pozorna na sodobnost digitalnih tehnologij, ki jih uporabljajo, lahko posredno postanejo tarče hekerjev, ki prežijo na takšne varnostne pomanjkljivosti v programski opremi. Prevarantski paketi kode lahko na prvi pogled delujejo popolnoma normalno, vendar pa ob zagonu izvršijo tudi zlonamerno programsko kodo, ki lahko ukrade informacije o uporabniku. Te lahko vključujejo podatke o piškotkih in žetonih za potrjevanje API dostopa, ki lahko v nekaterih primerih omogočijo hekerjem dostop do uporabniških računov tarče. Če napadalec pridobi dostop do računov socialnih omrežij tarče, lahko prek njih naprej širi svojo zlonamerno programsko opremo. Naprednejši virusi lahko tudi avtomatsko zamenjajo geslo na uporabniških računih tarče in tako podaljšajo čas, ki ga tarča potrebuje za povrnitev dostopa do svojega računa (Lakshmanan, 2022).

2.3.3 Okužene spletne strani

Digitalni kriminalci lahko okužijo naprave, povezane v internet z uporabo zlonamernih spletnih strani, ki ob uporabnikovem obisku poskušajo izkoristiti ranljivosti njegovega računalnika. Povezovanje okuženih naprav v omrežje, ki ga kriminalci izkoriščajo v svoj prid, imenujemo »botnet«. Te sisteme lahko uporabljajo za zbiranje podatkov o uporabnikih okuženih naprav prek zlonamerne programske opreme, ki beleži uporabnikove pritiske tipk. Botneti se lahko uporabljajo tudi za izvajanje kriminalnih dejavnosti, kot na primer napad porazdeljenega prekinjanja storitve, ko okuženi računalniki začenjajo pošiljati poizvedbe na določeno spletno mesto, ki ga želijo kriminalci preobremeniti (Fryer in drugi, 2015).

Prepričanje, da lahko uporabniki okužijo svojo napravo le na spletnih mestih, ki omogočajo pretočno deljenje datotek ali tistih z odraslimi vsebinami, se pogosto izkaže za nepravilno. Napadalci lahko okužijo legitimno spletno mesto, ki ga uporabijo za distribucijo svojih zlonamernih programov. Manj sofisticirano alternativo predstavlja uporaba spletnih naslovov, ki se od legitimnega naslova razlikujejo le za znak ali dva, in prežijo na uporabnike, ki se zmotijo pri ročnem vnašanju naslova spletnega mesta. Poleg tega obstajajo znaki, ki so si med seboj vizualno zelo podobni (pogost primer sta »l« in veliki »i«), s katerimi lahko zlikovci uporabnike zavedejo, da kliknejo na povezavo do okuženega spletnega mesta, ker niso pozorni, da je prikazan naslov »googIe.si« in ne »google.si« (Fryer in drugi, 2015).

Spletni posredniki in ponudniki storitev gostovanja spletnih strani nosijo odgovornost, da pomagajo preprečevati takšne zlorabe. Storitve v oblaku lahko to storijo z aktivnim

pregledovanjem in analizo datotek, ki jih gostijo na svojih strežnikih. Te datoteke lahko nato primerjajo s seznami poznane zlonamerne programske opreme, ki jih uporabljajo tudi protivirusni programi. Spletne strani in brskalniki bi lahko ozaveščali uporabnika o varnosti spletnega mesta, ki ga nameravajo obiskati. Če bi uporabnik izbral povezavo do spletnega mesta, ki nima vseh potrebnih varnostnih certifikatov, bi lahko trenutna spletna stran oz. uporabnikov brskalnik prikazal opozorilo, ki uporabnika vpraša, ali je popolnoma prepričan v njegovo legitimnost spletnega mesta, ki ga namerava obiskati (Fryer in drugi, 2015). Redna opozorila o posodobitvah uporabnikovega brskalnika lahko prav tako preprečijo marsikatero zlorabo, ki bi lahko nastala kot posledica uporabnikove malomarnosti, ker ni namestil nedavnih varnostnih popravkov (Hay Newman, 2023).

2.3.4 Človeški faktor

Čeprav se pogosto poroča o programskih hroščih in drugih tehničnih nepravilnostih, ki lahko pripeljejo do digitalnih vdorov, je le redko omenjeno, da je na koncu sistem toliko varen, kot so varni njegovi uporabniki. Hekerji pogosto izrabljajo socialni inženiring, ki je način vplivanja na posameznika z namenom pridobivanja informacij ali ogrožanja naprav v uporabnikovem omrežju. Namesto zlorab tehnoloških ranljivosti ti napadi izkoriščajo človeška čustva in navade. Tako lahko pod pretvezo, da predstavljajo uradnike legitimne organizacije, hekerji prepričajo svoje žrtve, da prostovoljno poženejo zlonamerno kodo misleč, da prihaja iz verodostojnega vira (Chetioui in drugi, 2022).

Napad socialnega inženiringa običajno poteka v naslednjih korakih (Chetioui in drugi, 2022):

- Preiskava: Napadalec izbere tarčo, razišče njeno ozadje in določi način napada.
- Ujemanje pozornosti: Napadalec se približa žrtvi, da bi vzpostavil odnos.
- Igra: Napadalec manipulira žrtev, da bi pridobil potrebne informacije.
- Izhod: Ko napadalec prejme potrebne informacije oz. tarča izvede želeno dejanje, napadalec prekine komunikacijo in se premakne na naslednjo tarčo (pri kateri ponovi omenjene korake).

V praksi obstajajo različne oblike socialnega inženiringa, ki se med seboj običajno razlikujejo predvsem v korakih ujemanja pozornosti in igre. Med pogostejše oblike spadajo (Chetioui in drugi, 2022):

- Napad z lažnim predstavljanjem: Napadalci se predstavljajo, da delajo za zaupanja vredno organizacijo z namenom manipulacije tarče. Z njimi lahko stopijo v kontakt prek lažnih e-sporočil, telefonskih klicev ali SMS-ov. Sporočila so zasnovana tako, da od prejemnikov zahtevajo določene osebne podatke in hkrati izgledajo dovolj verodostojno, da prejemniki ne podvomijo v njihovo legitimnost. Uporabnikove podatke lahko ukradejo tudi prek lažnih spletnih strani, ki od uporabnikov zahtevajo zasebne informacije, na primer gesla, naslov prebivališča itd. Pogost primer takšnega napada je

kontakt zaposlenih v podjetju s strani »Microsoftove tehnične podpore«, ki zaposleno osebo obvesti, da so zaznali na njeni napravi virus. Nato tarčo preusmerijo na »Microsoftovo« spletno stran, s katere naj prenese datoteko z varnostnimi popravki. Zaposlena oseba se ne zaveda, da je ta datoteka dejansko zlonamerna programska oprema.

- Nastavljanje vabe: Ti napadi uporabljajo vabe, da bi izzvali interes tarče, ki bi zasenčil posameznikove pomisleke glede varnosti njegovega početja. Vabe so pogosto USB ključi, lahko pa so tudi CD-ji ali drugi predmeti, s pomočjo katerih lahko napadalci ukradejo informacije. Napadalci nastavijo vabo na javnem mestu, kot so parkirišča, javna stranišča, parki itd. Ko žrtev vzame vabo in jo vstavi v svoj pametni telefon ali računalnik, vaba okuži žrtvino napravo z zlonamerno kodo. Vabe pa niso nujno oprijemljive. Prevaranti pogosto uporabljajo vabe v obliki brezplačnih pesmi, filmov ali video iger, ki jih lahko prenesemo brezplačno z interneta. Torrenti lahko vsebujejo zlonamerne programe, ki lahko okužijo uporabnikovo napravo, ko se nanjo prenesejo ali ko jim uporabnik dodeli zahtevane pravice za zagon na njegovi napravi.
- »Tailgating«: »Tailgating« se od prej omenjenih tehnik socialnega inženiringa razlikuje po tem, da ne uporablja spletne pošte ali drugih oblik digitalne komunikacije med prevaranti in žrtvami. Namesto tega se hekerji poskušajo približati svojim žrtvam skozi osebni stik. »Tailgating« se lahko uporablja za dostop do zavarovanih lokacij tako, da se hekerji pretvarjajo, da zares spadajo tja. Krinke so lahko najrazličnejše. Od poštnega uslužbenca, ki želi vstopiti v zgradbo, da bi dostavil pošiljko, do »uslužbenke iz druge enote«, ki ima polne roke in vljudno prosi varnostnika, da ji omogoči dostop brez potrebne identifikacije, ker se ji mudi na sestanek ali kaj podobnega.
- Quid Pro Quo: Ta pristop se od nastavljanja vabe razlikuje po tem, da prevaranti namesto vabe ponujajo tarči storitev v zameno za občutljive informacije. Med najpogostejše primere sodi pretvarjanje, da prevaranti delajo za IT podjetje in vračajo klic glede tehnične težave. Sčasoma bodo našli nekoga, ki je res imel omenjeno težavo. Lažna tehnična podpora od uporabnika zahteva gesla ali druge oblike identifikacije, da bi odpravili njegovo težavo. Manj prefinjene oblike »Quid Pro Quo« so lahko obrazci za neko tekmovanje na delovnem mestu ali različne ankete.

V tem poglavju sem predstavil definicijo in pomen kibernetske varnosti za uporabnike modernih tehnologij, največje digitalne vdore in najpogostejše razloge, ki lahko pripeljejo do digitalnih vdorov. Kriptovalute se od drugih digitalnih valut razlikujejo po tem, da se za svoja varnostna zagotovila zanašajo na verige blokov, ki uporabljajo napredno kriptografijo, namesto na zaupanja vredno osebo oz. entiteto (Rose, 2015). Zato bom v naslednjem poglavju predstavil razvoj kriptografije v času, praktične uporabe tehnologije veriženja blokov in primerjal tehnične lastnosti različnih decentraliziranih platform, ki omogočajo prenos in uporabo kriptovalut.

3 RAZVOJ KRIPTOGRAFIJE IN VERIG BLOKOV

Verige blokov oz. blockchain kot porazdeljena računalniška platforma uporabnikom omogoča uporabo programske opreme (t. i. pametne pogodbe) brez vključevanja zaupanja vredne tretje osebe (Singh in drugi, 2020). To pa bi bilo v praksi zelo težko izvedljivo brez uporabe kriptografije. Ta zagotavlja, da je transakcije, ki so že vključene v blockchain, računsko nepraktično razveljaviti (Nakamoto, 2008). Ker brez današnjega poznavanja kriptografije blockchain ne bi bil mogoč, bom prvo podpoglavje posvetil pregledu razvoja in uporabe te tehnologije v zgodovini.

3.1 Pregled razvoja šifrirnih algoritmov v času

Kriptografija je orodje za zagotavljanje zaupnosti sporočil pred 'sovražniki' ali ljudmi, ki nimajo pravice dostopa do njih. Arheologi so našli dokaze, da so se že stari Egipčani ~1900 pr. n. št. zavedali pomembnost šifrirane komunikacije med virom informacije in prejemnikom. Skoraj 4000 let od takrat je človeštvo odkrivalo nove načine (de)šifriranja informacij. Nekaj poznanih pristopov bom predstavil v tem poglavju. Pred 2000 leti je Julij Cezar uporabil osnovno preklopno kodo. Koda je delovala po principu zamika znakov abecede za neko število mest. Če označimo število zamikov s črko N, lahko predpostavimo, da bo črka, ki je v abecedi na mestu X, v šifriranem sporočilu predstavljena s črko na mestu X+N. Slika 1 prikazuje primer osnovne preklopne kode kjer je N = 22. Tak način šifriranja spada med najbolj preproste primere šifriranja in ga lahko danes z lahkoto dešifriramo (Kumar Sharma in drugi, 2022).

Slika 1: Primer osnovne preklopne kode

A	B	C	Č	D	E	F	G	H	I	J	K	L
V	Z	Ž	A	B	C	Č	D	E	F	G	H	I
M	N	O	P	R	S	Š	T	U	V	Z	Ž	
J	K	L	M	N	O	P	R	S	Š	T	U	

Vir: prirejeno po Kumar Sharma in drugi (2022).

Preprosta nadomestna koda oz. eno-abecedna šifra zamenja znake z določenim šifrirnim ključem. Ta ključ določi preslikavo znakov v razmerju 1:1 med izhodiščno in šifrirno abecedo, kjer je vsak znak zamenjan s svojim znakom. Slika 2 prikazuje primer šifriranja s preprosto nadomestno kodo. Za dešifriranje sporočila moramo postopek šifriranja ponoviti v obratni smeri.

Slika 2: Primer preproste nadomestne kode

A	B	C	Č	D	E	F	G	H	I	J	K	L
J	C	R	A	G	M	U	Č	F	S	N	Z	H
M	N	O	P	R	S	Š	T	U	V	Z	Ž	
Ž	K	D	T	V	B	L	O	Š	E	I	P	

Vir: prirejeno po Kumar Sharma in drugi (2022).

Transpozicijsko šifriranje zašifrira sporočilo tako, da izhodiščno sporočilo razdelimo v enako dolge odseke, ki jih zapišemo kot vrstice v tabeli. Izhodiščno besedilo: »ANALIZA TVEGANJ UPORABNIKOV KRIPTOVALUT« lahko razdelimo na 3 odseke dolžine 12 znakov, kot je prikazano na sliki 3.

Slika 3: Primer razdelitve izhodiščnega besedila pri transpozicijskem kodiranju

A	N	A	L	I	Z	A	T	V	E	G	A
N	J	U	P	O	R	A	B	N	I	K	O
V	K	R	I	P	T	O	V	A	L	U	T

Vir: prirejeno po Kumar Sharma in drugi (2022).

Nato določimo šifrirni ključ kot naključno kombinacijo števil od 1 do N, kjer je N število črk v posameznem odseku sporočila. Slika 4 prikazuje primer uporabe šifrirnega ključa: 9 12 1 3 7 2 10 6 5 8 4 11 na podatkih s slike 3.

Slika 4: Primer uporabe šifrirnega ključa pri transpozicijskem kodiranju

9	12	1	3	7	2	10	6	5	8	4	11
A	N	A	L	I	Z	A	T	V	E	G	A
N	J	U	P	O	R	A	B	N	I	K	O
V	K	R	I	P	T	O	V	A	L	U	T

Vir: prirejeno po Kumar Sharma in drugi (2022).

Stolpce črk zamenjamo med seboj tako, kot določa šifrirni ključ. Šifrirano besedilo ustvarimo z zapisom zaporedja črk, kjer začnemo v zgornjem levem kotu in se pomikamo dol in desno na vrh novega stolpca, ko pridemo do dna. Če sledimo navodilom transpozicijskega šifriranja s podatki iz primera, dobimo šifrirano sporočilo: AUR ZRT LPI GKU VNA TBV IOP EIL ANV AAO AOT NJK, kot prikazuje slika 5.

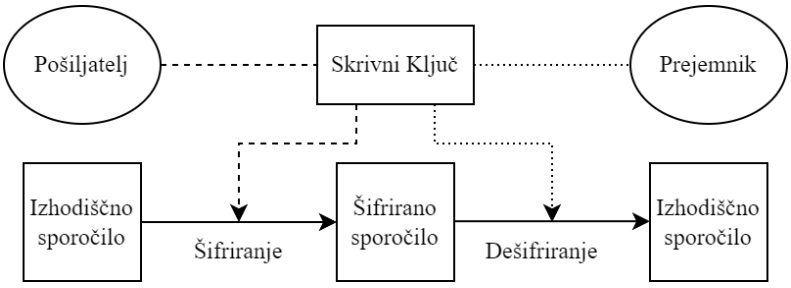
Slika 5: Primer transpozicijskega kodiranja

1	2	3	4	5	6	7	8	9	10	11	12
A	Z	L	G	V	T	I	E	A	A	A	N
U	R	P	K	N	B	O	I	N	A	O	J
R	T	I	U	A	V	P	L	V	O	T	K

Vir: prirejeno po Kumar Sharma in drugi (2022).

Šifriranje s simetričnim ključem uporablja za šifriranje in dešifriranje podatkov isti ključ, kot je razvidno na sliki 6. Skrivni ključ predstavlja zaupni podatek, ki mora biti dostopen vsem uporabnikom zaupnega komunikacijskega kanala. Cezarjeva šifra, preprosta nadomestna šifra in transpozicijsko šifriranje spadajo med primere simetrične enkripcije (Kumar Sharma in drugi, 2022).

Slika 6: Diagram simetričnega šifriranja

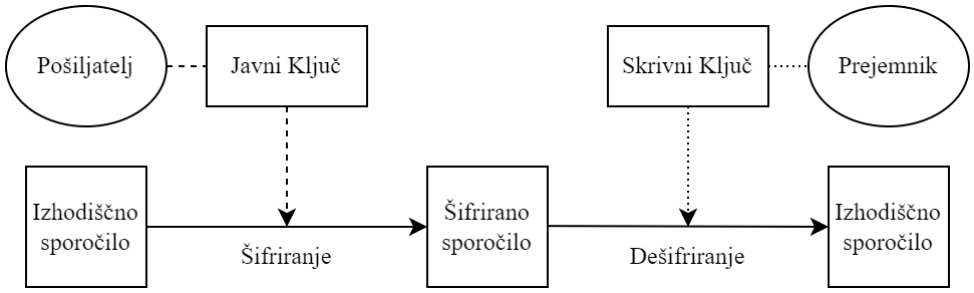


Vir: prirejeno po Kumar Sharma in drugi (2022).

Ena izmed slabosti simetričnega šifriranja je, da morata pošiljatelj in prejemnik dostopati do skupnega skrivnega ključa. Asimetrično šifriranje omogoča, da pošiljatelj s svojim javnim ključem zašifrira sporočilo, ki ga lahko prejemnik dešifrira z lastnim skrivnim ključem (Kumar Sharma in drugi, 2022). Slika 7 prikazuje diagram asimetričnega šifriranja, ki omogoča komunikacijo brez potrebe po dostopu do skupnega skrivnega ključa.

Slika 8 prikazuje diagram homomorfnega šifriranja, ki podatke zašifrira tako, da jih lahko procesiramo brez poznanja izhodiščnih vrednosti. Dešifriran rezultat funkcije, ki uporablja zašifrirane vrednosti, je isti, kot če bi v to funkcijo vstavili dešifrirane vhodne vrednosti. To omogoča hrambo in procesiranje zaupnih podatkov v oblaku in v drugih oblikah shrambe, kjer nimamo popolnega nadzora nad lastnimi podatki (Kumar Sharma in drugi, 2022).

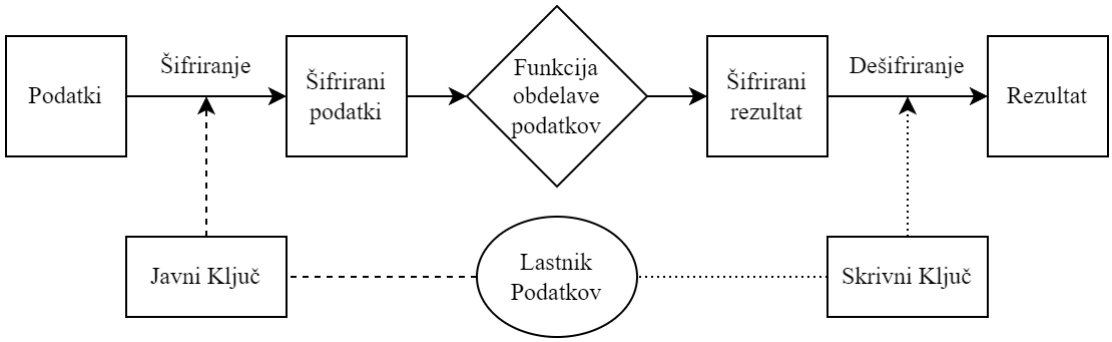
Slika 7: Diagram asimetričnega šifriranja



Vir: prirejeno po Kumar Sharma in drugi (2022).

SSL s pomočjo asimetričnega šifriranja omogoča varno komunikacijo med spletnim strežnikom in odjemalcem. Uporaba SSL v spletnih komunikacijah ima dve pomembni lastnosti. Prvič, podatki so zašifrirani, preden zapustijo pošiljateljevo napravo, in dešifrirani šele na prejemnikovi napravi, kar omogoča pošiljanje občutljivih podatkov prek komunikacijskega kanala. Drugič, potrjevanje prek SSL certifikatov omogoča preverbo avtentičnosti spletne strani, do katere dostopamo (Kernel, 2019). Zadnja verzija SSL je bila SSL 3.0, objavljena leta 1996. Leta 1999 je SSL nadomestil TLS, ki je odpravil varnostne ranljivosti, povezane s protokolom SSL. Danes v večini primerov uporabljamo TLS 1.3, ki je v uporabi od leta 2018 (Kinsta, 2022). Uporaba varnostnih certifikatov omogoča tehnologijo HTTPS, ki je danes standard za vzpostavljanje varnih internetnih povezav.

Slika 8: Diagram homomorfnega šifriranja



Vir: prirejeno po Kumar Sharma in drugi (2022).

3.2 Primeri praktičnih uporab tehnologije veriženja blokov

Kot sem navedel že na začetku poglavja, je blockchain porazdeljena računalniška platforma, kar pomeni, da za razliko od klasičnih baz podatkov informacije niso shranjene zgolj na eni napravi ali lokaciji. Porazdelitev shrambe in posledična redundanca podatkov omogoča uporabnikom dostop do njih tudi, če nekatera vozlišča platforme prenehajo delovati. Zapisani podatki si sledijo v zaporedju, v katerem so bili dodani v verigo. Blockchain ne spreminja zaporedja blokov zaradi decentraliziranosti svoje infrastrukture in družbenega

konsenza. Platforme z dovolj centralizirano infrastrukturo lahko po potrebi spreminjajo vsebino in zaporedje blokov, če pride do soglasja med lastniki večinskega deleža infrastrukture (rudarji, strežniki) platforme. Do podatkov, ki so zapisani na javnih verigah blokov, lahko dostopa vsakdo. Zato firme pogosto uporabljajo zasebne oblike blockchaina, do katerih lahko dostopajo le potrjeni udeleženci (Singh in drugi, 2020).

Na večini sodobnih verig blokov lahko poganjamo programe, imenovane pametne pogodbe. Ti programi omogočajo deterministično izvedbo določene funkcije brez potrebe po zaupanja vredni tretji osebi, ki bi jamčila izvedbo neke funkcije. Uporaba takšne logike pa ima tudi svojo ceno. Ker so pametne pogodbe programska oprema, obstajajo podobne varnostne grožnje kot pri drugih digitalnih tehnologijah. Pisanje varnih pametnih pogodb je lahko zelo zahtevno zaradi različnih logik poslovanja in potencialnih ranljivosti v programskih jezikih in platformah, ki jih uporabljajo. Nekatere primere uporabe verig blokov in pametnih pogodb bom predstavil v tem poglavju (Singh in drugi, 2020).

3.2.1 Decentralizirana finančna infrastruktura

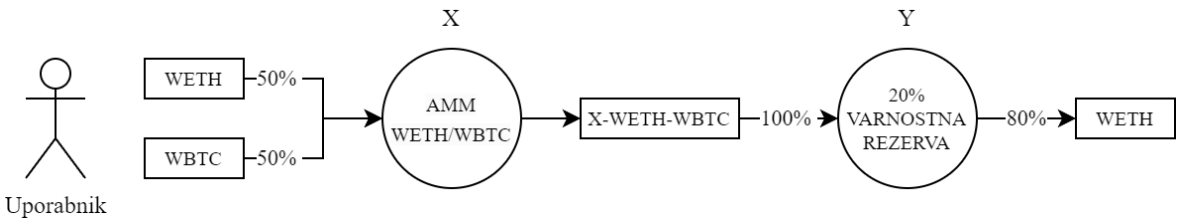
Glede na ime lahko predpostavljamo, da je namen uporabe kriptovalut podoben uporabi fiat valut, ki jih danes uporabljamo za vsakdanje prenose vrednosti. Bitcoin je nastal kot odziv na finančno krizo leta 2008. Njegov algoritem vsebuje zagotovila, da skupno število kovancev v obtoku nikoli ne bo preseglo 21 milijonov. Zato Bitcoinu marsikdo pripisuje lastnost hrambe vrednosti, ker mu algoritem onemogoča hiperinflacijo enot v obtoku (Cunha in drugi, 2021).

Z uporabo pametnih pogodb lahko ustvarimo aplikacije, ki opravljajo funkcije finančnih instrumentov na verigah blokov. Pametne pogodbe lahko služijo kot nevtralni posrednik med različnimi akterji, ker je njihova koda javno dostopna in deterministična. Z njimi lahko na verigah blokov izvajamo finančne storitve, ki poslujejo popolnoma transparentno, ker lahko vsakdo v vsakem trenutku vidi njihova sredstva in obveznosti. Tako lahko vsakdo revidira njihovo poslovanje in ima popoln vpogled v njihovo finančno stanje. Ta pristop se močno razlikuje od obstoječih podjetij, ki rezultate svojega poslovanja objavljajo le nekajkrat letno. Pomembna lastnost pametnih pogodb je tudi uporaba standardizirane tehnologije žetonov, ki so lahko kompatibilni z več pametnimi pogodbami. Takšen ekosistem si lahko predstavljamo kot škatlo finančnih Lego kock, ki jih lahko sestavljamo skupaj v kompleksnejšo strukturo (Singh in drugi, 2020).

Primer uporabe več pametnih pogodb lahko vidimo na sliki 9. Ta prikazuje uporabnika, ki doda sorazmerno vrednost žetonov WETH in WBTC v bazen avtomatiziranega vzdrževalca trga X. V zameno dobi žetone X-WETH-WBTC, ki predstavljajo njegov delež omenjenega bazena. Vrednost novih žetonov je načeloma sorazmerna gibanju cene WETH in WBTC. Nove žetone X-WETH-WBTC lahko uporabnik uporabi za jamstvo v pametni pogodbi Y. V zameno za vplačilo teh žetonov lahko uporabnik vzame posojilo WETH, vrednost katerega ne sme presegati vrednosti jamstva in neke varnostne rezerve, ki jo določa pametna

pogodba. Varnostna rezerva pogodbe Y je 20 %, zato lahko uporabnik vzame posojilo do maksimalno 80 % vrednosti jamstva X-WETH-WBTC.

Slika 9: Primer uporabe decentralizirane finančne infrastrukture



Vir: lastno delo.

3.2.2 Dobavne verige

Industrija 4.0 ima velik vpliv tudi na dobavne verige. Internet stvari, robotizacija, 3D tiskanje, virtualna resničnost, umetna inteligenca in blockchain spadajo med tehnologije, ki ponujajo dodatno učinkovitost na tem področju. Ker so med značilnimi lastnostmi blockchaina tudi preglednost informacij, zanesljivost sistemov in splošna učinkovitost, predstavlja ta tehnologija potencialno platformo za nadaljnjo digitalizacijo dobavnih verig Posamezni blok v verigi poleg seznam transakcij vsebuje tudi podatke o času nastanka bloka in indeks predhodnega bloka. Ker so podatki na verigah blokov dostopni vsem sodelujočim, lahko z uporabo deljene baze podatkov zagotavljamo transparenten vpogled v stanje sistema. Transakcije lahko vsebujejo podatke o zalogah, oddanih in sprejetih pošiljkah, oddanih naročilih ipd. Tako lahko vsi sodelujoči v dobavni verigi sledijo svojim procesom in procesom drugih, od katerih so odvisni. Poleg tega se lahko na nepričakovane spremembe hitreje odzovejo, kot če bi se zanašali na podatke zunanjega izvajalca (Sunmola in Burgess, 2023).

3.2.3 Digitalni zbirateljski predmeti

Enote valute lahko posamezniki prosto izmenjujejo med seboj, ker so med seboj izmenljive. Evrske kovance lahko v trgovini zamenjamo za isto količino dobrin ne glede na državo izvora kovanca. Temu načelu sledijo tudi mnoge kriptovalute, vendar ne vse. Neizmenljivi žetoni se med seboj lahko ločijo po različnih lastnostih, ki jih je določil njihov stvaritelj. Tako je na verigi jasno razvidno, v kateri denarnici je določen žeton, ker obstaja le ena verzija z njegovimi parametri (Chandra, 2022).

Med pogoste primere uporabe digitalnih zbirateljskih predmetov spadajo različne digitalne umetnine, slike, liki in predmeti v video igrah ipd. Ena izmed glavnih karakteristik digitalnih zbirateljskih predmetov je njihova redkost, ki do nastanka bitcoina ni bila praktično izvedljiva za stvari v digitalni obliki. Poleg tega imajo veliko prednost pred zbirateljskimi

predmeti v fizičnem svetu, ker se ne morejo obrabiti ali drugače poškodovati (v večini primerov), kar bi lahko negativno vplivalo na njihovo vrednost (Chandra, 2022).

Nekateri prodajalci fizičnih dobrin in storitev svojim strankam dajo tudi kriptografski žeton, ki ima vlogo potrdila, da je posameznik res kupil določeno dobrino ali storitev. Tako bi lahko ob nakupu oblačila poznane znamke poleg fizičnega izdelka prejeli tudi kriptografski žeton, ki bi hranil podatke o kupljenem izdelku, kot na primer ime ustvarjalca, vrsta materiala, iz katerega je narejen, čas in lokacija nakupa in druge informacije (Breia, 2022).

3.2.4 Decentralizirana identiteta

Pomembna lastnost neizmenljivih žetonov je njihova standardizirana oblika in fleksibilnost podatkov, ki jih lahko hranijo (lahko si jih predstavljamo kot seznam parov ključ – vrednost). Tako lahko v njih zapišemo različne vrednosti, ki jih naredijo unikatne, kot sem že omenil v prejšnji točki. Decentralizirana identiteta se od zbirateljskih predmetov razlikuje po tem, da v večini primerov ni prenosljiva med računi. Praktični primeri lahko vključujejo pridobljene certifikate, dokazila o udeležbi, dosežke in druge podatke o posamezniku, ki pripadajo le njemu in niso prenosljivi na druge osebe. Pomanjkanje prenosljivosti takšnih žetonov daje močna zagotovila o njihovi legitimni povezavi z lastnikom računa, ker jih ni mogel kupiti ali izmenjati z drugimi uporabniki (Buterin, 2022a).

3.3 Primerjava tehničnih lastnosti verig blokov

Verige blokov kot platforme za decentralizirano infrastrukturo optimizirajo svoje tehnične lastnosti glede na primere uporabe, ki jih nameravajo podpirati. V tem poglavju bom predstavil pregled programskih jezikov, ki jih podpirajo različne verige blokov, primerjal lastnosti trenutno najbolj pogostih mehanizmov soglasja ter predstavil trilemo razširljivosti, ki je osnova predpostavke, da je bolj smiselno imeti več specializiranih verig blokov kot eno, ki poskuša najti kompromis med vsemi primeri uporabe.

3.3.1 Pregled različnih platform in podprtih programskih jezikov

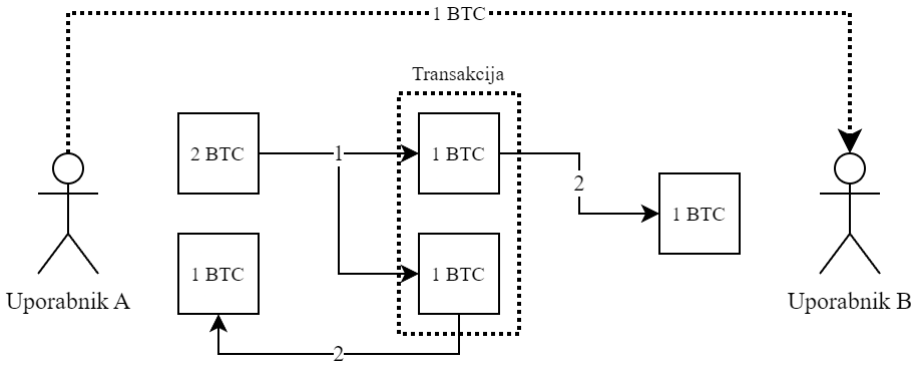
Nick Szabo je leta 2005 predstavil koncept zavarovanja lastninskih pravic s pooblastili lastnika, s katerim bi v razpršenih zbirkah podatkov beležili podatke o zemljiških pravicah. Ti podatki bi lahko bili temelj za različne aplikacije, ki bi dostopale do njih. Sistem v praksi ni zaživel, ker takrat še ni bilo tehnologije za razpršene zbirke podatkov. Kmalu po nastanku Bitcoina, so zaživele mnoge alternativne uporabe decentraliziranih podatkov. Namecoin je eden izmed prvih primerov alternativne uporabe, ki bi bil razpršena zbirka podatkov za registracijo imen. Decentralizirani protokoli, med katere sodita tudi Bitcoin in Tor, uporabljajo psevdonaključno zaporedje znakov za identifikacijo uporabnikov. Namecoin bi lahko bil razpršena alternativa sistemu DNS, ki prevaja imena spletnih domen med ljudem berljivo obliko in IP naslovi, ki jih za komunikacijo uporabljajo naprave (Buterin, 2022b).

Kasneje je na tem principu nastal ENS, ki omogoča registracijo naslovov s končnico ».eth« kot alternativo psevdonaključnemu nizu alfanumeričnih znakov.

Programski jezik, ki je implementiran v Bitcoin, ima določene omejitve, ki predstavljajo ovire za gradnjo pametnih pogodb, med katere sodijo (Buterin, 2022b):

- Pomanjkanje Turingove popolnosti: skriptni jezik Bitcoina sicer podpira veliko različnih funkcij, vendar pa mu manjka pomembna kategorija, ki so zanke. To pa zato, da bi se izognili potencialnim neskončnim ponavljanjem med preverjanjem transakcij. Teoretično so lahko zanke še vedno implementirane prek zaporedja if-izjav, kar pa pogosto vodi do obsežne in nepregledne kode.
- Slepota vrednosti: sistem UTXO ne omogoča finega določanja vrednosti, ki jo lahko prenašamo med računi. Slika 10 prikazuje uporabnika A, ki ima v denarnici 2 BTC in želi uporabniku B poslati 1 BTC. V tem primeru bi moral na omrežje oddati transakcijo, v kateri bi poslal 1 BTC uporabniku B in 1 BTC nazaj samemu sebi, ker mora transakcija vključevati vsa sredstva iz denarnice uporabnika A.

Slika 10: Primer pošiljanja transakcije UTXO



Vir: prirejeno po Buterin (2022b).

- Pomanjkanje stanja: sredstva v sistemu UTXO so lahko porabljena ali neporabljena. Ta pristop otežuje izvedbo pogodb, ki bi se izvajale v več stopnjah. Zato na Bitcoinu ne moremo direktno izvajati opcijskih pogodb, decentraliziranih menjalnic in drugih kompleksnejših operacij. Binarno stanje v kombinaciji s slepoto vrednosti onemogoča še eno pomembno aplikacijo, omejitve plačil;
- Slepota blockchaina: sistem UTXO dostopa le do podatkov, ki se nanašajo direktno na transakcije in prikrajša skriptni jezik za potencialno dragocen vir naključnosti. Ta bi se lahko uporabljal v aplikacijah na področju iger na srečo, umetnosti, simulacijah in še kje.

S temi in drugimi argumenti je Vitalik Buterin leta 2013 utemeljeval potrebo po naprednejšem decentraliziranem omrežju, na katerem bi lahko gradili kompleksnejše aplikacije. Ethereumov programski jezik ne bi bil omejen s prej navedenimi pomanjkljivostmi. Na njem bi lahko vsakdo kodiral pametne pogodbe in decentralizirane

aplikacije s poljubnimi pravili lastništva, oblikami transakcij in funkcijami sprememb stanja. Stanje Ethereuma sestoji iz objektov, imenovanih »računi«, in prehodi stanja, ki predstavljajo direkten prenos vrednost in informacij med računi. Takšen pristop omogoča širšo funkcionalnost kot izhodiščni sistem UTXO. Zato večina modernih verig blokov podpira pametne pogodbe in decentralizirane aplikacije. Različni ekosistemi podpirajo programe, spisane v različnih jezikih, kot je razvidno iz tabele 1.

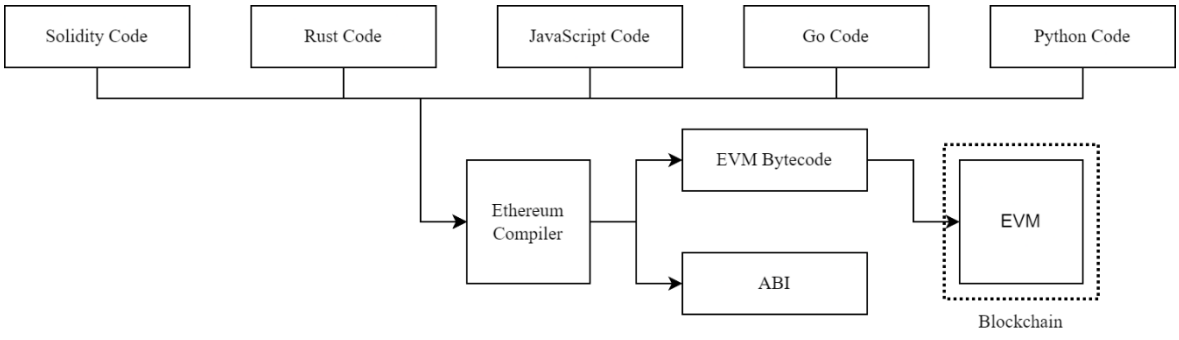
Tabela 1: Programski jeziki in blockchaini, ki jih podpirajo

Solidity	Ethereum, Binance Smart Chain, Polygon, Avalanche C-Chain, Hedera Hashgraph
Java	Ethereum, Hyperledger Fabric, IOTA, Neo
Python	Ethereum, Neo, Hive
C++	Bitcoin, Ripple, Litecoin, Stellar
C#	Neo, IOTA Stratis
Rust	Ethereum, Polkadot, Solana, Near, Elrond
Go	Ethereum, Gochain, Hyperledger

Vir: prirejeno po Afreen (2023), Wackerow (2022) in Weston (2022).

Nekateri ekosistemi podpirajo tudi širši nabor programskih jezikov, ki se pred zapisom na verigo blokov prevedejo v strojno kodo, ki jo podpira določen ekosistem. Kot primer takšnega ekosistema lahko navedemo Ethereum, ki glede na prej omenjeno tabelo podpira programske jezike: Solidity, Go, Python, JavaScript, Rust in tudi nekatere druge, ki niso navedeni v tabeli. Programi, spisani v teh jezikih, se pred zapisom decentraliziranih aplikacij na verigo blokov prevedejo v strojno kodo, ki ni berljiva ljudem, da bi optimizirali količino podatkov na verigi blokov in posledično stroške, povezane z njimi. Proces prevajanja kode iz različnih jezikov v zapis na verigi blokov prikazuje diagram na sliki 11.

Slika 11: Proces prevajanja kode iz različnih programskih jezikov



Vir: prirejeno po Shevtekar in drugi (2022).

3.3.2 Dokazilo o delu in dokazilu o deležu

Ideje o digitalnih plačilnih sredstvih so se začele razvijati v 80. letih 20. stoletja. Anonimni protokoli so se večinoma zanašali na slepe podpise, ki jih je vpeljal David Chaum (več o tem v poglavju 3.1). Tak pristop je omogočal visoko raven zasebnosti, vendar pa ni postal splošno uporabljen, ker se je še vedno zanašal na zaupanja vredno tretjo osebo. B-money, ki ga je leta 1998 ustvaril Wei Dai, je bil naslednji poskus vpeljave anonimnega, distribuiranega elektronskega finančnega sistema (Reiff, 2021). Bitcoin je prva decentralizirana digitalna valuta, ki jo je leta 2009 predstavil posameznik (ali skupina ljudi), znan pod imenom Satoshi Nakamoto. Dokazilo o delu, ki ga uporablja Bitcoin, je sočasno rešilo več problemov, povezanih s predhodnimi implementacijami digitalnih valut. Omogočilo je preprost in relativno učinkovit algoritem soglasja med vozlišči omrežja, ki določa trenutno stanje omrežja in katere transakcije mu bodo dodane. Poleg tega pa dokazilo o delu vsebuje mehanizem, ki dovoljuje prost dostop do procesa soglasja. Svobodno izvajanje transakcij reši problem izvajanja pritiska na zaupanja vredno tretjo osebo, da cenzurira transakcije določenega uporabnika omrežja. Dodajanje novih transakcij prek dokazila o delu zahteva strojno opremo in električno energijo. Cena transakcij se giblje sorazmerno s povpraševanjem in posledično zmanjšuje verjetnost prekinitve delovanja omrežja zaradi prevelikega števila transakcij (Buterin, 2022b). Dokazilo o deležu je alternativa dokazilu o delu na področju mehanizmov soglasja. Dokazilo o deležu moč vozlišča določa sorazmerno s količino enot valute, ki jih ima vozlišče v lasti. Medtem ko je dokazilo o delu lahko zelo potratno z vidika materialnih sredstev (proizvodnja in vzdrževanje strojne opreme, električna energija), je mehanizem dokazila o deležu načeloma procesorsko manj potraten, ker se moč vozlišča ne določa prek njegovih procesorskih zmogljivosti. Zagovorniki dokazila o delu pogosto kritizirajo dokazilo o deležu, češ da je pristransko do manjših lastnikov valute, ki redkeje sodelujejo v procesu soglasja, vendar pa je podrobnejša analiza takšnih trditev zunaj obsega magistrskega dela (Shevchenko, 2020).

3.3.3 Trilema razširljivosti

Trilema razširljivosti govori o potrebi po sklepanju kompromisov z vidika treh pomembnih lastnosti tehnologije veriženja blokov:

- Razširljivost: Razširljivost se nanaša na količino transakcij, ki jih lahko veriga blokov potrdi v določenem času in se v praksi pogosto meri v številu transakcij, ki jih lahko vozlišča potrdijo v času 1 sekunde (TPS). Ker vsaka posamezna transakcija zahteva določeno količino procesorskega časa in posredno električne energije, blockchaini z visokim TPS-om pogosto potrebujejo vozlišča z napredno strojno opremo, da lahko procesirajo veliko količino transakcij (Buterin, 2021).
- Decentraliziranost: Decentralizirana omrežja lahko delujejo brez potrebe po centraliziranih akterjih, ki bi zahtevali določeno mero zaupanja s strani uporabnikov omrežja. Pogosta metrika decentralizacije omrežja je število neodvisnih potrjevalnih

vozlišč. Decentralizirana omrežja težje cenzurirajo transakcije, ker posamezni akterji težko dosežejo prevladujoč delež potrjevalnih vozlišč, ki določajo, katere transakcije so vključene v naslednji blok. Primer tega je bila vzpostavitev sankcij ameriškega Urada za nadzor tujega premoženja (OFAC) glede uporabe pametne pogodbe Tornado Cash, ki omogoča mešanje žetonov na omrežju Ethereum (U.S. Department of the Treasury, 2022). Na spletni strani mevwatch.info lahko vidimo delež Ethereumovih blokov, ki so bili skladni z OFACovimi sankcijami v določenem obdobju. Dne 14. januarja 2023 je ta delež predstavljal 68 % v zadnjih 24 urah (Labrys, brez datuma). To pomeni, da uporabniki lahko še vedno komunicirajo s sankcionirano pametno pogodbo, vendar pa morajo čakati dlje, da se njihova transakcija zapiše v verigo blokov, ker je določen del potrjevalnih vozlišč ni pripravljen vključiti (Buterin, 2021).

- Varnost: Varnost omrežja določa, koliko surovin mora zlonamerni akter uporabiti, da bi lahko vplival na delovanje omrežja, oz. kolikšen delež omrežja mora imeti pod svojim nadzorom, da lahko upravlja z njim. Ta delež se lahko zelo razlikuje med različnimi tehnologijami. Če bi napadalec želel prevzeti nadzor nad omrežjem Bitcoin, bi za to potreboval večinski delež računskih zmogljivosti omrežja, iz česar izhaja tudi ime »51 % napad« (Nakamoto, 2008). Blockchain, ki se za svojo varnost zanaša na dokazilo o delu, svojo varnost prikazuje s stopnjo zgoščevanja, ki se v primeru Bitcoina trenutno meri v terahashih na sekundo (TH/s). Pri dokazilu od deležu je pomembno, da so lastniški deleži enakomerno porazdeljeni, da bi preprečili posamezni entiteti nadzor nad večino potrjevalnih vozlišč. Nekateri mehanizmi soglasja vsebujejo tudi obrambne mehanizme, ki zmanjšujejo vpliv zlonamernih deležnikov. V takem primeru so potrjevalna vozlišča izpostavljena potencialnim izgubam sredstev, če nepravilno sodelujejo v mehanizmu soglasja ali poskušajo v verigo vključevati neveljavne transakcije (Buterin, 2021).

V praksi se zasnova tehnologij veriženja blokov pogosto zanaša na prioritizacijo dveh lastnosti na račun tretje. Tako lahko večino pristopov razdelimo v eno izmed treh kategorij:

- Decentraliziran in varen blockchain: tradicionalni blockchain vključuje Bitcoin, Litecoin in druge podobne platforme. Vsak njihov uporabnik naj bi poganjal svoje polno vozlišče, ki bi preverjalo ustreznost transakcij na verigi blokov. Takšen pristop omogoča decentralizacijo in varnost, ne pa tudi razširljivosti;
- Razširljiv in varen blockchain: blockchaini z visokim TPS-jem se zanašajo na manjše število vozlišč (pogosto 10-100), ki vzdržujejo soglasje med seboj. Razlog za manjše število vozlišč je pogosto dejstvo, da število komunikacijskih kanalov med N-vozlišči narašča s kvadratom števila vozlišč: N(N-1)/2. Ker morajo vozlišča stalno komunicirati med seboj, da vzdržujejo soglasje o stanju, bi lahko preveliko število vozlišč privedlo do preobremenitve komunikacijskih kanalov ali strojne opreme vozlišča. To omogoča omrežju razširljivost in varnost, vendar pa ga zaradi relativno majhnega števila vozlišč ne moremo imeti za decentraliziranega;
- Decentraliziran in razširljiv blockchain: več-verižni ekosistemi imajo različne aplikacije na različnih verigah blokov in uporabljajo medverižno komunikacijo med aplikacijami.

Tak ekosistem je decentraliziran in razširljiv, ampak ni varen, ker lahko napadalec s pridobitvijo večinskega nadzora nad eno verigo v ekosistemu posredno povzroči škodo tudi aplikacijam na drugih verigah v tem ekosistemu.

Drobljenje (angl. Sharding) naj bi predstavljalo rešitev trileme razširljivosti in omogočilo izgradnjo ekosistema, ki mu ne bi bilo treba sklepati kompromisov na nobenem izmed treh omenjenih področij.

4 RAZVOJ IN POMEMBNOST VARNE HRAMBE KRIPTOVALUT

4.1 Pregled zgodovine razvoja kriptovalut

Pred 70. leti 20. stoletja so kriptografijo uporabljali predvsem v vojski za vzpostavljanje varnih komunikacij. Raziskave so opravljale obveščevalne agencije (GCHQ, NSA, itd.) ali pooblaščeni laboratoriji (IBM) (Calderbank, 2007). V tistem času je bilo na splošno predpostavljeno, da ni mogoče vzpostaviti varne komunikacije med dvema napravama, če nekdo prisluškuje sporočilom, ki si jih izmenjujeta. Ralph Merkle je med svojim študijem računalništva razvil koncept, ki ga mnogi niso jemali resno. Informacija o njegovem odkritju je sčasoma prišla do Diffieja, ki je skupaj s Hellmanom nadgradil Merklov koncept in ga objavil v dokumentu, imenovanem: »Nove smeri v kriptografiji« leta 1976. Koncepti, predstavljeni v tem dokumentu, so danes uporabljeni tudi za zavarovanje verig blokov. Kasneje se je izkazalo, da je bil pravzaprav GCHQ prvi, ki je odkril kriptografijo javnih ključev. NSA je sicer imel dostop do tehnologije, vendar tega niso smeli razkriti javnosti zaradi zaupne klasifikacije (Diffie in Hellman, 1976).

David Chaum je izvedel za kriptografijo iz prej omenjenega dokumenta, ki sta ga objavila Diffie in Hellman. Med študijem kriptografije je identificiral področje, ki je bilo prej spregledano – metapodatke. Čeprav je uporaba javnega ključa zašifrirala sporočilo, je bila to le delna rešitev problema zasebnega komuniciranja. Podatki o pošiljatelju, naslovniku in času sporočila lahko predstavljajo tveganje za zasebnost. Chaum je v svoji diplomski nalogi predstavil idejo anonimnega protokola za pošiljanje sporočil prek mešalnega omrežja, ki bi zaščitilo identiteto pošiljateljev in čas pošiljanja sporočil. To omrežje bi sestavljala vozlišča, ki bi uporabljala javno kriptografijo za potrjevanje sporočil. Vozlišča bi si med seboj pošiljala informacije, da bi zakrila identiteto izhodiščnega pošiljatelja in čas pošiljanja njegovega sporočila. Med načrtovanjem omrežja je zavrgel idejo uporabe enega potrjevalca sporočil, ker je menil, da ga je mogoče zlahka ogroziti, in namesto tega vztrajal, da bi v idealnem primeru lahko imel vsak udeleženec to avtoriteto (Chaum, 1981). Poleg tega je verjel v pomembnost zasebnosti posameznikovih podatkov. V svetu, ki je prek interneta postajal vse bolj povezan, je kriptografija predstavljala potencialno rešitev problema neomejenega zbiranja podatkov o uporabnikih. Kriptografija je digitalni zakon, ki ga uveljavljajo pravila matematike. Posamezniki, ki želijo imeti zasebnost, lahko nadzorujejo

in varujejo svoje podatke z uporabo kriptografije. Leta 1990 je ustanovil podjetje Digicash, ki je ustvarilo prvi digitalni denarni sistem (Hamacher, 2022).

Okrog preloma tisočletja je nastalo mnogo tehnoloških podjetij, kot so Google (1998), Paypal (1998), Facebook (2004), YouTube (2005), ki jih imamo danes za stalnice. Čeprav je ameriška vlada po napadu 11. 9. 2001 začela izvajati poostren nadzor nad digitalnimi komunikacijami, so še vedno obstajali protokoli, ki so sledili cypherpunkovskim načelom. Med bolj poznane sodita BitTorrent, ki omogoča pretočno deljenje datotek, in TOR, ki omogoča anonimno komunikacijo med napravami. Med poznejše projekte, ki so nastali na načelu odprte kode, proste komunikacije in osebne svobode, sodijo Pirate Bay, Wikileaks, Silk Road in tudi Bitcoin (Pilkington, 2021). Danes se zdi Bitcoin nekaj povsem vsakdanjega. Zato lahko pozabimo, koliko raziskav je bilo vloženih v to, da lahko danes dostopamo do tehnologije blockchaina.

Ker je bila izvorna koda Bitcoina javno dostopna, so kmalu po njegovem nastanku začele nastajati alternativne verige blokov. Te so bile v izhodišču zelo podobne Bitcoinu z manjšimi spremembami z vidika optimizacije, hitrosti potrjevanja transakcij in podobno. Oktobra 2011 je Charlie Lee objavil specifikacije omrežja Litecoin, ki se je močno opiralo na Bitcoinovo kodo. Litecoin je bil iztočnica za Luckycoin. Kodo Luckycoina sta programerja Billy Marcus in Jackson Palmer uporabila za kreacijo Dogecoina leta 2013; le-ta se še vedno pogosto znajde med top 15 kovanci po tržni kapitalizaciji (N26, 2022). Do velikega preboja je prišlo leta 2015, ko je Vitalik Buterin predstavil koncept Ethereuma, ki bi lahko poleg preprostih transakcij med uporabniki poganjal tudi kompleksnejše pametne pogodbe in decentralizirane aplikacije (Buterin, 2022b). Zmožnost izvajanja kompleksnejših operacij je postala stalnica v večini projektov, ki so nastali po njem. NEO (2016), Cardano (2017), EOS (2018), Tron (2018) in mnoga druga omrežja omogočajo izvajanje programske logike s pametnimi pogodbami.

4.2 Lastništvo nad kriptovalutami

Marsikateri uporabnik kriptovalut se premalo zaveda potencialnih nevšečnosti, ki se lahko pojavijo zaradi nepovratnost transakcij na blockchainu. Z vidika lastništva nad svojimi kriptovalutami lahko uporabnike delimo na tiste, ki imajo sredstva v svoji lasti, in tiste, ki se za varnost zanašajo na druge. V nadaljevanju bom predstavil tri najpogostejše primere lastništva in upravljanja s kripto sredstvi. Ob tem želim še dodati, da je težko izbrati »najboljšega«, ker ima vsak od njih svoje prednosti in slabosti in da je končna odločitev pogosto odvisna predvsem od uporabnikovih potreb in veščin.

4.2.1 Samostojno skrbništvo

Lastnost, ki marsikateremu uporabniku povzroča preglavice, je samostojno skrbništvo nad svojimi sredstvi. To daje uporabnikom veliko pravic in hkrati tudi odgovornosti, ker so

transakcije s kriptovalutami načeloma nepovratne. Pri digitalnih plačilih z bančno kartico ima kupec običajno pravico preklicati svojo transakcijo oz. povrniti nakazana sredstva, če kupljenega blaga ne dobi v takšnem stanju, kot je bilo oglaševano, če se blago po poti izgubi ali če se izkaže, da je šlo za spletno prevaro. Takšnih mehanizmov kriptovalute najpogosteje ne omogočajo, zato morajo uporabniki, ki se odločijo za samostojno skrbništvo, biti še posebej pozorni na svoja dejanja, ker sami nosijo posledice svojih napak. Po drugi strani je samostojno skrbništvo najvišja oblika finančne suverenosti, ker lahko razpolagajo s svojimi sredstvi brez potrebe po privoljenju kogarkoli drugega. Uporabnik, ki se odloči za samostojno skrbništvo mora namestiti digitalno denarnico, ki je kompatibilna z blockchainom na katerem želi hraniti in upravljati svoja sredstva. Dostop do svojih sredstev potrdi z vnosom zasebnega ključa, ki je pogosto hranjen v obliki med 12 in 24 naključno generiranimi besedami. Kdorkoli pozna ta ključ, ima popoln nadzor nad sredstvi na računih, povezanih s tem zasebnim ključem, zato je zelo pomembno, da ga uporabnik hrani na varnem mestu (Aydar in drugi, 2019).

4.2.2 Multisig

Transakcije na blockchainu morajo uporabniki potrditi s podpisom, ki potrjuje lastništvo zasebnega ključa in posledično poslanih sredstev. Od tod izvira izraz »multisig«, ki bi ga lahko v slovenščino prevedli kot »večpodpis«. Multisignature tehnologija omogoča premik sredstev le, če to dejanje potrdi N od M potrjenih naslovov. To tehnologijo pogosto uporabljajo decentralizirane organizacije, posamezniki, ki želijo dodatno zaščititi svoja sredstva z večfaktorskim potrjevanjem transakcij ali entitete, ki za upravljanje sredstev potrebujejo soglasje določenega števila članov sveta. Posameznik ima lahko na svojem osebnem računalniku denarnico A, na prenosniku denarnico B in na telefonu denarnico C, ki imajo pravico upravljanja z njegovim multisigom. Za primer ponazoritve privzemimo, da uporablja multisig 2/3, kar pomeni, da lahko z dvema od skupno treh denarnic uspešno potrdi transakcijo. Organizacija, ki ima 9 solastnikov, lahko uporabi multisig 5/9, kjer vsak solastnik prispeva enega izmed naslovov. Če se večina (v tem primeru vsaj 5 od 9) solastnikov strinja, da želijo izvesti nek prenos vrednosti, lahko vsak prispeva svoj podpis in multisig izvede transakcijo, ko je število podpisov enako minimalnemu sprejemljivemu številu podpisov. V praksi je tak način upravljanja s sredstvi bolj varen kor nadzor sredstev z enim računom, ker morajo napadalci pridobiti nadzor nad več kot eno denarnico, hkrati pa je tudi manj agilen, ker zahteva določeno stopnjo koordinacije za svoje delovanje (Islam in Biswas, 2014).

4.2.3 Zaupanja vredni posredniki

Med najpogostejše posrednike kriptovalut spadajo menjalnice, ki hranijo uporabnikova sredstva in mu omogočajo trgovanje med valutami, ki jih menjalnica podpira. V tem primeru gre za centraliziran nadzor nad uporabnikovimi sredstvi, ki se razlikuje od uporabe decentraliziranih aplikacij za trgovanje. Uporabnik nakaže svoja sredstva v denarnico

menjalnice, ki jo želi uporabljati. Ko je transakcija uspešno potrjena, dobi na platformi dobropis v višini nakazanega zneska, s katerim lahko trguje. Glavna prednost uporabe centraliziranih posrednikov za neuke uporabnike je prenos odgovornosti za varno hranjenje kriptovalut s posameznika na institucijo. Hkrati je to tudi glavna slabost uporabe posrednikov, ker menjalnice pogosto ne obratujejo transparentno oz. lahko uporabnikova sredstva investirajo v tvegane naložbe brez uporabnikovega privoljenja. Neuspešne naložbe in digitalni vdori v centralizirane menjalnice lahko prav tako pripeljejo do izgube premoženja, ker potem menjalnica nima dovolj sredstev, da bi lahko izplačala svoje uporabnike v celoti. Primerov izgube sredstev uporabnikov s strani menjalnic ni malo. Med najbolj poznana spadata incident Mt. Gox, ki predstavlja primer izgube sredstev zaradi digitalnega vdora, in FTX, kjer sta malomarnost in ne-transparentnost poslovanja pripeljala do izgube sredstev uporabnikov (Young in Keoun, 2022).

4.3 Največje odtujitve kriptovalut

Transakcije na decentraliziranih omrežjih praktično ne moremo preprečiti, zato so popularna tudi med kibernetskimi kriminalci, ki imajo lahko močna zagotovila, da so njihova sredstva na varnem, dokler ostanejo anonimni, oz. zunaj območja vpliva organov pregona. Takšni vdori lahko postanejo še posebej problematični, če jih izvajajo hekerske organizacije v sovražnih državah, ker lahko prek takšnih vdorov polnijo državno blagajno in znižujejo učinkovitost ekonomskih sankcij. Opisani vdori so povzeti iz objave »The Largest Cryptocurrency Hacks So Far« s spletnega vira investopedia.com. Za ta vir sem se odločil zato, ker je ugleden spletni vir s področja ekonomije in financ, ki obravnava tudi področje kriptovalut.

- Ronin Network ($625 mio.): Vdor v omrežje Ronin, ki gosti eno izmed popularnih kripto iger Axie Infiniy, je trenutno najvišje na lestvici glede na vrednost odtujenih sredstev (George, 2022). Poleg tega so razvijalci za vdor izvedeli šele 6 dni po dejanskemu vdoru od uporabnika, ki ni mogel dvigniti svojih sredstev. Omrežje Ronin deluje po podobnem principu kot multisig, ki sem ga opisal v prejšnjem poglavju. Vplačilo in dvig sredstev je varoval multisig 5/9. Od tega je 4 potrjevalce upravljalo podjetje Sky Mavis, ki je zasnovalo to omrežje. V svojem obvestilu skupnosti Sky Mavis ni navedel informacij o ranljivosti, ki je pripeljala do vdora v njihove potrjevalce. Dostop do petega potrjevalca, ki je napadalcu omogočil zadostno število za izpeljavo ropa, je lahko ta pridobil zaradi zastarane kode, ki bi morala potrjevalcu omogočati podpisovanje transakcij za določen čas, vendar ta dostop nikoli ni bil preklican (Rekt, 2022b).
- Poly Network ($611 mio.): Avgusta 2021 je bila platforma za decentralizirane finance Poly Network oškodovana za več kot $600 mio., kar je takrat predstavljalo največji vdor na področju kriptovalut (George, 2022). Napadalec je izkoristil ranljivost v pametnih pogodbah omrežja, ki jih je omrežje uporabljalo za prenos sredstev med različnimi verigami (Ethereum, BSC in Polygon). Razlog za to je bila površno zasnovana infrastruktura, ker je imela ena izmed pogodb, do katere so lahko dostopali vsi

uporabniki, vse potrebne privilegije za klicanje funkcije, ki je bila drugače dostopna le upravljalcem platforme. Tako je napadalec s skrbno zasnovanim vhodnim sporočilom uspel pretentati platformo, ki mu je omogočala posreden dostop do funkcije za izplačilo sredstev (Rekt, 2021a).

- FTX ($600 mio.): FTX, ki je leta 2022 spadal med eno izmed vodilnih centraliziranih kripto menjalnic, je novembra tega leta šla v stečaj (George, 2022). Na dan, ko je vložila zahtevo za stečaj, je iz njihovih denarnic izginilo $600 mio. Sam Bankman-Fried, ki je takrat opravljal vlogo izvršnega direktorja FTX, je možnost za napad pripisal nekdanjemu uslužbencu ali zlonamerni programski opremi, ki bi lahko okužila napravo zaposlenega v podjetju (Rekt, 2022e).
- Binance ($570 mio.): BSC Token Hub je bil most med dvema blockchainoma, ki ju je upravljala menjalnica Binance, ki je trenutno vodilna na svetu po številu uporabnikov in obsegu trgovanja (George, 2022). V napadu je heker uspel ukrasti 2 milijona novih žetonov BNB v takratni skupni vrednosti $570 mio. Napadalec je izkoristil hrošča v kodi, ki je potrjevala vplačana sredstva, za pošiljanje poljubnih transakcij. Napadalec je tako lahko ustvaril lažno sporočilo, ki ga je most prepoznal kot ukaz za izplačilo določenega števila žetonov. Ukradene žetone je poskušal zamenjati za druge kriptovalute, preden bi lahko kdo opazil primanjkljaj. Na koncu mu je uspelo odtujiti »le« $127 mio. sredstev, preden je izgubil dostop do preostalih žetonov (Rekt, 2022d).
- Coincheck ($534 mio.): Coincheck je januarja 2018 utrpel napad, v katerem je bilo odtujenih za $534 mio. kriptovalut, ki je takrat spadal v največjo krajo v zgodovini kriptovalut. Ranljivost je bila ustvarjena zaradi uporabe ti. vroče denarnice. Takšna kripto denarnica je neposredno povezana v splet in ne uporablja dodatnih varnostnih mehanizmov za zaščito uporabnikovega zasebnega ključa. Coincheck je kljub temu vdoru preživel in uspel nadaljevati s svojim poslovanjem (George, 2022).
- Mt. Gox ($473 mio.): Prvi velik digitalni vdor se je zgodil leta 2011, ko je bila takrat popularna kripto menjalnica Mt. Gox izgubila 25.000 bitcoinov v takratni skupni vrednosti $40.000. Takrat je Mt. Gox predstavljal okrog 70 % vseh transakcij bitcoina. Mt. Gox je bil ponovno napaden leta 2014, ko so hekerji odtujili skoraj 650.000 bitcoinov njihovih uporabnikov in 100.000 bitcoinov, ki so bili v lasti Mt. Goxa. Skupnih ~750.000 kovancev je takrat predstavljalo 7 % vseh bitcoinov v obtoku. Poznejši dokazi so razkrili, da je bil razlog za izgubo sredstev uporaba nezavarovanih vročih denarnic (George, 2022). Vrednost ukradenih sredstev bi leta 2021 presegla skupno vrednost $50 mrd., ko je en bitcoin dosegel vrednost $69.000.
- Wormhole ($325 mio.): Vdor v decentralizirano platformo Wormhole predstavlja največji vdor, povezan z omrežjem Solana, ki se za razliko od Ethereuma osredotoča bolj na pretočnost transakcij kot decentraliziranost vozlišč (George, 2022). Napad je omogočila ponarejena transakcija, ki je napadalcu omogočila izplačilo žetonov wETH na omrežju Solana, ki na njem služijo kot ekvivalent valute Ether. Te žetone je napadalec prenesel nazaj na omrežje Ethereum, še preden bi lahko upravljalci platforme preprečili prenos sredstev, kar je v veliki meri uspelo upravljalcem BSC Token Huba (Rekt, 2022a).

- BitMart ($196 mio.): BitMart, ki se je oglaševal kot »najbolj zaupanja vredna platforma za trgovanje s kriptovalutami«, je še ena centralizirana kripto menjalnica, ki je utrpela finančno škodo zaradi digitalnega vdora (George, 2022). V tem primeru je heker ilegalno pridobil $100 mio. sredstev na omrežju Ethereum in $96 mio. na omrežju BSC. Novice o potencialnem vdoru so upravljalci menjalnice sprva označili za neresnične, kasneje pa je izvršni direktor podjetja navedel vrednost odtujenih sredstev v višini $150 mio., ki je bila nižja od resnične. Razlogov, ki so pripeljali do vdora BitMart, ni navedel, čeprav na svoji spletni strani trdijo, da so imeli v t. i. vročih denarnicah le 0,5% sredstev. To bi pomenilo, da je imela menjalnica v času ropa več kot $39 mrd. sredstev, kar je malo verjetno (Rekt, 2021b).
- Nomad Bridge ($190 mio.): Nomad Bridge je platforma, ki omogoča prenos žetonov med različnimi verigami blokov podobno kot BSC Token Hub in Wormhole (George, 2022). Ta vdor je še posebej zanimiv s tega vidika, da je ranljivost po razkritju lahko zlorabil vsak uporabnik ne glede na svoje hekerske sposobnosti. Nadgradnja pametnih pogodb junija 2022 je v sistemu ustvarila ranljivost, ki ni pravilno preverila legitimnosti prejetih zahtevkov in potrdila vsakega ne glede na njegovo vsebino. Tako so lahko drugi uporabniki omrežja preprosto kopirali sporočilo napadalca in naslov njegove denarnice spremenili v svojega (Rekt, 2022c). Kasneje so nekateri računi vrnili svoja ilegalno pridobljena sredstva v skupni vrednosti $36 mio. (George, 2022).

5 METODOLOGIJA RAZISKAVE

Del praktičnega dela magistrskega dela bo vključeval raziskavo frekvenčne porazdelitve objav spletnih virov, ki se nanašajo na področje kriptovalut. Ker se magistrsko delo nanaša na področje tehnološke varnosti, se bo raziskava osredotočala na objave, ki poročajo o digitalnih vdorih in zlorabah tehnologije blockchaina. Za opravljanje raziskave sem moral izbrati orodje za avtomatizirano zbiranje podatkov s spleta in določiti spletne vire, s katerih bom zbiral podatke. Zbrane podatke sem nato primerno obdelal in analiziral ter jih predstavil v pregledni obliki. Poleg tega me je zanimalo tudi, ali in kako se digitalni vdori odražajo v številu objav. Nabor največjih vdorov sem pridobil s spletnega vira investopedia.com in jih označil na histogramu objav. Za doseganje ciljev magistrskega dela sem najprej z orodjem Octoparse zbral podatke o objavah, jih prečistil v MS Excelu in vizualiziral s pomočjo orodij Power BI in wordclouds.com. Za podkrepitev rezultatov sem opravil tudi intervju s strokovnjakom s področja kibernetske varnosti in kriptovalut. Uporabljena orodja in metodologijo bom podrobneje predstavil v naslednjih poglavjih.

5.1 Predstavitev orodja Octoparse

Octoparse je orodje, ki omogoča zbiranje podatkov s spletnih strani. Za uporabo tega orodja sem se odločil, ker znatno olajša strukturiranje logike zbiranja podatkov. To lahko definiramo z zaporedjem in gnezdenjem blokov, ki predstavljajo različne operacije. Zbrani

podatki so shranjeni v strukturiranih tabelah, ki jih lahko izvozimo v format:.xlsx,.json,.csv in.html. Orodje omogoča avtomatsko zaznavo strukture izbranega spletnega mesta, na podlagi katere predlaga najbolj primerno strukturo operacijskih blokov, ki definirajo proces zbiranja podatkov. Octoparse je dostopen v brezplačni in plačljivi obliki na njihovi uradni spletni strani: www.octoparse.com (Octoparse, 2023).

Pri zbiranju podatkov s spletnih strani sem uporabil logične bloke, ki predstavljajo naslednje operacije:

- Paginacija (angl. pagination): operacija, ki omogoča sistematično odpiranje zaporednih, oštevilčenih strani. Spletne strani z obsežnimi informacijami pogosto razdelijo podatke na več manj obsežnih strani, da brskalniku ni treba naložiti vseh podatkov hkrati. Octoparse pogosto avtomatsko zazna strani, kjer bi bila uporaba paginacije primerna, ker je pod razdelkom z vsebino številčno kazalo, ki prikazuje, na kateri izmed strani se uporabnik trenutno nahaja. Pogosto je zraven številčnega kazala tudi gumb »naprej«, ki pa ni obvezen za pravilno delovanje operatorja paginacije. Če ima Octoparse težave s prepoznavanjem razdelka na spletni strani, ki vsebuje številčno kazalo, po katerem naj bi se pomikal, mu lahko razdelek določimo ročno (s klikom) ali z vnosom vrednosti XPath tega razdelka.
- Element zanke (angl. loop item): element zanke v orodju Octoparse deluje podobno kot zanke programskih funkcij, ki jim lahko vnaprej določimo število ponovitev, ali pogoj, ki mu mora biti zadoščeno, da se zanka preneha izvajati. Element zanke se najpogosteje uporablja pri zajemu seznama elementov ali pri paginaciji različnih strani spletnega mesta. Element zanke sam po sebi ne opravlja drugih funkcij, zato mora vsebovati druge operatorje, ki opravljajo potrebne funkcije. Te operacije se ponavljajo, dokler niso izpolnjeni pogoji za končanje zanke. Elementu zanke lahko določimo tudi premor med ponovitvami oz. ali naj Octoparse počaka z izvedbo zanke, dokler se na spletni strani ne pojavi izbrani element, ki ga lahko določimo s ročno (s klikom) ali z vnosom vrednosti XPath izbranega elementa.
- Pomikanje po strani (angl. scroll page): nekatere spletne strani pokažejo starejše objave šele, ko se uporabnik premakne nižje na strani. Octoparse simulira pomikanje po strani z istoimenskim logičnim blokom. Ta blok lahko uporabnik prilagodi svojim potrebam prek različnih parametrov, med katere sodijo »pomikanje po strani, ko se ta naloži«, »delno pomikanje za velikost enega zaslona«, »čas čakanja pred naslednjim pomikom«, »število ponovitev pomikanja« in drugi. Ob uporabi pomikanja po strani v elementu zanke mora uporabnik označiti možnost: »zaključi zanko, ko zmanjka nove vsebine.«
- Klik predmeta (angl. click item): klik predmeta je med najpogosteje uporabljenimi elementi v diagramih poteka dela v Octoparsu. Klik predmeta omogoča simulacijo klika z miško kjerkoli na obiskani spletni strani. Ta element je lahko poimenovan tudi »klik URL-ov na seznamu«, če ima spletna stran predmete, ki so povezani z drugimi URL-i, ali »klik za paginacijo«, ki se avtomatsko ustvari, če v diagramu poteka dela uporabljamo paginacijo. Predmet, ki ga želimo klikniti, lahko določimo ročno (s klikom) ali z vnosom

vrednosti XPath izbranega elementa, ki je lahko določena absolutno ali relativno glede na vrednost XPath elementa zanke, znotraj katerega uporabljamo klik predmeta. Če se klik predmeta izvaja znotraj zanke, lahko določimo časovni zamik pred izvedbo naslednjega koraka. Klik predmeta omogoča možnost, da se izbrana povezava odpre v novem oknu; pri nalaganju z AJAX-om pa lahko določimo tudi časovni premor, preden se izvede naslednji korak in pomik po spletni strani, ko se ta naloži.

- Pridobivanje podatkov (angl. extract data): pridobivanje podatkov je ključni korak, brez katerega Octoparse ne more zbrati izbranih podatkov. Če ima element na spletni strani, iz katerega pridobivamo podatke, podelemente, se bodo njihove vrednosti prikazale v različnih stolpcih razpredelnice. Stolpce lahko ročno preimenujemo in tudi odstranimo, če nas podatki določenih podelementov ne zanimajo. Če pridobivamo podatke znotraj elementa zanke, je potrebno označiti vrednost »pridobivanje podatkov v zanki«. Pridobivanju podatkov lahko določimo tudi časovni zamik izvajanja in dodatne pogoje, če iščemo le določene vrednosti.

5.2 Zbiranje podatkov z orodjem Octoparse

Za zbiranje podatkov sem uporabil 8. verzijo orodja Octoparse, natančneje v8.5.8. Pri določanju obsega vzorca sem se odločil za izbor treh spletnih virov, ki čim bolje ustrezajo naslednjim zahtevam:

- Spletni vir mora redno objavljati novice s področja kriptovalut.
- Spletni vir mora imeti zgodovino objavljanja novic s področja kriptovalut.
- Spletni vir mora objavljati kvalitetne in verodostojne objave.
- Spletni vir mora imeti arhiv objav.
- Octoparse mora pravilno prepoznati metapodatke o objavah.

Po pregledu več kot 10 različnih potencialnih kandidatov sem se odločil za naslednje spletne vire podatkov: news.bitcoin.com, forbes.com in theblock.co. Primerjava števila objav in datumov prve objave, povezane s kriptovalutami, je prikazana v tabeli 2.

Tabela 2: Statistike izbranih spletnih virov naslovov

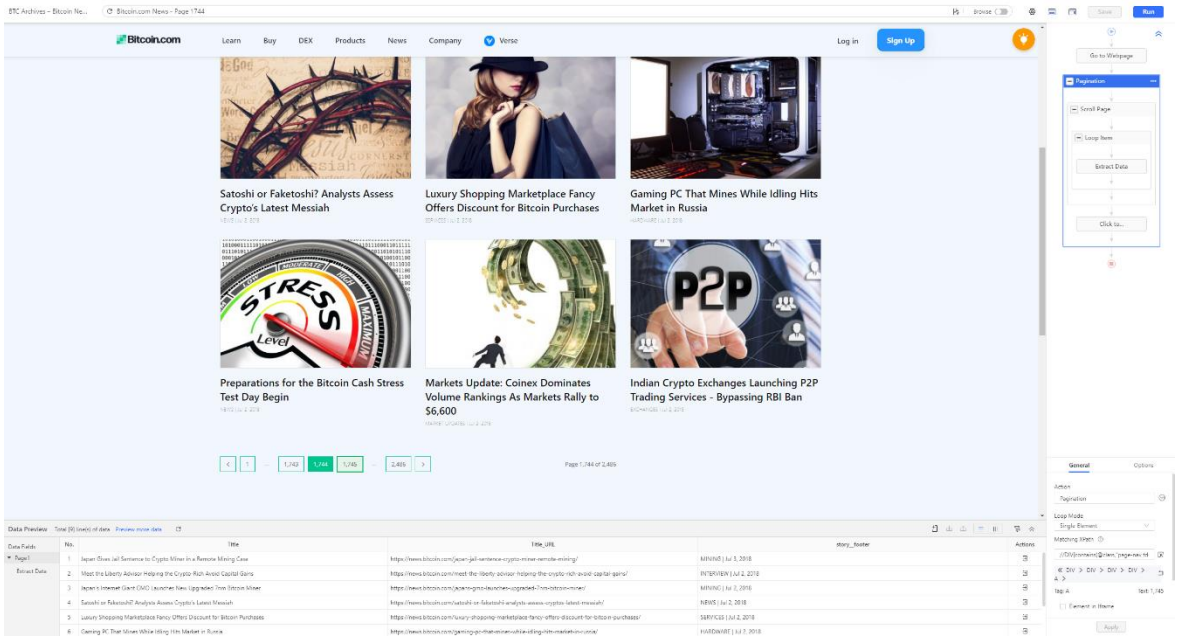
Naziv vira	news.bitcoin.com	forbes.com	theblock.co
Datum najstarejše objave v arhivu	18. 1. 2015	5. 6. 2013	19. 8. 2019
Število vseh objav v arhivu	23662	6519	14129

Vir: lastno delo.

Pri zasnovi logike agregacije podatkov v orodju Octoparse sem v izhodišču uporabil funkcijo avtomatske prepoznave podatkov na spletni strani. Octoparse je izoblikoval ogrodje logičnih blokov, v katerem sem ročno določil območja, iz katerih je bral podatke blok za pridobivanje podatkov. Postopek je moral biti prilagojen posameznemu viru, ker se oblike spletnih arhivov objav med izbranimi stranmi razlikujejo. Večina objav je vsebovala tudi

metapodatke, ki niso potrebni za analizo. Mednje sodijo: URL naslov slike objave, avtor objave itd. Stolpce, ki so vključevali te metapodatke, sem ročno odstranil, da bi zmanjšal čas zbiranja podatkov in velikost končnih datotek. Slika 12 prikazuje funkcijo logičnih operatorjev, ki sem jih uporabil za zbiranje podatkov z omenjene spletne strani in metapodatke o člankih, ki sem se jih odločil zbrati za nadaljnjo analizo. Vseeno je zbiranje podatkov iz arhiva news.bitcoin.com trajalo več kot 12 ur.

Slika 12: Spletna stran news.bitcoin.com/archive in uporabniški vmesnik v Octoparsu



Vir: Octoparse (brez datuma).

V prilogi 1 slika 1 in slika 2 prikazujeta funkciji logičnih operatorjev, ki sem ju uporabil za zbiranje podatkov na straneh forbes.com in theblock.co. Funkcije se med seboj v določeni meri razlikujejo, ker morajo biti prilagojene posamezni spletni strani zaradi strukture vsebine. Podatke posamezne agregacije sem izvozil v format .xlsx, ki ga podpirata programa MS Excel in PowerBI, ki ju bom v nadaljevanju uporabil za obdelavo in analizo zbranih podatkov.

5.3 Obdelava zbranih podatkov

Orodje PowerBI pri uvozu podatkov avtomatsko prepozna določene oblike zapisa datuma in ure. Ker PowerBI ni uspel prepoznati oblike zapisa datuma objave na spletni strani The Block, sem obliko datuma spremenil v MS Excelu, da bi ga PowerBI pravilno prepoznal pri ponovnem uvozu. Pri uvozu podatkov s strani Forbes se je izkazalo, da v nekaterih primerih na mestu datuma sploh ni bilo vrednosti, ki bi jo lahko pretvorili v datum. Na srečo sem lahko iz URL-a članka razbral datum objave. Ker se je to pojavilo le v 4 primerih, sem podatke popravil ročno. Zaradi obsežnosti arhiva news.bitcoin.com sem moral zbiranje

podatkov razdeliti na dva dela. Po končani agregaciji sem oba dela združil v MS Excelu v novo razpredelnico, ki je vsebovala metapodatke o vseh objavah iz arhiva news.bitcoin.com. Tako sem imel na koncu tega koraka 3 razpredelnice tipa .xlsx, v katerih so bili shranjeni podatki o objavah z izbranih virov.

V tem koraku sem želel vizualno prikazati pogostost objav, ki se nanašajo na temo tega magistrskega dela čez čas. Zato sem moral najti način, ki bi iz vzorca izbral le tiste naslove, ki so relevantni zame. DAX podpira funkcijo SEARCH(), ki na podlagi podanega niza znakov izbere le tiste vrstice, ki vsebujejo ta niz znakov. Tako sem lahko z uporabo niza funkcij SEARCH() izbral vse naslove, ki so vsebovali vsaj enega izmed iskanih korenov. Glavna prednost uporabe takšnega iskanja je ta, da ni potrebno eksplicitno navajati vseh permutacij določene besede. Pri iskanju s korenom »hack« sem dobil tudi naslove, ki so vsebovali besede, kot sta »hacker« in »hacked«. Ob tem pa sem moral paziti, ker lahko takšno iskanje občasno vrne tudi lažne pozitivne rezultate. V omenjenem primeru iskanja s korenom »hack« bi lahko dobil tudi naslov, ki vsebuje besedo »shack«, ki se sama po sebi na navezuje na temo magistrskega dela.

Za boljšo preglednost rezultatov in lažje diagnosticiranje potencialnih napak pri izvajanju sem se na začetku omejil le na analizo podatkov s Forbesa. Ker so podatki z drugih virov shranjeni v isti obliki, bi morali preizkušeni ukazi delovati tudi na agregirani zbirki podatkov. Za prvi test sem uporabil filter z dvema iskalnima korenoma: »steal« in »hack«. V prilogi 3 je navedena DAX funkcija, ki iz zbirke podatkov, imenovane »Forbes Data«, izlušči vrstice, ki v stolpcu z imenom »Naslov« vsebujejo besede s korenom »steal« ali »hack« in jih shrani v novi zbirki podatkov imenovani »Forbes Filtered«. Funkcija »CALCULATETABLE« zahteva za prvi argument naziv izhodiščne zbirke podatkov, ki mu sledijo filtrirni argumenti. Znotraj filtrirnega argumenta sem z ukazoma »SEARCH« podrobneje definiral korene besed in stolpec, v katerem sem iskal definirane korene. Med ukazoma sem uporabil logični operator ALI (||), ker me zanimajo naslovi, ki vsebujejo koren »hack« ALI koren »steal«.

Zagon ukaza vrne razpredelnico imenovano »Forbes Filtered«, ki ima 75 vrstic. Podrobnejši pregled prečiščenih podatkov razkrije zanimivo dejstvo, da so avtorji 15. aprila 2022 objavili članek z naslovom: »Who Are The Hackers Behind $625 Million Crypto Theft?« Ta se le za 1 črko razlikuje od naslova videoposnetka, objavljenega 21. aprila 2022: »Who Are The Hackers Behind A $625 Million Crypto Theft?« Zaradi relativno omejenega nabora podatkov v tabeli rezultatov lažje opazimo takšne anomalije, kot če bi že v izhodišču delali s celotnim vzorcem, ki je 6-krat večji. Ker se je določanje posameznih filtrirnih korenov besed izkazalo za relativno časovno zamudno, sem združil vse podatke, ki sem jih analiziral, v skupno tabelo imenovano »Vsi Podatki«. V prilogi 4 je navedena DAX funkcija, v kateri ukaz »SELECTCOLUMNS« kot prvi parameter zahteva zbirko podatkov, iz katere izbiramo stolpce. Nato so navedeni pari imen stolpcev v novi zbirki podatkov in sklicev na stolpce podatkov v obstoječih zbirkah podatkov. Zadnji stolpec z nazivom »Vir« bo v končnem naboru podatkov vseboval le 3 različne vrednosti, ki označujejo, iz katerega vira so bili

specifični podatki pridobljeni. Za ta dodatni stolpec sem se odločil zaradi lažjega preverjanja ustreznosti končnega nabora podatkov in možnosti razlikovanje med objavama v primeru, da bi imela različna vira identična naslova. Ukaz »UNION« združi podatke iz posameznih naborov v skupni nabor podatkov z nazivom »Vsi Podatki«.

V novo tabelo sem želel uvoziti le tiste metapodatke o objavah, ki mi bodo prišli prav pri ustvarjanju grafa frekvenčne porazdelitve člankov po mesecih. Zato sem iz izhodiščnega nabora podatkov izbral le stolpca »Naslov« in »Datum«. Naslove objav sem potreboval zato, da sem lahko iz celotnega nabora podatkov izbral le tiste, ki vsebujejo besede z iskanimi koreni. Datum objave mi je omogočil, da sem lahko določil število objav v določenem časovnem obdobju.

Po uspešni združitvi podatkov sem nadaljeval z določanjem korenov besed, ki sem jih uporabil za filtriranje naslovov. Pri tem sem moral paziti, da sem s primernim filtrom izločil lažne pozitivne rezultate, ki bi se lahko pojavili pri iskanju z določenimi koreni. Za pomoč pri določanju takšnih besed sem uporabil orodje AntConc. To orodje omogoča napredno iskanje zaporedja znakov v danem besedilu. Verzijo orodja 4.2.0 sem brezplačno prenesel s strani: laurenceanthony.net/software/antconc. Da bi določil, ali lahko pri iskanju z nekim korenom dobim neustrezne rezultate, sem nameraval v AntConc uvoziti slovar angleških besed, v katerem bi poiskal vse besede, ki vsebujejo iskano zaporedje črk. Na spletni strani github.com sem našel besedilno datoteko s 370.105 različnimi besedami od posameznih črk do besed, ki sem jih prvič videl. Preneseno datoteko sem uvozil v orodje AntConc in ročno pregledal rezultate, ki so vsebovali iskalni niz črk. Če so rezultati pri iskanju z določenim korenom vsebovali besede, ki bi se lahko pojavile med naslovi objav, sem moral v iskalni DAX funkciji temu primerno omejiti spekter iskanja. Na primer iskanje s korenom »steal« najde tudi naslove, ki vsebujejo besedi »stealth« in »subperiosteal«. Beseda »subperiosteal« se v praksi zelo redko pojavlja, zato sem več pozornosti namenil besedi »stealth« in njenim izpeljankam. Ker sem želel med rezultati obdržati besede s korenom »steal« (angl. steal, steals, stealing) in hkrati izločiti besede, ki se navezujejo na nevidnost (angl. stealth, stealthy), sem iskalnemu filtru dodal pogoj, ki je naknadno izločil besede, ki vsebujejo koren »stealt«. V prilogi 5 je navedena DAX funkcija, ki iz zbirke vseh zbranih podatkov, ki je imenovana »Full Data«, na podlagi iskalnih parametrov vrne zbirko podatkov, imenovano »Full Data Filtered«. Funkcija deluje po podobnem principu kot funkcija, navedena v prilogi 3, s to razliko, da ima ta več iskalnih parametrov. Ker ima logični-IN (&&) operator prednost pred logičnim-ALI (||), sem moral paziti na zaporedje filtrirnih parametrov, da je filter kot celota pravilno deloval. Po preizkusu delovanja na združenih podatkih sem filtru dodal korene »stole«, »thief«, »theft« in »attack«.

Filtrirana zbirka podatkov je vsebovala 997 vrstic podatkov, ki sem jih moral ročno pregledati, da slučajno ne bi vsebovale lažnih pozitivnih vrednosti, ker iskalni filter kljub večji natančnosti ni sposoben razlikovati med različnimi pomeni iskane besede in konteksti, v katerih so uporabljene. Kot primer lahko navedem marsikateri naslov, ki je vseboval besedo »attack«, vendar se kontekst ni nanašal na digitalni napad. V naslovu »Report: AAX

users storm crypto exchange's Nigerian offices, attack empoyees« se omenjeni napad ne nanaša na tehnološki napad ampak na fizično obračunavanje z zaposlenimi v nigerijskih pisarnah menjalnice AAX. Zato sem tabelo izvozil v MS Excel, v katerem sem odstranil vrstice z naslovi, ki se niso navezovali na tematiko tega dela. Pri določanju primernih naslovov sem sledil načelu, da se morajo vsebine objav nanašati na incidente, ki so negativno vplivali na uporabnike oz. lastnike kriptovalut. Primeri takšnih incidentov so lahko vdori v račune z veliko sledilci na družbenih omrežjih, kjer hekerji objavijo ali pošiljajo zlonamerna sporočila (Porterfield, 2022). Obstajajo pa tudi nezaželeni načini uporabe kriptovalut, ki imajo manjši učinek na končnega uporabnika. Kupovanje ilegalnih predmetov in pranje denarja na blockchainu ima redko vpliv na druge uporabnike, če pri tem ne ustvarja velikega števila transakcij v kratkem času, ki bi zmanjšale pretočnost omrežja. Drugi naslovi, ki sem jih tudi izločil, so se nanašali na krajo električne energije za rudarjenje bitcoina in hekerske napade na infrastrukturo, ki ni povezana s kriptovalutami, in plačevanje odkupnine v kriptovalutah. Dodatno pozornost sem namenil vdorom v račune z veliko sledilci na družbenih omrežjih. Nekateri so se izkazali zgolj za potegavščine kot na primer, ko je Indijski predsednik tvitnil o razdeljevanju bitcoina svojim državljanom (Helms, 2021). V drugih primerih so zlikovci dostop do računov izkoristili za objavljanje prevar, ki so jim nekateri sledilci oz. gledalci nasedli in posledično izgubili sredstva, ki so jih poslali na objavljeni naslov z mislijo, da bodo dobili nazaj več sredstev (Tassev, 2022). Med bolj unikatne poskuse ogrožanja uporabnikov kriptovalut spada pošiljanje okuženih strojnih denarnic proizvajalca Ledger preteklim strankam z namenom razkritja uporabnikovega zasebnega ključa. Napadalci so ciljali na stranke tega proizvajalca zato, ker so bili podatki o domačih naslovih Ledgerjevih strank objavljeni na internetu po predhodnem vdoru v Ledgerjeve strežnike (Goschenko, 2021).

Ker je izhodiščni nabor podatkov vseboval objave do vključno 8. januarja 2023, sem se odločil, da bom nabor podatkov razširil z naslovi objav, ki so bile objavljene do vključno 30. aprila 2023. Pri zbiranju podatkov o objavah med 8. januarjem 2023 in 30. aprilom 2023 sem moral zaradi nekaterih sprememb na straneh Forbes in TheBlock prilagoditi proces zbiranja podatkov. Največji izziv mi je predstavljala novo implementirana DDoS zaščita na strani TheBlock. Ta je kmalu po zagonu procesa v Octoparseu prekinila povezavo in mi preprečila dostop do spletne strani za nekaj časa, kar je prekinilo proces agregacije. Tej zaščiti sem se uspel izogniti s podaljšanjem časovnih intervalov med izvedbami operacij v Octoparseu, kot je navedeno v tabeli 3.

Tabela 3: Spremembe časovnih zamikov pri zbiranju podatkov z vira TheBlock.co

Operator	Izhodiščni časovni interval (s)	Novi časovni Interval (s)
Pagination	3	15
Scroll Page	0	1
Loop Item	2	5
Extract Data	0	1

Vir: lastno delo.

Podatke o nedavnih objavah sem obdelal po prej omenjenih postopkih, ki so se zopet v neki meri razlikovali med viri zaradi različnih oblik zapisa datuma objave. Nove podatke iz vseh treh virov sem nato uvozil v PowerBI, jih združil v skupno razpredelnico, ki je vsebovala 3238 vrstic podatkov, in jih filtriral s prej navedenim filtrom. 75 vrstic podatkov, ki so ustrezale mojemu filtru, sem nato še ročno pregledal, da bi po potrebi izločil katere lažne pozitivne rezultate. Tako sem začetnemu naboru podatkov dodal še 59 novih objav in na koncu dobil skupno zbirko podatkov velikosti 846 objav s pripadajočimi datumi objave in njihovim virom.

5.4 Sestava vprašalnika in izbor intervjuvanca

Cilj intervjuja je bilo določanje najpogostejših razlogov za digitalne vdore in ustreznih varnostnih praks z namenom zavarovanja pred potencialnimi grožnjami. Poleg tega sem želel ugotoviti, ali so uporabniki kriptovalut dejansko izpostavljeni dosti večjim varnostnim tveganjem kot uporabniki drugih tehnologij. Ob pregledu obstoječe literature sem odkril, da večina obstoječih raziskav obravnava tveganja, povezana s kriptovalutami z vidika vlagateljev in vpliva gibanja cen kriptovalut na njegov portfelj. Druge raziskave so obravnavale nevarnost rudarjenja kriptovalut z naravovarstvenega vidika. Zato sem se pri sestavi vprašalnika opiral predvsem na raziskave s področja kibernetske varnosti (El-Kady in drugi, 2023).

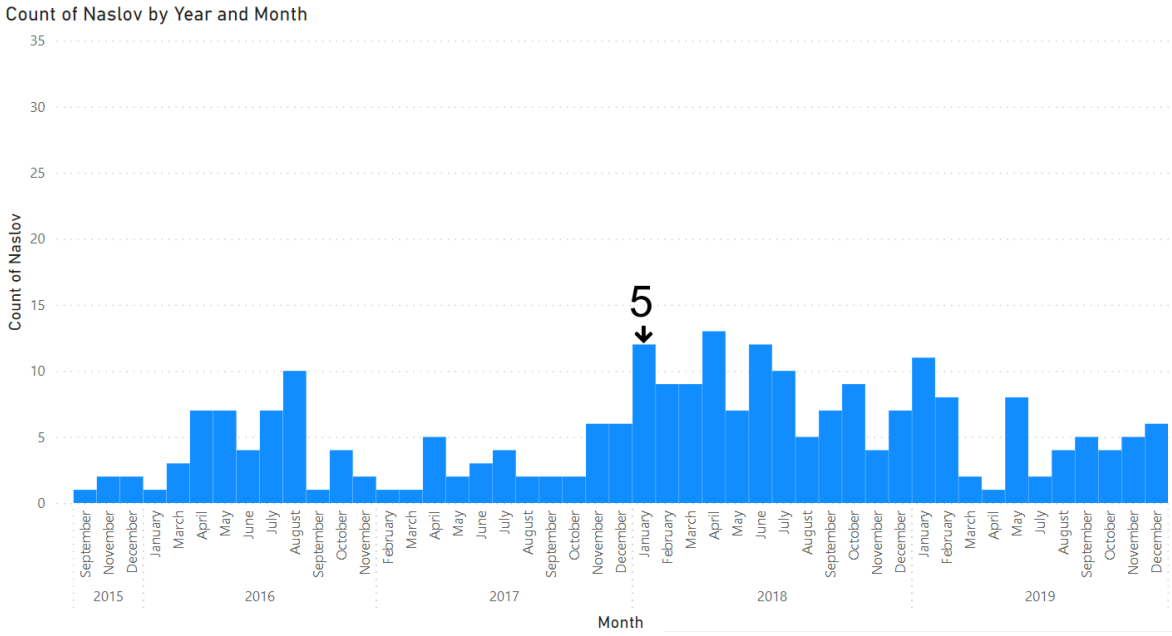
Z zastavljenimi vprašanji sem poskušal dobiti intervjuvančevo mnenje glede različnih oblik tehnoloških tveganj in varnostnih mehanizmov, ki lahko zmanjšajo vpliv določenih tveganj na končnega uporabnika. Vprašanja intervjuja, ki so navedena v prilogi 7, sem poskušal zastaviti relativno široko, da bi dobil celovit vpogled v mnenje intervjuvanca. Tako bi lahko med intervjujem namenila dodatno pozornost temam, ki se zdijo intervjuvancu pomembne z vidika tehnološke varnosti. S tem sem želel tudi zmanjšati verjetnost, da bi spregledala katero pomembno področje, če bi vprašanja zastavil preozko. Za intervju sem se uspel dogovoriti z odprtokodnim programerjem, strokovnjakom s področja IT storitev in blockchaina, ki je začel svojo karierno pot leta 1996. V času svoje kariere je sodeloval z mnogimi domačimi in tujimi zagonskimi podjetji, pomagal soustvariti blockchain standarda ERC-721 in ERC-2477 ter bil glavni avtor protokola 0xcert.

6 PREDSTAVITEV REZULTATOV RAZISKAVE

6.1 Rezultati analize objav

Prečiščeno zbirko podatkov sem prikazal v orodju PowerBI z grafom tipa »clustered column chart«, ki je prikazoval porazdelitev objav po mesecih od septembra 2015 do vključno aprila 2023. Na grafu, prikazanem na slikah 13 in 14, sem označil tudi 10 največjih vdorov na področju kriptovalut glede na podatke, objavljene na spletni strani investopedia.com (George, 2022). V omenjeni objavi je sicer navedenih 11 vdorov, vendar se je vdor v Mt. Gox zgodil leta 2011, ki je zunaj mojega nabora podatkov. Vdori, označeni na sliki 13 in sliki 14 ter količina odtujenih sredstev, so navedeni v tabeli 4.

Slika 13: Frekvenčna porazdelitev naslovov med septembrom 2015 in decembrom 2019

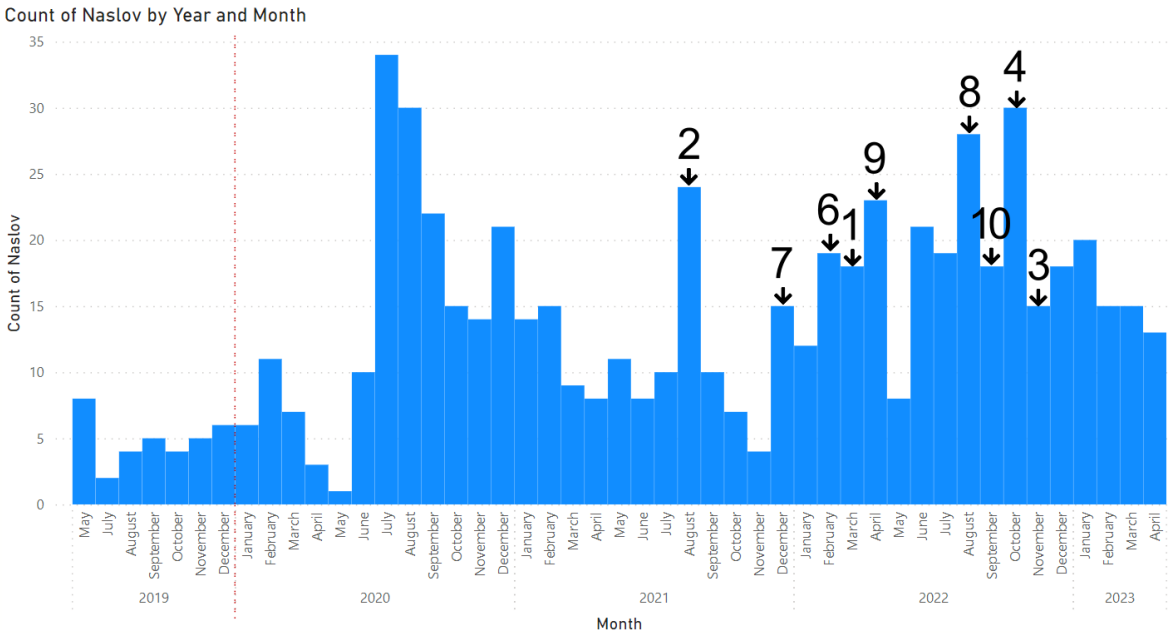


Vir: lastno delo.

Zaradi boljše preglednosti sem se odločil graf razdeliti na dve sliki. Ker se je število objav od leta 2020 v povprečju znatno povečalo, sem želel v drugi sliki (slika 14) vključiti tudi del leta 2019 za lažjo vizualno primerjavo. Zato tako slika 13 kot slika 14 prikazujeta stolpce, ki prikazujejo število objav v obdobju med majem 2019 in decembrom 2019. Prekrivanje podatkov sem označil z navpično črtkano črto na sliki 14. Na sliki 13 je s številko 5 označen vdor v platformo Coincheck. Na sliki 14 lahko vidimo velik skok v številu objav julija 2020, ki sovpada z nadaljevanjem bikovskega trenda na trgu kriptovalut, ki je leta 2021 prerasel v fazo evforije. Poleg tega je razvidno, da velikim vdorom pogosto sledijo obdobja povečanega števila objav. Tukaj je predvsem zanimiv osamelec, ki se je pojavil julija 2020. Ta sovpada z enim največjih vdorov v platformo Twitter, v katerem je napadalec ogrozil več kot 130 uporabniških računov (Tidy in Radford, 2023). Na njih je objavil lažna sporočila, s katerimi je želel napeljati naivne uporabnike kriptovalut, da pošljejo svoja sredstva na

napadalčev račun. Iz grafa je tudi razvidno, da se je večina velikih vdorov zgodila v nedavnih letih, predvsem v letu 2022.

Slika 14: Frekvenčna porazdelitev naslovov med majem 2019 in aprilom 2023



Vir: lastno delo.

Za analizo naslovov objav sem uporabil tudi generator besednih oblakov (angl. word clouds), ki iz danega besedila ustvari sliko, v kateri so pogostejše besede prikazane z večjimi črkami kot tiste, ki se v danem besedilu pojavijo redkeje. Vhodno besedilo za ta orodja sem ustvaril tako, da sem izvozil le podatke o naslovih filtriranih objav v datoteko tipa.txt, ker informaciji o datumu in viru objave za ustvarjanje besednih oblakov nista relevantni.

Slika 15: Besedni oblak najpogostejših besed v naslovih objav

https://www.wordclouds.com

Orodju sem določil omejitev, da prikaže le besede, ki se pojavijo vsaj 40-krat v prečiščenem naboru podatkov. Tako je algoritem na sliki 15 prikazal 989 različnih besed. Toda zaradi narave algoritma za izrisovanje besednih oblakov večino besed zaradi majhne pisave težko razločimo. Med najpogostejšimi se pojavljajo izpeljanke korenov »hack« in »attack«, kar je nekako pričakovano glede na metodologijo filtriranja naslovov. Zanimiva se mi je zdela tudi pogostost besede »million«, na podlagi katere sem sklepal, da odtujitve manjših zneskov niso deležne tolikšnega poročanja s strani analiziranih publikacij kot večji vdori.

Tabela 4: Podatki o največjih vdorih s področja kriptovalut

Št. na grafu	Naziv	Odtujena sredstva ($ mio.)	Mesec, leto vdora
1	Ronin Network	625	Marec, 2022
2	Poly Network	611	Avgust, 2021
3	FTX	600	November, 2022
4	Binance	570	Oktober, 2022
5	Coincheck	534	Januar, 2018
6	Wormhole	325	Februar, 2022
7	BitMart	196	December, 2021
8	Nomad Bridge	190	Avgust, 2022
9	Beanstalk	182	April, 2022
10	Wintermute	162	September, 2022

Vir: prirejeno po George (2022).

Na podlagi rezultatov analize naslovov objav zaključujem, da se je pogostost objav o zlorabah kriptovalut v zadnjih letih izrazito povečala glede na število objav pred poletjem 2020. Dokler bo skupna vrednost trga kriptovalut (izražena v fiat valutah) v daljšem časovnem obdobju naraščala, bo s tem posledično tudi vrednost odtujenih sredstev, ki jih lahko odtujijo spletni kriminalci. Na podlagi te ugotovitve lahko z določeno mero verjetnosti predpostavimo, da bomo v prihodnosti priča še večjim vdorom, če bo vrednost celotnega kripto trga presegla rekordno vrednost $3,058 bilijona, ki jo je dosegel novembra 2021.

6.2 Mnenje strokovnjaka s področja kibernetske varnosti in kriptovalut

Za podkrepitev rezultatov analize spletnih objav sem izvedel tudi intervju s strokovnjakom s področja kibernetske varnosti in kriptovalut. Med intervjujem je sogovornik izpostavil pomembnost poznavanja tehnologije in njenega delovanja. Ob tem je omenil, da lahko vsaka tehnologija, ki je uporabnik ni vešč, predstavlja potencialno nevarnost za posameznika. To se najpogosteje vidi pri otrocih in starejših uporabnikih, ki se ne zavedajo, da se z uporabo različnih aplikacij v veliki meri odpovejo zasebnosti; poleg tega je na spletu veliko dezinformacij v najrazličnejših oblikah. Problem zasebnosti in dostopa do kvalitetnih informacij lahko postane še večji, če upoštevamo vpliv algoritmov, ki uporabnikom ponujajo različne vsebine in oglase glede na njihove preference. Tako se lahko posameznik znajde v mehurčku informacij, ki zgolj potrjujejo njegovo mnenje brez omembe alternativnih stališč

in informacij. Poleg tega ima marsikatero gospodinjstvo kakšno pametno napravo (poleg pametnega telefona), ki lahko prav tako predstavlja potencialno nevarnost svojim lastnikom. Po eni strani uporabniki nimamo nadzora nad tem, katere podatke te naprave posredujejo na strežnike in kdo ima dostop do njih, po drugi strani pa pogosto predstavljajo šibke točke z vidika tehnološke varnosti, sploh če njihova programska oprema ni redno posodobljena (Thouti in drugi, 2022).

Intervjuvanec je na vprašanje o razliki v izpostavljenosti tveganjem med uporabniki kriptovalut in drugimi uporabniki odgovoril: »Bistvenih razlik med tveganji za uporabnike tehnologije na splošno in tveganji za uporabnike kriptovalut ni. Če posameznik kriptovalut ne razume, zanj uporaba tovrstnih tehnologij predstavlja nevarnost.« Ob tem je želel tudi izpostaviti, da veliko tveganj izvira iz napačne percepcije področja kriptovalut. Pametne pogodbe omogočajo ustvarjanje denarja, ki ga lahko programiramo. Čeprav tehnologija deluje na prvi pogled relativno preprosto, predstavlja enega večjih tehnoloških napredkov v zadnjih desetletjih, kar sem na kratko predstavil v poglavju o zgodovini kriptovalut. Uporaba blockchaina omogoča posameznikom zagotovila glede varnosti in trajnosti njihovih podatkov brez potrebe po posrednikih. Tako lahko družba postavi svoje delovanje na višji nivo, ker omogoča varno, pravično in predvsem pa matematično korektno interakcijo posameznika z drugimi člani družbe. Podatke na blockchainu lahko preverjamo in dokazujemo z gotovostjo, brez potrebe po centralni avtoriteti. Zato ta tehnologija predstavlja idealno družbeno koristno digitalno infrastrukturo, ki omogoča upravljanje z denarnimi sredstvi s kriptografskimi zagotovili brez posrednikov.

Ob predpostavki, da je velik del medmrežnih komunikacij zlonamerne narave (vsiljena pošta, preskušanje nezavarovanih računalniških vhodov, napadi za prekinitev dostopa itd.), je po sogovornikovih izkušnjah tega na blockchainu manj. Toda izkupiček je neprimerno višji. Iskanje varnostnih lukenj v blockchainu je lahko podobno iskanju varnostnih pomanjkljivosti v internetnih tehnologijah. Sogovornik je tudi izpostavil pomembno razliko med večino internetnih aplikacij in programov na blockchainu: »Za razliko od splošnega interneta so ta omrežja navadno odprtokodni projekti, kjer skupnost programerjev iz celega sveta skrbi za varnost in odpravlja pomanjkljivosti. Bolj kot kriptovalute so za hekerje zanimive pametne pogodbe, ki jih na blockchain nameščajo najrazličnejši posamezniki.« Pri tem je sogovornik izpostavil potencialno problematiko varnostnih lukenj v pametnih pogodbah, ker jih v veliki meri ustvarjajo nevešči, neizkušeni in neodgovorni programerji. Ker ima večina sredstev na blockchainu neko vrednost, takšne varnostne luknje predstavljajo idealne tarče za spletne kriminalce, ki lahko prek njih finančno oškodujejo legitimne uporabnike. Centralizirane menjalnice lahko prav tako predstavljajo potencialna tveganja, ker uporabnik skrbništvo nad svojimi sredstvi preda posredniku. V tem primeru so lahko tveganja tehnološke ali regulatorne narave, lahko pa se tudi zgodi, da je poslovanje posrednika neodgovorno in v nekaterih primerih celo kriminalno, kar lahko pripelje do izgub uporabnikovih sredstev (Young in Keoun, 2022).

Ko sem sogovornika povprašal po mnenju okrog zadostne informiranosti uporabnikov kriptovalut, je potrdil mojo hipotezo, da uporabniki v veliki meri niso dovolj podučeni o delovanju tehnologije blockchaina in pametnih pogodb. To je podkrepil z navedbo: »Čeprav so nepovratne transakcije ena izmed osrednjih lastnosti blockchaina, se pogosto najdejo uporabniki, ki se dejansko ne zavedajo, kaj to v praksi pomeni.« Čeprav danes še vedno obstajajo določene prepreke za nove uporabnike blockchaina (namestitev denarnice, generacija zasebnega ključa in hramba na varnem mestu, itd.), se še vedno prepogosto dogajajo primeri izgube sredstev zaradi različnih razlogov, ki se pogosto navezujejo na pomanjkanje uporabnikovega znanja ali pretirano zaupanje neznancem na internetu (Misoch, 2015). Ob tem je sogovornik pripomnil: »Prav tako se premalo zavedamo potencialnih pomanjkljivosti trenutnega sistema digitalnega bančništva in zato trenutno ne vidimo veliko prednosti v uporabi kriptovalut, če jih primerjamo z obstoječim sistemom.«

Na vprašanje glede največjih dejavnikov, ki ogrožajo uporabnike kriptovalut, je intervjuvanec odgovoril: »Pogosto so največja nevarnost uporabniki sami. Ker večina ljudi ne poseduje veščin, ki bi jim omogočale neodvisno preverjanje varnosti pametnih pogodb, morajo zaupati programerjem, ki so jih ustvarili.« V mnogih primerih so varnostne luknje posledica malomarnosti programerjev, obstajajo pa tudi primeri, ko so jih ustvarjalci namerno ustvarili, da bi se lahko okoristili na račun nič hudega slutečih uporabnikov njihove platforme. Poleg tega se uporabniki decentraliziranih aplikacij pogosto ne zavedajo, da varnostne luknje v pametnih pogodbah pomenijo dokončne finančne izgube, ker niso navajeni nepovratnosti transakcij. Danes uporabniki tehnologije na mnogih področjih prelagajo odgovornost na druge osebe ali institucije in niso vajeni prevzeti odgovornost za svoja dejanja. V primeru odtujitve bančne kartico ali pozabljene kodo za dostop do bančnega računa, lahko banka svojim strankam povrne dostop. V primeru izgube ključa do računa na blockchainu ali prenosu sredstev na drug naslov, ki ni v uporabnikovi lasti, pa do teh sredstev ne more več dostopati.

Uporabniki kriptovalut lahko relativno preprosto zmanjšajo tveganja, katerim so izpostavljeni. Med ključne dejavnike spada zavedanje o lastnih kompetencah glede razumevanja ekonomskih in tehnoloških dejavnikov, povezanih z različnimi projekti. »Laik bo vedno ranljiv in odvisen od kroga ljudi, ki jim zaupa,« je ob tem dodal intervjuvanec. V mnogih primerih lahko pride do t. i. Dunning-Kruger efekta, ko subjekti z malo znanja o določenem področju precenijo svoje poznavanje tega področja (Kruger in Dunning, 1999). Tako lahko mnogi uporabniki zmotno ocenijo tveganja, povezana s svojimi »investicijami« in pogosto za svoje finančne odločitve ne prevzamejo odgovornosti, ampak jo prelagajo na druge. Racionalni posameznik bi lahko zaključil, da kupovanje žetonov novih projektov brez dokaza o delujočem produktu in dejanskih uporabnikih ni smiselno. Ob tem pa ne smemo zanemariti psihološkega in družbenega vpliva, če je posameznik izpostavljen informacijam o dobičkih, ki jih uspe vnovčiti nekaterim vlagateljem. Pogosto pozabijo tiste uporabnike, ki so izgubili vse, ker so sledili finančnim nasvetom vplivnežev na družbenih omrežij, ki niso

korektno predstavili tveganj, povezanih žetoni, ki so jih oglaševali svojim sledilcem (Asmakov, 2022).

7 PREDLOGI ZA ZMANJŠANJE TVEGANJ UPORABNIKOV KRIPTOVALUT

V svojem delu sem do sedaj predstavil in opisal najrazličnejše dejavnike, ki lahko privedejo do izgube kriptovalut. Do tega lahko pride tako zaradi tehnoloških ranljivosti ter človeškega pohlepa in naivnosti (Singh in drugi, 2020). Trenutno žal ne obstaja absolutno najboljši način zaščite, ki bi lahko vsem uporabnikom zagotovil popolno varnost. Poleg tega je ranljivosti težko označiti za bolj ali manj resne, ker v mnogih primerih varnostne luknje pomenijo popolno izgubo sredstev in ne želim dajati vtisa, da je varnost na tem področju kadarkoli smiselno zanemarjati. Poleg tega želim ponoviti nasvet intervjuvanca, da se je potrebno pri rokovanju s to novo tehnologijo še posebej zavedati lastnih kompetenc in na podlagi teh izbrati način uporabe, ki je najbolj primeren zanj. Varnost svojih sredstev lahko vzamemo v svoje roke ali pa jo delegiramo drugi osebi oz. instituciji. Žal pa na podlagi dogodkov iz preteklosti ne morem trditi, da je zaupanje institucijam absolutno boljša izbira, ker tudi njihovi uporabniki pogosto nosijo posledice digitalnih vdorov. Diverzifikacija sredstev je lahko uporabnikom v veliko korist, ker v primeru nepričakovanega dogodka ne izgubijo vsega (Khan in drugi, 2017). V nadaljevanju želim predstaviti najpogostejše tehnološke, psihološke in sociološke ranljivosti, ki sem jih opazil med pisanjem svojega magistrskega dela, in navesti načine, kako lahko uporabniki zmanjšajo svojo izpostavljenost predstavljenim tveganjem.

7.1 Najpogostejše tehnološke ranljivosti in priporočene varnostne prakse

7.1.1 Izguba zasebnega ključa

Izguba zasebnega ključa spada med najpogostejše nezgode, ki se zgodijo neprevidnim uporabnikom. Izguba zasebnega ključa v veliki večini primerov pomeni izgubo vseh sredstev v tej denarnici, ker napadalec dobi popoln nadzor nad njimi (Aydar in drugi, 2019). Če napadalec ni dovolj hiter, lahko lastnik to opazi in nakaže svoja sredstva v drugo denarnico, do katere napadalec nima dostopa. Zasebni ključ lahko uporabnik izgubi na več načinov, ki so lahko bolj ali manj sofisticirani. Ena izmed pogostih napak novih uporabnikov je hramba zasebnega ključa v nešifrirani digitalni obliki. Tako lahko napadalec, ki pridobi dostop do uporabnikovega računalnika ali oblaka, brez težav kopira zasebni ključ. Zato je na splošno odsvetovana hramba zasebnega ključa v kakršnikoli digitalni obliki, ker se moramo za njegovo varnost zanašati na moč šifrirnega algoritma in programske opreme, ki jo za to uporabljamo (Aydar in drugi, 2019). Zapis na papir ali drugačna oblika shrambe v fizični obliki je s tega vidika pogosto bolj primerna. Druga napaka, ki jo lahko storijo uporabniki, je uporaba t. i. vroče denarnice, ki prav tako hrani zasebni ključ v digitalni obliki,

ker ga potrebuje za podpisovanje transakcij (Nakamoto, 2008). Takšno malomarnost lahko hitro izkoristijo okužene spletne strani, ki ob vstopu zaženejo zlonamerni program, ki iz uporabnikove programske denarnice izlušči njegov zasebni ključ. Uporabniki se lahko pred takšnimi napadi zaščitijo z uporabo t. i. strojne denarnice, ki zasebni ključ hrani na napravi, ki je ločena od računalnika in je namenjena zgolj podpisovanju transakcij in varni hrambi zasebnega ključa. Pri tem pa morajo biti uporabniki pazljivi tudi na to, da so lahko v strojne denarnice, ki jih ne kupijo direktno od njihovega proizvajalca, namerno vgrajena stranska vrata ali druge varnostne luknje, ki bi lahko pripeljale do izgube zasebnega ključa in posledično uporabnikovih sredstev (Ivanov in Yan, 2021). Zato osebno odsvetujem nakup takšnih naprav prek posrednikov, ker nikoli ne vemo, kdo vse je imel dostop do njih pred nami.

7.1.2 Varnostne ranljivosti v pametnih pogodbah

Pametne pogodbe morajo biti zelo previdno zasnovane, ker njihova odprtokodna narava omogoča vsakomur vpogled v njihovo logiko. Zato je zelo pomembno, da pametne pogodbe, ki upravljajo z večjo količino sredstev, pišejo izkušeni programerji s širokim poznavanjem potencialnih zlorab, kar je izpostavil tudi sogovornik med intervjujem. Problematika površno zasnovanih platform je pogosto najbolj opazna med obdobji evforije, ko mnogo neizkušenih programerjev poskuša ustvariti naslednji popularni projekt, v katerega naivni uporabniki brez pomislekov pošljejo svoja sredstva. Poleg tega obstajajo tudi zlonamerni programerji, ki v svoje projekte namerno vgradijo stranska vrata, ki jim omogočajo oškodovanje uporabnikov (He in drugi, 2020). V idealnem svetu bi vsak posameznik imel znanje, ki je potrebno za razumevanje delovanja pametnih pogodb, da bi lahko sam dobro ocenil, ali je varno uporabljati neko platformo ali ne. Zato obstajajo specializirana podjetja in organizacije, ki se ukvarjajo s testiranjem varnosti pametnih pogodb, vendar pretekli incidenti kažejo, da tudi profesionalci kdaj spregledajo kakšno varnostno luknjo (George, 2022). S tega vidika je pogosto bolj smiselno uporabljati bolj preproste in dalj časa obstoječe pametne pogodbe, ker so imeli drugi razvijalci in hekerji več priložnosti, da bi jih v preteklosti že zlorabili, če bi vsebovale varnostne ranljivosti. Tak pristop je večini novih uporabnikov tuj, ker se preveč osredotočajo na potencialne donose in ne ozavestijo tveganj, povezanih s takšnim ravnanjem (Brown, 2017). Poleg tega se je potrebno zavedati, da vlagatelji v kriptovalute načeloma niso primorani v uporabo pametnih pogodb in se jim je morda smiselno izogniti, če niso sigurni o svojem razumevanju njihovega delovanja. Če pa se uporabnik za njihovo uporabo vseeno odloči, je smiselno uporabiti le del premoženja, ki ga je pripravljen v najslabšem primeru izgubiti. Pri tem lahko pomaga tudi diverzifikacija, da v primeru vdora v eno platformo uporabnik ne izgubi vsega svojega premoženja na blockchainu (Khan in drugi, 2017).

7.1.3 Podpisovanje transakcij neznanih virov

Uporabniki morajo za potrjevanje dejanj na blockchainu podpisati sporočila in transakcije s svojim zasebnim ključem (Nakamoto, 2008). Žal pa uporabniški vmesnik pri tem pogosto ne omogoča podrobnejšega vpogleda v to, kaj dejansko potrjujejo. Zato morajo uporabniki zaupati aplikacijam, da bodo dejansko izvedle dejanje, ki ga uporabniki zahtevajo od njih. Podpisovanje sporočil je tudi pogost način prijave v decentralizirane aplikacije, podobno kot prijava z uporabniškim imenom in geslom v spletne strani. Pri tem pa obstaja možnost, da spletna stran ustvari zahtevo za podpis, ki bi omogočil dostop do uporabnikovih sredstev drugi osebi (He in drugi, 2020). Nepozorni uporabniki lahko podpišejo to zahtevo misleč, da se prijavljajo v spletno stran, v resnici pa omogočijo neznancem dostop do svojih žetonov. Da se takšne nezgode ne dogajajo le neukim uporabnikom, priča primer Kevina Rosea, ki je zaradi površnosti izgubil $1,4 mio. NFT-jev januarja 2023 (Nagarajan, 2023). Uporabniki lahko pridejo v stik s takšnimi zlonamernimi transakcijami prek okuženih ali ponarejenih spletnih strani legitimnih aplikacij ali novih projektov z vgrajenimi ranljivostmi, ki prežijo na nepozorne uporabnike (Fruhlinger, 2017). Takšni napadi se od izgube zasebnega ključa razlikujejo predvsem po tem, da uporabnik sam potrdi zlonamerno transakcijo, zato uporaba strojne denarnice ali multisiga praviloma ni zadostna zaščita pred takšnim tipom napada (Nagarajan, 2023). Uporabniki lahko svoja tveganja znatno zmanjšajo z uporabo preverjenih aplikacij, označevanjem legitimnih spletnih naslovov, da bi se izognili preusmeritvi na lažno spletno stran, in spremljanjem opozoril na družbenih omrežjih o identificiranih zlorabah. Dodaten varnostni mehanizem je lahko razpršitev sredstev med več računi, da v primeru potrditve zlonamerne transakcije napadalec ne dobi nadzora nad vsemi uporabnikovimi sredstvi (Khan in drugi, 2017). Uporaba naprednih programskih denarnic, ki simulirajo potek transakcije, lahko prav tako znatno zmanjša uporabnikova tveganja, ker mu na bolj pregleden način predstavijo, kateri uporabnikovi žetoni so vključeni v določeno transakcijo in kaj lahko uporabnik pričakuje v zameno zanje. Tako lahko uporabnik hitro opazi, če se sredstva na vhodu ali izhodu transakcije razlikujejo od pričakovanih vrednosti in transakcijo pravočasno zavrne.

7.2 Najpogostejše psihološke in sociološke ranljivosti in priporočene varnostne prakse

7.2.1 Nestrpnost in napačna pričakovanja

Laiki se s kriptovalutami ne ukvarjajo, dokler ne zasledijo senzacionalnih novic o gibanju cene iz medijev. Zgodbe o donosnosti sektorja v nedavni preteklosti marsikoga premamijo, da »investira« v to panogo. Takšna dejanja pa se lahko pogosto izkažejo za prenagljena, ker ti »vlagatelji« nimajo izkušenj z dejanskimi finančnimi trgi in prepogosto pričakujejo, da bo cena nadaljevala pozitivni trend v nedogled (Kruger in Dunning, 1999). Poleg tega lahko podcenijo kratkoročno nihanje cen. Čeprav se sprva odločijo za »dolgoročno« investicijo, lahko sunkoviti padci cen zamajejo njihovo prepričanje v dolgoročni uspeh njihovega

portfelja. Drugi se raje odločijo za aktivno trgovanje s kriptovalutami, ker nimajo potrpljenja za strategijo »kupi in drži«. Pri tem se pogosto zanašajo na relativno preproste strategije in indikatorje, ki jih oglašujejo vplivneži na različnih platformah z obljubami preprostega zaslužka. Trgovanje z vzvodom se lahko sliši mamljivo nekomu, ki verjame zgolj v pozitivno gibanje cen. Pogosto pa se takšna oseba ne zaveda, da lahko izgubi ves svoj denar, če se cena premakne v drugo smer od pričakovane. Razmišljanje s trezno glavo in zavedanje lastnih kompetenc pomagata pri zmanjšanju izpostavljenosti takšnim tveganjem. Če se posameznik odloči, da ga zanimajo kriptovalute, je smiselno začeti z majhno vsoto, ki jo je v najslabšem primeru pripravljen izgubiti (Dorfleitner in Lung, 2018).

7.2.2 Pretirano zaupanje neznancem

Internet, družbena omrežja in platforme za deljenje video vsebin so v zadnjih desetletjih korenito spremenile način komunikacije in širjenja informacij. Ob tem pa se je potrebno zavedati, da imajo takšne spremembe lahko tako pozitivne kot negativne posledice (Fruhlinger, 2017). Kot je omenil tudi sogovornik v intervjuju, je za nove uporabnike kriptovalut zelo pomembno, katerim virom zaupajo, ker ima kvaliteta informacij še večji vpliv, ko se soočajo s finančnimi odločitvami. Pri tem je pomembno poudariti, da najbolj zabavni viri nimajo nujno najboljših informacij in da so dejanja t. i. vplivnežev pogosto motivirana z željo po lastnem dobičku: naj bo to promocija nepreverjenih projektov ali promocija projektov, v katerih imajo solastniški delež, brez potrebnih opozoril za svoje sledilce (Asmakov, 2022). Poleg tega obstajajo številne prevare, kjer z uporabniki navezujejo stik računi, ki se izdajajo za poznane posameznike. Pri tem morajo biti uporabniki še posebej pozorni na identifikatorje, ki omogočajo razlikovanje med resničnimi uporabniki in računi, ki zgolj kopirajo ime, sliko in opis profila vplivnežev (Chetioui in drugi, 2022). Poleg tega je smiselno informacije od ljudi, ki jih ne poznajo osebno, jemati z rezervo, ker najverjetneje ne poznajo njihovih motivov za neko objavo.

7.2.3 Slepo sledenje in čredni nagon

Ljudje redko sprejemajo odločitve le na podlagi objektivne logike. K neracionalnosti njihovih odločitev lahko prispevajo različni dejavniki, od lastnih čustev do tega, kaj počnejo drugi. V situacijah, ko ljudje niso prepričani, kako odreagirati, se pogosto ozirajo na dejanja drugih in jim slepo sledijo, ker se počutijo bolj varno v čredi, iz katere ne izstopajo. Primeri črednega nagona so lahko vidni tudi na finančnih trgih, ko vlagatelji slepo sledijo zgledu drugih, ker sami niso pripravljeni vložiti truda. Takšno ravnanje je pogosto najbolj razvidno na razvijajočih se trgih (med katere lahko vključimo tudi kriptovalute) zaradi asimetrije informacij. Čredni nagon lahko pripelje do pretiranega optimizma, ker vlagatelji kritično razmišljanje prepustijo drugim, sami pa zgolj ponavljajo svoje trenutno stališče in ne dopuščajo možnosti, da bi se lahko trend na neki točki spremenil. Pred črednim nagonom se je težko zaščititi zaradi predpostavke, da ima večina običajno prav. Po drugi strani je potrebno najti primerno raven skeptičnosti, ker absolutno zanikanje vsega praviloma tudi ni

produktivno. Menim, da morajo uporabniki dopuščati različna mnenja, poslušati različne argumente za in proti, jih razumeti in se na koncu pri sebi odločiti, katera stran jih je bolj prepričala. Ta proces je smiselno ponavljati v določenih časovnih intervalih, da preverijo, ali imajo vse strani še vedno enako močne argumente, ali se je morda situacija sčasoma spremenila (Dang in Lin, 2016).

7.3 Omejitve raziskave

Največji izziv mi je predstavljalo zbiranje podatkov, ker je bilo težko najti spletne strani z arhivi objav s celega področja kriptovalut. Pri tem sem iskal predvsem strani z daljšo zgodovino objav, da bi lahko s podatki prikazal trende, ki so se dogajali v daljšem časovnem obdobju. S tega vidika bi lahko izhodiščni nabor podatkov razširil z več viri, vendar pa bi to verjetno močno vplivalo na trajanje obdelave podatkov, ker jih nisem obdeloval zgolj s pomočjo računalnika ampak tudi ročno. Poleg tega bi lahko za identifikacijo relevantnih objav uporabil bolj prefinjen filter, čeprav je včasih težko predvideti kvaliteto rezultatov pri velikem naboru vhodnih podatkov. To mislim predvsem z vidika lažnih pozitivnih ali lažnih negativnih naslovov objav, ker filter v PowerBI gleda le na to, ali neko besedilo vsebuje določene besede in ne upošteva konteksta, v katerem je beseda uporabljena. Lestvica največjih vdorov v zgodovini kriptovalut se lahko sčasoma spreminja; prav tako sem med pregledom različnih virov opazil, da se oškodovanci in vsote odtujenih sredstev lahko med njimi v neki meri razlikujejo. Odločil sem se za vir vdorov, ki ga smatram za legitimnega, lahko pa bi ob uporabi podatkov z drugih virov prišel do rahlo drugačnih rezultatov, čeprav dvomim, da bi uporaba drugega vira največjih vdorov drastično spremenila rezultate moje raziskave. Svoje ugotovitve bi lahko tudi podkrepil z več intervjuvanci. Žal mi zaradi predvidenih časovnih okvirov in neodzivnosti nekaterih potencialnih sogovornikov ni uspelo dobiti mnenja več kot enega strokovnjaka. Menim, da bi lahko bila to dobra iztočnica za nadaljnje raziskovanje, ki bi omogočila celovitejši vpogled v obravnavano problematiko.

8 SKLEP

Namen magistrskega dela je bila identifikacija in analiza ključnih varnostnih praks na področju uporabe kriptovalut, da bi z njimi prispeval k zmanjšanju števila uporabnikov, ki zaradi pomanjkanja razumevanja tega področja izgubljajo svoja sredstva. Nepovratnost transakcij na blockchainu je lahko še posebej problematična za nove uporabnike, ker lahko kakršnokoli neprevidno dejanje pripelje do trajne izgube denarja. Menim, da sem uspel doseči cilje, ki sem si jih zadal v uvodu. V magistrskem delu sem predstavil definicije ključnih pojmov na področjih kibernetske varnost in decentraliziranih omrežij. Ob tem sem predstavil tudi različne tehnike, ki jih uporabljajo kriminalci za razbijanje uporabniških gesel, največje digitalne vdore na področju kriptovalut in na sploh razvoj šifrirnih algoritmov, ki so temelji modernih finančnih sistemov in različne tehnične lastnosti decentraliziranih platform, na katerih lahko uporabljamo kriptovalute.

Analizo pogostosti objav o digitalnih vdorih na področju kriptovalut sem prikazal s stolpčnim diagramom, na podlagi katerega sem ugotovil, da večjim vdorom pogosto sledijo obdobja povečanega števila objav. Prav tako sem opazil, da se je večina največjih vdorov na področju kriptovalut zgodila v obdobju enega leta med decembrom 2021 in decembrom 2022. Na podlagi svojih opažanj in ugotovitev zaključujem, da mnoge platforme in institucije niso primerno poskrbele za varnost svojih uporabnikov. Na podlagi besednega oblaka, ki sem ga ustvaril, ugotavljam, da publikacije pogosteje poročajo o večjih odtujitvah premoženja in redkeje o nezgodah posameznikov, če niso oškodovani za veliko količino denarja. Svojo raziskavo sem dodatno podkrepil z intervjujem s strokovnjakom s področja kibernetske varnosti in razvoja kriptovalut. Ta je potrdil, da mnogi uporabniki niso dovolj informirani in previdni pri uporabi kriptovalut. Poleg tega pogosto nepravilno ocenjujejo tveganja, povezana z njihovo uporabo, in precenjujejo lastno poznavanje tega področja.

Na podlagi ugotovitev pregleda literature, analize naslovov objav in intervjuja s strokovnjakom sem pripravil seznam najpogostejših nevarnosti za uporabnike kriptovalut. Da bi s svojim delom dodatno prispeval k zmanjšanju števila oškodovanih uporabnikov, sem ponudil predloge za zaščito pred najpogostejšimi varnostnimi ranljivostmi. Pri tem pa se je potrebno zavedati, da je praktično nemogoče popolnoma izničiti vsa tehnološka tveganja, ki se nanašajo na področje tehnologije, ki je trenutno še v razvoju. Lahko pa poskrbimo za potrebne varnostne ukrepe, da zmanjšamo izpostavljenost takšnim tveganjem in posledično izgubo finančnih sredstev.

LITERATURA IN VIRI

1. Afreen, S. (2023, 24. februar). Simplilearn. *Top 10 Programming Languages for Blockchain App Development*. Pridobljeno 1. avgusta 2023 s https://www.simplilearn.com/blockchain-programming-languages-article
2. Agency. (2021, 20. avgust). Cybersecurity & Infrastructure Security Agency. *Top Routinely Exploited Vulnerabilities*. https://cisa.gov/uscert/ncas/alerts/aa21-209a
3. Asmakov, A. (2022, 3. oktober). Decrypt. *Kim Kardashian to Pay $1.26 Million Fine for Illegally Shilling Ethereum Token*. Pridobljeno 8. maja 2023 s https://decrypt.co/111085/sec-charges-kim-kardashian-unlawfully-touting-cryptocurrency-ethereummax
4. Aydar, M., Cetin, S. C., Ayvaz, S., & Aygun, B. (2019). *Private key encryption and recovery in blockchain*. arXiv: 1907.04156.
5. Breia, R. (2022, 22. februar). Sensorium Arc. *Physical NFTs Explained*. Pridobljeno 24. marca 2023 s https://sensoriumxr.com/articles/physical-nfts-explained
6. Brown, J. (2017, 31. julij). ProQuest. *The Risks And Benefits Of Investing In Cryptocurrency*. https://www.proquest.com/pq1business/docview/1924628012
7. Buterin, V. (2021, 7. april). *Why sharding is great: demystifying the technical properties*. Pridobljeno 14. januarja 2023 s https://vitalik.ca/general/2021/04/07/sharding.html
8. Buterin, V. (2022a, 26. januar). *Soulbound*. Pridobljeno 25. marca 2023 s https://vitalik.ca/general/2022/01/26/soulbound.html

9. Buterin, V. (2022b, 23. april). Ethereum. *Whitepaper*. Pridobljeno 14. februarja 2023 s https://ethereum.org/en/whitepaper/
10. Calderbank, M. (2007, 20. avgust). The University of Chicago. *The RSA Cryptosystem: History, Algorithm, Primes*. https://www.math.uchicago.edu/~may/VIGRE/VIGRE2007/REUPapers/FINALAPP/Calderbank.pdf
11. Chandra, Y. (2022). Non-fungible token-enabled entrepreneurship: A conceptual framework. *Journal of Business Venturing Insights 18* (e00323).
12. Chaum, D. L. (1981). Untraceable electronic mail, return addresses, and digital pseudonyms. *Communications of the ACM*, 24(2), 84-90.
13. Chetioui, K., Bah, B., Alami, A. O., & Bahnasse, A. (2022). Overview of Social Engineering Attacks on Social Networks. *Procedia Computer Science*, 198, 656-661.
14. Computer security. (brez datuma). V *Encyclopaedia Britannica*. https://www.britannica.com/technology/computer-security
15. Cunha, P. R., Melo, P., & Sebastiao, H. (2021). From Bitcoin to Central Bank Digital Currencies: Making Sense of the Digital Money Revolution. *Future Internet*, 13(7), 165.
16. Cybersecurity. (brez datuma). V *Merriam-Webster dictionary*. https://www.merriam-webster.com/dictionary/cybersecurity
17. Dang, H. V., & Lin, M. (2016). Herd mentality in the stock market: On the role of idiosyncratic participants with heterogeneous information. *International Review of Financial Analysis*, 48, 247-260.
18. Davis, B. (2013, 21. avgust). The Guardian. *A brief history of banking: the link between money and society*. Pridobljeno 14. maja 2023 s https://www.theguardian.com/sustainable-business/history-banking-money-society
19. Diffie, W., & Hellman, M. (1976). New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6), 644-654.
20. Dorfleitner, G., & Lung, C. (2018). Cryptocurrencies from the perspective of euro investors: a re-examination of diversification benefits and a new day-of-the-week effect. *Journal of Asset Management*, 19(7), 472-494.
21. Dteckt (brez datuma). *Top 10 Critical Hacks Of All Time*. Pridobljeno 26. februarja s https://www.dteckt.com/critical-hacks
22. El-Kady, A. H., Halim, S., El-Halwagi, M. M., & Khan, F. (2023). Analysis of safety and security challenges and opportunities related to cyber-physical systems. *Process Safety and Environmental Protection*, 173, 384-413.
23. Elsevier Ltd. (2004). Sasser worm rises out of MS patch thicket. *Computer Fraud & Security*, 2004(5), 2.
24. Fernando, J. (2015, 20. april). Investopedia. *Bitcoin Vs. Litecoin: What's The Difference?* Pridobljeno 14. februarja 2023 s https://www.investopedia.com/articles/investing/042015/bitcoin-vs-litecoin-whats-difference.asp

25. Fruhlinger, J. (2017, 23. junij). CSO. *New social media scams: Can you tell friend from foe?* Pridobljeno 31. julija 2023 s https://www.csoonline.com/article/562085/new-social-media-scams-can-you-tell-friend-from-foe.html
26. Fryer, H., Stalla-Bourdillon, S., & Chown, T. (2015). Malicious web pages: What if hosting providers could actually do something…. *Computer Law & Security Review*, 31(4), 490-505.
27. Furnell, S. (2022). Assessing website password practices – Unchanged after fifteen years? *Computers & Security*, 120, 102790.
28. George, K. (2022, 17. november). Investopedia. *The Largest Cryptocurrency Hacks So Far*. Pridobljeno 10. maja 2023 s https://www.investopedia.com/news/largest-cryptocurrency-hacks-so-far-year/#toc-mt-gox-473-million
29. Gkioulos, V., Wangen, G., Katsikas, S. K., Kavallieratos, G., & Kotzanikolaou, P. (2017). Security Awareness of the Digital Natives. *Information*, 8(2), 42.
30. Goschenko, S. (2021, 19. junij). Bitcoin.com. *Ledger Customers Are Being Mailed Fake Wallets to Steal Their Private Seeds*. https://news.bitcoin.com/ledger-customers-are-being-mailed-fake-wallets-to-steal-their-private-seeds/
31. Blackhat Ethical Hacking. (brez datuma). *Mafiaboy, the hacker who took down the internet*. Pridobljeno 28. februarja 2023 s https://www.blackhatethicalhacking.com/articles/hacking-stories/mafiaboy-the-hacker-who-took-down-the-internet/
32. Hamacher, A. (2022, 6. april). Decrypt. *How David Chaum Went From Inventing Digital Cash to Pioneering Digital Privacy*. Pridobljeno 29. junija 2023 s https://decrypt.co/95109/david-chaum-from-inventing-digital-cash-to-pioneering-digital-privacy
33. Hay Newman, L. (2023, 4. marec). Wired. *Security News This Week: The LastPass Hack Somehow Gets Worse*. https://www.wired.com/story/lastpass-engineer-breach-security-roundup/
34. He, D., Deng, Z., Zhang, Y., Chan, S., Cheng, Y., & Guizani, N. (2020). Smart Contract Vulnerability Analysis and Security Audit. *IEEE Network*, 34(5), 276-282.
35. Helms, K. (2021, 12. december). Bitcoin.com. *Prime Minister Modi's Twitter Account Hacked - Tweets Bitcoin Legal Tender in India, Government Giving Away BTC*. https://news.bitcoin.com/prime-minister-modis-twitter-account-hacked-tweets-bitcoin-legal-tender-in-india-government-giving-away-btc/
36. Islam, S. K. H., & Biswas, G. P. (2014). Certificateless short sequential and broadcast multisignature schemes using elliptic curve bilinear pairings. *Journal of King Saud University - Computer and Information Sciences*, 26(1), 89-97.
37. Ivanov, N., & Yan, Q. (2021). EthClipper: A Clipboard Meddling Attack on Hardware Wallets with Address Verification Evasion. *2021 IEEE Conference on Communications and Network Security (CNS)*
38. Kernel, E. (2019, 6. avgust). ITBriefcase. *How the SSL Protocol Changed the Internet*. https://www.itbriefcase.net/how-the-ssl-protocol-changed-the-internet

39. Khan, M. T. I., Tan, S.-H., Chong, L.-L., & Ong, H.-B. (2017). Investment characteristics, stock characteristics and portfolio diversification of finance professionals. *Borsa Istanbul Review*, 17(3), 164-177.
40. Kinsta (2022, 20. september). *TLS vs SSL: What's the Difference? Which One Should You Use?* Pridobljeno 23. februarja 2023 s https://kinsta.com/knowledgebase/tls-vs-ssl/
41. Kruger, J., & Dunning, D. (1999). Unskilled and unaware of it: How difficulties in recognizing one's own incompetence lead to inflated self-assessments. *Journal of Personality and Social Psychology*, 77(6), 1121-1134.
42. Kumar Sharma, D., Chidananda Singh, N., Noola, D. A., Nirmal Doss, A., & Sivakumar, J. (2022). A review on various cryptographic techniques & algorithms. *Materials Today: Proceedings*, 51, 104-109.
43. Labrys (brez datuma). MEV Watch. *Post-Merge OFAC Compliant Blocks*. Pridobljeno 14. januarja 2023 s https://www.mevwatch.info/
44. Lakshmanan, R. (2022, 23. februar). The Hacker News. *25 Malicious JavaScript Libraries Distributed via Official NPM Package Repository*. https://thehackernews.com/2022/02/25-malicious-javascript-libraries.html
45. Wang, K. (2021). Crypto.com. *Measuring Global Crypto Users*. https://crypto.com/images/202107_DataReport_OnChain_Market_Sizing.pdf
46. Misoch, S. (2015). Stranger on the internet: Online self-disclosure and the role of visual anonymity. *Computers in Human Behavior*, 48, 535-541.
47. N26. (2022, 10. oktober). *What is Dogecoin (DOGE) and how does it work?* Pridobljeno 8. aprila 2023 s https://n26.com/en-at/blog/what-is-dogecoin
48. Nagarajan, S. (2023, 26. januar). Blockworks. *Lessons From Proof Founder Kevin Rose's $1.4M NFT Phishing Experience*. https://blockworks.co/news/lessons-from-proof-founder-kevin-roses-1-4m-nft-phishing-experience
49. Nakamoto, S. (2008, 31. oktober). Bitcoin.org. *Bitcoin: A Peer-to-Peer Electronic Cash System*. https://bitcoin.org/bitcoin.pdf
50. Octoparse. (brez datuma). Pridobljeno 23. januarja 2023 s www.octoparse.com
51. Pilkington, E. (2021, 4. september). The Guardian. *'Panic made us vulnerable': how 9/11 made the US surveillance state – and the Americans who fought back*. https://www.theguardian.com/world/2021/sep/04/surveillance-state-september-11-panic-made-us-vulnerable
52. Porterfield, C. (2022, 3. julij). Forbes. *British Army's YouTube And Twitter Accounts Hacked—And Flooded With Crypto Posts*. https://www.forbes.com/sites/carlieporterfield/2022/07/03/british-armys-youtube-and-twitter-accounts-hacked-and-flooded-with-crypto-posts/
53. Reiff, N. (2021, 25. oktober). Investopedia. *B-Money: Overview, Goals, Differences From Bitcoin*. Pridobljeno 26. marca 2023 s https://www.investopedia.com/terms/b/bmoney.asp
54. Rekt. (2021a, 11. avgust). *Poly Network - Rekt*. https://rekt.news/polynetwork-rekt/
55. Rekt. (2021b, 5. december). *BitMart - Rekt*. https://rekt.news/bitmart-rekt/
56. Rekt. (2022a, 3. februar). *Wormhole - Rekt*. https://rekt.news/wormhole-rekt/
57. Rekt. (2022b, 29. marec). *Ronin Network - Rekt*. https://rekt.news/ronin-rekt/

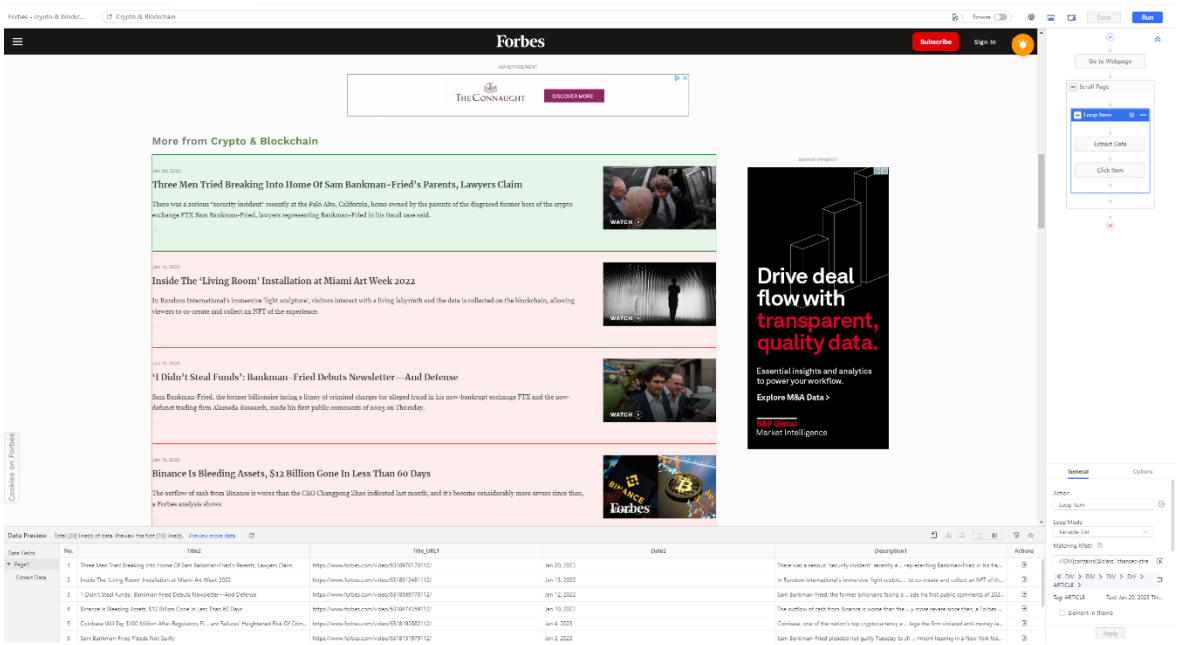
58. Rekt. (2022c, 2. avgust). *Nomad Bridge - Rekt*. https://rekt.news/nomad-rekt/
59. Rekt. (2022d, 7. oktober). *BNB Bridge - Rekt*. https://rekt.news/bnb-bridge-rekt/
60. Rekt. (2022e, 18. november). *SBF - Mask Off*. https://rekt.news/sbf-mask-off/
61. Rose, C. (2015). The Evolution Of Digital Currencies: Bitcoin, A Cryptocurrency Causing A Monetary Revolution. *The International Business & Economics Research Journal (Online)*, 14(4), 617.
62. Shevchenko, A. (2020, 1. april). Cointelegraph. *Proof-of-Stake vs. Proof-of-Work: Which one is 'Fairer'?* https://cointelegraph.com/news/proof-of-stake-vs-proof-of-work-which-one-is-fairer
63. Shevtekar, P., Raut, A., & Chaudhari, P. (2022). Fundraising Tracking System Using Blockchain. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 165-172.
64. Singh, A., Parizi, R. M., Zhang, Q., Choo, K.-K. R., & Dehghantanha, A. (2020). Blockchain smart contracts formalization: Approaches and challenges to address vulnerabilities. *Computers & Security*, 88, 101654.
65. Sukianto, A. (2023, 11. januar). Upguard. *IT Risk Management vs Cybersecurity?* Pridobljeno 14. februarja 2023 s https://www.upguard.com/blog/it-risk-management-vs-cybersecurity
66. Sundar, V. (2017, 28. marec). Indusface. *12 Most Notorious Hacks History*. Pridobljeno 25. februarja 2023 s https://www.indusface.com/blog/12-notorious-hacks-history/
67. Sunmola, F., & Burgess, P. (2023). Transparency by Design for Blockchain-Based Supply Chains. *Procedia Computer Science*, 217, 1256-1265.
68. Tassev, L. (2022, 4. september). Bitcoin.com. *South Korean Government's Youtube Channel Hacked to Play Crypto Video With Elon Musk*. https://news.bitcoin.com/south-korean-governments-youtube-channel-hacked-to-play-crypto-video-with-elon-musk/
69. Thouti, S., Venu, N., Rinku, D. R., Arora, A., & Rajeswaran, N. (2022). Investigation on identify the multiple issues in IoT devices using Convolutional Neural Network. *Measurement: Sensors*, 24, 100509.
70. Tidy, J., & Radford, A. (2023, 10. maj). BBC. *Briton pleads guilty in US to 2020 Twitter hack*. Pridobljeno 11. maja 2023 s https://www.bbc.com/news/technology-65540901
71. U.S. Department of the Treasury. (2022, 8. avgust). *U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash*. Pridobljeno 14. januarja 2023 s https://home.treasury.gov/news/press-releases/jy0916
72. Wackerow, P. (2022, 15. avgust). Ethereum.org. *Programming Languages*. Pridobljeno 1. aprila 2023 s https://ethereum.org/en/developers/docs/programming-languages/
73. Weston, G. (2022, 21. december). 101Blockchains. *List Of Top Blockchains Using The Rust Programming Language*. https://101blockchains.com/top-blockchains-using-rust-programming-language/
74. Wolff, J. (2022, 22. februar). Slate. *Is Multifactor Authentication Less Effective Than It Used To Be?* https://slate.com/technology/2022/02/google-multifactor-authentication-effective-research.html

75. Yildirim, N., & Varol, A. (2019). A Research on Security Vulnerabilities in Online and Mobile Banking Systems. *2019 7th International Symposium on Digital Forensics and Security (ISDFS)*
76. Young, S. D., & Keoun, B. (2022, 12. november). Coindesk. *The Epic Collapse of Sam Bankman-Fried's FTX Exchange: A Crypto Markets Timeline*. https://www.coindesk.com/markets/2022/11/12/the-epic-collapse-of-sam-bankman-frieds-ftx-exchange-a-crypto-markets-timeline/
77. Yu, F., & Huang, Y. (2015). An Overview of Study of Passowrd Cracking. *2015 International Conference on Computer Science and Mechanical Automation (CSMA)*

PRILOGE

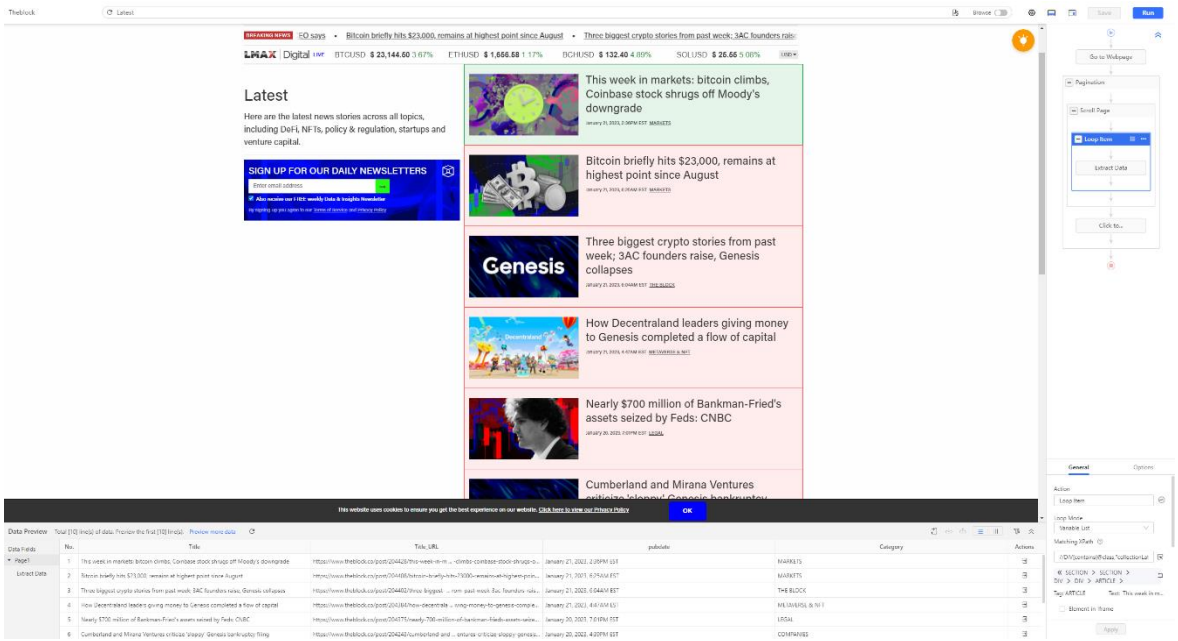
Priloga 1: Sliki posnetkov zaslona orodja Octoparse pri zbiranju podatkov s spletnih virov

Slika 1: Spletna stran forbes.com/archive in uporabniški vmesnik v Octoparsu



Vir: Octoparse (brez datuma).

Slika 2: Spletna stran theblock.co/archive in uporabniški vmesnik v Octoparsu



Vir: Octoparse (brez datuma).

Priloga 2: Nabor izhodiščnih vprašanj intervjuja

1. Katera so po vaših izkušnjah najpogostejša tveganja, ki smo jim izpostavljeni uporabniki kriptovalut?
2. Ali menite, da se tveganja povezana z uporabo kriptovalut razlikujejo od drugih tehnoloških tveganj?
3. Kolikšen deleža zaznanega kriminala je po vaših informacijah povezanega s kriptovalutami?
4. Se vam zdi, da so uporabniki kriptovalut dovolj podučeni o delovanju tehnologije blockchaina in pametnih pogodb, ki se na njih izvajajo?
5. Kateri so po vašem mnenju ključni dejavniki, ki ogrožajo varnost uporabnikov kriptovalut?
6. Kako lahko po vašem mnenju uporabniki zmanjšajo izpostavljenost tehnološkim tveganjem, povezanim z uporabo kriptovalut?

Priloga 3: DAX funkcija, ki iz vhodnih podatkov obdrži tiste, ki vsebujejo besede s korenom »steal« ali »hack«.

```
Forbes Filtered = CALCULATETABLE('Forbes Data',
   FILTER( ALL('Forbes Data'),
      SEARCH("steal", 'Forbes Data'[Naslov],, BLANK ())
      || SEARCH("hack", 'Forbes Data'[Naslov],, BLANK ())
))
```

Priloga 4: DAX funkcija, ki združi nabore podatkov s treh virov v skupni nabor z nazivom »Vsi Podatki«

```
Vsi Podatki = UNION(
        SELECTCOLUMNS('Forbes Data',
                "Naslov", 'Forbes Data'[Naslov],
                "Datum", 'Forbes Data'[Datum],
                "Vir", "Forbes"),
        SELECTCOLUMNS('Bitcoin.com Data',
                "Naslov", 'Bitcoin.com Data'[Naslov],
                "Datum", 'Bitcoin.com Data'[Datum],
                "Vir", "Bitcoin.com"),
        SELECTCOLUMNS('The Block Data',
                "Naslov", 'The Block Data'[Naslov],
                "Datum", 'The Block Data'[Datum],
                "Vir", "The Block")
)
```

Priloga 5: DAX funkcija, ki iz celotnega nabora zbranih podatkov izlušči relevantne podatke na podlagi iskalnih parametrov

```
Full Data Filtered = CALCULATETABLE('Full Data',
   FILTER( ALL('Full Data'),
      SEARCH("steal", 'Full Data'[Naslov],, BLANK ())
       && NOT SEARCH("stealt", 'Full Data'[Naslov],, BLANK())
       || SEARCH("hack", 'Full Data'[Naslov],, BLANK ())
       || SEARCH("thief", 'Full Data'[Naslov],, BLANK ())
       || SEARCH("theft", 'Full Data'[Naslov],, BLANK ())
       || SEARCH("stole", 'Full Data'[Naslov],, BLANK ())
       || SEARCH("attack", 'Full Data'[Naslov],, BLANK ())
))
```