VILNIAUS UNIVERSITETAS KAUNO FAKULTETAS

SOCIALINIŲ MOKSLŲ IR TAIKOMOSIOS INFORMATIKOS INSTITUTAS

Finansų technologijų studijų programa
Kodas 6211BX022

ELIGIJUS ABROMIKAS

MAGISTRO BAIGIAMASIS DARBAS

BELAIDĖS NUO TINKLO ATJUNGTOS APARATINĖS BITCOINŲ PINIGINĖS PROTOTIPAS

Kaunas 2025

VILNIAUS UNIVERSITETAS KAUNO FAKULTETAS

SOCIALINIŲ MOKSLŲ IR TAIKOMOSIOS INFORMATIKOS INSTITUTAS

ELIGIJUS ABROMIKAS

MAGISTRO BAIGIAMASIS DARBAS

BELAIDĖS NUO TINKLO ATJUNGTOS APARATINĖS BITCOINŲ PINIGINĖS PROTOTIPAS

PROTOTYPE OF AN OFFLINE AIR-GAPPED HARDWARE BITCOIN WALLET

Magistrantas _____
(parašas)

Darbo vadovas _____
(parašas)

Darbo vadovas doc. dr. Saulius Masteika
(darbo vadovo mokslo laipsnis, mokslo pedagoginis vardas, vardas ir pavardė)

Darbo įteikimo data:
Registracijos Nr.

Kaunas 2025

TURINYS

SANTRUMPŲ SĄRAŠAS

API – Aplikacijų programavimo sąsaja (angl. Application Programming Interface)

BIP – standartai, specifikacijų ir pasiūlymų rinkiniai, skirti Bitcoin protokolui tobulinti (angl. Bitcoin Improvment Proposal).

CLI – Komandinės eilutės sąsaja.

CSI – tai jungtis, naudojama kameroms prijungti prie procesorių ar mikrokontrolierių.

DeFi – Decentralizuotas finansavimas.

EAL – Vertinimo užtikrinimo lygis, tarptautinis standartas (angl. Evaluation Assurance Level).

ECDSA – Elipsinių kreivių skaitmeninio parašo algoritmas, šifravimo algoritmas. (angl, Elliptic Curve Digital Signature Algorithm).

GUI – Grafinė vartojo sąsaja.

HDMI – standartizuota sąsaja, skirta perduoti aukštos raiškos vaizdo ir garso signalus tarp įrenginių.

HDR – vaizdo technologija, kuri pagerina spalvų, kontrasto ir spalvų diapazoną.

LCD – ekrano technologija, kuri naudoja skystuosius kristalus šviesai moduliuoti.

MITM – „Žmogus viduryje“, atakos forma, kai užpuolikas perima ir galimai modifikuoja ryšį tarp dviejų šalių.

NFC – Artimojo lauko ryšys (angl. Near Field Comunication).

PSBT – standartizuotas Bitcoin operacijos formatas, skirtas sudaryti ir dalinai pasirašyti operacijas (angl. Partially Signed Bitcoin Transaction).

QR kodas – dvimatė brūkšninių kodų forma, kuri koduoja informacija į kvadratinę matrica.

SE – Saugus elementas.

SHA-256 – Saugus maišos algoritmas, kriptografinė funkcija.

SPI – duomenų perdavimo protokolas, skirtas mikrokompiuterių ir periferinių įrenginių ryšiui.

USB – standartizuota sąsaja, skirta duomenų perdavimui ir energijos tiekimui tarp įrenginių.

PAVEIKSLŲ SĄRAŠAS

LENTELIŲ SĄRAŠAS

Eligijus Abromikas (2025). *Prototype of an offline air-gapped hardware bitcoin wallet*. MBA Graduation Paper. Kaunas: Vilnius University, Kaunas Faculty, Institute of Social Sciences and Applied Informatics. 74 p.

SUMMARY

The contemporary financial sector, particularly the cryptocurrency and Bitcoin ecosystem, is undergoing rapid transformation, driving and development of new technological solutions and financial innovations. As their adoption and value continue to grow, the need for secure and reliable storage methods has become increasingly critical. While many users still store cryptocurrencies online, there is a rising demand for solutions that offer enhanced security and greater user control. To address this need, the market has introduced various commercial hardware wallets capable of safeguarding users' private keys by storing them offline, within the wallet, rather than on a network.

However, many hardware wallets users encounter security vulnerabilities related to the collection and potential misuse of personal data, especially in the context of social engineering attacks. Supply chain attacks pose additional risks during production or logistics, as devices may be compromised with malicious software or hardware.

Non-custodial wireless hardware Bitcoin wallets, operating without direct network connectivity, has emerged as an innovative and reliable solution that ensures greater security, anonymity and independence from third party control. The objective of this study was to develop a non-custodial wireless air gapped Bitcoin wallet constructed using standard, universal components that were not originally designed for the fintech or cryptocurrency markets.

A prototype of the wallet was successfully developed, functioning offline and utilizing QR codes for transaction operations. The prototype, was assembled from universal and standard components and with Python base software, delivers all the basic Bitcoin wallet functionalities. Its modular architecture and use of standard components mitigate the risk with supply chain attacks, enhancing overall security. The developed wallet is non-custodial, operates offline, and effectively renders attacks such as social engineering or software-based exploits ineffective.

This paper has 55 pages, 9 tables and 12 pictures.

ĮVADAS

Temos aktualumas

Šiuolaikinio finansų sektorius sparčiai transformuojasi, skatindamas naujų technologinių sprendimų ir finansinių inovacijų kūrimą. Kriptovaliutos, tokios kaip Bitcoin, tapo neatsiejama finansų rinkų dalimi, keičiančia tradicinio finansų valdymo ir investavimo būdus, pritraukiančius tiek institucijų, investuotojų, tiek individualių vartotojų dėmesį. Didėjant jų naudojimo mastui ir vertei, vis aktualesnis tampa saugaus ir patikimo jų laikymo poreikis.

Daugelis kritptovaliutas saugo internete, tačiau, didėjant sumoms bei augant kibernetinių grėsmių skaičiui, kai technologiją pradeda suprasti vis daugiau žmonių, išryškėjo poreikis kurti saugias ir nepriklausomas nuo interneto aparatines pingines, kurios leidžia apsaugoti turimus skaitmeninius aktyvus. Populiarėjant kriptovaliutų naudojimui, didėja ir poreikis įdiegti atitinkamus sprendimus, užtikrinančius didesnį saugumą. Rinkoje šiam poreikiui patenkinti atsirado įvairių komercinių ir net tik, aparatūrinių piniginių, kurios gali užtikrinti didesnį saugumą, saugant vartotojų privačius raktus, juos laikant piniginės viduje, o ne tinkle. Komercinės aparatinės piniginės, dažnai veikiančios su tinklo ryšiu, taip pat kelia papildomų pavojų, susijusių su asmeninių duomenų rinkimu ir jų galimai neteisėtu panaudojimu. Tokios aplinkybės sukuria būtinybę ieškoti sprendimų, kurie užtikrintų didesnį vartotojų saugumą, anonimiškumą ir nepriklausomybę.

Belaidės aparatinės Bitcoinų piniginės, veikiančios be tiesioginio tinklo ryšio, išryškėja kaip inovatyvus ir patikimas sprendimas, užtikrinantis didesnį saugumą, anonimiškumą bei nepriklausomumą nuo trečiųjų šalių kontrolės. Atsižvelgiant į spartų kriptovaliutų naudojimo augimą, tokios piniginės ne tik atitinka saugumo reikalavimus, bet ir atliepia reguliavimo institucijų bei vartotojų poreikius dėl didesnio kriptovaliutų valdymo skaidrumo ir kontrolės. Moksliniame darbe nagrinėjama, kodėl iš nepriklausomų elementų surinkta belaidė nuo tinklo atjungta aparatūrinė Bitcoinų piniginė yra optimalus sprendimas, kuris apsaugo vartotojų privatumą, išlaiko anonimiškumą ir sumažina kibernetinių grėsmių, tokių kaip socialinės inžinerijos, tiekimo grandinės rizikas.

Problemos ištyrimo lygis

Šiuolaikinėje skaitmeninėje ekonomikoje Bitcoin, kaip decentralizuota kriptovaliuta, įgyja vis didesnį populiarumą, tačiau kartu auga ir su ja susijusios saugumo rizikos. Aparatinės piniginės, laikomos saugesnėmis už internetines alternatyvas, vis dėlto nėra visiškai apsaugotos nuo grėsmių. Moksliniai tyrimai rodo, kad net ir neprijungtos prie interneto piniginės nėra visiškai apsaugotos nuo

saugumo grėsmių (Davenport ir Shetty (2019), Guri, (2018)). Literatūroje aprašomos šalutinio kanalo atakos, kenkėjiškų programų panaudojimas ir socialinės inžinerijos ataka (Park ir kt. (2023), Voletly ir kt., (2019)). Be to, tyrimai rodo, kad Bitcoin piniginių naudotojai kartais nesilaiko saugumo rekomendacijų, todėl padidėja jų pažeidžiamumas. Pavyzdžiui, jie gali naudoti silpnus slaptažodžius, nepakankamai apsaugoti savo įrenginius arba tapti sukčiavimo aukomis (Khanum ir Mustafa, (2022), Houy ir kt. (2023)).

Belaidės nuo tinklo atjungtos aparatūrinės Bitcoinų piniginės saugumo problemų sprendimas yra itin svarbus dėl kelių priežasčių (finansinių nuostolių prevencija, pasitikėjimo kriptovaliutų ekosistema skatinimas ir reguliacinių reikalavimų atitikimas). Atsižvelgiant į tai, itin svarbu kurti ir tobulinti saugias, patikimas ir naudotojui patogias Bitcoinų pinigines, kurios būtų atsparios įvairioms saugumo grėsmėms. Šio tyrimo tikslas – ištirti ir įvertinti belaidės nuo tinklo atjungtos aparatūrinės Bitcoin piniginės prototipo saugumo aspektus, siekiant prisidėti prie Bitcoin ekosistemos saugumo stiprinimo.

Darbo problema. Kaip sukurti belaidės nuo tinklo atjungtos aparatūrinės Bitcoinų piniginės prototipą, kuris būtų decentralizuotas, privatus, sudarytas iš standartinių elementų ir atjungtas nuo tinklo?

Darbo objektas. Belaidė nuo tinklo atjungta aparatūrinė Bitcoinų piniginė.

Darbo tikslas. Sukurti anonimišką, decentralizuotą belaidės nuo tinklo atjungtos aparatūrinės Bitcoinų piniginės prototipą, kuris užtikrintų nepriklausomą veikimą be interneto ryšio ir leistų atlikti pavedimus naudojant belaidžio ryšio sprendimus.

Darbo uždaviniai:

1. Išnagrinėti esamus kriptovaliutų piniginių tipus, jų veikimo principus, privalumus.
2. Nustatyti aparatinių kriptovaliutų piniginių trūkumus ir saugumo spragas.
3. Išanalizavus egzistuojančias problemas, pasiūlyti pinginės sprendimą, prototipą kuris sumažina tiekimo grandinės, tarpininko ir socialinės inžinerijos grėsmių riziką.
4. Atlikti prototipo sukūrimą ir testavimą.
5. Įvertinus eksperimentus ir sukurtą prototipą, suformuluoti išvadas ir galimus tolimesnius veiksmus, sprendimus, kuriant belaidę nuo tinklo atjungtą aparatūrinę Bitcoinų piniginę.

Darbo struktūra

Pirmojoje darbo dalyje „Aparatūrinių kriptovaliutų piniginių apžvalga“ atlikta išsami esamų aparatūrinių Bitcoin piniginių analizė. Aptariami jų tipai, funkcionalumo ypatumai ir pagrindinės klasifikacijos, pabrėžiant įvairius technologinius sprendimus bei naudojamus kriptografinius

algoritmus. Taip pat analizuojamos ir saugumo problemos, įvardijami kibernetinių atakų metodai, dažniausiai taikomi prieš vartotojus, siekiant identifikuoti pagrindinius aparatūrinių piniginių pažeidžiamumus.

Antroje darbo dalyje „Prototipo sprendimo metodika ir modelis“ pristatomas siūlomas sprendimas pagrindinių aparatūrinių piniginių pažeidžiamumų, nustatytų pirmojoje dalyje, sprendimui. Detalizuojami prototipui naudojami techniniai komponentai ir programinė įranga, kartu pateikiama pagrįsta argumentacija dėl pasirinkimo. Taip pat pateikiamas išsamus modelio veikimo principų aprašymas.

Trečiojoje darbo dalyje „Belaidės nuo tinklo atjungtos aparatūrinės Bitcoin piniginės prototipas“ pagal pateiktą sprendimą kuriamas prototipas.

Darbo pabaigoje pateikiama atlikto darbo rezultatai ir išvados, siūlymai, kaip būtų galima tobulinti sukurtą prototipą bei gairės tolimesniems tyrimams.

Darbe naudoti literatūros šaltiniai

Teorinėje dalyje remtasi užsienio autorių moksliniais tyrimais, analizuojančiais aparatines Bitcoin pinigines, jų tipus ir problematiką, išskiriant pagrindinius aparatinių piniginių pažeidžiamumus. Naudota mokslinė literatūra, nagrinėjanti piniginių veikimo principus ir technologijos pagrindus, informacija iš internetinių šaltinių, kur pateikiama išsami analizė apie aparatinių piniginių programinę bei aparatūrinę įrangą, apimant technines specifikacijas, veikimo principus ir praktinio pritaikymo aspektus.

Darbo ir tyrimo metodai

Analizuojant aparatines Bitcoinų pinigines, jų tipus ir problematiką, taikyti lyginamosios analizės, mokslinės literatūros analizė, sintezės, abstrahavimo, indukcijos ir dedukcijos metodai. Kuriamas pasiūlytas piniginės prototipas.

Darbo rezultatų teorinė ir praktinė reikšmė

- Išanalizuoti ir aprašyti rinkoje esantys aparatūrinių piniginių tipai.
- Išanalizavus esamas aparatūrines pinigines, palyginti esami sprendimai ir technologijos.
- Susistemintos literatūros šaltiniuose pateikiamos atakos prieš aparatūrines pinigines, jų tipai.
- Išanalizavus problemas, pasiūlytas sprendimas, prototipas, kuris išsprendžia tiekimo grandinės, socialinės inžinerijos ir programavimo grėsmių riziką.
- Suskurtas piniginės prototipas.

• Įgyvendinus prototipą pateikiamas rekomendacinis tobulinimų aprašymas.

Darbo apribojimai ir sunkumai

Belaidžių neprijungtų aparatinių Bitcoin piniginių inovatyvumas ir technologinis naujumas lėmė ribotą mokslinių tyrimų ir literatūros kiekį šia tema. Itin mažai darbų, susijusių su savadarbėmis aparatūrinėmis piniginėmis, tačiau tokių pavyzdžių yra daugiau ne mokslinio pagrindo erdvėje.

Darbo struktūra ir apimtis

Darbą sudaro įvadas, 3 darbo dalys, išvados ir pasiūlymai. Pagrindinė darbo dalis 55 puslapiai, įskaitant 9 lenteles ir 12 paveikslų. Literatūros sąrašą sudaro 38 šaltiniai.

1. APARATŪRINIŲ KRIPTOVALIUTŲ PINIGINIŲ APŽVALGA

Šiame skyriuje analizuojama kriptovaliutų piniginių tipai, ypatingą dėmesį skiriant aparatinių Bitcoin piniginių klasifikacijai. Aptariamos skirtingos aparatinių piniginių rūšys, jų funkcionalumo ypatumai ir technologiniai sprendimai. Pateikiama naudojamų komponentų apžvalga, atliekamas esamų piniginių palyginimas, išryškinami jų trūkumai ir aptariamos pagrindinės problemos. Taip pat nagrinėjami kibernetiniai išpuoliai ir kiti potencialių grėsmių tipai, nukreipti prieš aparatines pinigines.

1.1. Bitcoin, kaip finansinio instrumento, svarba finansų rinkose

Bitcoin, kaip pirmoji ir žinomiausia kriptovaliuta, nuo savo atsiradimo 2009 m. tapo reikšmingu finansiniu instrumentu, darančiu vis didesnę įtaka tradicinėms finansų rinkoms. Šiame skyriuje analizuojama Bitcoin reikšmė finansų rinkose, akcentuojant jo unikalius bruožus, teikiamas galimybes ir kylančius iššūkius. Aptariamas nuolat augantis poreikis sukurti saugias ir patikimas šios kriptovaliutos saugojimo priemones, siekiant užtikinti jos efektyvų ir saugų naudojimą.

Pasak Dumitrescu (2017), vienas pagrindinių Bitcoin privalumų yra tai, kad ši valiuta yra atspari infliacijai. Dėl savo ribotos pasiūlos kiekio yra puikus apsidraudimo nuo infliacijos įrankis, ypač šalyse, kuriose infliacija itin aukšta. Autorius taip pat išskiria, kad atsiskaitymai kriptovaliutomis užtikrina anonimiškumą, apsaugo vartotojų privatumą ir suteikia papildomą saugumo lygį. Autoriai Badea ir Mungiu-Pupazan (2021) taip pat pažymi, kad Bitcoin yra globaliai prieinama valiuta, leidžianti atlikti sandorius visame pasaulyje bet kuriam asmeniui, turinčiam interneto prieigą, todėl ją galima laikyti universaliu finansiniu instrumentu. Autorių teigimu, valiuta veikia decentralizuotame tinkle, ji nepriklauso nuo jokios centrinės institucijos, tokios kaip bankas ar šalies vyriausybė, ir ši savybė tampa itin reikšminga siekiant finansinės nepriklausomybės.

Didėjant Bitcoin vertei ir populiarumui, vis svarbesnis tampa saugus ir patikimas šios valiutos saugojimas. Neprijungtos prie interneto (angl. offline) piniginės tampa vis populiaresnės, nes jos yra atsparesnės įsilaužimams ir kitoms saugumo grėsmėms. Šiame darbe nagrinėjama, kaip neprijungtos prie interneto piniginės gali prisidėti prie Bitcoin, kaip patikimos finansinės priemonės, plėtros.

Bitcoin yra novatoriškas finansinis instrumentas, galintis pakeisti finansų rinkų veikimą. Nors jis suteikia daug galimybių, svarbu atsižvelgti ir į su juo susijusius iššūkius, ypač saugumo srityje. Tolesniuose šio darbo skyriuose išsamiau nagrinėjamos konkrečios Bitcoin taikymo sritys ir jų

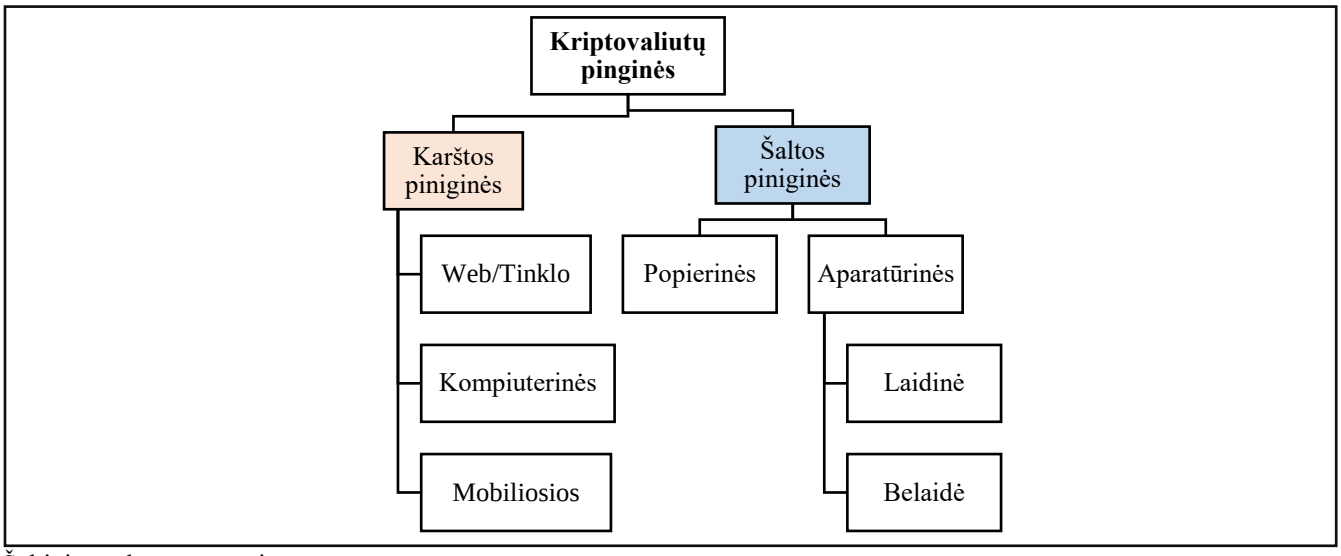
pasekmės finansų sistemai, ypatingą dėmesį skiriant saugioms ir patikimoms Bitcoin saugojimo priemonėms.

1.2. Kriptovaliutų piniginių tipai

Kriptovaliutų piniginės – pagrindinis įrankis, užtikrinantis vartotojams galimybę saugiai saugoti, siųsti ir gauti Bitcoin bei kitas kriptovaliutas, taip sudarant sąlygas efektyviam ir patikimam šių skaitmeninių aktyvų valdymui. Jos veikia kaip virtualios piniginės, kuriose yra saugomi vartotojo viešieji ir privatūs raktai, leidžiantys pasiekti ir valdyti jų turimus turto aktyvus. Kriptovaliutų piniginės gali būti įvairių formų – internetinės, programinės ar fiziniai įrenginiai, suteikiantys vartotojams platų pasirinkimų spektrą atsižvelgiant į jų individualius poreikius. Bitcoin piniginės turi svarbią vietą finansų ekosistemoje, nes jos užtikrina saugų ir patogų būdą tvarkyti savo turimą turtą, kartu palaikydamos vartotojų privatumą ir saugumą.

Pasak Taylor, Kim ir kitų (2022), yra išskiriamos trys Bitcoin piniginių rūšys: programinės piniginės, aparatūrinės piniginės ir popierinės piniginės. Programinės piniginės tokios, kurias galima atsiųsti į savo kompiuterį, mobilųjį telefoną ar kitą išmanųjį įrenginį. Aparatūrinės piniginės yra kaip atskiras įrenginys, skirtas laikyti ir atsiskaityti kriptovaliutomis (šiam įrenginiui atskiros programinės įrangos nereikia). Popierinės piniginės, pasak autorių– ant popieriaus ar kito pagrindo sugeneruotas QR kodas, kurį galima taip pat vadinti pinigine, nes į ją galima pervesti lėšas. Skirtingai nuo Taylor, Kim ir kt. (2022), Masahiko ir Kento (2019) išskiria tik dvi Bitcoin piniginių rūšis: šaltas ir karštas. Karštos piniginės yra tokios, kurios veikia nuolat prijungtos prie interneto ryšio, todėl jas galima naudoti realiu laiku atliekant sandorius. O šaltos piniginės yra nepriklausomos nuo interneto ryšio, jos veikia autonomiškai arba gali būti naudojamos kaip ilgalaikės kriptovaliutų saugyklos. Khanum ir Mustafa (2022) savo tyrime išskiria dvi Bitcoin piniginių rūšis: „Custodial“ ir „Non-Custodial“. „Custodial“ tokia, kuri saugo piniginės turėtojo raktus, slaptažodžius trečiojoje šalyje, o „Non-Custodial“– kai raktai ir slaptažodžiai yra saugomi vartotojo piniginėje.

Dar vieną pinginių rūšį – universalias piniginės – išskiria Jorgensen ir Beck (2022). Šios piniginės gali būti tiek programinės tiek aparatūrinės. Jų išskirtinumas yra tas, kad jos paremtos kriptografiniu algoritmu ir jose galima saugoti ne tik kriptovaliutas, bet ir įvairius asmens tapatybės atpažinimo dokumentus, biometrinius duomenis, vairuotojo pažymėjimus, universiteto ar kitos mokymo įstaigos baigimo diplomus ar pažymėjimus. Šio tipo piniginės, anot autorių, yra ateitis – ji palengvins mūsų atpažinimą internete, užtikrins didesnį saugumą ir privatumą.



Šaltinis: sudarytas autoriaus.

1 pav. Kriptovaliutų piniginių tipai

Kaip matyti iš 1 pav., kriptovaliutų piniginės skirstomos į dvi pagrindines kategorijas: karštas ir šaltas. Karštos piniginės, skirtos nuolatiniam naudojimui su interneto ryšiu, apima internetines, kompiuterines ir mobiliąsias pinigines. Šaltos piniginės, veikiančios nepriklausomai nuo interneto, skirstomos į popierines bei aparatūrines, kurios gali būti laidinės arba belaidės, užtikrinant didesnį saugumo lygį.

Apibendrinant galima teigti, kad Bitcoin piniginės yra esminis įrankis, leidžiantis vartotojams saugiai laikyti, siųsti ir gauti Bitcoin bei kitas kriptovaliutas. Jos veikia kaip virtualios piniginės, kuriose yra saugomi vartotojo raktai ir slaptažodžiai, leidžiantys pasiekti ir valdyti jų turimus kripto turto kiekius. Šios piniginės gali būti tiek internetinės, tiek programinės įrangos arba netgi fizinių įrenginių forma ir suteikia vartotojams įvairias pasirinkimo galimybes, priklausomai nuo jų poreikių ir saugumo reikalavimų. Bitcoin piniginės užima svarbią vietą kriptovaliutų ekosistemoje, nes jos užtikrina saugų ir patogų būdą tvarkyti savo portfelius, kartu palaikydamos vartotojų privatumą ir saugumą. Skirtingi autoriai išskiria įvairias bitcoin piniginių rūšis, tačiau visos jos atlieka svarbų vaidmenį kriptovaliutų saugumo ir prieinamumo srityje.

Žemiau esančiame skyriuje plačiau nagrinėjamos aparatinės kriptovaliutų piniginės, jų tipai ir naudojamos technologijos bei pateikiami pavyzdžiai.

1.2.1 Aparatūrinės kriptovaliutų piniginės, technologinės savybės ir funkcionalumo analizė

Aparatinės kriptovaliutų piniginės yra specializuoti įrenginiai, skirti saugiai saugoti privačius raktus. Jos veikia izoliuotai nuo interneto ryšio, todėl yra atsparios įsilaužimams ir kenkėjiškoms

programoms. Šios piniginės naudoja saugias mikroschemas ir pažangius kriptografinius algoritmus, užtikrinančius aukščiausią saugumo lygį jūsų skaitmeniniam turtui. Šiame skyriuje apžvelgiamos aparatinės kriptovaliutų piniginės, išsamiai analizuojami įvairūs jų tipai ir pagrindinės technologijos, užtikrinančios saugų skaitmeninių valiutų saugojimą. Analizuojami populiariausi gamintojų modeliai, pavyzdžiai, kurie padeda geriau suprasti, kaip šie įrenginiai veikia ir kuo jie skiriasi.

Analizuotos aparatūrinės kriptovaliutų piniginės, jų požymiai, technologiniai skirtumai ir veikimo principai palyginamos lentelėje Nr. 1:

1 lentelė

Aparatūrinių kriptovaliutų piniginių tipai

Piniginės tipas	Ryšys ir prisijungimas	Piniginės pavyzdys	Privalumai, kam skirta	Kaip veikia
Nejungiama belaidė piniginė (*angl. air-gapped*)	Naudoja QR kodus arba microSD korteles; neturi papildomų funkcijų tokių kaip NFC ar Bluetooth ar tinklo plokštės.	ColdCard, SafePal X1	Itin aukštas saugumo lygis, nes neturi ryšio su internetu, todėl yra sumažinta nuotolinių atakų rizika. Tinka ilgalaikiam turto saugojimui (10 000 – 100 000 € vertės). Skirta asmenims ir įmonėms kurie siekia užsitikrinti skaitmeninio turto saugumą, duomenų privatumą ir valdymo kontrolę be tarpininkų.	Operacijos pasirašomos visiškai neprisijungus prie tinko, taip užkertant privačių raktų nutekėjimui. Norint pervesti lėšas, transakcija sukuriama išoriniame įrenginyje, perduodama į piniginę QR kodą ar mircsoSD, pasirašoma neprisijungus ir grąžinama į išorinį įrenginį, kuris perduoda į tinklą.
Bluetooth piniginė (*angl. Bluetooth Wallet*)	Bluetooth 4.1 ar naujesnis protokolas, veikimo nuotolis iki 100 metrų	Ledger Nano S, Trezor Model One	Patogu naudoti mobiliuosiuose įrenginiuose. Palaiko daugiau negu 100 kriptovaliutų ir gali veikti iki 6 valandų nepertraukiamo veikimo režime.	Operacijos atliekamos įrenginio viduje nepriklausomai nuo išorinio įrenginio. Transakcija sukuriama mobiliajame telefone arba kompiuteryje, prijungtame prie Bluetooth piniginės. Piniginė gauna transakcijos informaciją ir pasirašo ją savo viduje esančiu privačiu raktu. Pasirašyta transakcija siunčiama atgal į mobilųjį įrenginį, kuris ją perduoda į blokų grandinę per internetą.
NFC pinginė (angl. *NFC Wallet*)	NFC ryšys, veikimo nuotolis iki 4 cm	Tangem, ColdCard MK4	Greitos ir patogios bekontaktės operacijos, daugiau tinkančios kasdieninėms operacijoms ir prekybos vietose. Gali palaikyti iki 1000 nuskaitymo sesijų iki kito pakrovimo.	Operacijos inicijuojamos suderinamame įrenginyje (dažniausiai išmaniajame telefone). Piniginė pasirašo operaciją naudodama NFC, išlaikydama privačius raktus saugius kortelėje.
USB piniginė (angl. *USB Wallet*)	USB 2.0, 3.0 arba USB-C, suderinamos su „Windows“, „MacOS“ ir „Linux“ operacinėmis sistemomis	Trezor Model One, Ledger Nano S Plus, Ellipal Titan	Universalios, kurios gali palaikyti daugiau negu 1000 kirpto valiutų ir yra labiau skirtos pradedantiesiems.	Prisijungia prie kompiuterio per USB. Operacijos atliekamos piniginės viduje, kompiuteriui suteikiant tik transakcijų inicijavimo ir siuntimo funkcijas.
Vienkartinė pinginė (angl.	Pradinė prieiga per USB, vėliau naudojama tik su	OpenDime piniginė	Labai saugi ir praktiška fiziniam vertės perdavimui – tinka palikimui ar dovanoms.	Vienkartinės piniginės naudojamos kaip fiziniai vertės perdavimo įrenginiai. Privatūs

Disposable Wallet arba One-time Wallet)	fizine prieiga		Naudojamas kaip fizinis pinigų ekvivalentas, nes leidžia atskleisti privatų raktą tik sunaikinus įrenginį.	raktai laikomi paslėpti tol, kol piniginė fiziškai neatidaroma ar nesugadinama, kad būtų pasiektas privatus raktas.
Kelių parašų piniginė (angl. *Multi-signature Wallet arba Multisig Wallet*)	Bluetooth, NFC, USB, priklauso nuo įrenginio specifikacijos	BitBox02, Passport	Padidintas saugumas dėl kelių parašų reikalavimo, operacijoms reikalingas kelių asmenų ar įrenginių sutikimas. Naudojamas didelėms sumoms, bendroms sąskaitoms saugoti.	Reikalauja kelių įrenginių arba asmenų, kad būtų pasirašyta operacija. Kiekviena šalis turi dalį privataus rakto, užtikrinant, kad joks vienas asmuo neturi visiškos kontrolės.
Kortelės tipo piniginė (angl. *Card-based Wallet*)	Reikalingas kortelių skaitytuvas pagal ISO/IEC 7816	Satochip, D'CENT	Labai saugi, dažnai naudojama kartu su papildomu PIN kodu. Gali būti naudojama saugiam autentifikavimui ir skaitmeniniam pasirašymui, labiau tinkamos juridiniams asmenims, nes galima pasiskirstyti.	Privatūs raktai saugomi saugioje mikroschemoje kortelės viduje. Kortelė įdedama į skaitytuvą, o operacijos patvirtinamos naudojant PIN kodą. Naudotojas inicijuoja transakciją suderinamame kortelių skaitytuve, dažniausiai mobiliajame telefone ar kompiuteryje. Transakcija pasirašoma kortelės mikroschemoje, o pasirašyta transakcija grįžta į įrenginį, kuris ją išsiunčia į tinklą.
Modulinės pinginės (angl. *Modular Wallet*)	Įvairūs prisijungimo būdai (Bluetooth, NFC, USB ir t.t.)	Blockstream Jade, Zymbt HSM6	Pritaikoma ir lanksti, leidžia vartotojams pasirinkti norimas funkcijas ir galimybes, gali būti pritaikyta specifiniams poreikiams, galimybė ateityje atnaujinti ir plėsti.	Funkcionalumas priklauso nuo naudojamų konkrečių komponentų. Kai kurie moduliai gali pasiūlyti neprisijungus prie tinklo pasirašymą, o kiti gali naudoti Bluetooth arba NFC.
Savadarbės aparatūrinės pinginės (angl. *DIY Hardware Wallet*)	Įvairūs prisijungimo būdai (Bluetooth, NFC, USB ir t.t.)	PiTrezor, SeedSigner	Pritaikoma ir lanksti, pats vartotojas pasirenka, iš kokių komponentų – seno kompiuterio ar paprasto USB kietojo disko. Kuriama siekiant decentralizuoto valdymo ir norit apsaugoti nuo pagrindinių kenkėjiškų atakų: fišingo ir įsilaužimo atakų.	Funkcionalumas priklauso nuo naudojamų konkrečių komponentų. Kai kurie moduliai gali pasiūlyti neprisijungus prie tinklo pasirašymą, o kiti gali naudoti Bluetooth arba NFC.
NPC piniginės (angl. *Non-Custodial Wallet*)	Prisijungiama prie išmaniojo įrenginio, naudojant internetą	Trust Wallet, MetaMask, Torus, TokenPocket	NPC piniginės yra mobiliosios programinės įrangos piniginės, kurios dažniausiai veikia kaip programos telefonuose arba naršyklės plėtiniai. Šios piniginės neturi trečiosios šalies, kontroliuojančios lėšas – privatūs raktai saugomi tik vartotojo įrenginyje.	Naudotojas sukuria transakciją programėlėje ir pasirašo ją, o pasirašyta transakcija siunčiama į tinklą tiesiogiai per programėlę, naudojant interneto ryšį. NPC piniginės dažniausiai palaiko įvairias blokų grandines, todėl gali siųsti transakcijas į kelis tinklus (pvz., „Ethereum“, „Bitcoin“).

Šaltinis: sudarytas autoriaus.

Lentelėje Nr. 1 pateikiama išsami ir struktūruota aparatinių kriptovaliutų piniginių apžvalga, atskleidžianti jų funkcionalumo ir pritaikomumo įvairovę skirtingiems vartotojų poreikiams. Piniginės klasifikuojamos pagal ryšio tipą, techninį funkcionalumą ir fizinę formą, leidžiančius šias pinigines

palyginti ir išskirti privalumus. Belaidės piniginės, tokios kaip „Ledger Nano X“ ir „Trezor Model T“, išsiskiria patogumu naudoti ir galimybe prisijungti prie mobilių įrenginių. Jos palaiko platų funkcijų spektrą, įskaitant decentralizuotų finansų rinkų paslaugas, taip pat leidžia lengvai valdyti turimas kriptovaliutas tiesiai iš mobilaus įrenginio. USB tipo piniginės, pavyzdžiui, „Ledger Nano S“ ir „Trezor Model One“, yra sukurtos taip, kad privatūs raktai visada lieka apsaugotoje mikroschemoje, kad nebūtų atskleisti išoriniams įrenginiams. Jos taip pat pasižymi ilgesniu fiziniu patvarumu, nes yra kompaktiškos ir atsparios aplinkos veiksniams. NFC piniginės yra labai patogios naudoti kasdieniams mokėjimams ir dažniausiai yra kompaktiškos, kortelės formos, todėl jas lengva nešiotis piniginėje ar kišenėje. Funkcionalumo požiūriu vienkartinės piniginės idealiai tinka šaltam saugojimui ir siuntimui, o kelių parašų piniginės, pavyzdžiui, „BitBox02“, užtikrina papildomą saugumo sluoksnį, nes reikalauja bent dviejų ar daugiau patvirtinimų prieš atliekant operacijas. Tokia struktūra mažina vieno taško gedimo riziką ir apsaugo nuo neteisėtų operacijų, kai naudojama didelės vertės turto saugojimui. Modulinės piniginės, tokios kaip „Cobo Vault“ ar „Blockstream Jade“, suteikia vartotojams galimybę pritaikyti piniginę konkrečiam naudojimo scenarijui. Modulinės piniginės dažniausiai yra atsparios dulkėms, vandeniui ir smūgiams, todėl puikiai tinka naudoti ekstremaliomis aplinkos sąlygomis. O kortelės tipo piniginės išsiskiria savo kompaktiškumu ir patogumu nešiotis, tačiau yra jautresnės fiziniams pažeidimams nei kitų tipų piniginės. Savadarbės piniginės yra skirtos labiau pažengusiems naudotojams, kurie vertina galimybę patys kontroliuoti kiekvieną piniginės aspektą.

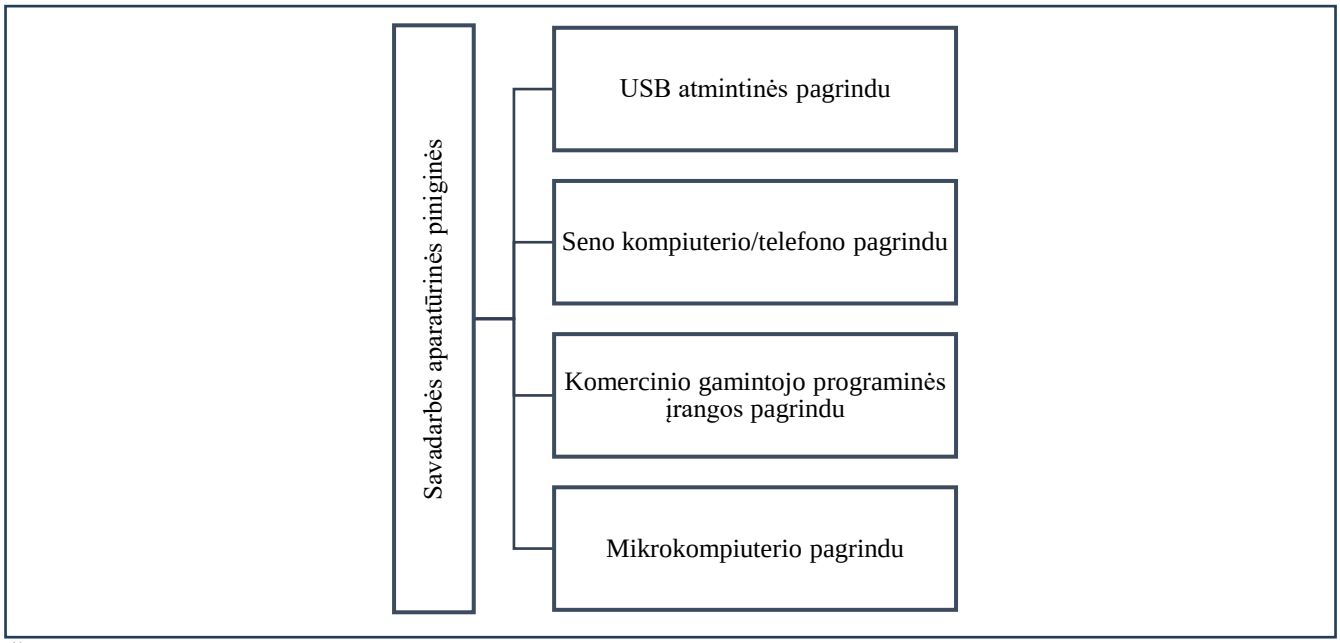
Apibendrinant galima teigti, kad aparatinės kriptovaliutų piniginės yra pagrindinė saugumo priemonė šiuolaikiniame skaitmeninių finansų sektoriuje. Jos suteikia aukštą apsaugos lygį nuo kibernetinių grėsmių, užtikrindamos kriptovaliutų saugumą nuo įsilaužimų ir kenkėjiškų programų. Nors rinkoje yra įvairių tipų ir modelių, kiekvienas jų pasižymi specifiniais privalumais ir trūkumais, todėl vartotojams svarbu įvertinti savo individualius poreikius ir prioritetus prieš pasirenkant tinkamą sprendimą. Aparatinė piniginė yra strategiškai svarbi investicija, prisidedanti prie skaitmeninio turto apsaugos ir suteikianti vartotojams užtikrintumo bei pasitikėjimo valdyti savo finansus.

Žemiau pateiktame skyriuje plačiau nagrinėjamos savadarbės aparatinės Bitcoin piniginės, jų tipai, prototipai ir kokių šiuo metu galima rasti rinkoje.

1.2.2. Savadarbės aparatinės kriptovaliutų piniginės

Be komercinių gamintojų siūlomų aparatinių piniginių, egzistuoja alternatyvus metodas, leidžiantis vartotojams individualiai konstruoti unikalias Bitcoin pinigines, pasitelkiant įvairias komponentes ir programinę įrangą. Šis nestandartinis ir inovatyvus požiūris reikalauja specifinių

techninių žinių tiek kūrimo, tiek valdymo etapuose, tačiau suteikia vartotojams didesnę kontrolę ir lankstumą. Vartotojai, pasirinkę šį kelią, dažnai vadovaujasi nepasitikėjimu esamais piniginių tiekėjais, siekiu eliminuoti trečiųjų šalių įtaką ir užtikrinti maksimalų saugumą nuo kibernetinių grėsmių, kurioms komercinių piniginių gamintojai gali būti labiau pažeidžiami dėl savo žinomumo ir patrauklumo įsilaužėliams. Individualiai kuriamos piniginės leidžia vartotojams pritaikyti saugumo parametrus pagal savo poreikius, pasirinkti patikimiausius komponentus ir programinę įrangą, taip pat kontroliuoti visus piniginės veikimo aspektus. Šiame skyriuje detaliai analizuojami tokių individualiai kuriamų aparatinių piniginių tipai, jų veikimo principai, reikalingi komponentai ir programinė įranga, taip pat kiekvieno modelio privalumai ir trūkumai, siekiant įvertinti jų technologinį potencialą ir saugumo lygį. Taip pat nagrinėjami įvairūs techniniai sprendimai, aptariami galimi iššūkiai ir rizikos, susijusios su individualiu piniginių kūrimu.



Šaltinis: sudarytas autoriaus.

2 pav. Savadarbių piniginių tipai

Kaip matyti iš 2 pav., galima išskirti 4 pagrindines rūšis, kokiu pagrindu yra pagamintos ir veikia, aparatūrinės pinigines.

USB atmintinės pagrindu sukurta Bitcoin piniginė yra patrauklus pasirinkimas tiems, kurie ieško ekonomiško ir lanksčiai pritaikomo sprendimo savo kriptovaliutų saugojimui. Šis metodas suteikia vartotojams galimybę individualiai pasirinkti ir įdiegti norimą piniginės programinę įrangą bei šifravimo algoritmus, taip pat užtikrina didesnį anonimiškumą, nes nereikalauja registracijos ar asmeninės informacijos pateikimo. Tačiau svarbu suprasti, kad šis sprendimas reikalauja didesnio

vartotojo atsargumo ir sąmoningumo dėl padidėjusios rizikos. Skirtingai nuo komercinių piniginių, USB atmintinės pagrindu sukurtos piniginės neturi integruotų saugumo funkcijų, tokių kaip saugūs lustai, PIN kodo apsauga ar atsarginės kopijos atkūrimo mechanizmas, todėl yra labiau pažeidžiamos tiek fizinių, tiek programinių atakų. Todėl būtina imtis papildomų saugumo priemonių, tokių kaip stiprių slaptažodžių naudojimas, programinės įrangos atnaujinimas, atsarginių kopijų kūrimas ir saugojimas bei vengimas prijungti piniginę prie nesaugių įrenginių ar tinklų. Nepaisant šių iššūkių, USB atmintinės pagrindu sukurtos piniginės išlieka patrauklia alternatyva tiems, kurie vertina kontrolę, lankstumą ir privatumą, tačiau yra pasirengę prisiimti didesnę atsakomybę už savo skaitmeninio turto saugumą.

Kito tipo savadarbių aparatinių piniginių kūrimo metodas apima nebenaudojamų išmaniųjų telefonų, planšetinių kompiuterių ar nešiojamų kompiuterių panaudojimą. Šių piniginių kūrimo principas yra analogiškas USB atmintinės pagrindu sukurtoms piniginėms: įrenginys atjungiamas nuo interneto ir įdiegiama pasirinkta kriptovaliutų piniginės programinė įranga, pvz.: „Electrum“, „Mycelium“, „Exodus“, „Wasabi Wallet“. Siekiant padidinti saugumą, galima įdiegti specializuotas, saugumu orientuotas operacines sistemas, tokias kaip „GrapheneOS“ ar „CopperheadOS“. Kai kurie vartotojai netgi modifikuoja įrenginių aparatūrą, pašalindami nereikalingus komponentus. Transakcijų atlikimui naudojama „tik peržiūros“ (angl. view-only) piniginė, kuri negali pasirašyti operacijų, tačiau yra naudojama kaip neprisijungus vykdomų operacijų pasirašymo dalis. Ši piniginė sukuria nepasirašytus sandorius, kurie vėliau pasirašomi neprijungtoje piniginėje ir galiausiai išsiunčiami į tinklą. Šio tipo pinginės privalumai – tvarumas, nes yra panaudojami nebenaudojami įrenginiai, taip sumažinant elektronikos atliekų kiekį ir nereikalaujant papildomų išlaidų naujai įrangai, lankstumas (vartotojai gali pasirinkti ir įdiegti norimą piniginės programinę įrangą bei operacinę sistemą ir, jei įrenginys turi kamerą ir atitinkamas jungtis ar aparatūrinę įrangą, pvz., Bluetooth ar NFC, galima atlikti belaides operacijas). Svarbu nepamiršti ir galimų iššūkių. Senesnė programinė ir aparatinė įranga gali būti labiau pažeidžiama įsilaužimų ir kenkėjiškų programų, todėl būtina imtis papildomų saugumo priemonių. Operacinė sistema gali automatiškai prisijungti prie interneto norėdama atsinaujinti, taip sukeldama riziką paviešinti jūsų privačius raktus, todėl nuolatinis atjungimas nuo interneto yra būtinas siekiant užtikrinti maksimalų saugumą. Be to, vartotojai turi būti technologiškai išprusę ir pasiruošę skirti laiko bei pastangų tinkamam piniginės konfigūravimui ir priežiūrai, nes kiekvienas neatsargus žingsnis gali turėti rizikos lėšų atskleidimui.

Alternatyvus savadarbių aparatinių kriptovaliutų piniginių kūrimo metodas apima atvirojo kodo programinės įrangos, dažnai sukurtos komercinių gamintojų, integravimą į mikrokompiuterius arba komercinės piniginės aparatūros kopijas. Šis požiūris leidžia vartotojams pasinaudoti žinomomis ir

patikimomis programinėmis sistemomis, tokiomis kaip „Trezor“, pritaikant jas prie individualių poreikių ir įtraukiant papildomus saugumo funkcionalumus. Pavyzdžiui, „PiTrezor“ projektas leidžia įdiegti „Trezor“ programinę įrangą į „Raspberry Pi“ mikrokompiuterį, taip suteikiant vartotojams galimybę naudotis pažįstama sąsaja ir funkcijomis, kartu papildant jas dviejų faktorių autentifikavimu ar operacijų šifravimu. Atvirojo kodo pobūdis leidžia vartotojams modifikuoti programinę įrangą, įtraukiant palaikymą naujiems žetonams ar papildomoms funkcijoms. Savadarbių aparatinių piniginių kūrimas, naudojant atvirojo kodo programinę įrangą, suteikia vartotojams reikšmingų privalumų, įskaitant žymiai mažesnę kainą nei komercinės alternatyvos, platų modifikavimo galimybių spektrą, leidžiantį pritaikyti piniginę pagal individualius poreikius bei galimybę apeiti sankcijas šalyse, kuriose kriptovaliutos yra ribojamos. Be to, aktyvios atvirojo kodo bendruomenės teikia vertingą pagalbą ir palaikymą vartotojams. Tačiau šis metodas turi ir minusų, tokių kaip specializuotų saugumo lustų ar kitų aparatūros lygio apsaugos mechanizmų trūkumas, retesni programinės įrangos atnaujinimai, reikalaujantys didesnio vartotojo atsargumo, būtinybė turėti techninių įgūdžių, reikalingų piniginės sukūrimui ir priežiūrai, bei rizika parsisiųsti užkrėstą atvirojo kodo programinę įrangą iš nepatikimų šaltinių.

Savadarbių aparatinių piniginių kūrimas naudojant mikrokompiuterius, tokius kaip „Raspberry Pi“ ar „M5StickV“, bei atvirojo kodo arba individualiai kuriamą programinę įrangą, yra dar vienas alternatyvus metodas kriptovaliutų saugojimui. Šiuo metu egzistuoja įvairūs atvirojo kodo projektai, pavyzdžiui, „SeedSigner“, „Krux‘ ir „Jade DIY“, teikiantys išsamias instrukcijas ir programinę įrangą, skirtą savadarbių piniginių kūrimui. Šio metodo privalumai apima: ekonominį efektyvumą (savadarbių piniginių kaina yra žymiai mažesnė nei komercinių alternatyvų), lankstumą ir modifikavimo galimybes (vartotojai gali pritaikyti piniginės funkcionalumą pagal savo poreikius, įskaitant įvairias transakcijų pasirašymo opcijas) ir papildomų įrenginių, tokių kaip QR kodo skaitytuvai, NFC, integravimą. Šis metodas taip pat turi trūkumų: aparatūrinės apsaugos trūkumą (mikrokompiuteriai dažniausiai neturi specializuotų saugumo lustų ar kitų aparatūros lygio apsaugos mechanizmų, būdingų komercinėms piniginėms), žmogiškųjų klaidų riziką (netinkamas programinės įrangos kūrimas ar konfigūravimas gali lemti pažeidžiamą piniginę), todėl šis metodas reikalauja techninių žinių ir kruopštumo. Apibendrinant galima prieiti prie išvados, kad savadarbių piniginių kūrimas, naudojant mikrokompiuterius ir atvirojo kodo programinę įrangą, suteikia vartotojams lankstumo ir ekonominio efektyvumo, tačiau reikalauja techninių įgūdžių ir sąmoningumo dėl galimų saugumo rizikų.

Savadarbių aparatinių kriptovaliutų piniginių kūrimas yra patraukli alternatyva komerciniams sprendimams, suteikianti vartotojams didesnę kontrolę, lankstumą ir ekonominį efektyvumą. Šios piniginės gali būti kuriamos naudojant įvairius metodus, tokius kaip USB atmintinės, nebenaudojami

įrenginiai, mikrokompiuteriai su atvirojo kodo arba individualiai sukurta programine įranga. Nors kiekvienas metodas turi unikalių privalumų, tokių kaip anonimiškumas, modifikavimo galimybės ir tvarumas, jie taip pat kelia tam tikrų iššūkių, susijusių su saugumu, techninių žinių poreikiu ir papildomų saugumo priemonių taikymu. Nepaisant to, savadarbės piniginės išlieka patrauklia alternatyva tiems, kurie vertina individualų pritaikymą ir yra pasirengę prisiimti didesnę atsakomybę už savo skaitmeninio turto saugumą.

Kitame skyriuje analizuojami aparatinių piniginių saugumo mechanizmai ir jų atsparumas kenkėjiškoms atakoms, įskaitant įvairių apsaugos sistemų, tokių kaip saugūs elementai, kriptografiniai algoritmai ir fizinės saugos priemonės, taikymą..

1.3. Aparatinių piniginių algoritmai ir jų taikomi saugumo mechanizmai

Šiame skyriuje analizuojami esminiai aparatinių kriptovaliutų piniginių saugumo aspektai, siekiant išsamiai išanalizuoti jų atsparumą įvairioms kenkėjiškoms atakoms ir užtikrinti vartotojų skaitmeninio turto saugumą. Aparatinės piniginės, kaip izoliuoti ir specializuoti įrenginiai, yra laikomos vienu saugiausių būdų saugoti kriptovaliutas, tačiau jų patikimumas priklauso nuo daugelio veiksnių. Todėl šiame skyriuje nagrinėjami ne tik pagrindiniai saugumo mechanizmai, tokie kaip saugūs elementai, kriptografiniai algoritmai ir fizinės saugos priemonės, bet ir jų tarpusavio sąveika, užtikrinanti privačių raktų ir vartotojų lėšų apsaugą, aptariama, kaip veikia aparatinės piniginės ir kokios technologijos yra naudojamos siekiant užtikrinti aukščiausią saugumo lygį.

Pasak Guri (2018), neprijungtos prie interneto aparatinių kriptovaliutų piniginės saugumas yra tiesiogiai proporcingas jų gebėjimui užšifruoti ir saugoti privačius raktus. Saugiausios piniginės pasižymi daugiasluoksne kriptografine apsauga, reikalaujančia įsilaužėliui įveikti kelis saugumo lygius prieš pasiekiant pagrindinį raktą. Davenport ir Shetty (2019) pabrėžia, kad privačių raktų saugumas priklauso nuo sinergetinio įvairių saugumo priemonių, tokių kaip saugūs elementai, PIN kodo generatoriai ir programinė įranga, veikimo. Tačiau Suratkar, Shirole ir Bhirud (2020) teigia, kad net ir pažangiausios saugumo sistemos negarantuoja visiško saugumo, jei vartotojas nesilaiko atsakingo elgesio ir prijungia piniginę prie interneto ar vietinio tinklo, taip padidindamas riziką patirti kenkėjiškas atakas, duomenų nutekinimą ar piniginės klonavimą, dėl kurių gali būti prarastos visos lėšos.

Norint geriau suprasti, kaip yra apsaugota aparatūrinė kriptovaliutų piniginė ir kokias saugumo sistemas, aparatūrines ir programines sistemas naudoja jų gamintojai, reikia kiekvieną komponentą detaliai apžvelgti.

Aparatinių kriptovaliutų piniginių saugumo užtikrinime esminį vaidmenį atlieka saugus elementas, specializuotas mikroprocesorius, skirtas privačių raktų apsaugai. Park ir kt. (2023) tyrimas pabrėžia, kad piniginės be šio lusto yra itin pažeidžiamos kompromitavimui ir lėšų praradimui. Saugus elementas, dažniausiai integruotas į pagrindinę plokštę arba veikiantis kaip atskiras lustas, užtikrina privačių raktų izoliaciją ir apsaugą saugioje, kriptografiškai apsaugotoje atmintyje. Visi kriptografiniai veiksmai atliekami lusto viduje, o su pagrindiniu procesoriumi bendraujama tik perduodant transakcijų duomenis ir pasirašytus rezultatus. Piniginės su SE pasižymi padidintu saugumu, neprisijungus veikiančiu raktų generavimu, saugiu transakcijų pasirašymu ir atsparumu fizinėms atakoms. SE dažnai sertifikuojami pagal bendruosius kriterijus (CC), o jų saugumo užtikrinimo lygis (EAL) siekia iki CC EAL5+. Šiuos lustus naudoja žinomi komerciniai gamintojai, tokie kaip „Trezor, Ledger“ ir „ColdCard“, taip patvirtindami jų svarbą užtikrinant aukščiausią kriptovaliutų turto saugumo lygį. Apibendrinant galima teigti, kad saugūs elementai yra esminis komponentas, užtikrinantis aparatinių piniginių atsparumą įvairioms grėsmėms ir didinantis kriptovaliutų saugojimo saugumą, lyginant su kitais metodais.

Siekiant visapusiškai suprasti privačių raktų saugojimo aparatūrinėse piniginėse mechanizmus, būtina detaliai išanalizuoti jų generavimo procesą, kuris yra neatsiejamas nuo tikrųjų atsitiktinių skaičių generatoriaus. Šis generatorius yra esminis komponentas, užtikrinantis privačių raktų saugumą ir unikalumą. Šio lusto pagrindinė funkcija yra generuoti unikalią pradinę sėklą, kuri yra ne tik pamatinis elementas formuojant privatų raktą, bet ir naudojama operacijų pasirašymui, taip sukuriant papildomą saugumo sluoksnį. Ši sėkla yra kritinė kuriant atsarginę piniginės kopiją, nes ji leidžia atkurti privatų raktą ir susigrąžinti prieigą prie lėšų. Svarbu pabrėžti, kad generatoriai gali būti dviejų tipų: aparatūriniai ir programiniai. Aparatūriniai išsiskiria savo patikimumu ir yra atsparesni nuspėjamumui, kadangi jie remiasi fiziniais procesais, siekiant generuoti atsitiktinius skaičius. Programiniai, kita vertus, remiasi algoritmais ir yra potencialiai greičiau pažeidžiami, jei algoritmas yra žinomas arba turi trūkumų. Integruojant atsitiktinių skaičių generatorių į aparatines pinigines, didžiausias prioritetas teikiamas aparatūriniams dėl jų aukštesnio saugumo lygio. Vis dėlto jų integravimas yra sudėtingesnis ir brangesnis, todėl kai kuriais atvejais gamintojai gali rinktis programinius dėl jų mažesnės kainos ir paprastesnio įdiegimo. Remiantis Voletly ir kt. (2019) tyrimu, šio generatoriaus integravimas, ypač aparatūrinio, yra efektyvi strategija, užtikrinanti operacijų aparatūrinėse piniginėse saugumą ir atsparumą įvairioms atakoms, įskaitant tradicines atakas, nukreiptas į privataus rakto atskleidimą.

PIN kodų generatoriai yra esminis pirminis autentifikavimo mechanizmas, naudojamas aparatūrinėse Bitcoin piniginėse. Jie veikia kaip skaitmeninis barjeras, neleidžiantis neautorizuotai prieigai pasiekti įrenginio ir jo turinio. PIN kodas, dažniausiai sudarytas iš 4–8 skaitmenų, yra būtinas

tiek įrenginio atrakinimui, tiek operacijų autorizavimui. Semyanova ir Grezina (2023) savo tyrime pabrėžia, kad PIN kodų generatoriai suteikia papildomą saugumo lygį, ypač pametus įrenginį. Neteisingai įvedus PIN kodą kelis kartus, visi piniginėje esantys duomenys gali būti ištrinti, taip apsaugant vartotojo lėšas nuo neteisėtos prieigos.

„Shamir“ atsarginės kopijos ir BIP-39 sėklos frazės yra du esminiai kriptografiniai metodai, naudojami aparatūrinėse kriptovaliutų piniginėse siekiant užtikrinti skaitmeninio turto saugumą. „Shamir“ atsarginės kopijos leidžia padalinti atkūrimo frazę (mnemoninę frazę) į kelis fragmentus, kurie gali būti saugomi skirtingose vietose, taip apsaugant nuo fizinių vagysčių ir duomenų praradimo. O BIP-39 frazės yra standartizuotas, žmonėms suprantamas formatas, naudojamas generuoti ir atkurti pinigines, suteikiantis vartotojams patogų būdą valdyti savo kriptovaliutų prieigą. Tačiau svarbu pažymėti, kad abi šios frazės yra labai jautrios ir neturėtų būti atskleidžiamos jokioms trečiosioms šalims.

2 lentele

Aparatinių piniginių naudojami algoritmai ir procesoriai

Piniginės pavadinimas (gamintojas)	**Naudojamas procesorius, SE saugumo sertifikatas**	**Naudojami kriptografiniai algoritmai**	**Saugumo funkcijos**
Ledger Nano S/X (Ledger)	Saugumo elementas ST31H320, CC CC EAL5+	SHA-256, AES-128, ECDSA, HMAC	Privatūs raktai saugomi izoliuotoje aplinkoje saugumo elemente. Naudojama apsauga nuo „tamper detection“, kur, aptikus nenormalius signalus (pvz., bandant nuskaityti atmintį lazeriu), procesorius iškart išjungiamas arba sunaikina duomenis. PIN apsauga, po 3 nesėkmingų bandymų įrenginys ištrina visus duomenis
Trezor One / T (SatoshiLabs)	STM32F205 ARM Cortex-M, nesertifikuotas	SHA-256, ECDSA, BIP39/BIP44	Nėra atskiro saugumo elemento, todėl visos kriptografinės operacijos vykdomos bendroje STM32F205 architektūroje. PIN kodo apsauga: eksponentinis laiko vėlavimas po kiekvieno neteisingo PIN įvedimo.
ColdCard (Coinkite)	STM32ARM Cortex-M (SE), nesertifikuotas	ECDSA, ECC (Elliptic Curve Cryptography), AES-128, SHA-256	Turi ATECC608A saugumo elementą, kuris šifruoja ECC su ECDSA parašais ir AES-128 palaikymu. Turi „Anti-tamper“ ir „Active sheald ir yra belaidė (angl. airgaped)
SeedSigner (SeedSigner)	Raspberry Pi zero ARM Cortex-M,	SHA-256, ECDSA,	Privatūs raktai laikomi Raspberry RAM atmintyje, todėl, užgesus įrenginiui, visi laikini duomenys

	nesertifikuotas	BIP39/BIP44	prarandami.
Krux (Krux)	Xtensa LX6	SHA-256, ECDSA, BIP39/BIP44	Neturi jokios fizinės apsaugos. Naudoja tik bazinę PIN apsaugą nuo pažangesnių atakų.
Cobo Vault (Cobo)	Saugumo elementas, CC EAL5+	SHA-256, ECDSA, BIP39/BIP44	Turi šilumos, vibracijos, elektromagnetinių laukų jutiklius. Aptikęs neįprastą signalą, įrenginys sunaikina duomenis. Saugumo elementas, esantis viduje, turi registrą, kuriame fiksuojami visi duomenys.
Blockstream Jade (Blockstream)	STM32 ARM Cortex-M, nesertifikuotas	SHA-256, ECDSA, BIP39/BIP44, AES-128 ir HMAC	Visos žinutės šifruojamos AES-128 algoritmu. Taip pat naudoja HMAC funkciją, kuri tikriną ryšį prieš perduodant duomenis
BitBox02 (Shift Crypto)	STM32 ARM Cortex-M (SE), CC EAL5+	SHA-256, ECDSA, BIP39/BIP44	Saugumo elementas naudojamas tik kriptografiniai apsaugai, visi skaičiavimai atliekami STM32 procesoriuje.
SatoChip (SatoChip)	Išmaniosios kortelės SE su CC EAL5+	SHA-256, ECDSA, BIP39/BIP44	Naudoja PIN ir PUK kodus nuo fizinių atakų. Saugumo elementas naudojamas tik kriptografiniai apsaugai.
Zymbit (Zymbit)	Saugumo modulis su CCEAL6+, CC EAL6+	SHA-256, ECDSA, BIP39/BIP44	Gali aptikti mikroprocesoriaus lygio manipuliacijas ir, jei taip nutinka, automatiškai ištrina visus duomenis. Turi aukšto lygio CC EAL6+ lygio apsaugą.

Šaltinis: sudarytas autoriaus

2 lentelėje lyginamos skirtingos aparatinės pinginės, skirtos kriptovaliutų saugojimui, saugumo funkcijos, kriptografiniai algoritmai ir procesoriai. Kiekviena piniginė naudoja specifinius procesorius ir saugumo sertifikatus, skirtus privačių raktų apsaugai. Pavyzdžiui, „Ledger Nano“ modeliai naudoja CC EAL5+ sertifikuotą saugų elementą (ST31H320), kuris saugo raktus izoliuotoje aplinkoje ir turi įsilaužimų aptikimo funkciją, ištrinančią duomenis po nenormalių signalų ar daugybės nesėkmingų prisijungimo bandymų. „Trezor“ modeliai neturi saugaus elemento ir remiasi bendrosios paskirties ARM Cortex-M architektūra su pagrindine PIN kodo apsauga, kuri eksponentiškai didina užlaikymą po neteisingų PIN įvedimų. „ColdCard“ ir „Cobo Vault“ integruoja papildomus saugumo jutiklius ir atsparias įsilaužimams funkcijas, apsaugančias nuo neteisėtos prieigos, o kiti modeliai, tokie kaip „SeedSigner“, laikinai saugo raktus nepastovioje atmintyje, kuri praranda duomenis išjungus įrenginį. Kai kurios piniginės, tokios kaip „BitBox02“ ir „SatoChip“, koncentruojasi į kriptografinę apsaugą naudodamos saugius elementus, bet neturi pažangių fizinės apsaugos mechanizmų. Priešingai, tokie

modeliai, kaip „Zymbit“ su „CCEAL6+“, sertifikatu aptinka manipuliacijas procesoriaus lygmenyje ir automatiškai ištrina visus duomenis neteisėtos prieigos bandymo atveju. Aparatinės įrangos ir saugumo mechanizmų įvairovė šiose piniginėse suteikia vartotojams skirtingus apsaugos lygius, atitinkančius jų specifinius saugumo poreikius ir su tuo susijusias rizikas.

Aparatinių kriptovaliutų piniginių fizinės saugumo priemonės yra tokios pat svarbios kaip ir jų skaitmeninės apsaugos sistemos. Siekdami užtikrinti, kad įrenginys nebūtų pažeistas fiziškai, gamintojai diegia įvairias technologijas. Pavyzdžiui, „Trezor“ modeliai pasižymi tvirtais metaliniais korpusais, kurie yra atsparūs smūgiams ir lenkimui, o „Ledger Nano X“ turi tvirtą plastikinį korpusą su nerūdijančio plieno dangteliu, kuris apsaugo ekraną ir mygtukus. Kai kurie gamintojai, pavyzdžiui, „ColdCard“, naudoja specialius korpusus, kurie yra atsparūs vandeniui, smūgiams ir dulkėms. Be to, „BitBox02“ turi unikalią savybę - korpusas yra pagamintas iš aliuminio, kuris yra atsparus įbrėžimams ir korozijai. Kai kurios piniginės, tokios kaip „Ledger Nano S“ ir „Trezor Model T“, turi korpuso technologijas, kurios palieka matomus pėdsakus, jei kas nors bando neteisėtai atidaryti įrenginį. Tai suteikia vartotojams papildomą saugumo lygį, nes jie gali lengvai pastebėti, ar jų įrenginys buvo pažeistas.

Kitame skyriuje nagrinėjami esminiai aparatinių kriptovaliutų piniginių saugumo aspektai, siekiant užtikrinti vartotojų skaitmeninio turto saugumą. Aparatūros piniginės, kaip izoliuoti ir specializuoti įrenginiai, laikomos vienu saugiausių būdų saugoti kriptovaliutas, tačiau jų patikimumas priklauso nuo daugelio veiksnių. Čia aptariami pagrindiniai saugumo mechanizmai: saugūs elementai , kriptografiniai algoritmai, fizinės saugos priemonės ir jų tarpusavio sąveika. Saugus elementas yra specializuotas mikroprocesorius, skirtas privačių raktų apsaugai. Tikrųjų atsitiktinių skaičių generatorius yra esminis komponentas, užtikrinantis privačių raktų saugumą ir unikalumą. PIN kodų generatoriai yra pirmoji gynybos linija, apsauganti aparatūrinę piniginę. „Shamir“ atsarginės kopijos ir BIP-39 žodžių frazės yra du esminiai kriptografiniai metodai, naudojami aparatūrinėse kriptovaliutų piniginėse, siekiant užtikrinti skaitmeninio turto saugumą. Šie įvairūs saugumo mechanizmai kartu užtikrina, kad aparatūrinės piniginės būtų patikima ir saugi priemonė kriptovaliutų saugojimui.

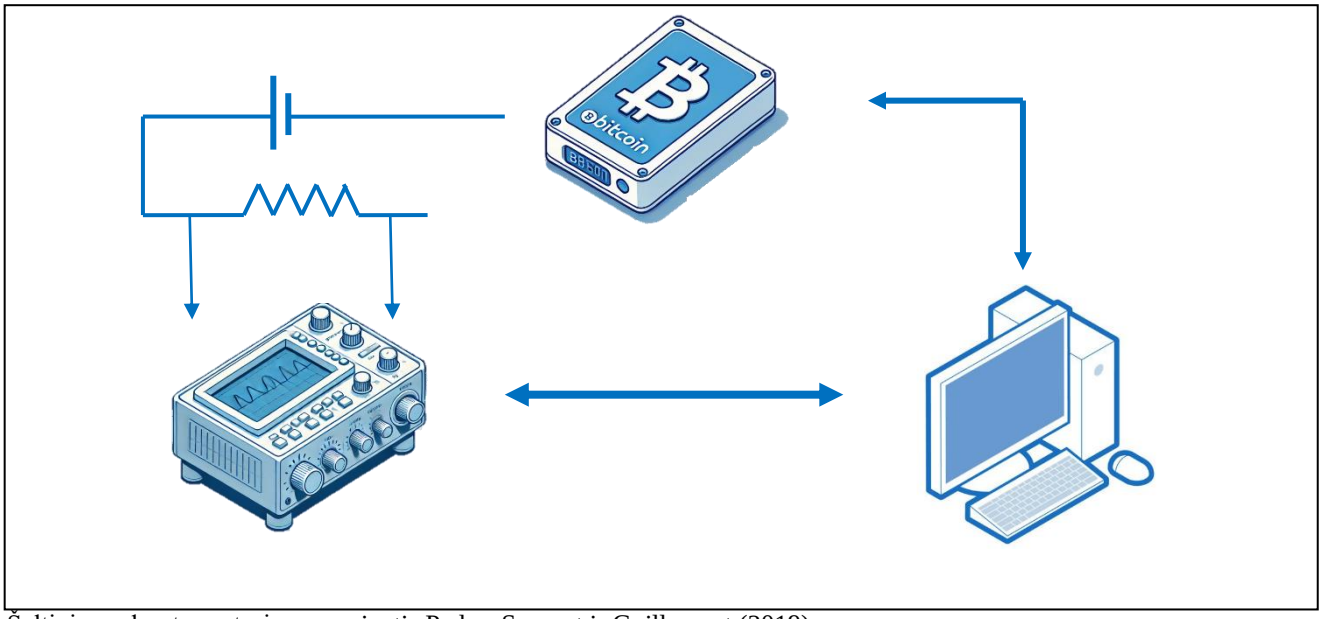
1.4. Aparatūrinių kriptovaliutų piniginių saugumo problemos

Sparčiai augant kriptovaliutų populiarumui, didėja ir su jų saugojimu susijusių saugumo iššūkių aktualumas. Šiame skyriuje analizuojami esminiai saugumo aspektai, su kuriais susiduria aparatinių piniginių naudotojai, siekiantys užtikrinti savo skaitmeninio turto neliečiamumą. Nors aparatinės piniginės suteikia patogų ir universalų priėjimą prie kriptovaliutų, jos taip pat tampa potencialiu

taikiniu įvairioms grėsmėms – tiek kibernetinėms, tiek fizinėms. Didėjanti kriptovaliutų rinkos kapitalizacija ir reikšmingos šioje technologijoje saugomos lėšos skatina vartotojus ir verslo subjektus aktyviai ieškoti efektyvių saugumo sprendimų, siekiant apsisaugoti nuo tokių grėsmių kaip piniginės kompromitavimas, kibernetiniai įsilaužimai, socialinės inžinerijos atakos ir kitos. Šiame skyriuje detaliai aptariami pagrindiniai kriptovaliutų saugumo iššūkiai, analizuojamos dažniausiai pasitaikančios ir veiksmingiausios atakų formos, siekiant suteikti vartotojams išsamų supratimą apie grėsmių pobūdį ir galimus jų prevencijos būdus.

Thomas, Piscitelli, Shavrov, ir Baggili (2020) savo tyrime išskiria fizines atakas, kada užpuolikas gauna fizinę prieigą prie įrenginio, jį atėmęs ar pavogęs iš tiesioginio jo valdytojo. Pinginę turėdamas savo rankose, jis ją gali išardyti, naudoti kitus įvairius metodus išgauti pinginės privačius raktus, PIN kodus ar kitą susijusią informaciją. Anot autorių jeigu piniginė nėra apsaugota saugumo elementu, fizinę ataką būtų galima įvykdyti ir be didelių technologinių žinių.

Autoriai Park ir kt. (2023) savo tyrime analizuoja, kaip veikia šonininio kanalo atakos, daugiausia dėmesio skirdami energijos analizės atakoms, kurios išnaudoja aparatinės įrangos piniginių energijos suvartojimo modelius atliekant kriptografines operacijas. Šios atakos išnaudoja informaciją, nutekėjusią įrenginio veikimo metu, pvz., energijos suvartojimą ar elektromagnetinę spinduliuotę. Išanalizavę šiuos šoninio kanalo signalus, užpuolikai gali iššifruoti privačius raktus.



Šaltinis: sudarytas autoriaus, remiantis Pedro, Servant ir Guillement (2019)

3 pav. Šoninio kanalo ataka

Šoninio kanalo ataką analizuoja autoriai Pedro, Servant ir Guillement (2019), kurie savo tyrime stebi, kaip osciloskopo pagalba galima fiksuoti aparatūrinės piniginės fizinius elgesio signalus, kad būtų įmanoma išgauti jautrią informaciją (žr. 3 pav.). Mokslininkai savo tyrime naudojo šią ataką, kad išgautų PIN raktus ir, atlikdami šią ataką, nustatė kiekvieną PIN kodo skaitmenį apeinant visas saugumo sistemas. Taip pat jiems pavyko pažeisti skaliarinės daugybos procesą, kuris yra esminis atskleidžiant piniginės saugumo spragas privačių raktų apsaugoje.

Dar kitą atakų rūšį analizuoja Guri (2018), kuris savo tyrime įrodo, jog, nors aparatinės įrangos piniginės yra izoliuotos ir atjungtos nuo interneto, kenkėjiškos programos vis tiek gali į jas įsiskverbti įvairiomis priemonėmis. Autorius analizuoja, kaip kenkėjiškos programos, tokios kaip „BeatCoin“, gali užkrėsti pinigines per užkrėstus USB diskus arba pažeistas programinės įrangos diegimo programas. Kai kenkėjiška programa yra įrenginyje, ji gali išfiltruoti privačius raktus, naudodama slaptus kanalus (pvz., elektromagnetinius, akustinius ar optinius signalus).

Guri (2018) taip pat analizuoja kitą atakų metodą prieš aparatūrines pinigines ir išskiria, kad, nors mažai tikėtina, bet visada gali įvykti tiekimo grandinės ataka. Įsilaužėliai gali sugadinti įrenginio aparatinę ar programinę-aparatinę įrangą, įtraukdami pažeidžiamumų, kuriais vėliau bus galima pasinaudoti; šios atakos nukreiptos į aparatinės įrangos piniginę gamybos ar platinimo metu. Semyanova and Grezina (2023) įvardija, kad ši ataka gali būti atlikta, jei vartotojas perka ir naudotą aparatūrinę pinginę, siekdamas sutaupyti lėšas ir nusipirkti ją pigiau antrojoje rinkoje. Pardavėjas gali būti įdiegęs pažeistą programinę įrangą ar pakeitęs piniginės komponentus.

Semyanova and Grezina (2023) taip pat išskiria ir dar vieną atakų rūšį, kada užpuolikas naudoja kodų generatorius ar įvairius kitus algoritmus, kad atspėtų pinginės PIN kodą ar sėklą. Nors dabartinės pinginės yra apsaugotos nuo šių atakų, limituodamos neteisingo PIN kodo įvedimų skaičių, tačiau, jei piniginė turi silpnus algoritmus ar neturi visiškos apsaugos prieš slaptažodžių generatorių ataką, užpuolikai gali išbandyti visus įmanomus derinius, kad iššifruotų piniginę ir pasiektų privačius raktus.

Ivanov ir Yan (2021) savo tyrime išskiria socialinės inžinerijos ataką, kuri išnaudoja vartotojų elgseną. Analizuojama „EthClipper“ ataka, kuri apima nukopijuoto kriptovaliutos adreso pakeitimą vizualiai panašiu, kurį valdo užpuolikas, apgaule išviliojant vartotoją, kad jis patvirtintų kenkėjišką operaciją.

Veksler (2024) išskiria, kad vartotojai dažnai praranda savo turimas lėšas ne tik dėl kenkėjiškų atakų, bet ir dėl paprastos žmogiškosios klaidos. Jis teigia, kad vienas dažniausiai pasitaikančių lėšų praradimo atvejų yra, kai vartotojas pamiršta savo atkuriamąją sėklą ar PIN kodą. Suvesdamas šiuos kodus neteisingai, vartotojas užblokuoja savo piniginę – kartais taip, kad jos atkurti tampa nebeįmanoma (ypač tai būdinga Ledger piniginės vartotojams). Pasak Jorgensen ir Beck (2022),

žmogiškoji klaida yra viena antroji po sukčiavimo (angl. phishing) atakų, kurios dėka daugiausiai prarandama turto. Žmonės pamiršta, pameta savo užsirašytas atkūrimo sėklas ar užsirašo jas klaidingai. Todėl jie turi būti atsakingi ir techniškai išprusę, kitaip jų lėšos, turimos investicijos gali būti greitai prarastos.

Dar viena ataką, pavojų išskiria Semyanov ir Grezina (2023), kurie išskiria, kad užpuolikai gali pasinaudoti įrenginio programinės įrangos trūkumais ir kartu su programinės įrangos atnaujinimu įrašyti kenkėjišką programą. Vienas iš galimų aparatinių piniginių pažeidžiamumų yra susijęs su programinės įrangos atnaujinimo procesu. Kenkėjiškos programos gali būti įdiegtos kartu su legitiminiais atnaujinimais apeinant saugumo mechanizmus ir suteikdamos prieigą prie privačios informacijos. Tokios atakos gali būti vykdomos tiek kompromituojant programinės įrangos tiekimo grandinę, tiek tiesiogiai įdiegiant kenkėjišką kodą atnaujinimo proceso metu. Šios atakos gali būti sunkiai pastebimos. Todėl svarbu sekti tik oficialiuose gamintojų portaluose skelbiamą informaciją apie galimus programinės įrangos atnaujinimus ir nepasikliauti melaginga informacija.

Vienas pagrindinių ir dažniausiai pasitaikiančių metodų, naudojamų kriptovaliutų savininkams apgauti, yra sukčiavimo (angl. phishing) atakos. Veksler (2024) išskiria, kad nusikaltėliai kuria netikras svetaines, identiškas komercinių aparatūrinių piniginių teikėjų puslapiams, siekdami išgauti vartotojų prisijungimo duomenis ar privačius raktus. Thomas, Piscitelli, Shavrov, ir Baggili (2020) išskiria, kad taip pat naudojami ir suklastoti el. laiškai, SMS žinutės ar socialinių tinklų pranešimai, kuriuose pateikiama melaginga informacija ir prašoma atskleisti asmeninę informaciją ar suvesti privačius raktus, prisijungimo duomenis. Šios atakos dažnai būna labai įtikinamos ir sunkiai pastebimos, todėl vartotojams svarbu būti budriems ir atidžiai tikrinti visus gaunamus pranešimus bei vengti spausti įtartinas nuorodas.

Lentelė 3

Atakos prieš aparatūrines kriptovaliutų pinigines

Atakos pavadinimas	Apibūdinimas	Pavyzdys	Prevencija	Pažeidžiamos piniginės tipai
Fizinė ataka (angl. *Physical Attack*)	Aparatūrinė piniginė yra fiziškai pavagiama iš vartotojo ar laikinai pasisavinama, kad būtų išgauti privatūs raktai ar kita asmeninė informacija.	2018 m. Trys užpuolikai įsiveržė į kriptovaliutų investuotojo namus, jį privertė atrakinti pinginę, kėsindamiesi į jo gyvybę. Investuotojas atskleidė visus privačius raktus ir pervedė turimus lėšas į užpuoliko piniginę.	Prievartos PIN kodas: kai kuriose aparatinės įrangos piniginėse yra priverstinio PIN arba kodo funkcija, leidžianti įvesti netikrą PIN kodą, kuris suaktyvina paslėptą piniginę arba savaiminio sunaikinimo mechanizmą. Kelių parašų piniginės: naudojant kelių parašų	Visi tipai yra pažeidžiami

			pinigines, kai kelios šalys turi įgalioti operacijas, gali būti papildomas apsaugos nuo fizinių atakų sluoksnis.	
Programinė ataka (kai įrašoma kenkėjiška programa) (angl. *Software Attack*)	Kai su piniginės programos įrangos atnaujinimu, jos spraga, ar nesaugia USB jungtimi ar kita įrašoma kenkėjiška programa, kuri leis pasisavinti lėšas ar nutekinti privačią informaciją.	2023 m. Ledger patyrė ataką, kai NPM modulio atnaujinimo metu užpuolikas pamatė programinę spragą, įterpė kenkėjišką kodą, kurio pagalba iš vartotojų buvo pasisavinta daugiau nei 600 000 eurų vertės kriptovaliutų.	Visada atnaujinimus siųstis tik iš oficialių gamintojų puslapių. Programinę įrangą atnaujinti išjungus interneto ryšį. Sekti oficialius gamintojo puslapius ir pasitikrinti, ar tikrai yra išleistas atnaujinimas ir kokia jo versija.	USB, NPC, NFC, Bluetooth
Šoninio kanalo ataka (angl. *Side-channel Attack*)	Stebima aparatūrinė pinginė ir matuojamos jos fizinės charakteristikos (energijos suvartojimas, šiluma, elektromagnetinės bangos) veikimo metu ir taip, taikant specialus algoritmus, išgaunamas privatus raktas.	2017 m. buvo pademonstruota, kaip, naudojant elektromagnetinę analizę, PIN tikrinimo proceso metu buvo atspėtas Trezor One piniginės PIN raktas. 2020 m. ChipWhisperer įrankis, kuris analizuoja elektrinius skleidžiamus signalus, juo naudojantis buvo nulaužtas, atskleisti privatūs raktai pinginių: Trezor Model T, Ledger Nano S, Keepkay.	Įsigyti pinigines, kurios turi specialus HSM modulius, galinčius apsaugoti nuo šoninio kanalo atakos, ar bent prailginti laiką, kol ataka bus įgyvendinta.	Visi tipai yra pažeidžiami, išskyrus NPC
Tiekimo grandinės ataka (angl. *Supply Chain Attack)*	Gamybos ar platinimo metu yra pažeidžiama pinginė, programiškai arba sugadinant esančią aparatūrinę įrangą, įdiegiant kenkėjiškas programas tol, kol įrenginys nepasiekia galutinio naudotojo.	2020 m. buvo pardavinėjamos padirbtos Ladger Nano S pinginės. Po šio gamintojo duomenų nutekinimo ir vartotojų duomenų atskleidimo (2020 m.) nusikaltėliai siuntė kenkėjiškus laiškus, kuriuose už „ačiū“ siūlė šios piniginės modelį. Šie netikri įrenginiai sukurti taip, kad primintų tikrus Ledger gaminius su įpakavimu ir dokumentacija. Tačiau jie buvo iš anksto įkelti su kenkėjiška programa, skirta pavogti vartotojo atkūrimo frazę.	Visada pirkti komercines aparatūrines piniginės tik iš oficialaus gamintojo. Niekada nepirkti tokio tipo piniginės antrojoje rinkoje, siekiant sutaupyti. Pinginių gamintojai pateikia instrukcijas, kaip patikrinti jūsų įrenginio autentiškumą. Tai apima pakuotės, paties įrenginio ir atkūrimo lapo konkrečių saugos funkcijų patikrinimą.	Visi tipai, ypač USB, Bluetooth, NFC tipo
Socialinės inžinerijos ataka (angl. *Social Engineering Attack (Phishing)*)	Manipuliavimas ir apgaudinėjimas vartotojų, kad šie atskleistų neskelbtiną, privačią informaciją, taip sukeliant pavojų piniginės saugumui. Dažnai yra	Ledger netikros klientų aptaravimo žinutės, elektroniniai laiškai vartotojams, kurie siunčiami iki šiol. 2022 m. buvo aptikta Trezor gamintojo netikra	Stebėti, iš kur ateina el. laiškai ar žinutės. Prieš patvirtindami operacijas, dar kartą patikrinkite gavėjų adresus. Niekada su niekuo nesidalykite savo atkūrimo fraze.	Visos komercinės piniginės

	renkama informacija apie vartotoją, o tik vėliau pradedama ataka prieš jį, panaudojant surinktus duomenis.	svetainė, kuri net turėjo galiojantį SSL sertifikatą, taip atrodydama kaip oficiali. Vartotojai, juose suvedę atkūrimo fazę, iš karto prarasdavo lėšas.	Prieš įvesdami neskelbtiną informaciją, visada dar kartą patikrinkite svetainių URL ir el. pašto adresus. Patikrinti oficialias gamintojų svetaines, nes ten reguliariai skelbiama informacija apie tokio tipo atakas.	
Tarpininko ataka (angl. *Man in the Middle Attack*)	Užpuolikas pertraukia ryšį tarp piniginės ir kompiuterio/ programos ar kito įrenginio, kad pavogtų, manipuliuotų informacija. Tarpininkas gali atsirasti tarp įvairių ryšiu, tokių kaip Bluetooth, NFC, Wifi ir t.t.	Bluetooth Low Energy (BLE) ataka prieš Ledger Nano X pinginę (2019). Užpuolikas perima signalą tarp piniginės ir mobiliojo ryšio, kuris veikia Bluetooth pagalba, taip užpuolikas gali matyti atliekama operacija, ar net įvesti kenkėjimas programas.	Naudoti patikimus ir saugius ryšius, vengti viešų interneto tinklų. Prieš atliekant transakciją ar kitą operaciją, patikrinti svetainių, kodo, ir programų autentiškumą.	Visi tipai, ypač USB, Bluetooth, NFC tipo

Šaltinis: sudarytas autoriaus

Kad būtų galima geriau suprasti, kaip veikia ir kokios būna, dėl kokių priežasčių aparatūrinių piniginių turėtojai praranda savo turimas lėšas, visos galimos atakos yra palyginamos lentelėje Nr. 3. Joje lyginamos skirtingos atakos, apibūdinant jų veikimo mechanizmus ir pateikiant konkrečius pavyzdžius, kaip jos buvo panaudotos realiame pasaulyje. Be to, lentelėje pateikiamos praktinės prevencinės priemonės, kurių naudotojai gali imtis, kad apsisaugotų nuo kiekvienos atakos rūšies, taip pat pabrėžiama, kaip svarbu būti budriems ir imtis aktyvių veiksmų, siekiant apsaugoti savo skaitmeninį turtą.

1 skyriuje nagrinėjama Bitcoin, kaip finansinio instrumento, svarba finansų rinkose, pabrėžiant jo unikalias savybes, galimybes ir iššūkius bei vis didėjantį poreikį saugioms bei patikimoms šios kriptovaliutos saugojimo priemonėms. Taip pat šiame skyriuje apžvelgiamos įvairios Bitcoin piniginės, jų tipai, veikimo principai, privalumai ir trūkumai bei saugumo mechanizmai, kurie padeda apsaugoti vartotojų lėšas ir užtikrinti saugias operacijas. Be to, analizuojami ir pagrindiniai saugumo iššūkiai, su kuriais susiduria aparatinių piniginių naudotojai, siekiantys užtikrinti savo skaitmeninio turto neliečiamumą. Apibendrinant galima reziumuoti: 1 skyriuje pateikiama išsami Bitcoin ir jo piniginių apžvalga, pabrėžiant Bitcoin svarbą finansų rinkose, įvairių tipų piniginių privalumus ir trūkumus, saugumo mechanizmus ir iššūkius. Ši informacija yra svarbi, norint suprasti Bitcoin ekosistemą ir galimus pavojus, susijusius su kriptovaliutų saugojimu ir naudojimu.

1 skyriuje nagrinėjama Bitcoin, kaip finansinio instrumento, svarba finansų rinkose, pabrėžiant jo unikalias savybes, galimybes ir iššūkius, bei vis didėjantį poreikį saugioms bei patikimoms šios

kriptovaliutos saugojimo priemonėms. Taip pat šiame skyriuje apžvelgiamos įvairios Bitcoin piniginės, jų tipai, veikimo principai, privalumai ir trūkumai, bei saugumo mechanizmai, kurie padeda apsaugoti vartotojų lėšas ir užtikrinti saugias operacijas. Be to, šiame skyriuje analizuojami ir pagrindiniai saugumo iššūkiai, su kuriais susiduria aparatinių piniginių naudotojai, siekiantys užtikrinti savo skaitmeninio turto neliečiamumą. Apibendrinant, 1 skyriuje pateikiama išsami Bitcoin ir jo piniginių apžvalga, pabrėžiant Bitcoin svarbą finansų rinkose, įvairių tipų piniginių privalumus ir trūkumus, saugumo mechanizmus ir iššūkius. Ši informacija yra svarbi norint suprasti Bitcoin ekosistemą ir galimus pavojus, susijusius su kriptovaliutų saugojimu ir naudojimu.

Iš atliktos analizės nustatyta, kad tiek komercinės, tiek savadarbės aparatūrinės Bitcoin piniginės turi reikšmingų trūkumų, kurie kelia saugumo, privatumo ir patogumo rizikų. Komercinės piniginės, tokios kaip „Ledger“, „Trezor“, „SafePal“ ir kitos, nors ir plačiai naudojamos dėl patogumo ir įmontuotų saugumo mechanizmų, turi svarbių trūkumų. Visų pirma, jos yra priklausomos nuo interneto ryšio tam tikroms funkcijoms, tokiomis kaip programinės įrangos atnaujinimams, kas padidina galimybę tapti kibernetinių atakų taikiniu. Statistiškai atnaujinimai atliekami kas 1-3 mėnesius, vadinasi, per šį periodą jums reikės jungti savo piniginę į tinklą. Tai reiškia, kad kibernetinės atakos galimybė išlieka, ypač kai prisijungiama prie nesaugaus tinklo arba naudojamos užkrėstos programinės įrangos atnaujinimai, o, neįsidiegus atnaujinimų, nusipirkta piniginė gali veikti netinkamai arba visiškai sutrikti jos veikimas. Vartotojui gali būti sunku atskirti oficialius atnaujinimus nuo kenkėjiškų. Taip pat kai kurios komercinės piniginės naudoja Bluetooth arba Wi-Fi ryšius patogumui užtikrinti, tačiau tai kelia papildomų rizikų. Naudojantis nesaugiu Bluetooth ryšiu (pavyzdžiui, viešose vietose), įsilaužėliai gali pasinaudoti spragomis ir užgrobti ryšį, perimti duomenis ar net pasirašyti neteisėtas operacijas. Wi-Fi ryšys taip pat gali būti nesaugus, ypač jei jungiamasi prie atvirų ar nešifruotų tinklų, kuriuose įsilaužėliai gali stebėti srautą ir išnaudoti pažeidžiamumus, siekdami pavogti privačius raktus ar prieigą prie piniginės. Įsilaužėliai dažnai taikosi į šias žinomas platformas dėl didesnės potencialios naudos, žinomumas ir didelė vartotojų bazė daro šias pinigines patraukliu taikiniu. Pasak „Kaspersky“, apie 21% visų socialinės inžinerijos atakų 2021 metais buvo nutaikytos į kriptovaliutų vartotojus, ypač komercinių piniginių, turinčių milijonines vartotojų bazes, tokias kaip „Ledger“ ir „Trezor“, savininkus. Šios atakos dažnai imituoja programinės įrangos atnaujinimus, o apgaulingi el. laiškai nukreipia vartotojus į kenksmingas svetaines. Komercinės piniginių gamintojai dažnai reikalauja, kad vartotojai pateiktų asmeninę informaciją, pavyzdžiui, el. paštą ar kitus duomenis, registracijai ir naudojimui. Tai kelia riziką, kad šie duomenys gali būti saugomi ir pasiekiami ne tik įmonėms, bet ir nusikaltėliams, jei įmonės duomenų bazės bus pažeistos. Šis centralizuotas duomenų saugojimo modelis pažeidžia kriptovaliutų esmę – anonimiškumą ir privatumą. Savadarbės piniginės,

tokios kaip „SeedSigner“ ar „Krux“, nors suteikia daugiau kontrolės ir anonimiškumo, taip pat turi didelių trūkumų. Jų programiniai kodai ne visada yra visiškai aiškūs ar atviri ir ne visi vartotojai gali atlikti reikiamą patikrą, ar jie yra saugūs. Tai sukuria riziką, kad į kodą gali būti įrašytos saugumo spragos arba netinkamai parašyti algoritmai. Šių piniginių programinis kodas turi apie 3000 eilučių, ir be kriptografijos žinių neįmanoma nustatyti, ar jis yra visiškai saugus. Šios piniginės neturi integruotų saugumo mechanizmų, tokių kaip saugūs elementai (SE), kurie naudojami komercinėse piniginėse apsaugoti nuo šalutinio kanalo atakų ar fizinių įsilaužimų. Tiek komercinės, tiek savadarbės Bitcoin piniginės gali būti paveiktos tiekimo grandinės atakų, pažeidžiamumai gali būti įdiegiami jau gamybos metu, o vartotojas apie tai nežinos. 2020 metais apie 62% visų kibernetinių atakų buvo įvykdyta per tiekimo grandinę, todėl rizika kyla tiek komercinėms, tiek savadarbėms piniginėms.

Iš analizės matyti, kad tiek komercinės, tiek savadarbės aparatūrinės piniginės turi rimtų trūkumų. Komercinės piniginės yra pažeidžiamos kibernetinių atakų dėl priklausomybės nuo interneto ir reikalauja asmeninės informacijos, ir tai sudaro didesnę riziką kibernetinių ir socialinės inžinerijos atakų. Savadarbės piniginės neturi pakankamų saugumo mechanizmų ir gali turėti programinių spragų.

2. PROTOTIPO SPRENDIMO METODIKA IR MODELIS

Šiame skyriuje aptariama siūloma sprendimo metodika, detalizuojama sistemos architektūra, transakcijų apdorojimo algoritmai ir taikomi kriptografiniai bei fiziniai saugumo mechanizmai. Šio skyriaus tikslas – pristatyti prototipo struktūrą, veikimo principus ir pagrindinius techninius sprendimus.

2.1. Prototipo siūlymas ir technologijų pasirinkimas

Didėjant kriptovaliutų vertei ir daugėjant kibernetinių atakų, saugių Bitcoin laikymo sprendimų poreikis rinkoje sparčiai auga. Aparatinės piniginės, ypač veikiančios neprisijungus ir pagrįstos fiziniais įrenginiais, tampa patrauklia alternatyva, nes jos užtikrina privačių raktų apsaugą ir sumažina kibernetinių grėsmių riziką. Internetinės ir komercinės piniginės dažnai tampa įsilaužėlių taikiniu, o aparatinės neprisijungusios piniginės leidžia išlaikyti aukštą saugumo lygį be interneto ryšio. Šie sprendimai tenkina augantį vartotojų poreikį apsaugoti savo turtą nepriklausomai nuo interneto ir trečiųjų šalių priežiūros.

Pagrindinis darbo tikslas yra sukurti belaidę nuo tinklo atjungtą aparatinę Bitcoin piniginę, užtikrinančią aukštą saugumo ir anonimiškumo lygį. Šis sprendimas užtikrintų, kad privatūs raktai, esminiai kriptografiniai elementai ir jų valdymas liktų visiškai izoliuoti nuo internetinių tinklų, taip minimizuojant duomenų vagystės riziką. Tyrimas, atliktas Nowroozi ir kt.(2023), rodo, kad belaidės nuo tinklo atjungtos aparatinės piniginės ženkliai sumažina kibernetinių atakų pavojų, nes jos nėra tiesiogiai susietos su tinklo ryšiais, o atnaujinimai gali būti atliekami tik fiziškai atjungus įrenginį nuo tinklo. Be to, šio tipo piniginėse paprastai naudojami aukšto lygio šifravimo algoritmai, tokie kaip ECDSA ir SHA-256, kurie užtikrina papildomą duomenų apsaugą.

Ebrahimi ir kt. (2021) savo tyrime šias pinigines vadina šaltomis ir savo tyrime teigia, kad 90 % atakų, tokių kaip MITM ar socialinės inžinerijos atakos, prieš aparatūrines pinigines yra vykdomos per interneto ryšį, todėl visiškas atjungimas nuo tinklo drastiškai sumažina rizikas. Autoriai taip pat teigia, kad šio tipo piniginės sumažina šalutinio kanalo atakų galimybę, kadangi dažniausiai jos yra vykdomos skaičiuojant galios pokyčius įrenginiuose, kad būtų galima nuskaityti privačius raktus. Belaidė piniginė nėra prisijungusi prie tinklo, neturi didelių galios sunaudojimo pokyčių, todėl sumažina tokios informacijos nutekėjimo galimybę, kadangi galios signalai osciloskopu yra sunkiau fiksuojami.

Papildomų neprijungtų prie interneto belaidžių piniginių privalumų išskiria Ernile ir kt. (2023), kurie savo tyrime pabrėžia, kad šios piniginės pasižymi paprastu ir patogiu naudojimu. Autorių teigimu, šio tipo piniginės dažniausiai naudoja QR kodus arba kitus fizinius duomenų perdavimo būdus, kurie leidžia saugiai ir efektyviai vykdyti transakcijas net ir neprijungtoje aplinkoje. Toks sprendimas ne tik padidina vartotojo patogumą, bet ir užtikrina papildomą saugumo lygį, nes eliminuojama būtinybė naudotis interneto ryšiu, kuris dažnai tampa pagrindiniu kibernetinių atakų taikiniu.

„Non-custodial“ aparatės kriptovaliutų piniginės yra viena iš pagrindinių decentralizuotos finansų (DeFi) ekosistemos inovacijų, suteikiančių vartotojams visišką savo privačių raktų ir turto kontrolę, nereikalaujant pasitikėjimo trečiųjų šalių saugotojais. Pasak Bower ir kt. (2024), tokios piniginės padidina saugumą, nes suteikia vartotojams galimybę savarankiškai valdyti savo raktus, taip sumažinant riziką, su centralizuotomis sistemomis bei kibernetinėmis grėsmėmis susijusias rizikas. Be to, autoriai Barbereau ir Bodo (2023) pabrėžia, kaip „non-custodial“ sprendimai palaiko vartotojų privatumą ir anonimiškumą, o taip pat prisideda prie finansinės įtraukties spragų mažinimo, suteikdami nebrangią prieigą prie finansinių paslaugų asmenims, kuriems trūksta bankų infrastruktūros. Vadlamani ir Sharma (2023) taip pat akcentuoja, kad šios piniginės yra efektyvi priemonė finansinių paslaugų prieinamumui didinti, ypač socialiai ir ekonomiškai atskirtoms grupėms. Dėl jų sąveikumo su įvairiomis platformomis jos tampa esminiu įrankiu, skatinančiu inovacijas ir mažinančiu priklausomybę nuo tarpininkų. Kaip teigia Barbereau ir Bodo (2023), „non-custodial“ piniginės yra transformacinis žingsnis decentralizuotos, atsparios ir prieinamos skaitmeninės ekonomikos link, kuri stiprina ne tik technologinę ir ekonominę pažangą, bet ir žymi naują finansų sistemos etapą.

Remiantis autorių įžvalgomis ir ankstesne piniginių tipų analize, siekiant užtikrinti maksimalų kriptovaliutų turto saugumą, nepriklausomybę nuo trečiųjų šalių ir išlaikyti anonimiškumą, šio darbo autorius siūlo sukurti belaidę nuo tinklo atjungtą aparatinę Bitcoin piniginę. Toks sprendimas suteikia jos vartotojui visišką turimos informacijos kontrolę užtikrinant aukštą apsaugos lygį ir mažinant kibernetinių atakų rizika. Šis tipas yra pasirinktas dėl šių savybių:

- **Saugumas** – apsauga nuo internetinių ir tinklo grėsmių, nes privatus raktas bus laikomas neprijungtoje aplinkoje.
- **Anonimiškumas** – visiškas vartotojo duomenų ir transakcijų privatumas be trečiųjų šalių įsikišimo ar informacijos rinkimo.
- **Patikimumas ir prieinamumas** – stabili patikima aplinka ir paprastai suprantamas bei programuojamas programos kodas.

- **Komponentų prieinamumas –** šiam prototipui sukurti reikalingi techniniai komponentai yra lengvai prienami ir plačiai naudojami rinkoje užtikrinant sprendimą, kurį galima susirinkti ir naudoti įvairiose vietose.
- **Universali ir lanksti –** piniginės prototipas, paremtas „Raspberry Pi Zero“ mikrokompiuteriu, leidžia vartotojui pasirinkti ir pritaikyti komponentus, tokius kaip ekranas, mygtukai ar dėklas, atsižvelgiant į individualius poreikius bei naudojimo aplinką.

Prototipui pasirinkta Bitcoin valiuta dėl jos plataus pripažinimo, naudojimo, stabilumo ir unikalių savybių, kurios ypač tinkamos neprijungusiam sprendimui. Smales (2020) pažymi, kad Bitcoin užsitarnavo aukštą pasitikėjimą rinkoje ir laikomos diversifikacijos pagrindu, padedančiu mažinti portfelių riziką dėl savo stabilumo lyginant su kitomis kriptovaliutomis. Bitcoin decentralizuota struktūra ir UTXO modelis, kaip teigia Bouri ir kt. (2018), užtikrina efektyvų transakcijų valdymą ir apsaugą nuo kibernetinių grėsmių ir centralizuotų sistemų pažeidžiamumų.

Koutmos ir kt. (2021) Bitcoin apibūdina kaip „skaitmeninį auksą“, veiksmingą apsidraudimo priemonę ekonominio neapibrėžtumo sąlygomis, o Shahzad (2020) pažymi, kad mažas koreliacijos lygis su tradiciniais finansų aktyvais padeda diversifikuoti turtą. Be to, atvirojo kodo bendruomenė ir stipri palaikymo bazė užtikrina Bitcoin technologijos saugumą ir ilgaamžiškumą.

Bitcoin tinklas pasižymi itin aukštu „hash rate“, siekiančiu apie 250 EH/s, kas užtikrina apsaugą nuo išpuolių, pranokstant kitų kriptovaliutų, tokių kaip Ethereum ir Litecoin, saugumo lygį. Plačiai išskirstyta tinklo struktūra suteikia atsparumą cenzūrai ir nepriklausomybę nuo centralizuotų institucijų, kas itin svarbu be tinklo veikiančioms piniginėms. Dėl šių savybių Bitcoin yra idealus pasirinkimas neprisijungusiam prie tipo prototipui, siekiant užtikrinti vartotojų turto saugumą ir stabilumą įvairiomis rinkos sąlygomis.

Aparatinės, neprisijungusios prie interneto Bitcoin piniginės sprendimas grindžiamas augančiu poreikiu užtikrinti kriptovaliutų saugumą ir anonimiškumą, mažinant kibernetinių grėsmių riziką. Šis pasirinkimas leidžia išlaikyti privačių raktų izoliaciją nuo tinklo, naudojant UTXO modelį ir pažangius šifravimo algoritmus, tokius kaip ECDSA ir SHA-256, kurie užtikrina aukštą duomenų apsaugos lygį. Be to, ši piniginė išsiskiria universalumu – ją galima lengvai pritaikyti pagal individualius poreikius, naudojant QR kodų sąsają ir pasirenkamus techninius komponentus. Bitcoin, kaip valiutos, pasirinkimas suteikia papildomą pranašumą dėl jo stabilumo ir saugumo, kas yra ypač reikšminga siekiant patikimo ir ilgaamžio sprendimo neprisijungusioje aplinkoje.

2.2. Privatumo ir anonimiškumo aspektai kriptovaliutų technologijose

Anonimiškumas ir privatumas kriptovaliutų prekyboje yra neatsiejami nuo šiuolaikinių decentralizuotų finansų sistemų, užtikrinančių saugumą ir apsaugą nuo kibernetinių grėsmių. Pastaraisiais metais šios savybės tapo itin svarbios dėl augančių vartotojų privatumo nuogąstavimų, interneto reguliavimo iššūkių ir kibernetinių grėsmių masto.

Anonimiškumas leidžia naudotojams atlikti finansines operacijas nesidalijant asmenine informacija, taip mažinant galimų piktnaudžiavimų riziką. Pavyzdžiui, QR kodais pagrįstos neprisijungus veikiančios Bitcoin piniginės, kaip aptarta moksliniuose tyrimuose, užtikrina privatumo ir saugumo balansą, leidžiant naudotojams valdyti savo lėšas neprisijungus prie interneto, kas reikšmingai sumažina kibernetinių atakų tikimybę.

Mokslinės analizės rodo, kad neprisijungus veikiančios piniginės, tokios kaip „Ledger“ ar „Trezor“, yra vertingos, nes iš esmės eliminuoja internetines saugumo spragas. Šios technologijos ne tik apsaugo nuo galimo kibernetinio įsikišimo, bet ir padeda apsaugoti vartotojo asmeninius duomenis užtikrindamos, kad operacijos lieka anoniminės.

Neprisijungus prie interneto veikianti belaidė aparatūros Bitcoin piniginė su QR kodų funkcija gali būti esminis sprendimas užtikrinant aukštą anonimiškumo ir saugumo lygį kriptovaliutų operacijose. Kaip nurodo Erinle ir kt. (2023), QR kodų naudojimas leidžia atlikti sandorius neprisijungus, minimalizuojant duomenų nutekėjimo riziką ir užkertant kelią galimoms kibernetinėms atakoms. Jūsų kuriamo prototipo funkcionalumas, pagrįstas vien QR kodais, eliminuoja poreikį tiesioginiam ryšiui su internetu. Tokia architektūra suteikia naudotojams galimybę saugiai generuoti ir perduoti operacijų informaciją neprisijungus, taip užtikrinant, kad privatūs raktai ar kiti jautrūs duomenys liktų izoliuoti nuo galimų kibernetinių grėsmių. Hunter ir Kerr (2019) savo tyrime pabrėžia, kad tokie anonimiškumą skatinantys sprendimai atlieka svarbų vaidmenį kovojant su privatumo pažeidimais bei užtikrina vartotojų pasitikėjimą decentralizuotomis sistemomis.

Privatumo svarbą dar labiau pabrėžia „blockchain“ technologijos skaidrumo ypatybės, kurios leidžia matyti visas operacijas, bet nesuteikia tiesioginės informacijos apie vartotojo tapatybę. Ši technologija yra kritiškai svarbi ne tik siekiant apsaugoti vartotojus nuo reguliavimo pertekliaus, bet ir užtikrinant jų teisę į finansinį privatų savarankiškumą. Tokios kriptovaliutos kaip „Monero“ ir „Zcash“ naudoja pažangius šifravimo metodus, kad sustiprintų operacijų anonimiškumą, tuo pačiu papildant neprisijungus veikiančių piniginių saugumą.

Ekonominiu požiūriu anonimiškumas taip pat užtikrina apsaugą nuo nepastovių reguliavimo pokyčių ir galimo turto konfiskavimo. Tokios priemonės ypač aktualios regionuose su griežta

valstybine priežiūra. Be to, jos padeda palaikyti decentralizuoto finansų modelio stabilumą ir prieinamumą, skatindamos inovacijas ir decentralizuoto finansų sektoriaus plėtrą.

Apibendrinant galima teigti, kad anonimiškumas ir privatumas yra kertiniai šiuolaikinių decentralizuotų finansų principai. Šie bruožai ne tik skatina pasitikėjimą technologijomis, bet ir prisideda prie ilgalaikio finansinio sistemos atsparumo, užtikrindami asmens teises bei saugumą globalioje skaitmeninėje erdvėje**.**

2.3. Prototipo sistemos architektūra ir veikimo principų analizė

Aparatinės Bitcoinų piniginės prototipo kūrimui, pasirinkti standartiniai ir universalūs komponentai kurie nėra tiesiogiai pritaikyti kirptovaliutų rinkai, tačiau užtikrina reikiamą saugumą ir efektyvumą neprisijungusio prie tinklo sprendimo kontekste. Šiame skyriuje išsamiai nagrinėjami pagrindiniai aparatūriniai elementai, formuojantys belaidė nuo tinklo atjungtą Bitcoinų piniginę, bei analizuojama jų tarpusavio sąveikia. Taip pat pateikiamos techninės priežastys, pagrendančios kiekvieno komponento pasirinkimą, išvardinama kokie parametrai reikalingi, kuriant prototipą. Komponentų atranka atlikta, atsižvelgiant į jų pajėgumą vykdyti sudėtingas kriptografines operacijas, atvaizduoti ir užfiksuoti QR kodus bei techninėmis charakteristikomis, kurios garantuos aukštą duomenų saugumo lygį, sistemos patikimumą.

Aparatūriniai komponentai, sudarantys prototipą:

- **Raspberry Pi Zero V 1.3** – mikrokompiuteris, turintis 1 Ghz procesorių ir 512 MB operatyviosios atminties, yra kompaktiškas, pakankamai galingas, kad galėtų atlikti visus reikiamus kriptografinius algoritmus ir QR kodų apdorojimą. Integruotos universalios įvesties/išvesties jungtys leidžia lengvai prijungti papildomus komponentus, tokius kaip ekranas ir mygtukai. Taip pat šis kompiuteris gali efektyviai valdyti Phyton tipo programas, kurių pagrindu kuriamas prototipas. Jis neturi nei Wifi, nei Bluetooth modulių, todėl yra visiškai atjungtas nuo tinklo.
- **Ekrano ir mygtukų modulis –** LCD ekranas, turintis 240x240 taškų raišką, kuris būtų suderinamas su Raspberry Pi Zero kompiuteriu užtikrina pakankamą detalumą sudėtingų QR kodų atvaizdavimui, kurie naudojami transakcijų duomenims perduoti. Taip pat šis ekranas turi SPI sąsają, kuri leidžia duomenis greitai perduoti į ekraną, be to kompaktiškas ekrano dydis leidžia visą sistemą laikyti nešiojamą. Integruoti mygtukai, valdomi universalios

įvesties/išvesties jungtimis, užtikrina paprastą ir saugų vartotojo sąveikos mechanizmą, kuris leidžia vartotojui fiziškai patvirtinti kiekvieną veiksmą.

- **Kamera –** 5 MP kamera yra naudojama QR kodų nuskaitymui. Kamera užtikrina greitą ir tikslų QR kodų nuskaitymą, belaidį duomenų nuskaitymą be jokio tinklo ryšio turint omenyje, kad visa transakcijų informacija yra izoliuota nuo išorinių ryšių.
- **Energijos šaltinis –** naudojamas Li-ion akumuliatorius arba USB power bankas (3000 mAh, 5V 2A).
- **SD kortelė –** 32 GB talpos, užtikrina patikimą duomenų saugojimą ir palaiko greitą prieigą prie operacinės sistemos bei programinės įrangos, būtinos neprisijungusiai piniginei.

Šie prototipo komponentai buvo pasirinkti atsižvelgiant į techninės galimybes siekiant užtikrinti neprisijungusios sistemos funkcionalumą. Sistema sukurta iš komponentų, kurie lengvai prieinami prekybos tinkluose ir elektroninėse parduotuvėse, nėra brangūs ir ypač tinkami mažiems projektams įgyvendinti. „Raspberry Pi Zero V 1.3“ pasirinktas dėl 1 GHz procesoriaus ir 512 MB operatyviosios atminties, kurios pakanka kriptografiniams skaičiavimams bei raktų generavimui. Pasirinktas mikrokompiuteris turi universalias įvesties/išvesties jungtis, kurios leidžia prijungti įvairius komponentus ir lengvai surinkti kompaktišką prototipą. 5 MP „Waveshare“ gamintojo kamera pasirinkta dėl jos techninių savybių kurios turėtų užtikrinti gerą QR kodų nuskaitymą neprisijungusioje aplinkoje. Kamera suderinama su Raspberry Pi Zero per CSI sąsają, kuri palaiko didelės spartos duomenų perdavimą, o 5 MP raiška (2592x1944 pikselių), turėtų užtikrinti sudėtingų kodų nuskaitymą. „Waveshare“ gamintojo „1.3-inch 240x240 IPS LCD (HAT)“ ekranas pasirinktas dėl savo 240x240 raiškos ir IPS technologijos, kuri užtikrina gerą spalvų atkūrimą ir plataus kampo matomumą. Mažas ekrano buferis (~57,600 baitų su 8-bit spalvų gylio schema) puikiai tinka mažo galingumo mikrokompiuteriams. Taip pat pasirinktas ekranas naudoja SPI protokolą, kuris užtikrina greitą duomenų perdavimą su minimalia procesoriaus duomenų apkrova. Visos detalės, skirtos šiam įrenginiui, yra standartizuotos ir lengvai prieinamos. Taip pat šis mikrokompiuteris išsiskiria plačiu suderinamumu su Python bibliotekomis, tokiomis kaip „bitcoinlib“, „qrcode“ ir „PIL“, kurios būtinos raktų valdymui, QR kodų generavimui bei nuskaitymui.

Šiame skyriuje aptarta Bitcoin piniginės prototipo sistemos architektūra ir veikimo principai. Prototipas sukurtas naudojant komponentus, kurie užtikrina neprisijungusios piniginės saugumą, efektyvumą ir patikimą vartotojo sąveiką. Parinkti komponentai, tokie kaip Raspberry Pi Zero W, ekranas, mygtukai, kamera, energijos šaltinis ir SD kortelė, sudaro belaidę izoliuotą nuo tinklo aplinką.

Šie elementai buvo pasirinkti dėl jų tinkamumo kriptografinėms operacijoms bei lengvai prieinamų sprendimų, kurie suteikia galimybę sukurti funkcionalią ir prieinamą piniginės prototipo sistemą.

2.3.1. Mikrokompiuterių analizė ir pasirinkimo kriterijų pagrindimas

Pasirenkant mikrokompiuterį šiam Bitcoin piniginės prototipui, buvo atlikta palyginimo analizė, įvertinus pagrindinius savadarbių piniginių projektuose naudojamos modelius, kuriuos renkasi tokie projektai kaip „Seedsigner“, „Krux“, „Coldcard“. Buvo palygintos jų techninės specifikacijos, apdorojimo pajėgumas, pritaikomumas kriptografinėms algoritmams, įvesties/išvesties jungtys ir priedai, Phyton programavimo kalbos palaikymas. Tyrimas taip pat nustato kiekvieno mikrokompiuterio prieinamumą rinkoje ir įvertina bendruomenės, kurios užtikrina techninę pagalbą, instrukcijas ir papildomą dokumentacija įvairiems projektams kurti.

Lentelėje Nr. 4 pateikiama išsami mikrokompiuterių analizė:

4 lentelė

Mikrokompiuterių palyginimo lentelė

Mikrokompiuteris	**Procesorius**	**Operatyvioji atmintis (RAM)**	**Įvesčių/išvesčių jungčių kiekis**	**Phyton palaikymas**	**SD kortelės palaikymas**	**Kaina (€)**
Raspberry Pi Zero V1.3	1 GHz ARM1176JZF-S	512 MB	40	Didelis	Taip	~15-20
NanoPi Neo Air	1.2 GHz Cortex	512 MB	24	Didelis	Ne	~20-25
Onion Omega2+	580 MHz MIPS CPU	128 MB	15	Ribotas	Taip	~10-15
M5StickV	Kendryte K210	8 MB	8	Labai ribotas	Ne	~40-50

Šaltinis: sudarytas autoriaus

Atlikta analizė įrodė, kad geriausiai kuriamam prototipui tinka „Raspberry Pi Zero V1.3“. Šis mikrokompiuteris turi palyginti galingą 1 GHz procesorių ir 512 MB darbinę atmintį, kurie yra daugiau negu pakankami atlikti kriptografinius skaičiavimus. Jis taip pat turi didelį įvesčių/išvesčių, leidžiančių prijungti įvarius periferinius komponentus, skaičių. Taip pat šis kompiuteris puikiai palaiko Phyton bibliotekas, tokias kaip „bitvoinlib“, „qecode“, „cv2“ ir „hashlib“, kurios yra skirtos kurti kriptografinius algoritmus ar QR kodo apdorojimą. „Raspberry Pi Zero V1.3“ turi SD kortelės palaikymą, leidžiantį naudoti išorinę saugyklą operacinei sistemai ir duomenų failams, kas yra itin naudinga neprisijungusiam sprendimui, kai reikalinga talpi ir lanksti atmintis.

„Nano Neo Air“ turi 1.2 GHz keturių branduolių Cortex procesorių ir 512 MB RAM atminti aprūpintas mikrokompiuteris, palaikantis Linux sistemas ir Python bibliotekas. Nors jis turi integruotą 8 GB atmintį, jam trūksta atminties kortelės palaikymo ir turi tik 24 jungtis, kas riboja jo funkcionalumą. Palyginus su „Rasberry Pi Zero V 1.3“, „Nano Neo Air“ pasižymi aukštesne kaina, mažesniu pasiekiamumu rinkoje ir ribotų priedų pasirinkimu, bei mažesnė bendruomene, bei palaikymų, todėl jis nėra tinkamas mikrokompiuterio pasirinkimas.

„Onion Omega2+“ mikrokompiuteris turi 580 MHz MIPS procesorių ir 128 MB RAM atminti. Nors šis mikrokompiuteris turi pilnavertį Linux operacinės sistemos palaikymą, tačiau ji yra skirtingo tipo (OpenWRT) ir tik dalinai palaiko Python bibliotekas. Taip pat „Omega2+“ turi mažiau jungčių tik 15, o priedų ir periferinių įrenginių pasirinkimas yra ribotas. Nors šis mikrokompiuteris yra pigesnis nei „Raspberry“ jis nėra tinkamas pasirinkimas piniginės prototipo kūrimui.

„M5StickV“ su Kendryte K210 (RISC-V) procesoriumi ir 8 MB RAM, nors ir silpnesnis už aptartus įrenginius, tačiau aptartas dėl plataus naudojimo savadarbių piniginių projektuose. Dėl RISC-V architektūros ir riboto Python palaikymo šis mikrokompiuteris nėra tinkamas visoms kriptografinėms operacijoms, reikalaujančioms „bitcoinlib“ ar „ecdsa“ bibliotekų. Nors M5StickV gali vykdyti kai kurias kriptografinio apdorojimo funkcijas, jo ribotas jungčių skaičius ir mažas bendruomenės palaikymas apsunkina šio mikrokompiuterio pritaikymą Bitcoin piniginei. Be to, M5StickV neturi SD kortelės palaikymo, todėl negali tinkamai atlikti išorinės duomenų saugojimo funkcijos, būtinos neprisijungusiam sprendimui.

Atlikta analizė rodo, kad „Raspberry Pi Zero V 1.3“ yra optimaliausias pasirinkimas Bitcoin piniginės prototipui dėl savo funkcionalumo, plataus programinės įrangos palaikymo ir išorinių komponentų integravimo galimybių. Šis mikrokompiuteris užtikrina reikiamą stabilumą ir lankstumą, svarbų kriptografiniams skaičiavimams bei duomenų saugojimui neprisijungus. Kiti variantai, kaip „Nano Neo Air“, „Onion Omega2+“ ir „M5StickV“, ne visiškai atitinka reikalavimus dėl riboto pritaikomumo ir nepalaiko visų būtinų funkcijų, todėl nėra tinkami Bitcoin piniginės funkcijoms užtikrinti.

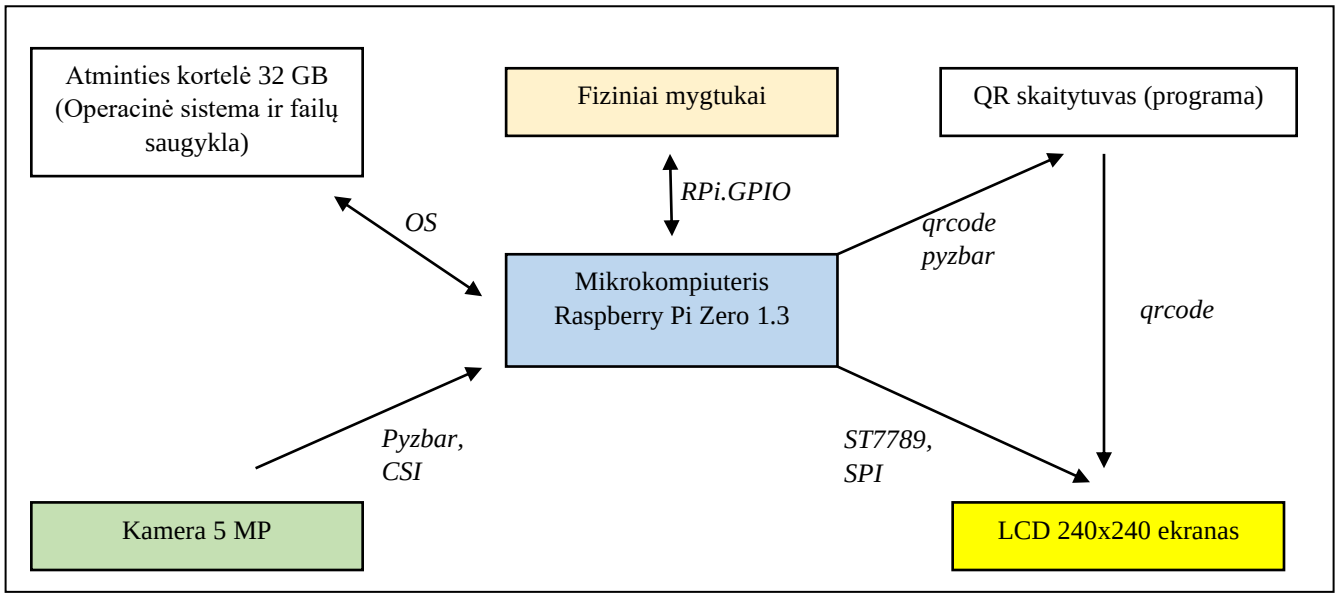
2.3.2. Prototipo architektūros struktūra ir veikimo schema

Šiame skyriuje aptariama kuriamo prototipo architektūra ir veikimo schema (žr. 4 pav.), kaip ir kokiomis Python bibliotekomis tarpusavyje bendrauja ir veikia atskiri komponentai bei kokią funkciją atlieka. Ši architektūra yra sukurta siekiant išlaikyti visišką izoliaciją nuo išorinių tinklų.

Mikrokompiuteris „Raspberry Pi Zero V 1.3“ yra pagrindinis valdikis, kuriame įdiegta Python programa, atsakinga už pagrindinių piniginės funkcijų vykdymą. Šios funkcijos apima Bitcoin piniginės adresų generavimą, nepasirašytų ir dalinai pasirašytų kriptografinių operacijų dekodavimą bei operacijų pasirašymą. Siekiant užtikrinti aukščiausią saugumo lygi, visos kriptografinės operacijos atliekamos neprisijungus prie tinklo. Privatūs raktai yra šifruojami kriptografinėmis bibliotekomis, „hashlib“ ir „ecdsa“ ir yra saugomi atminties kortelėje, kurioje taip pat yra metaduomenys bei laikini operacijų failai. Prieiga prie kortelės yra valdoma per „OS“ biblioteką, kuri įgalina saugias skaitymo ir rašymo operacijas.

Vartotojo sąsaja yra sukurta aplink įvesties/išvesties jungtimis prijungtais mygtukais, naudojant „RPi.GPIO“ biblioteką. Fiziniai mygtukai leidžia vartotojams bendrauti su minimalistine prototipo meniu sistema. LCD ekranas veikia kaip pagrindinis išvesties įrenginys, veikiantis per „ST7789“ biblioteką ir SPI, perteikiantis grafinius elementus, tokius kaip tekstas ir QR kodai.

Sandorių duomenys perduodami į mikrokompiuterį per prijungtą 5 MP kamerą, naudojant biblioteką „picamera“. Kamera fiksuoja QR kodus su operacijų duomenis, kurie iššifruojami į tinkamus formatus naudojant „pyzbar“ biblioteką. Kamera pajungta per mikrokompiuterį esančią CSI jungtį. Šis metodas suteikia saugų ir izoliuotą būdą perkelti operacijų duomenis į piniginę, laikantis oro tarpo veikimo pricipo ir visiškai išvengiant tinklo.



Šaltinis: sudarytas autoriaus

4 pav. Prototipo veikimo schema

Pinginės kriptografinės funkcijos įgyvendinamos naudojant „bitcoinlib“, „hashlib“ ir „ecdsa“ bibliotekas, kurios palaiko plačiai naudojamus Bitcoin standartus, įskaitant BIP-32, BIP-39 ir BIP-174. Sistema išvesti duomenims į išorę naudoja „qrcode“ biblioteką, kuri generuoja QR kodus, nurodančius piniginės adresus arba pasirašytas operacijas. Šie QR kodai rodomi skystųjų kristalų ekrane, kad juos būtų galima nuskaityti išoriniu įrenginiu ir saugiai perduoti operacijų duomenis.

Darbo eiga prasideda nuo to, kad vartotojai per fotoaparatą nuskaito nepasirašytus operacijų QR kodus į piniginę. Operacijos duomenys iškoduojami, pasirašomi privačiu raktu, saugomu atminties kortelėje, ir išvedami kaip pasirašytas operacijos QR kodas. Pasirašytą operaciją galima nuskaityti atskiru, tinkle veikiančiu įrenginiu, transliuoti į Bitcoin tinklą. Šis žingsnis po žingsnio procesas garantuoja, kad jautrios operacijos, tokios kaip privataus rakto tvarkymas ir operacijų pasirašymas, būtų atliekamos tik neprisijungus prie piniginės.

Prototipo architektūra užtikrina maksimalų saugumą, vykdant operacijas visiškai izoliuotoje aplinkoje, be tiesioginio ryšio su tinklu. Kuriamos sistemos struktūra pagrįsta moduliškumu, saugumo principų laikymusi ir efektyvia Python bibliotekų integracija, užtikrinančia patikimą kriptografinių funkcijų įgyvendinimą.

2.4. Naudojamos Python bibliotekos

Šiame skyriuje nagrinėjama kuriamo prototipo programinė architektūra ir pasirinktos bibliotekos, išsamiai aprašant, kaip tarpusavyje sąveikauja ir kokias funkcijas atlieka skirtingi komponentai, naudojant Python programavimo kalbos bibliotekas. Pagrindinis dėmesys skiriamas sistemai, sukuriančiai visiškai izoliuotą nuo išorinių tinklų aplinką.

Naudojamas Raspberry Pi Zero V 1.3 mikrokopiuteris yra sukurtas lengviems projektams ir operacijoms, kadangi 1 GHz ARM11 procesorius nėra galingas ir turi limituotą resursą. Python naudojimas yra tinkamas tokioms aplinkoms, nes gali atlikti tiek aukšto, tiek žemo lygio operacijas be didelių procesoriaus užkrovimo išlaidų. Taip pat jis gerai pritaikomas naudojamoje Raspberry Pi Legacy Lite operacinėje aplinkoje. Veiksmingas Python atminties valdymas sumažina išteklių naudojimą. Tai užtikrina, kad mikrokompiuteris gali atlikti kelias užduotis tuo pačiu metu, tokias kaip QR kodo nuskaitymas, kriptografinės operacijos ir fotoaparato įvestis, be didelių problemų. Lengvi procesai ir modulinis Python dizainas leidžia sumažinti didelių priklausomybių poreikį, taip išsaugant ribotą naudojamo įrenginio darbinę atmintį. Python siūlo tiesiogines bibliotekas, skirtas sąveikai su

aparatūros periferiniais įrenginiais, tokiais kaip GPIO kaiščiai ir kameros moduliai, tuo pat metu įgalindamas aukšto lygio kriptografinius skaičiavimus ir programinės įrangos projektavimą.

Python programavimo kalba siūlo reikšmingus privalumus, kuriant belaidę, nuo tinklo atjungtą Bitcoin piniginę. Vienas iš pagrindinių jos pranašumų – galimybė efektyviai integruoti aparatinės ir programinės įrangos funkcionalumus. Python leidžia tiesiogiai valdyti aparatinę įrangą, pavyzdžiui, GPIO sąsajas, užtikrinant sklandų duomenų mainą tarp fizinių komponentų ir kriptografinių procesų. Tai itin svarbu užtikrinant patikimą veikimą nuo tinklo izoliuotoje aplinkoje. Be to, modulinis Python architektūros pobūdis suteikia galimybę lengvai išplėsti piniginės funkcionalumą, įtraukiant tokias funkcijas kaip daugiaparašų (angl. multi-signature) palaikymas ar papildomų Bitcoin protokolų, pvz., BIP-44, integravimas.

Šiame projekte naudojamos bibliotekos (žr. lentelę Nr. 5) buvo pasirinktos atsižvelgiant į jų technines savybes ir testavimo metu atliktus bandymus.

5 lentelė

Naudojamos Python bibliotekos prototipo kode

Pavadinimas	Techninės funkcijos
RPi.GPIO	- Įgalina tiesioginį įvesties/išvesties kaiščių valdymą per Python kodą; - Užtikrina minimalių atsakymų realiuoju laiku delsą (<1 ms); - Visiškai suderinamas su Raspberry Pi BMC architektūra.
qrcode	- Koduoja Bitcoin adresus ir sandorių duomenis į QR kodus; - Palaiko iki 4296 raidinių ir skaitmeninių simbolių viename QR kode; - Įgyvendina klaidų taisymą, kad jos būtų lengvai nuskaitomos, bei užtikrina mažą išteklių naudojimą generuojant QR kodą. Naudoja Reed-Solomon algoritmą klaidų taisymui.
pyzbar	- Dekoduoja įvairių tipo kodus: QR, DataMatrix, PDF417; - Naudoja „zbar“ bibliotekos branduolį greitam ir tiksliam dekodavimui; - Apima klaidų aptikimo mechanizmus, susijusius su pažeistais arba neišsamiais QR kodais; - Užtikrina tikslų duomenų gavimą neprisijungus prie tinklo saugioje aplinkoje.
picamera	- Vaizdo apdorojimo modulis, fiksuoja aukštos kokybės kadrus, reikalingus QR kodų identifikavimui. - Įdiegti vaizdų apdorojimo mechanizmai (pvz. triukšmo mažinimas, histogramų analizė, spalvų balansavimą). - Palaiko JPEG, PNG ir kitus formatus.
hashlib	- Įdiegia SHA-256 saugiam kriptografiniam maišymui, kuris būtinas Bitcoin sandoriams; - Užtikrina Bitcoin protokolo standartų laikymąsi.
ST7789, PIL	- Leidžia valdyti TFT LCD ekraną naudojant SPI sąsają. - Užtikrina aukštos kokybės spalvų vaizdą (262K arba 16-bit RGB spalvų palaikymas). - Optimizuotas mažam išteklių naudojimui, tinkamas realaus laiko atvaizdavimo operacijoms.

Šaltinis: sudarytas autoriaus

Python taip pat išsiskiria plačia bibliotekų ekosistema, kuri yra itin naudinga realaus laiko reakcijų ir saugaus kriptografinio funkcionalumo užtikrinimui. Bibliotekos, tokios kaip „pyzbar ir „PIL“, leidžia greitai apdoroti QR kodų nuskaitymą ir inicijuoti sandorius, o kriptografinės bibliotekos, tokios kaip „hashlib“ ir „bitcoinlib“, užtikrina patikimą raktų valdymą ir skaitmeninių parašų generavimą pagal Bitcoin standartus. Python efektyviai naudoja sistemos resursus, todėl gali vykdyti procesoriaus išteklių reikalaujančias užduotis, tokias kaip QR kodų generavimas ar kriptografiniai skaičiavimai, net ir tokiuose ribotų galimybių įrenginiuose kaip „Raspberry Pi Zero V 1.3“. Šios savybės daro Python idealia technologija saugiai, funkcionaliai ir našiai piniginės plėtrai.

2.4.1. Prototipo pagrindinio variklio pasirinkimas: Bitcoinlib, Electrum ir Btcpy palyginimas

Kriptovaliutų saugumo srityje, ypač kalbant apie neprisijungusias Bitcoin pinigines, kelios programinės įrangos bibliotekos išpopuliarėjo dėl savo tvirtų funkcijų ir bendruomenės palaikymo. Kuriant tokias saugias savadarbes piniginių sistemas, dažnai naudojami „Bitcoinlib“, „Electrum“ ir „btcpy“. Kuriant šią neprisijungusią prie tinklo Bitcoin piniginę, reikia įsivertinti ir pagrindinius programinės įrangos įrankius, naudojamus valdyti kriptografines operacijas, operacijų eigą ir saugius duomenų perdavimo elementus. Šiame skyriuje įvertinamos ir palyginamos trys bibliotekos („Bitcoinlib“, „Electrum“ ir „btcpy“), daugiausia dėmesio skiriant jų tinkamumui naudoti šiame prototipe. Išnagrinėjami pagrindiniai veiksniai, tokie kaip priklausomybės valdymas, neapdorotų operacijų kūrimo palaikymas, suderinamumas su oro tarpų darbo eigomis ir QR kodo integravimas. Ši analizė nustato, kad „Bitcoinlib“ yra patikimiausias ir efektyviausias sprendimas. Vertinimas ne tik pabrėžia „Bitcoinlib“ technines stipriąsias puses, bet ir nustato šias galimybes pagal platesnius saugios ir minimalistinės Bitcoin piniginės sistemos reikalavimus, taip padėdamas pagrindą jos pasirinkimui pagal siūlomą dizainą.

Python programavimo kalbos biblioteka „bitcoinlib“ yra tinkamas sprendimas aplinkoms be grafinių vartotojo sąsajų (angl. GUI), todėl jis tinkamas „Raspberry Pi Legacy Lite“ operacinei sistemai, kurioje pirmenybė teikiama minimaliam išteklių naudojimui. Skirtingai „electrum“, siūlo komandų eilutės sąsają (angl. LCI), bet yra paremta išorinių serverių arba asmeninių „elektrum“ serverių, „bitcoinlib“ išvengią nereikalingo sudėtingumo. Papildomos „elektrum“ priklausomybės, įskaitant ir grafinę vartotojo sąsajos komponentus, tokius kaip „PyQt“, tik apsunkina jo naudojimą aplinkoje be GUI. Panašiai, nors „btcpy“ yra lengvas ir tinkamas pagrindinėms kriptografinės

operacijoms, bet jame trūksta integruotų piniginių valdymo funkcijų, o tai apriboja jo naudojimo galimybes.

„Bitcoinlib“ palaiko „Bitcoin Improvement Proposals“ (BIP), pvz., BIP32, BIP39 ir BIP44, palaikymą, kurie yra būtini hierarchiniam deterministiniam (HD) piniginės valdymui. Šios funkcijos leidžia sukurti saugias ir nešiojamas Bitcoin pinigines, visiškai suderinti su mnemoninėmis frazėmis ir atlikti patikimas kriptografines operacijas, įskaitant elipsinės kreivės skaitmeninio parašo algoritmo (ECDSA) pasirašymą. „Elektrum“, nors ir palaiko BIP32 ir BIP39, šias funkcijas glaudžiai su savo programos architektūra, sumažindama darbo eigos neprisijungus prie tinklo, lankstumą. „Btcpy“ siūlo pagrindines kriptografines galimybes, tačiau trūksta abstrakcijos sluoksnių, todėl reikia papildomų bibliotekų ir elementų, norint pasiekti panašias funkcijas, kurias turi „electrum“ ar „bitcoinlib“.

Esminis šio prototipo ir Bitcoin piniginių bruožas yra QR kodų naudojimas saugiai transakcijų duomenims perduoti tarp neprisijungusių interneto sistemų. „Bitcoinlib“ palengvina sklandų integravimą su kitomis Python bibliotekomis, leidžia generuoti pasirašytų operacijų QR kodus ir juos iššifruoti, kad būtų galima importuoti operacijų duomenis iš tinklo įrenginių. „Elektrum“ neturi vietinio QR kodo palaikymo, todėl šiai funkcijai atlikti reikalingi išoriniai įrankiai ir papildomos bibliotekos. „Btcpy“ nesiūlo jokio tiesioginio QR kodo skaitymo, integravimo ir palaikymo, todėl būtinas pritaikymas, diegimas, bibliotekos ir išoriniai įrenginiai ir dar labiau apsunkina darbo eigą.

Lengvas „bitcoinlib“ dizainas sumažina išorines priklausomybes, atakų paviršių ir užtikrina suderinamumą izoliuotose neprijungtose aplinkose, tokiose kaip „Raspberry Pi Legacy lite“, kuri naudojama prototipo kūrime. Šio dizainas prieštarauja „elektrum“ siūlomam, kuriai reikalinga grafinė vartotojo sąsaja, išnaudojanti daug operatyvinės mikrokompiuterio atminties ir taip apsunkinanti diegimą minimalistinėse aplinkose, tokiuose projektuose kaip šis. Nors „btcpy“ turi minimalistinį dizainą, jo funkcionalumas apsiriboja neapdorotomis Bitcoin protokolo operacijomis, nes trūksta integruotų funkcijų. Kartu šios stipriosios pusės įrodo, kad „bitcoinlib“ – efektyviausias, saugiausias ir universaliausias neprijungtos prie interneto belaidės „Bitcoin“ piniginės diegimo sprendimas. Lentelėje Nr. 6 pateikiama detalesnė šių bibliotekų analizė.

Lentelė Nr. 6

Išplėstinis bibliotekų „Bitcoinlib“, „Electrum“ ir „btcpy“ palyginimas

Funkcija	Bitcoinlib	Electrum	btcpy
Suderinimas su **ne** GUI aplinka	Optimalus, pilnai pritaikytas CLI apliktoms.	Vidutinis: CLI reikalauja papildomų konfigūracijų.	Tinkamas, minimalistinis ir veikia be GUI.
Neapdoroto sandorio kūrimas	Visiškai pritaikomas su intuityviais metodais	Palaikomas, bet reikalauja papildomų JSON procesų	Palaikymas, tačiau reikalauja rankinio įgyvendinimo.
Sandorių pasirašymas neprisijungus	Pilnai funkcionalus su ECDSA, neprisijungusiam prie tinklo naudojimui	Funkcionalus, bet turi papildomų priklausomybių nuo bibliotekų „ecdsa“ ir „protobuf“	Galimas, bet reikia papildomų išplėstinių nustatymų.

QR kodo integracija	Lengvai integruojama su išoriniais įrenginiais, „qrcode“ biblioteka	Galimas, bet reikalauja papildomų bibliotekų „qrcode“ ir „Pillow“	Nepalaikoma, reikia išorinių bibliotekų ar pritaikymų rankiniu būdu,
BIP32/39/44 palaikymas	Visapusiškas, HD piniginės ir mnemoninės fazės	Palaikomas BIP32 ir BIP39 per serverio „ElectrumX“ architektūra	Palaiko tik BIP32, trūksta BIP39/44. Riboja naudojimą su mnemoninėmis frazėmis
Diegimo paprastumas	Paprastas, minimalios priklausomybės	Vidutinis, nes reikalauja papildomų GUI procedūrų.	Paprastas, bet reikalingos didesnės techninės žinios.
Lankstumas ir pritaikymas	Lankstus: Modulinė API, tinkama pritaikymui.	Vidutinis: Mažiau lankstus dėl serverio, API integracijos.	Ribotas: Trūksta piniginės abstrakcijos.
Naudojimas paprastose sistemose	Pritaikytas: Minimalios išteklių sąnaudos RAM naudojimas ~30 MB, tinkamas senesnėms platformoms, Python 3.6+.	Apribotas: Didelės priklausomybės sudaro kliūtis. RAM naudojimas 50-80 MB, Python 3.7+	Tinkamas, bet reikalauja papildomų bibliotekų. RAM naudojimas ~20 MB Python 3.8+

Šaltinis: sudarytas autoriaus

„Bitcoinlib“ yra aiškiai pranašesnis pasirinkimas, kuriant neprisijungusią (air-gapped) Bitcoinų piniginę, dėl savo techninio patikimumo, minimalistinio dizaino ir pritaikomumo ne-GUI aplinkoms. Jo suderinamumas su komandine eilute (CLI), pvz., „Raspberry Pi Legacy Lite“ sistemoje, užtikrina efektyvų veikimą ribotų išteklių sistemose. Integruota QR kodų funkcionalumo palaikymo galimybė leidžia užtikrinti saugų duomenų perdavimą neprisijungusio darbo srauto metu. „Bitcoinlib“ siūlo išsamią piniginės valdymo, neapdorotų sandorių kūrimo ir kriptografinio pasirašymo palaikymo sistemą, kuri suteikia patikimą pagrindą saugioms ir izoliuotoms Bitcoin operacijoms. Be to, modulinis ir lankstus API dizainas leidžia kūrėjams pritaikyti darbo srautus įvairioms neprisijungusio veikimo situacijoms. Lyginant su alternatyvomis, tokiomis kaip „electrum“ ar „btcpy“, „bitcoinlib“ išsiskiria kaip lengvas, funkcionalus ir gerai subalansuotas sprendimas, todėl jis laikomas optimaliausiu pasirinkimu, kuriant saugias Bitcoinų pinigines neprisijungusioje aplinkoje.

Python programavimo kalba ir jos biblioteka „bitcoinlib“ pasirodė kaip technologiškai pažangūs sprendimai, tinkami neprisijungus veikiančiai Bitcoin piniginei kurti. Python išsiskiria savo universalumu, leidžiančiu valdyti tiek aukšto, tiek žemo lygio operacijas, o jo modulinė architektūra užtikrina sklandžią sąveiką tarp aparatūros ir kriptografinių funkcijų. Naudojant tokias bibliotekas kaip „RPi.GPIO“, „qrcode“, ir „pyzbar“, Python užtikrina stabilų duomenų perdavimą, raktų valdymą bei skaitmeninių parašų kūrimą laikantis Bitcoin protokolų standartų. Šios funkcijos leidžia pasiekti aukštą sistemos efektyvumą net ribotų resursų įrenginiuose, pvz., Raspberry Pi Zero V1.3.

„Bitcoinlib“, lyginant su „electrum“ ir „btcpy“, parodė didžiausią suderinamumą su projekto reikalavimais. Jo pranašumai apima sudėtingas, bet intuityvias kriptografines operacijas, QR kodų generavimo palaikymą bei mažą priklausomybių lygį. Palyginus su „electrum“, kuris reikalauja serverių integracijos, „bitcoinlib“ yra lengvesnis ir paprasčiau pritaikomas neprijungtoms darbo eigoms. „Btcpy“, nors ir minimalistinis, trūksta piniginių valdymo funkcijų ir patogumo. Todėl

„bitcoinlib“ buvo pripažinta optimaliausia biblioteka, leidžiančia užtikrinti saugų, funkcionalų ir efektyvų Bitcoin piniginės prototipo įgyvendinimą.

Apibendrinant galima teigti, kad Python programavimo kalba ir Bitcoinlib biblioteka užtikrina tvirtą techninį pagrindą kuriant neprisijungusias Bitcoin pinigines, kurios atitinka saugumo, funkcionalumo ir efektyvumo standartus. Šie pasirinkimai pabrėžia jų svarbą kriptografinių sprendimų plėtrai ribotų resursų aplinkose.

2.5. Prototipo lyginamoji analizė su rinkoje egzistuojančiais sprendimais

Siekiant išsamiau įvertinti siūloma prototipo teikiamą pridėtinę vertę, atlikta jo palyginamoji analizė su šuo metu rinkoje populiariausiomis komercinėmis aparatūrinėmis kritpovaliutų piniginėmis, tokiomis kaip „Trezor Model T“, „Trezor Model One“, „Ledger Nano S“ ir „X“ bei „Ethical Titan“ taip pat savadarbe pingine, projektu „Krux“. Toks vertinimas leidžia išskirti esamus prototipo privalumus, bei įvertinti jo potencialą rinkoje.

Lentelė Nr. 7

Prototipo palyginimas su aparatūrinėmis piniginėmis

Ypatybė	**Prototipas**	**Trezor Model One/T**	**Ledger Nano S/X**	**Ethical Titan**	**Projektas Krux**
Kaina	60 €	80/220 €	80/150 €	100 €	60 €
Prieinamumas	Aukštas, surenkamas iš standartinių komponentų	Aukštas, galima įsigyti oficialiame tinklapyje, tačiau yra regioniniai apribojimai	Aukštas, galima įsigyti oficialiame tinklapyje.	Ribota platinimo geografija	Vidutinis, komponentai yra sunkiau gaunami arba ribojami dėl sankcijų
Programinės įrangos skaidrumas	Atviro kodo, naudojamas „Microphyton“	Iš dalies, kadangi Trezor remiasi trečiųjų šalių paslaugomis kurios nėra visiškai skaidrios	Uždarojo kodo, pilnai priklauso nuo gamintojo, nėra galimybės patikrinti	Atviro kodo, tačiau aparatinė įranga nėra visiškai dokumentuota	Atvirojo kodo, tačiau visiškai priklausoma nuo bendruomenės su ribotu dokumentavimu
Centralizacijos rizika	Žema, visiškai decentralizuota, nėra gamintojo priklausomybės	Vidutinė, „Firmware“ atvira, tačiau priklausoma nuo Trezor	Aukšta, Ledger infrastruktūra pilnai centralizuota, priklausomybė nuo gamintojo sprendimų	Vidutinė, aparatinės gamybos centralizacija ir gamintojo kontrolė	Vidutinė Priklauso projekto bendruomenės
Duomenų rinkimas	Nėra, visiškai atjungta nuo tinklo, belaidis sprendimas	Vidutinis, Trezor gali rinkti metaduomenis per Trezor „Suite“ integracijas	Aukštas, centralizuotai kontroliuoja gamintojas, 2020 m. duomenų nutekėjimas tą parodė	Nėra, visiškai atjungta nuo tinklo	Nėra, visiškai atjungta nuo tinklo, tačiau priklauso nuo surenkamų komponentų

Naudotojo kontrolė	Aukšta, leidžia pilnai kontroliuoti sėklos generavimą	Vidutinė, sėklos generavimas priklauso nuo RNG mikrovaldiklio	Žema: RNG procesas pilnai valdomas uždaro gamintojo algoritmo	Vidutinė: Sėklos generavimas priklauso nuo uždaro Ethical proceso	Vidutinė, ribota sėklos sukūrimo kontrolė naudotojui
Apsauga nuo tiekimo grandinės atakos	Aukšta, surinktas iš komponentų, kurie yra universalūs ir nėra skirti tik kripto rinkai	Vidutinė, komponentai tiekimo metu gali būti pakeistos.	Žema, tiekimo grandinė ne karta buvo pažeista.	Vidutinė, centralizuotos detalės, tiekimo metu gali būti pakeistos ar užkrėstos	Vidutinė, reikalingi spec. trečiųjų šalių komponentai, kurie gali būti tiekimo metu pažeisti
Apsauga nuo socialinės inžinerijos atakos	Aukšta, fizinė sąsaja ir visiška izoliacija nuo tinklo sumažina atakų pavojų.	Vidutinė, socialinės inžinerijos atakos galimos per trečiųjų šalių integracijas ir metaduomenis	Žema, centralizuota gamintojo infrastruktūra sukuria papildomų vektorių atakoms.	Aukšta, tinklo izoliacija ir fizinis kontaktas būtinas operacijoms atlikti.	Aukšta, fizinė izoliacija nuo tinklo ir aparatinės įrangos konfigūracijos užtikrina saugumą.

Šaltinis: sudarytas autoriaus

Lentelėje Nr. 7 pateikta lyginamoji penkių kriptovaliutų piniginių prototipų analizė, daugiausiai dėmesio skiriant techninei informacijai. Piniginių kaina svyruoja nuo 60 iki 220 eurų, Krux ir belaidės nuo tinklo aparatinės bitcoinų piniginės prototipas yra pačios prieinamiausios. Daugumos piniginių prieinamumas yra didelis. „Ethical Titan“ susiduria su geografiniais ribojimais, yra labiau prieinamas Azijos ir Šiaurės Amerikos rinkoms, o projektas „Krux“ priklauso nuo sunkiau gaunamų komponentų, su kuo teko susidurti ir pačiam šio darbo autoriui, kadangi užsakytas iš Kinijos mikrokompiuteris „M5StickV“, šio projekto aparatūrinė dalis, nebuvo gautas ir užsakymą teko atšaukti. Programinės įrangos skaidrumas taip pat skiriasi: „Ledger“ ir „Trezor“ nėra pilnai atvirojo kodo, be to, „Ledger“ centralizacija yra pati didžiausia.

Duomenų rinkimas siūlomame prototipe, „Krux“ ir „Ethical Titan“, nerenka visiškai jokių vartotojų duomenų, skirtingai nei „Trezor“ ar „Ledger“. Naudotojo kontrolė sėklų generavimui yra didžiausia belaidės nuo tinklo aparatinės bitcoinų piniginės prototipe, o Ledger ir Ethical Titan riboja kontrolę dėl uždarų sistemų. Kuriamas prototipas pasižymi skaidrumu, decentralizavimu ir vartotojo visišku valdymu, todėl yra saugus ir į vartotoją orientuotas sprendimas.

Prototipo palyginimas su populiariausiomis kriptovaliutų piniginėmis atskleidžia jo pranašumus, tokius kaip skaidrumas, decentralizacija ir aukštas naudotojo kontrolės lygis. Skirtingai nei komerciniai sprendimai, prototipas visiškai yra atvirojo kodo, nerenka vartotojų duomenų, nėra priklausoma nuo trečiųjų šalių ir užtikrina privatumą dėl neprisijungimo prie tinklo. Todėl šis prototipas gali būti laikomas saugiu ir į vartotoją orientuotu sprendimu, pranokstančiu daugelį esamų rinkos alternatyvų.

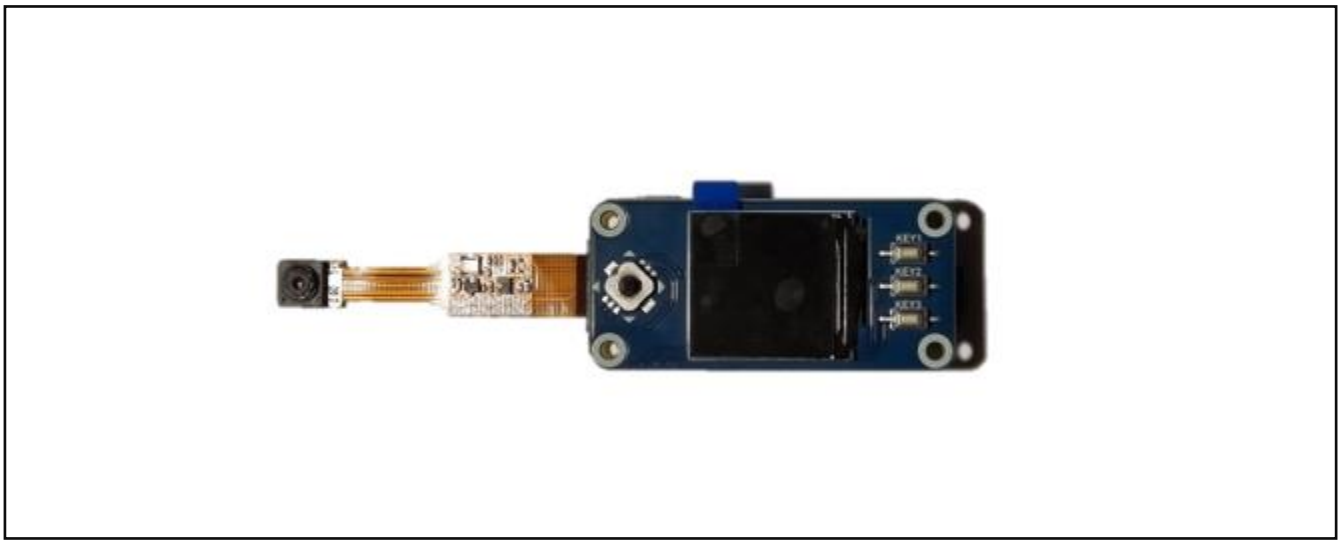
3. BELAIDĖS NUO TINKLO ATJUNGTOS APARATINĖS BITCOIN PINIGINĖS PROTOTIPO EKSPREIMENTAS

Šiame skyriuje analizuojamas siūlomas sprendimas, orientuotas į belaidės nuo tinklo atjungtos Bitcoinų piniginės prototipo kūrimą. Aprašoma pagrindinių prototipui reikalingų įrankių diegimo ir sujungimo procesai. Atliekamas sukurto prototipo testavimas siekiant patikrinti, ar pasiūlytas prototipas veikia ir ar atlieka visas pagrindines funkcijas.

.

3.1. Prototipo surinkimas, reikalingų įrankių diegimas ir bibliotekų testavimas

Kaip aptarta prieš tai iš visų aparatūrinių komponentų buvo surinktas belaidės nuo tinklo atjungtos Bitcoinų piniginės prototipas (žr. 5 pav.)



Šaltinis: sudarytas autoriaus.

5 pav. Sujungtas prototipas

Sujungus komponentus į atminties kortelę, buvo įdiegta „Raspberry Pi Legacy Lite“ operacinė sistema, kuri yra „Linux“ pagrindu ir neturi vartotojo grafinės sąsajos, nereikalingos ribotų išteklių įrenginiuose. Pirminis tikslas buvo įdiegti naujesnę „Rasberry Pi OS Lite“ operacinę sistemą, tačiau, ją sudiegus ir pradėjus įrašyti antroje darbo dalyje aprašomas bibliotekas (žr. lenteles Nr. 5 ir Nr. 6), buvo susidurta su problemomis, kadangi niekaip nepavyko prisijungti ir ištestuoti, ar veikia LCD ekranas. Problemai spręsti buvo pritaikytos įvairios modifikacijos prototipo kode, įvairios Python bibliotekos, tokios kaip „lcd“, „Pillow“, tačiau jos taip pat nedavė rezultatų. Dėl užsitęsusio testavimo buvo

susisiekta su ekrano ir mygtukų modelio gamintoju „Waveshare“ ir pateikta užklausa dėl nesėkmingo ekrano testavimo. Modulio gamintojas nurodė, kad ekranui valdyti naudojama biblioteka „ST7789“ neveikia su naujausia operacine sistema ir šiuo momentu jie neturi pasiūlymo, kaip tai išspręsti. Todėl buvo nuspręsta įdiegti gamintojo rekomenduojamą „Raspberry Pi Legacy Lite“ operacinę sistemą, kuri leido įjungti ir ištestuoti, ar veikia LCD ekranas ir mygtukų modulis.

Paskui, naudojantis Python bibliotekomis „picamera“ ir „PIL“, ištestuota prijungta 5 MP kamera. Buvo ištestuotas užfiksuotų elementų atvaizdavimas LCD ekrane bei ekrane per HDMI jungtį, taip pat fotofiksacijų saugojimas ir daugkartinis atvaizdavimas sistemoje.

Vėliau buvo sudiegtos visos antrojoje dalyje aprašomos bibliotekos (žr. lenteles Nr. 5 ir Nr. 6) ir parašytas pagrindinis prototipo kodas (žr. priedą Nr. 5), atliksiantis visas funkcijas. Kadangi kuriamas prototipas turi būti saugus ir nepriklausomas nuo trečiųjų šalių, buvo ištestuotos ir visos įdiegtos bibliotekos ir elementai tikslu užtikrinti, kad nė viena iš jų nekaupia jautrios informacijos ir neturi jokių pašalinių prisijungimų. Kadangi prototipas sukurtas ant mikrokompiuterio „Raspberry Pi Zero V1.3“, kuris neturi nei tinklo, nei Bluetooth modulio, viskas buvo testuojama atjungtoje prototipo aplinkoje. Testavimui pasitelkti buvo panaudotos ir išrašytos papildomos bibliotekos „strace“ ir „lsof“.

8 lentelė

Testavimo bibliotekos „strace“ ir „lsof“

Pavadinimas	Techninės funkcijos
strace	- Stebi sistemos iškvietimus, tokius kaip „open“, „write“, „connect“ ir „read“. - Stebi su tinklu susijusius iškvietimus tokius kaip „conncet“, „sendto“, „recvfrom“, kad aptiktų neautorizuotą tinklo veiklą. - Seka visus procesus ir potvarkius, pateikdamas išsamų visų inicijuotų programų sistemos veiksmų atvaizdą.
lsof	- Parodo visus atidarytus failus, bibliotekas, lizdus ir jungtis, kuriuos naudoja sistema ar kodas; - Stebi visą vykdoma veiklą ir procesų atidaromus failus, užtikrindamas, kad nebūtų neteisėtos prieigos. Veiksminga stebint tinklo lizdus ir procesų naudojamus išteklius.

Šaltinis: sudarytas autoriaus.

Įdiegus papildomas programinės įrangos priežiūros bibliotekas, buvo atlikta kuriamos piniginės prototipo kodo analizė, siekiant įvertinti jo veikimo saugumą ir patikrinti, ar nėra vykdomi nereikalingi arba potencialiai kenksmingi veiksmai. Taip pat užtikrinti, kad sukurtas programinis kodas nefiksuoja ir nebando perduoti jautrios informacijos, kaip sėklos frazė ar privatūs raktai. Sistemos iškvietimų analizė, paleidus programos kodą, atlikta naudojantis „strance“ įrankį, apėmė pagrindines failų operacijas, tokias kaip „open“, „read“, „write“ ir „close“. Rezultatai parodė, kad piniginės

programinis kodas naudoja tik iš anksto nustatytus išteklius, failą „pin_hash.txt.“ ir piniginės duomenų bazė bei biblioteka „bitcoinlib“. Papildomai buvo patikrint ar nėra vykdomi ir tinklo iškvietimai „socket“, „connect“ ir „sendto“. Atlikus analizė, buvo patvirtina, kad nėra vykdomi tinklo iškvietimai, kad nėra inicijuojamos neleistinos išorinės komunikacijos, kurios galėtų kelti riziką saugumui. Naudojant įrankį „lsof“ identifikuoti visi failai ir lizdai yra naudojami tinkamai. Analizė neparodė nei vienos netikėtos tinklo veiklos, nei duomenų nutekėjimo požymių, kas užtikrina, kad programa veikia saugiai.

Apibendrinant, buvo integruoti visi būtini komponentai ir įdiegtos visos reikiamos bibliotekos į sukonstruotą Bitcoin piniginės prototipą, įskaitant ir operacinę sistemą. Atlikta išsami sukurto programinio kodo analizė parodė, kad naudojamos Python bibliotekos nekaupia ir neperduoda jokios jautrios informacijos.

3.2. Prototipo valdymas ir funkcijų paskirtis

Kuriant pagrindinį piniginės belaidės nuo tinklo atjungtos Bitcoin piniginės kodą, buvo panaudotos visos 2 darbo dalyje aptartos bibliotekos, jos sudėtos į funkcijas. Šiame skyriuje aprašomos pagrindinės kodo (žr. 5 priedą) funkcijos ir veikimo principai, aptarta kokias užduotis jos atlieka, ir kaip yra valdomas piniginės prototipas.

9 lentelė

Sukurto prototipo kodo funkcijų paskirtis

Funkcijos pavadinimas kode	**Techninės funkcijos**
def hash_pin	- Užtikrina, kad PIN kodas būtų užšifruotas ir saugiai saugomas. - Naudoja „haslib.sha256“ duomenų šifravimui, generuoja 64 simbolių šešioliktainę maišą PIN kodui saugoti.
def sha256_hash	- Užtikrina, kad PSBT transakcijos būtų šifruoti ir apsaugoti nuo klastojimo. - Naudoja „haslib.sha256“ šifravimo algoritmą, kuris informacija užšifruoja šešioliktainio formatu.
def pin_exists def save_pin def load_pin	- Visos funkcijos susijusios su PIN įvedimu ar užkrovimu. - pin_exists patikrina ar PIN failas „pin_hash.txt.“ egzistuoja, ir nustato ar reikia kurti naują kodą ar naudoti esamą. - save_pin saugo užšifruotą vartotojo naujai įvesta PIN kodą „pin_hash.txt.“ dokumente. - def load_pin nuskaito PIN kodą iš „pin_hash.txt.“ dokumento.
def display_text	- Sukuria ir atvaizduoja LCD ekranui perduodama informacija (tekstą, QR kodus). - Naudoja „PIL“, „ST7789“ bibliotekas. - Nauda „PIL.Imagedraw“ įrankį, atvaizduoti tekstą RGB ekrane, kurio dydis 240x240 pikselių. - Leidžia vartotojui aiškiai matyti PIN įvedimo būsena, meniu ar kitą perduodama informacija.
def input_pin def request_pin	- input_pin PIN kodo atvaizdavimas ir įvedimas naudojant GPIO mygtukus. - request_pin tvarko PIN nuskaitymą ir autentifikaciją.

def wallet_exists	- Naudojantis “os.path.expanduser“ Bitcoinlib bibliotekos duomenų bazėje tikrina ar yra egzistuojanti piniginė ar nėra. - Naudoja „os“ biblioteką, kuri ieško duomenų „~/.bitcoinlib/wallets/” direktorijoje.
def create_or_load_wallet	- Jei yra egzistuojanti jau sukurta pinigine, ją užkrauna ir peršoka į meniu langą. - Jei piniginės nėra, sukuria naują, sukūrus atvaizduoja piniginės BIP-39 sėklą LCD ekrane, naudojantis „mnemonic“ biblioteka, padalindamas ją į 6 dalis. - Sukurta piniginė „SegWit“ tipo, užtikrina piniginės suderinamumą su Bitcoin tinklo standartais
def show_wallet_address	- Atvaizduoja informacija QR kodu, naudojantis „qrcode.QRCode“ biblioteka. Konfigūruoja QR kodo dydi ir parametrus, kad būtų suderinamas su LCD ekranu - Parodo piniginės gavimo adresą kaip QR kodą. Vaizdas konvertuojamas į RGB formatą, kad būtų suderinamas su „ST7789“ modifikuota biblioteka.
def sign_psbt	- Skanuoja QR kodą, iššifruoja gauta informacija, pasirašo nuskanuota PSBT transakcija ir atvaizduoja ją LCD ekrane pasirašytą, kaip QR kodą. - Naudoja „picamera“ biblioteka užfiksuoti QR kodo vaizdą. Nuskaitomas 640X480 pikselių rezoliucijos formatas. - Naudoja „pyzbar“, kad dekoduotų QR kodo vaizdą ir išgautų PSBT duomenis eilutės formatu. - Įrankiu „wallet.transaction_sign“ pasirašo transakcija privačiais raktais ir ją užšifruoja.
def main_menu	- Atvaizduoja pagrindinį piniginės menu, kur galima pasirinkti kokią operacija norima atlikti - Suteikia grafinę vartotojo sąsają (GUI) piniginės operacijoms valdyti, naudojant mygtukus. - Atpažįsta ką įveda vartotojas, stebi mygtukų įvesti ir iškviečia atitinkamas funkcijas.
def main	- Tarnauja kaip kodo įėjimo taškas, koordinuojantis autentifikaciją, piniginės valdymą ir vartotojo sąveiką.

Šaltinis: sudarytas autoriaus.

Lentelėje Nr. 9 aptartos visos pagrindiniame kode naudojamos funkcijos. Iš viso naudojamos 14 funkcijų valdyti pinginės prototipą. Funkcijos „display_text“ ir „show_wallet_address“ naudoja „PIL“ ir „ST7789“ bibliotekas tekstui ir QR kodams atvaizduoti LCD ekrane. Kriptografinėse operacijose, tokiose kaip operacijų kūrimas ar pasirašymas, deterministiniam piniginės valdymui laikantis BIP standartų naudojamos „bitcoinlib“, „hashlib“ ir „mnemonic“ bibliotekos. Funkcija „request_pin“ patvirtina 4 skaitmenų PIN kodą, naudodama GPIO mygtukus per „RPi.GPIO“ biblioteką. Piniginės valdymą atlieka „wallet_exists“ ir „create_or_load_wallet“ funkcijos, kurios naudoja „bitcoinlib“ ir „mnemonic“ bibliotekas BIP-39 mnemoninės frazės kūrimui ir atvaizdavimui. Transakcijų operacijos apdorojama „sing_psbt, kuri nuskaito ir iššifruoja PSBT, naudojant bibliotekas „picamera“ ir „pyzbar“, ir saugiai jas pasirašo. Funkcija „show_wallet_address“ tiesiog atvaizduoja piniginės adresą gauti lėšoms QR kodu. Prototipo kodo integracija su kriptografinėmis bibliotekomis, aparatinės įrangos valdikliais ir blokų grandinės standartais užtikrina saugią, nuo interneto atskirtą aplinką Bitcoin operacijų valdymui, siūlant vartotojui patogų, tačiau itin saugų sprendimą neprisijungusioms piniginėms.

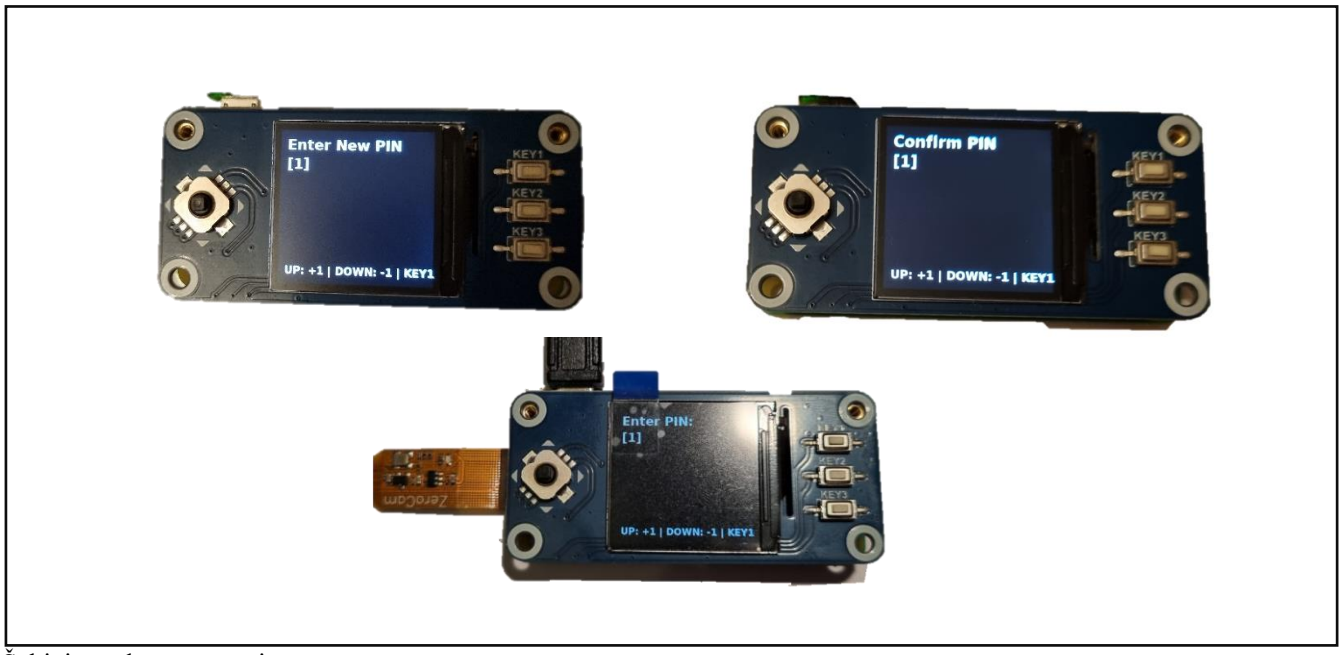
Belaidės nuo tinklo piniginės prototipas yra valdomas 3 mygtukų pagalba. Mygtukai aukštyn ir žemyn naudojami, naršymui PIN kodo įvedimui ir pagrindinėje meniu operacijos pasirinkimui.

Mygtukas „KEY1“ naudojamas kaip patvirtinimo mygtukas, įvairiose darbo eigos dalyse, leisti vartotojui patvirtinti veiksmus arba pereiti prie kito žingsnio.

Šiame skyriuje aptartos pagrindinės prototipo kodo operacijos, ir kokias funkcijas jos atlieka. Išanalizuotus pagrindinės funkcijos ir jų veikimo principai, kokios bibliotekos buvo panaudotos. Taip pat aptartas ir prototipo valdymas.

3.3. Piniginės veikimo analizė ir transakcijų atlikimas

Šiame skyriuje analizuojamas belaidės nuo tinklo atjungtos aparatinės Bitcoin piniginės veikimas ir transakcijų vykdymo procesas, Pateikiama, kaip piniginė sąveikauja su vartotoju, kaip apdorojamos operacijos. Taip pat aptariami techniniai iššūkiai ir problemos su kuriomis buvo susidurta įgyvendinant prototipo funkcionalumą. Dėmesys skiriamas pagrindinėms programinėmis ir aparatūrinėms kliūtims, kurios išryškėjo testuojant ir vystant piniginės sistemą.



Šaltinis: sudarytas autoriaus.

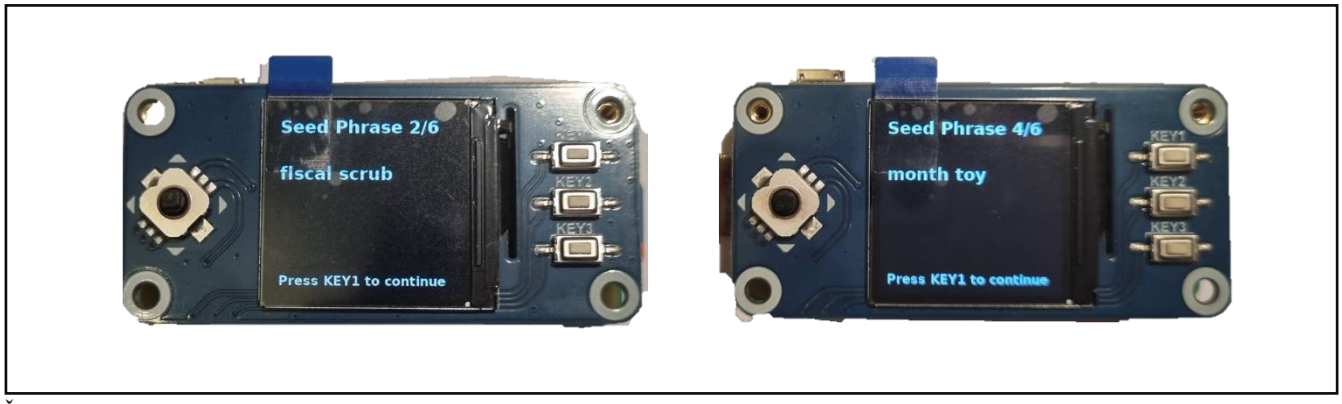
6 pav. PIN kodo įvedimas

Įjungus piniginės prototipą, pirmasis veiksmas yra PIN kodo sukūrimas. Kodas susideda iš 4 skaitmenų, jį suvedus reikia dar kartą patvirtinti. Antrą kartą įjungus programinis kodas automatiškai tikrina ar kodas egzistuoja, jei egzistuoja užkrauną jį. Sukurtas kodas yra saugomas atskirame faile, kuris naudojantis „hashlib“ biblioteka yra užšifruotas SHA-256 algoritmu. PIN kodo įvedimui naudojama valdymo svirtis „aukštyn“ ir „žemyn“, kai „aukštyn“ padidina skaičių,“ žemyn“ –

sumažina. Šis procesas yra atvaizduojamas meniu apačioje, o įvedimą patvirtina „KEY1“, kuris fiksuoja vartotojo pasirinkimą.

Teisingai įvedus PIN kodą, sistema automatiškai atlieka vieną iš dviejų veiksmų: užkrauna jau egzistuojančią piniginę (jeigu ji buvo sukurta anksčiau) arba sugeneruoti naują Jei kodas įvedamas neteisingai, vartotojui suteikiamos dar dvi galimybės atlikti korektišką įvedimą. Nesėkmingai įvedus PIN kodą, programa automatiškai užsidaro. Patvirtinimo ir atmetimo tekstą galima matyti priede Nr. X. Šis sprendimas užtikrina bazinį saugumo lygį.

Įvedus PIN kodą teisingai, sistema pereina prie kito veiksmų etapo, kuris susideda iš dviejų dalių. Pirmiausia piniginės kodas automatiškai tikrina, ar piniginė buvo sukurta. Jei piniginė egzistuoja, programa tiesiai keliauja į pagrindinį meniu lauką. Priešingu atveju, jei piniginės nėra sukurtos, sistema automatiškai generuoja naują piniginę ir ekrane atvaizduoja BIP39 mnemoninę frazę, sudarytą iš 12 žodžių. Dėl nedidelio LCD ekrano dydžio sistema automatiškai padalina frazę į šešias dalis, rodydama du žodžius vienu metu (žr. 7 pav.).



Šaltinis: sudarytas autoriaus.

7 pav. Mnemoninės frazės atvaizdavimas

Mnemoninė frazė ekrane rodoma tik vieną kartą, todėl vartotojui būtina užsirašyti ir išsisaugoti ją saugioje vietoje. Testuojant prototipą, buvo naudojamas pirminis „bitcoinlib“ bibliotekos įrankis „mnemonic“. Tačiau detalesnės analizės metu paaiškėjo, kad šio įrankio generuojama sėkla neatitinka BIP-39 standarto. Ji yra specifinė „bitcoinlib“ bibliotekai ir nepalaikoma kitose piniginėse. Šis trūkumas buvo išspręstas, priimant sprendimą pereiti prie naujos „mnemonic“ bibliotekos.

Nauja biblioteka leidžia generuoti sėklos frazę, kuri atitinka BIP-39 standartą. Tai užtikrina, kad sugeneruotą piniginę bus galima atkurti kitose platformose ar įrenginiuose, nepriklausomai nuo naudojamos piniginės tipo. Sugeneravus sėklos frazę, sistema toliau keliauja į pagrindinį menių langą.

Pagrindiniame meniu lange (žr. 8 pav.) vartotojui pateikiami du pagrindiniai pasirinkimai: atvaizduoti sugeneruotos piniginės QR kodą ekrane arba pasirašyti PSBT transakciją. Šis pasirinkimas užtikrina bazinį prototipo funkcionalumą, būtiną pagrindinėms operacijoms su pinigine atlikti.

.

Šaltinis: sudarytas autoriaus.

8 pav. Pagrindinis meniu langas

Testavimo metu buvo sugeneruota nauja piniginė kurios adresas yra bc1qe9u7mquvt8l072j5ztyuqcf739yejx6z7h07t5. Šis adresas nėra tiesiogiai atvaizduojamas ekrane, kaip tekstas, todėl jį galima pasiekti tik pasirinkimus meniu funkcija „Show Address“. Pasirinkus valdiklio aukštyn, sistema automatiškai sugeneruoja QR kodą ir jį atvaizduoja ekrane (žr. 9 pav.). Sugeneruotas kodas yra rodomas 10 sekundžių, po kurių sistema automatiškai grįžta į pagrindinį meniu langą. Grįžus į pagrindinį langą vartotojui vėl suteikiama galimybė pasirinkta vieną iš dviejų galimų operacijų.

Šaltinis: sudarytas autoriaus.

9 pav. Piniginės adresas QR kodu

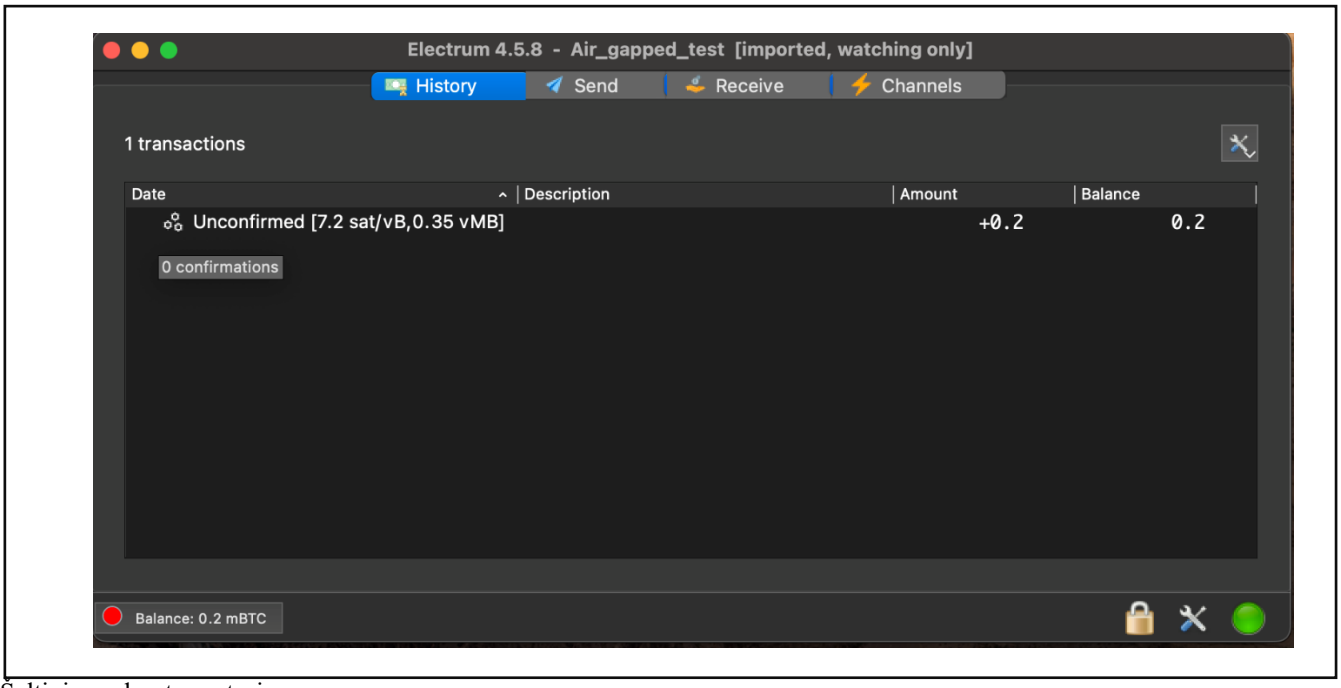
Toliau testuojant belaidės atjungtos nuo tinklo aparatūrinės piniginės prototipą, buvo atlikta transakcija į piniginę, siekiant jos funkcionalumą patikrinti realiomis sąlygomis. Testavimo metu karštoje piniginėje buvo nuskenuotas sukurtos piniginės adresas ir perversta 0.2 mBTC (žr. priedą Nr.

1). Testavimas buvo vykdomas Bitcoin tinkle, kadangi tęstinio tinklo veikimas tuo metu buvo nestabilus ir ribojo galimybes pademonstruoti sklandų transakcijų atlikimą.

Sugeneruotas transakcijos ID 76a9655bd72f9e8f779c6a8a74d8399d675dbcc1bcc76b6ae727ede7e406cffe leido tinkle stebėti transakcijos eigą (žr. priedą Nr. 1) . Naudojant „Elektrum“ darbalaukio piniginę, buvo sukurta stebėjimo režimo (angl. watch-only) piniginė šio prototipo testavimui. Šio tipo piniginė leidžia stebėti viešuosius piniginės adresus, gauti pilną piniginės transakcijų istoriją ir stebėti gaunamus mokėjimus. Ji neleidžia atlikti tokių aktyvių veiksmų kaip lėšų pervedimas ir adresų generavimas. Sukurtą stebėjimo piniginę galima matyti 10 paveiksle.

Stebėjimo piniginė ypač naudinga prototipams, veikiantiems visiškai autonominiu režimu, kokia yra ši kuriama piniginė, nes suteikia saugiai stebėti Bitcoin balansą. Ši piniginė taip pat palaiko PSBT transakcijų generavimo funkciją, kuris taip pat naudojamas šiame prototipe. Kaip matyti iš 10 paveikslo, atliktą transakciją jau galima stebėti piniginėje, tačiau ji vis dar nėra patvirtinta.

Praėjus tam tikram laikui, Bitcoin tinklo platformoje „Blockstream“ buvo užfiksuota, kad transakcija yra patvirtinta ir lėšos sėkmingai pasiekė prototipo sugeneruotą adresą. Informacija buvo patvirtina tiek stebėjimo režimo piniginėje, tiek blokų grandinės duomenyse (žr Priedą. Nr. 1, 2). Šis rezultatas patvirtino, kad prototipas tinkamai atlieka pagrindines savo funkcijas: jis generuoja tinkamus Bitcoin adresus ir užtikrina galimybę pervesti lėšas į sugeneruotą piniginę.



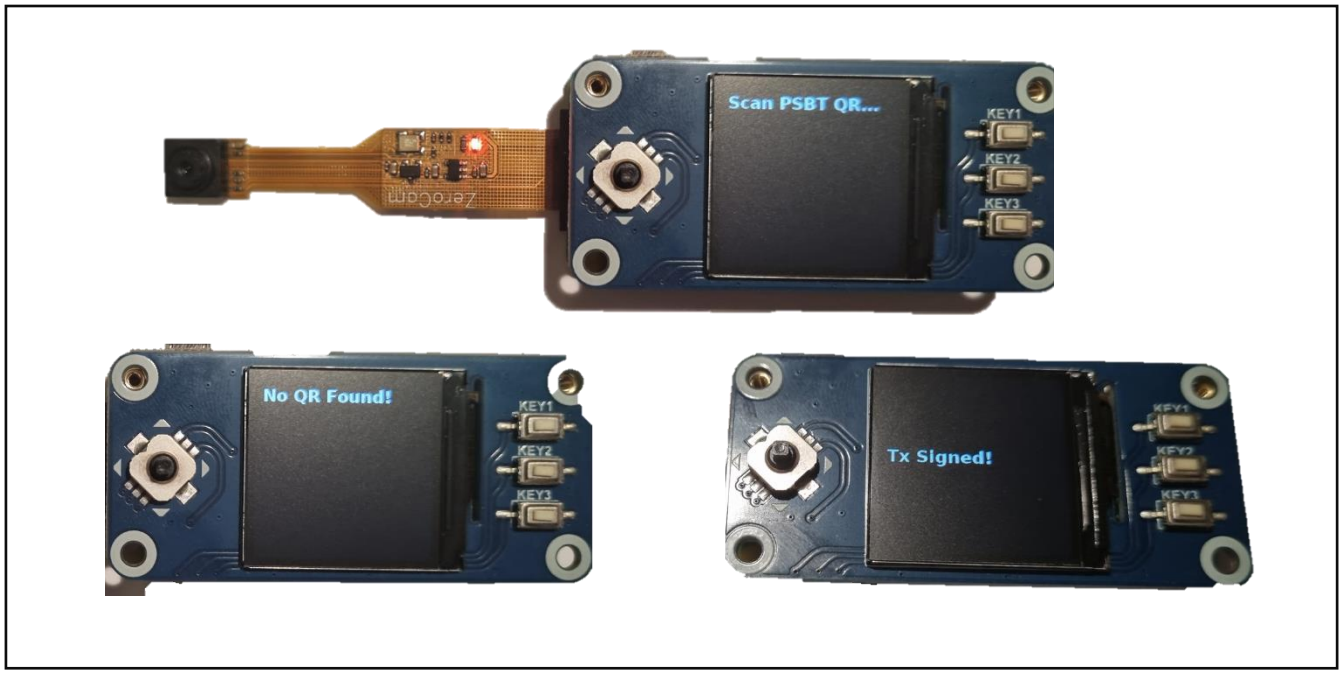
Šaltinis: sudarytas autoriaus.

10 pav. Sugeneruota stebėjimo piniginė

Sėkmingai pervedus lėšas į prototipą, buvo pereita prie tolesnio funkcionalumo testavimo, transakcijų PSBT pasirašymo funkcijos išbandyme. Šis procesas yra vienas esminių belaidės neprijungtos prie tinklo aparatinės piniginės funkcionalumo elementas. Testavimo metu buvo siekiama patikrinti, ar prototipas sėkmingai pasirašo transakcijas.

Pasirinkus valdikiu meniu funkciją „Sign PSBT“, sistema pereina į naują režimą, kuriame inicijuojamas QR kodo nuskaitymo procesas. Atsidariusiame lange pateikiama informacija, kad aktyvuojama kamera, skirta QR nuskaitymui. Tai patvirtina ir raudonos spalvos lemputė, kuri signalizuoja, kad kamera veikia ir fiksuoja QR kodą (žr. 11 pav.).

Jei kodo nuskaitymas nepavyksta, LCD ekrane pasirodo pranešimas, kad kodas nebuvo rastas. Tokiu atveju grįžtama į pagrindinį meniu, kuriame vėl galima inicijuoti transakcijos pasirašymą. Jei sistema sėkmingai atpažįsta ir dekoduoja perduodamą informaciją, prototipas naudoja piniginėje saugomą privatų raktą transakcijos pasirašymui. Procesas atliekamas automatiškai. Pasirašius transakciją, LCD ekrane pateikiama informacija, kad transakcija pasirašyta sėkmingai. Po to automatiškai sugeneruojamas QR kodas, kuriame užkoduota pasirašyta transakcija. Šį QR kodą galima nuskaityti naudojant prie tinklo prijungtą piniginę ir transliuoti transakciją į Bitcoin tinklą, taip užbaigiant visą procesą.



Šaltinis: sudarytas autoriaus.

11 pav. Transakcijos pasirašymas

Patvirtinus lėšų gavimą Bitcoin blokų grandinėje, pradėtas testuoti transakcijų funkcionalumas. Pasirašymui buvo panaudota prieš tai sukurtoje „Elektrum“ stebėjimo režimo

piniginės funkcija PSBT. Šis sprendimas pasirinktas atsižvelgiant į tai, kad surinktame prototipe įdiegtos tik bazinės funkcijos, kurios neleidžia tiesiogiai įvesti piniginės adresų ar siunčiamos valiutos kiekio, ir dėl to, kad piniginė visiškai veikia režime be tinklo.

PSBT pasirodė tinkamas sprendimas, nes piniginė suteikia galimybę atlikti išsamią transakcijos konfigūraciją. Joje galima nurodyti adresatą, pervedamą valiutos kiekį, nustatyti transakcijos mokestį, be vėliau transakcijos duomenis atvaizduoti kaip QR kodą. Sukurtas prototipas buvo pritaikytas dirbti su PSBT formatu: programinis kodas iššifruoja perduodamus transakcijos duomenis, pateikus juos QR kodo formatu, ir automatiškai pasirašo juo naudodamas privačius raktus, saugomus aparatinėje piniginėje.

Sukurtoje stebėjimo režimo piniginėje buvo sukurta PSBT transakcija ir ji atvaizduota kaip QR kodas (žr. priedą Nr. 2). Padidinus QR kodą, ir atvaizdavus jį ryškesniame ekrane, pavyko nuskaityti transakcijos QR kodą. Nuskaičius kodą, atsirado informacinė žinutė, kad transakcija yra pasirašyta, ir ji buvo atvaizduota (žr. 12 pav.). Vėliau, naudojantis prie tinklo prijungta pinigine, šis kodas buvo ištransliuotas į blokų grandinę. Praėjus tam tikram laikui, transakcija buvo patvirtinta ir ją galima buvo matyti tiek blokų grandinėje, tiek stenėjimo režimo piniginėje (žr. priedą Nr. 3, 4).

.

Šaltinis: sudarytas autoriaus.

12 pav. Pasirašytos transakcijos atvaizdavimas

Lėšų pervedimas buvo sėkmingai įvykdytas, transakcijos ID 913d616fc518e46e7e34dd1785712e1c7abb74e2da91299557e5dad25caec762. Identifikatorius atspindi operacijos registracija blokų grandinėje.

Apibendrinant galima reziumuoti, kad šiame skyriuje buvo ištestuotos bazinės belaidės nuo tinklo atjungtos piniginės funkcijos, įskaitant PIN kodo įvedimą, mnemoninės frazės generavimą, transakcijų pasirašymą ir QR kodų naudojimą. Analizuojami techniniai iššūkiai, kuriuos pavyko išspręsti testavimo metu.

3.4. Prototipo įvertinimas ir tobulinimo galimybių analizė

Šiame skyriuje įvertinamas sukurtas belaidės atjungtos nuo tinklo Bitcoin piniginės prototipas. Aptariamos technologinės kliūtys ir iššūkiai, su kuriais buvo susidurta kuriant, testuojant prototipo sistemą.

Sukurtas prototipas užtikrina visas bazines Bitcoin piniginės funkcijas, veikiant visiškai autonominiu režimu, atjungus nuo tinklo, o informaciją perduodant naudojantis QR kodais. Prototipas užtikrina patikimą piniginės privačių raktų saugojimą, papildomai juos šifruojant naudojantis „Bitcoinlib“ biblioteka. Testavimu buvo patikrintas PIN kodo mechanizmas, kuris užtikrina paprastą bazinį piniginės saugumą. Taip pat buvo sėkmingai ištestuotas naujos piniginės, kuri leidžia generuoti naujus privačius ir viešuosius raktus, kūrimas. Prototipas sėkmingai atvaizdavo BIP-39 standarto, 12 žodžių mnemonės frazę, kuri naudojama piniginės atkūrimui. Atlikus prototipo testavimą, nustatyta, kad lėšų pervedimas į piniginę yra intuityvus ir paprastas, LCD ekranas aiškiai atvaizduoja piniginės adresą QR kodu, kurį galima nuskaityti net iš fotografijos. Testavimo metu paaiškėjo, kad kamerai reikalingas ryškus ekranas ir apšvietimas tam, kad tinkamai atpažintų QR kodą, kas skatina poreikį tolimesniam techninės įrangos tobulinimui.

Piniginės prototipas buvo sukurtas naudojantis standartinius komponentus, kurie nėra specialiai pritaikyti kriptovaliutų saugojimui ar Fintech sprendimams. Pagrindiniai techniniai elementai apima „Raspberry Pi Zero V 1.3“ mikrokompiuterį, 240x240 LCD ekraną su integruotais mygtukais bei 5 MP kamera. Šie komponentai yra universalaus pobūdžio ir dažniausiai naudojami įvairiuose elektronikos sistemų projektuose tokiuose kaip: matavimo įrenginiai, vaizdo stebėjimui, ar daiktų interneto sprendimams. Naudoti komponentai yra prieinami įvairiuose elektronikos prekių parduotuvėse, todėl šios piniginės surinkimas yra gana paprastas ir prieinamas.

Modulinė architektūra sudaryta iš visiškai nepriklausomų ir tarpusavyje nesusietų dalių, o tai žymiai sumažina tiekimo grandinės atakų riziką. Šis pažeidžiamumas, kaip buvo aprašyta pirmoje darbo dalyje, yra dažnas tarp komercinių aparatinių piniginių gamintojų, tokių kaip „Legder“ ir „Trezor“, kur gamybos ar platinimo metu, gali būti įdiegiami kenkėjiški įskiepiai ar programinis kodas. Naudojant atskirus komponentus, įsigytus iš skirtingų tiekėjų, dar labiau sumažinama rizika ir tikimybė, kad gali būti įtarta apie numatomą projekto paskirtį.

Kadangi sukurta piniginė yra „non-custodial“ tipo, ji veikia visiškai autonomiškai ir nepriklausomai nuo trečiųjų šalių tiekėjų. Privatūs raktai yra saugomi atskirai nuo tinklo. Tai leidžia išvengti nepageidaujamų atnaujinimų ir pažeidimų, izoliacija užtikrina, kad visi programinės įrangos pakeitimai ir patobulinimai būtų griežtai valdomi tik vartotojo. Architektūrinių požiūriu sistema

teoriškai pasižymi atsparumu šoninio kanalo atakoms, nes įrenginio spinduliuotės, elektromagnetinių bangų skleidimas yra minimalios. Tačiau šis teiginys reikalauja eksperimentinio patikrinimo, naudojant elektromagnetinio nutekėjimo analizę osciloskopu. Unikali prototipo architektūra, kartu su belaidžiu nuo tinklo atjungtu sprendimu ir pilnai vartotojo kontroliuojama sistema, užtikrina tvirtą sprendimą kriptografinio turto apsaugai.

Atlikus eksperimentą taip pat pastebėti ir tobulinti dalykai, kurie galėtų pagerinti prototipo funkcionalumą ir naudojimo patirtį. Pirmiausia vertėtų pasirinkti ekraną, kuris galėtu palaikyti naujesnes operacines sistemas. Pavyzdžiui, gamintojo „Waveshare“ ekranas „3.5 HDMI IPS LCD Resistive Touchscreen“, kurie prie „Raspberry Pi“ mikrokompiuterio jungiasi per GPIO ir HDMI jungtis, galėtų būti tinkamas sprendimas. Šis ekranas galėtų veikti naudojantis naujausias operacines sistemas. Tai leistų įdiegti papildomas bibliotekas „ecsda“, „pycryptodome“ bei „secp256k“, kurių integracija suteiktų galimybę įgyvendinti BIP-32 tyliuosius mokėjimus (angl. silent payments), kurie užtikrintų dar didesnį privatumo lygį. Naudojant šią technologiją, mokėjimai taptų neatskleidžiami blokų grandinės analizės įrankiams, o operacijų susiejimas su konkrečiais piniginės adresais būtų apsunkintas.

Eksperimentas ir testavimas parodė, kad jei butų naudojama geresnio modelio kamera QR kodų skenavimas galėtų vykti efektyviau, ypač sudėtinguose apšvietimo sąlygose. Pavyzdžiui, „Raspberry Pi Camera Module 3“, turinti 12 megapikselių jutiklį ir aukšto dinaminio diapazono (HDR) technologija, galėtų užtriktini detalesnį ir kokybiškesnį vaizdo atvaizdavimą. Toks atnaujinimas palengvintų QR kodų nuskaitymą, padidinamas greitį esant sudėtingoms aplinkybėms.

Piniginės prototipo konstrukcijai vertėtų sukurti specialių dėklą, naudojantis 3D spausdintuvu. Dėklas užtikrintų fizinę komponentų apsaugą ir patogesnį valdymą. Įdiegus specialias tvirtinimo vietas kameros modulis būtų stabiliai pritvirtintas, apsaugant jį nuo pažeidimų ir eliminuojant judėjimo trikdžius fiksuojant QR kodą.

IŠVADOS

1. Atlikta kriptovaliutų piniginių analizė parodė, kad šis įrankis yra esminis skaitmeninio turto ekosistemos dalis. Piniginės yra klasifikuojamos į dvi pagrindines kategorijas: programinės ir aparatines. Aparatinės pinginių, tokių kaip USB, Bluetooth ir NFC įrenginiai, privatūs raktai yra saugomi izoliuotai įrenginyje. Šios piniginės naudoja saugius elementus (SE) bei pažangius kriptografinius algoritmus, tokius kaip SHA-256 ir ECDSA, siekiant maksimaliai apsaugoti vartotojų turtą.
2. Darbe išskiriami pagrindiniai aparatinių kriptovaliutų piniginių saugumo trūkumai ir susijusios grėsmės. Komercinės piniginės, tokios kaip „Ledger“ ar „Trezor“, pažeidžiamos dėl viešai prieinamos informacijos apie jų įsilaužimo metodus. Tiekimo grandinės atakos sukelia pavojų gamybos ar logistikos metu, nes įrenginiai gali būti užkrėsti kenkėjiška programinė ar aparatūrine įranga. Informacijos rinkimas apie piniginių vartotojus gali būti panaudotas socialinės inžinerijos atakoms vykdyti. Savadarbės piniginės dažnai turi nepakankamus saugumo mechanizmus, kurie didina programinių atakų riziką.
3. Pasiūlytas sprendimas – belaidė nuo tinklo atjungta Bitcoinų aparatinė piniginė – paremta „Raspberry Pi Zero V 1.3“ ir standartiniais komponentais, kurie nėra specialiai pritaikyti kriptovaliutų saugojimui ar Fintech sprendimams. Šis mikrokompiuteris užtikrina saugų privačių raktų valdymą ir šifravimą naudojant SHA-256 algoritmą, kurie įgyvendinami per Python bibliotekas, tokias kaip „bitcoinlib“ ir „hashlib“. QR kodų technologija, integruota naudojant „qrcode“ ir „pyzbar“ bibliotekas, leidžia duomenis perduoti neprisijungus prie tinklo.
4. Sukurto prototipo komponentai sujungti į vieningą sistemą, įdiegtos bibliotekos „bitcoinlib“, „hashlib“, „qrcode“, „pyzbar“, „ST7789“, „PIL“, „picamera“, „mnemonic“ ir RPi.GPIO bibliotekos. Dėl papildomo saugumo, sukurtas prototipo programinis kodas buvo testuotas „strace“ ir „lsof“ įrankiais, kurie patvirtino, kad kodas nekaupia ir neperduoda jokios jautrios informacijos.
5. Sukurta Bitcoinų piniginė užtikrina autonominį veikimą nuo tinklo, naudojant QR kodus duomenų pardavimui. Naudojant „Bitcoinlib“ biblioteką, privatūs raktai yra šifruojami, PIN kodas apsaugo nuo neautorizuotos prieigos, o BIP-39 mnemoninė frazė leidžia piniginės atkūrimą. Modulinė architektūra ir standartiniai komponentai mažina tiekimo grandinės atakos riziką. Prototipas veikia be tinklo ir nepriklausomai nuo trečiųjų šalių, sumažindama įsilaužimo galimybę, tarpininko ir socialinės inžinerijos atakų rizikas.

PASIŪLYMAI

1. Siekiant gerinti sukurtą piniginės prototipą siūloma sukurti 3D spausdintuvu pagamintą dėklą, kuris užtikrintų fizinę komponentų apsaugą ir stabilizuotų kamera.
2. Norint pagerinti QR kodų skenavimo greitį ir kokybė esant sudėtingoms apšvietimo sąlygoms, vertėtų atnaujinti prototipo kamera su didesne raiška ir aukšto dinaminio diapazono technologija.
3. Piniginės prototipo saugumui ir funkcionalumui gerinti vertėtų atnaujinti ekraną, suderinama su naujesne operacinė sistema.

LITERATŪROS SĄRAŠAS:

1. Badea, L., ir Mungiu-Pupazan, M. C. (2021). The Economic and Environmental Impact of Bitcoin. *IEEE access*, *9*, p. 48091-48104. Prieiga per: https://ieeexplore.ieee.org/document/9385063
2. Barbereau, T. ir Bodo, B. (2023). Beyond financial regulation of crypto-asset wallet software: In search of secondary liability. *Computer Law & Security Review*. Vol. *49*. Prieiga per: https://www.sciencedirect.com/science/article/pii/S0267364923000390?via%3Dihub
3. BitBox (2024). https://bitbox.swiss/
4. BlockStream Jade (2024). Prieiga per: https://blockstream.com/jade/
5. Bowler, R., Goodell, G., Revans, J., Bizama, G. ir Speed, C. (2024). A non-custodial wallet for digital currency: design challenges and opportunities. *Cornell University Library*. Prieiga per: https://arxiv.org/abs/2307.05167
6. Coldcard (2024). Prieiga per https://coldcard.com/;
7. Davenport, A., ir Shetty , S. (2019). Modeling Threat of Leaking Private Keys from Air-Gapped Blockchain Wallets. *2019 IEEE International Smart Cities Conference (ISC2)*, p. 9-13. Prieiga per: https://ieeexplore.ieee.org/document/9071725
8. Dumitrescu, G. C. (2017). Bitcoin – A Brief Analysis of the Advantages and Disadvantages. *Global economic observer*, *5*(2), p. 63-71. Prieiga per: https://www.proquest.com/scholarly-journals/bitcoin-brief-analysis-advantages-disadvantages/docview/1990422140/se-2?accountid=15307
9. Ebrahimi, S., Hasanizadeh, P., Aghamirmohammadali, S., M., ir Akbari, A.(2021). Enhancing Cold Wallet Security with Native Multi-Signature schemes in Centralized Exchanges. *Cornell University Library*. Prieiga per: https://arxiv.org/abs/2110.00274
10. Ellipal Wallet (2024). Prieiga per https://www.ellipal.com/
11. Foundation Passport wallet (2024). Prieiga per: https://foundation.xyz/passport/
12. Guri, M. (2018). BeatCoin: Leaking Private Keys from Air-Gapped Cryptocurrency Wallets. *arXiv.org 2018-14.* Prieiga per: https://www.proquest.com/working-papers/beatcoin-leaking-private-keys-air-gapped/docview/2072080374/se-2?accountid=15307
13. Houy, S., Schmid P., ir Bartel, A. (2023). Security Aspects of Cryptocurrency Wallets—A Systematic Literature Review. *ACM Computing Surveys*, *56*(1), p. 1-31. Prieiga per: https://dl.acm.org/doi/10.1145/3596906

14. Jorgensen, K. P., ir Beck, R. (2022). Universal Wallets. *Business & information systems engineering, 64*(1), p. 115-125. Prieiga per: https://link.springer.com/article/10.1007/s12599-021-00736-6
15. Khan, A., G., Zahid, A., H., Hussain, M., ir Riaz, U. (2019). Security Of Cryptocurrency Using Hardware Wallet And QR Code. *2019 International Conference on Innovative Computing (ICIC).*
16. Khanum, S., ir Mustafa, K. (2022). Exposure of Sensitive Data Through Blockchain Wallets: A Comparative Analysis. *International Conference on Innovative Computing and Communications*, p. 161–169. Prieiga per: https://link.springer.com/chapter/10.1007/978-981-19-2821-5_13
17. Koutmos, D. King, T., ir Zopounidis C. (2021). Hedging uncertainty with cryptocurrencies: Is bitcoin your best bet? *The Journal of financial research*, Vol.*44* (4), p.815-837. Prieiga per: https://onlinelibrary.wiley.com/doi/full/10.1111%2Fjfir.12264
18. Krux DIY Hardware Wallet (2024). Prieiga per https://walletscrutiny.com/hardware/kruxdiyhw/;
19. Ledger Developer Portal (2024). Prieiga per https://developers.ledger.com/;
20. M5StickV K210. (2024) *M5StickV K210 Product Features.* Prieiga per https://shop.m5stack.com/products/stickv?srsltid=AfmBOooc-Tr5-dVzGV_ys0HFa4FaVzy7dZFhT-4gWiXkVseh1Bc9Z0MD
21. Masahiko, M., ir Kento, S. (2019). Wallet device for cryptocurrency and method of signature for the use thereof. Prieiga per: https://typeset.io/papers/wallet-device-for-cryptocurrency-and-method-of-signature-for-2n38z28qhttps://patents.google.com/patent/US201903789A1/en
22. NanoPi Neo Air. (2024). *NanoPi NEO Air Diagram, Layout and Dimension.* Prieiga per http://nanopi.io/nanopi-neo-air.html
23. Nowroozi, E., Seyedshoari, S., Mekdad, Y., Erkay S., ir Conti, M. (2023). Cryptocurrency wallets: assessment and security. *Cornell University Library*. Prieiga per https://www.proquest.com/docview/2790192885?pqorigsite=primo&sourcetype=Working%20Papers
24. Onion Omega2+. (2024). *Onion Omega2+ technical documentation*. Prieiga per https://docs.onion.io/omega2-docs/omega2.html
25. Opendime Wallet (2024). Prieiga per https://opendime.com/
26. Park, D., Choi, M., Kim, G., Bae, D., Kim, H., ir Hong, S. (2023). Stealing Keys From Hardware Wallets: A Single Trace Side-Channel Attack on Elliptic Curve Scalar Multiplication

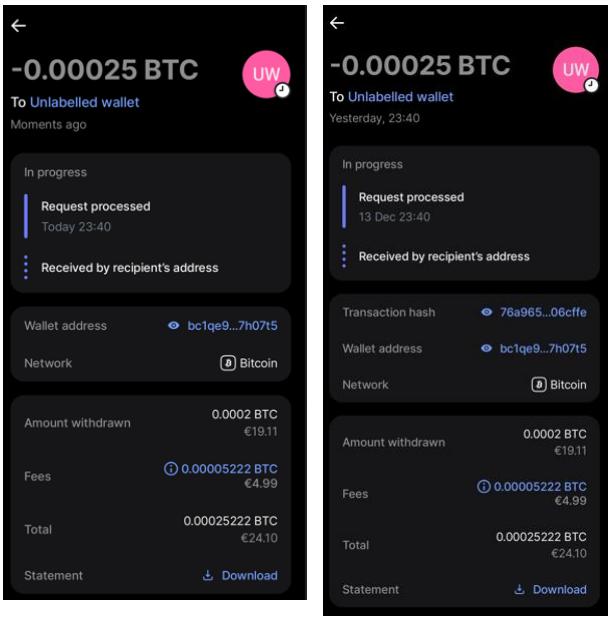
Without Profiling. *IEEE access, 11*, p. 1-1. Prieiga per: https://ieeexplore.ieee.org/document/10115517

27. PiTrezor (2024). Prieiga per https://www.pitrezor.com/2018/02/pitrezor-homemade-trezor-bitcoin-wallet.html;
28. Raspberry Pi Documentation. (2024). *Getting started with your Raspberry Pi*. Prieiga per https://www.raspberrypi.com/documentation/computers/getting-started.html
29. SatoChip (2024). Prieiga per: https://satochip.io/;
30. SeedSigner (2024). Prieiga per https://seedsigner.com/;
31. Semyanov, P. V. ir Grezina, S. V. (2023). Analysis of Cryptographic Protection of the Bitcoin Core Cryptographic Wallet. *Automatic control and computer sciences, 57*(8), p. 914-921.
32. Suraktar, S., Shirole, M., ir Brihud, S. (2020). Cryptocurrency Wallet: A Review. *4th International Conference on Computer, Communication and Signal Processing (ICCCSP)*
33. Taylor, S., Kim, S. H., Ariffin, K. A. Z., ir Abdullah, S. N. H. S. (2022). A comprehensive forensic preservation methodology for crypto wallets. *Forensic Science International: Digital Investigation 42-43*, p. 301477. Prieiga per: https://www.sciencedirect.com/science/article/pii/S2666281722001585?via%3Dihub
34. Tangem (2024). Prieiga per: https://tangem.com/en/ ;
35. Trezor community (2024). Forumas. Prieiga per https://forum.trezor.io/;
36. Veksler, D. (2024). Understanding the Security Model of Hardware Wallets. Prieiga per https://davidveksler.substack.com/p/understanding-the-security-model;
37. Voletly, T., Saini, S., McGhin, T., Liu, C. Z., ir Cho K. K. R. (2019). Cracking Bitcoin wallets: I want what you have in the wallets. *Future generation computer systems, 91*, p. 136-143. Prieiga per: https://www.sciencedirect.com/science/article/pii/S0167739X18302929?via%3Dihub
38. Wang, H., Li, X., Goa, J., ir Li, W. (2019). MOBT: A kleptographically-secure hierarchical-deterministic wallet for multiple offline Bitcoin transactions. *Future generation computer systems, 101*, p. 315-326.

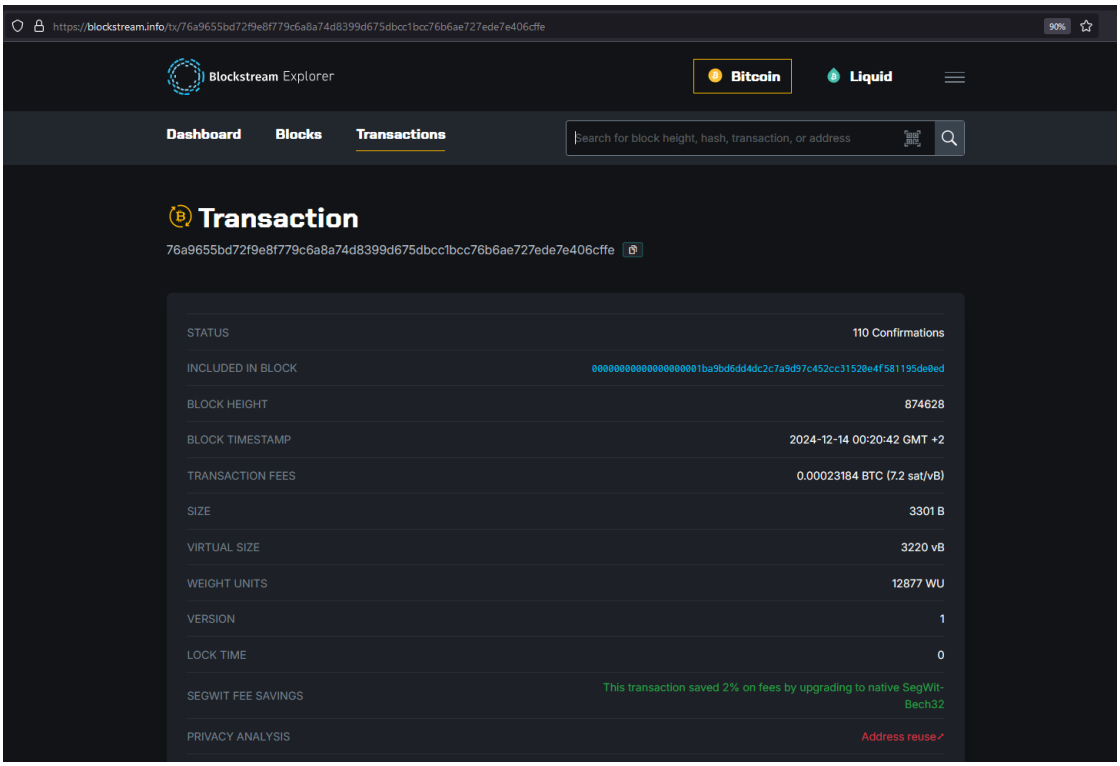
PRIEDAI

1 PRIEDAS

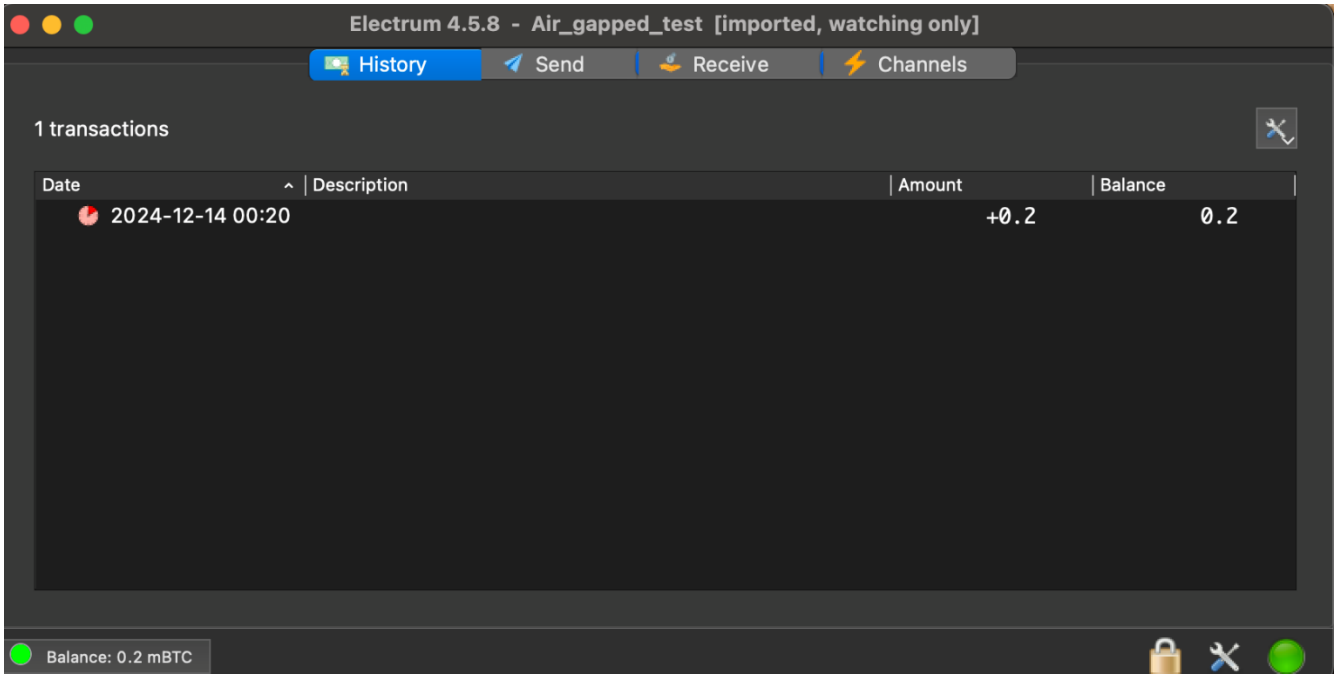
Transakcijos atlikimas į sukurtą piniginės prototipą



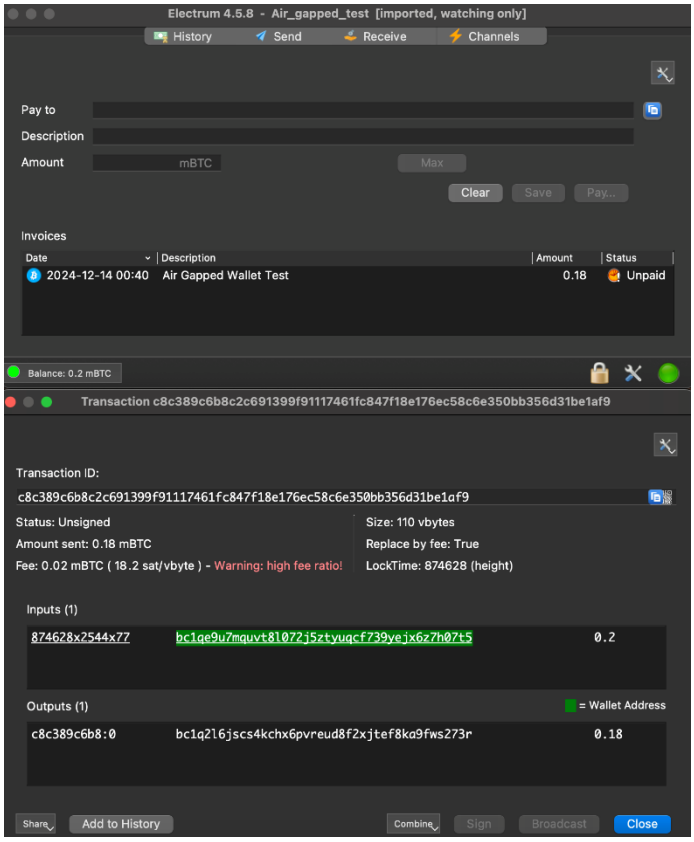
Atlikta transakcija į sukurtos piniginės adresą, blokų grandinėje



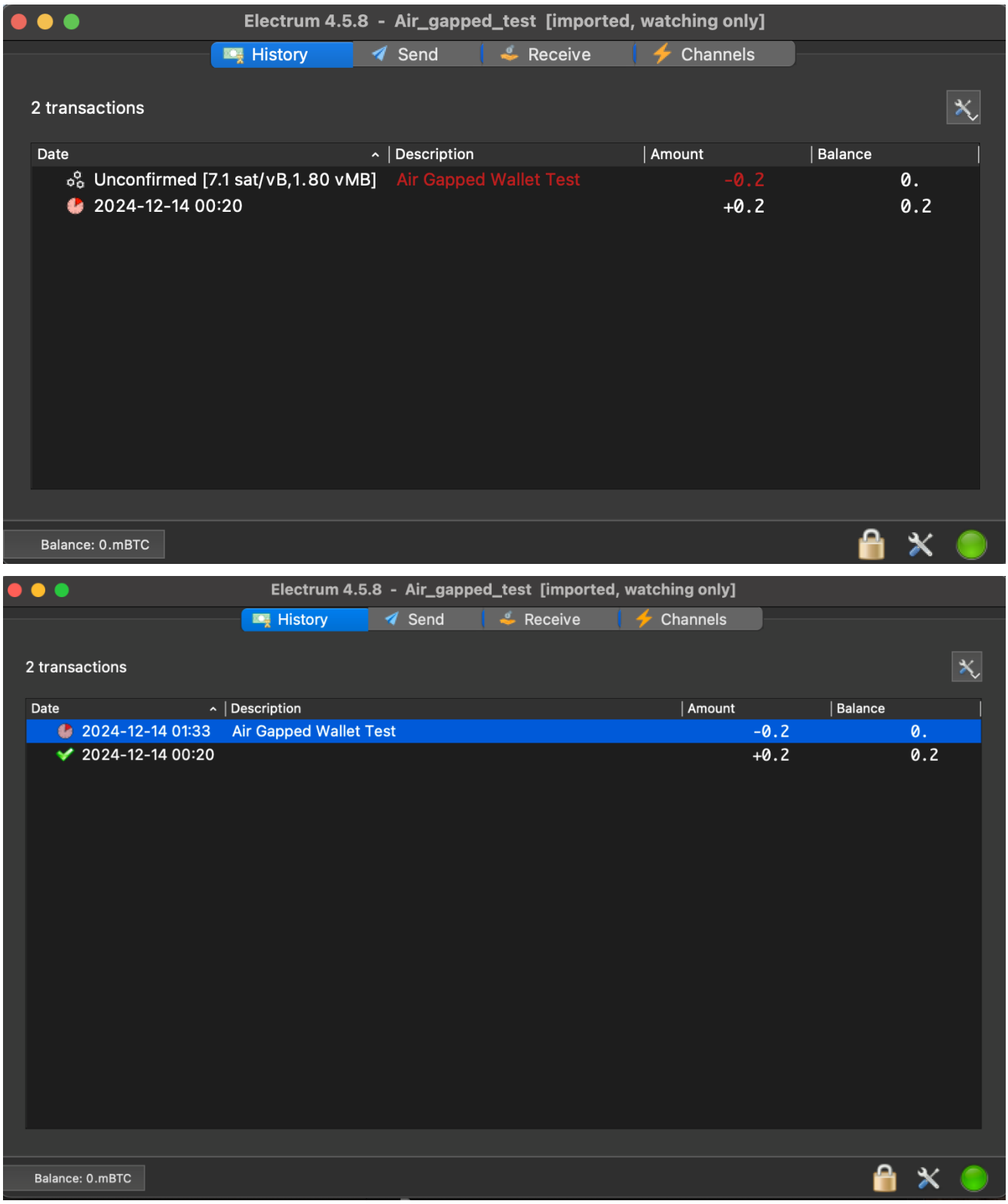
Transakcija sugeneruotoje ir matoma stebėjimo piniginėje



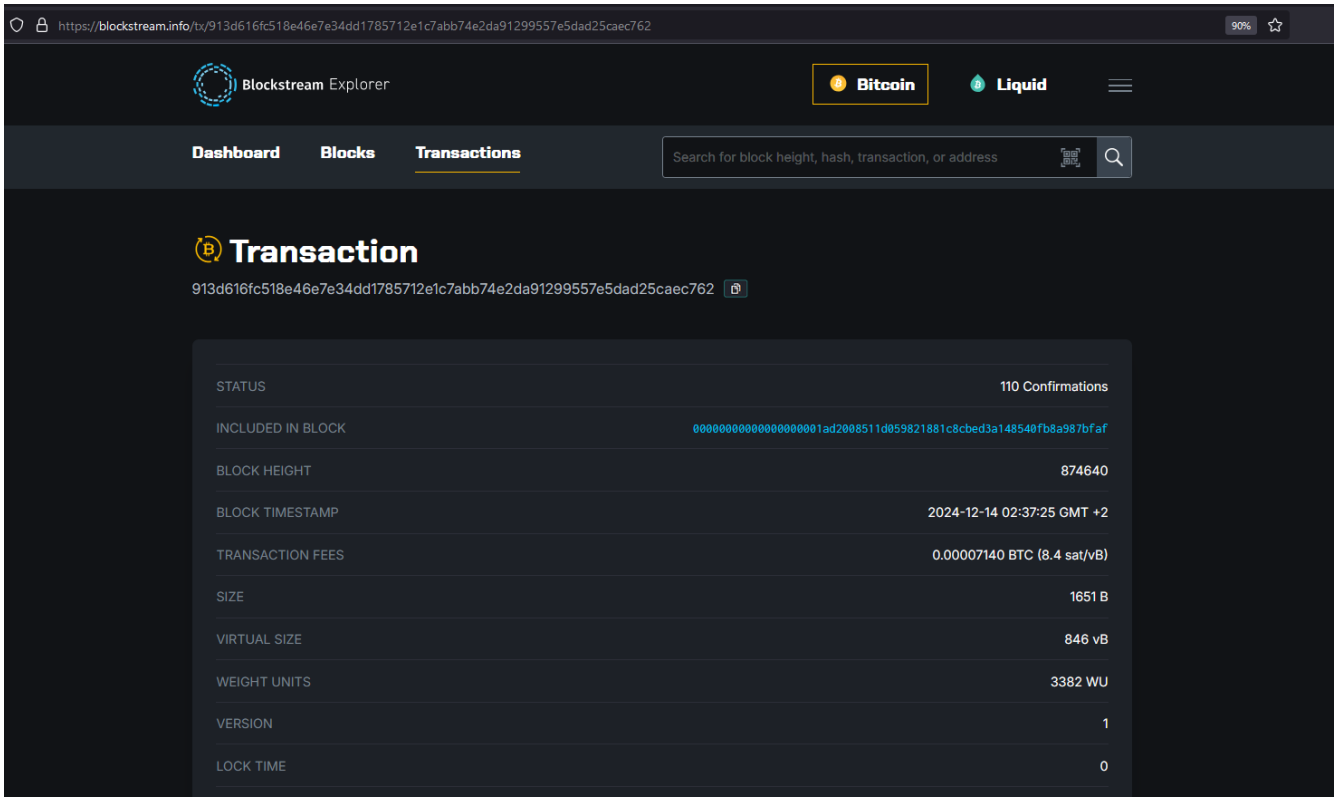
Sugeneruotas PSBT transakcijos QR kodas, lėšoms perversti



Pasirašytos transakcijos atvaizdavimas stebėjimo piniginėje



Pasirašytos transakcijos atvaizdavimas blokų grandinėje



Belaidės atjungtos nuo tinklo Bitcoinų piniginės sukurtas programinis kodas

```
import os
import hashlib
import time
import RPi.GPIO as GPIO
from PIL import Image, ImageDraw, ImageFont
import qrcode
from mnemonic import Mnemonic
from bitcoinlib.wallets import Wallet
from pyzbar.pyzbar import decode
import picamera
import ST7789

#Mygtuku konfiguracija
KEY_UP_PIN = 6
KEY_DOWN_PIN = 19
KEY_LEFT_PIN = 5
KEY_RIGHT_PIN = 26
KEY_PRESS_PIN = 21

GPIO.setmode(GPIO.BCM)
GPIO.setwarnings(False)
GPIO.setup(KEY_UP_PIN, GPIO.IN, pull_up_down=GPIO.PUD_UP)
GPIO.setup(KEY_DOWN_PIN, GPIO.IN, pull_up_down=GPIO.PUD_UP)
GPIO.setup(KEY_LEFT_PIN, GPIO.IN, pull_up_down=GPIO.PUD_UP)
GPIO.setup(KEY_RIGHT_PIN, GPIO.IN, pull_up_down=GPIO.PUD_UP)
GPIO.setup(KEY_PRESS_PIN, GPIO.IN, pull_up_down=GPIO.PUD_UP)

# LCD ekrans
LCD_WIDTH = 240
LCD_HEIGHT = 240
FONT = ImageFont.truetype("/usr/share/fonts/truetype/dejavu/DejaVuSans-Bold.ttf", 22)
FOOTER_FONT = ImageFont.truetype("/usr/share/fonts/truetype/dejavu/DejaVuSans-Bold.ttf", 16)

lcd = ST7789.ST7789()
lcd.Init()
lcd.clear()
lcd.bl_DutyCycle(50)

WALLET_NAME = "Airgapped_wallet"
PIN_FILE = "pin_hash.txt"
# Funkcijos
def hash_pin(pin):
    return hashlib.sha256(pin.encode()).hexdigest()

def sha256_hash(data):
    return hashlib.sha256(data.encode('utf-8')).hexdigest()
```

```
def pin_exists():
    return os.path.exists(PIN_FILE)

def save_pin(pin):
    with open(PIN_FILE, "w") as f:
        f.write(hash_pin(pin))

def load_pin():
    with open(PIN_FILE, "r") as f:
        return f.read().strip()

def display_text(lcd, text, footer=None):
    image = Image.new("RGB", (LCD_WIDTH, LCD_HEIGHT), "black")
    draw = ImageDraw.Draw(image)

    lines = text.split("\n")
    y = 10
    for line in lines:
        draw.text((10, y), line, font=FONT, fill="white")
        y += 30

    if footer:
        draw.text((10, LCD_HEIGHT - 30), footer, font=FOOTER_FONT, fill="white")

    lcd.ShowImage(image)

def input_pin(prompt):
    entered_pin = ""
    current_number = 1

    while len(entered_pin) < 4:
        display_text(
            lcd,
            f"{prompt}\n[{current_number}]\n" + "*" * len(entered_pin),
            footer="UP: +1 | DOWN: -1 | KEY1: OK",
        )

        if GPIO.input(KEY_UP_PIN) == 0:
            current_number = current_number + 1 if current_number < 9 else 1
            time.sleep(0.2)
        elif GPIO.input(KEY_DOWN_PIN) == 0:
            current_number = current_number - 1 if current_number > 1 else 9
            time.sleep(0.2)
        elif GPIO.input(KEY_PRESS_PIN) == 0:
            entered_pin += str(current_number)
            time.sleep(0.2)
```

```
    return entered_pin

def request_pin():
    if not pin_exists():
        display_text(lcd, "Set up your PIN")
        new_pin = input_pin("Enter New PIN")
        confirm_pin = input_pin("Confirm PIN")

        if new_pin == confirm_pin:
            save_pin(new_pin)
            display_text(lcd, "PIN Set Successfully!")
            time.sleep(2)
            return True
        else:
            display_text(lcd, "PIN Mismatch!")
            time.sleep(2)
            return False
    else:
        stored_pin_hash = load_pin()
        entered_pin = input_pin("Enter PIN")

        if hash_pin(entered_pin) == stored_pin_hash:
            display_text(lcd, "Access Granted")
            time.sleep(2)
            return True
        else:
            display_text(lcd, "Access Denied")
            time.sleep(2)
            return False


def wallet_exists(wallet_name):
    wallet_path = os.path.expanduser(f"~/.bitcoinlib/wallets/{wallet_name}.sqlite")
    return os.path.exists(wallet_path)


def create_or_load_wallet():
    wallet_path = os.path.expanduser(f"~/.bitcoinlib/wallets/{WALLET_NAME}.sqlite")

    try:
        if os.path.exists(wallet_path):
            wallet = Wallet(WALLET_NAME)
            display_text(lcd, "Wallet Loaded")
            time.sleep(2)
            return wallet
        else:
            mnemonic = Mnemonic("english").generate(strength=128)
            wallet = Wallet.create(
                WALLET_NAME,
```

```
            keys=mnemonic,

            network="bitcoin",
            witness_type="segwit"
        )
        display_text(lcd, "Wallet Created\nSave Seed")
        print(f"Seed Phrase: {mnemonic}")

        words = mnemonic.split()
        for i in range(0, len(words), 2):
            chunk_index = (i // 2) + 1
            progress = f"Seed Phrase {chunk_index}/6"
            text = f"{progress}\n\n{' '.join(words[i:i + 2])}"
            footer = "Press KEY1 to continue"
            display_text(lcd, text, footer=footer)

            while GPIO.input(KEY_PRESS_PIN) == 1:
                time.sleep(0.1)
        return wallet
    except Exception as e:
        display_text(lcd, f"Wallet Error!")
        print(f"Error: {e}")
        time.sleep(2)
        return None

def show_wallet_address(wallet):
    try:
        address = wallet.get_key().address
        print(f"Wallet Address: {address}")

        qr = qrcode.QRCode(version=1, box_size=4, border=4)
        qr.add_data(address)
        qr.make(fit=True)
        qr_img = qr.make_image(fill="black", back_color="white").resize((LCD_WIDTH, LCD_HEIGHT))
        qr_img = qr_img.convert("RGB")
        lcd.ShowImage(qr_img)

        time.sleep(5)
    except Exception as e:
        display_text(lcd, f"Error: {e}")
        print(f"Error fetching address: {e}")
        time.sleep(2)

def sign_psbt(wallet):
    display_text(lcd, "Scan PSBT QR...")
    time.sleep(2)

    camera = picamera.PiCamera()
    camera.resolution = (640, 480)
```

```
    camera.capture("psbt.jpg")

    camera.close()

    decoded = decode(Image.open("psbt.jpg"))
    if not decoded:
        display_text(lcd, "No QR Found!")
        time.sleep(2)
        return

    psbt = decoded[0].data.decode()
    print(f"PSBT: {psbt}")

    try:
        signed_psbt = wallet.transaction_sign(psbt)
        hashed_signed_psbt = sha256_hash(signed_psbt)
        display_text(lcd, "Tx Signed!")
        display_qr(lcd, hashed_signed_psbt)
        print(f"Signed PSBT (hashed): {hashed_signed_psbt}")
        time.sleep(5)
    except Exception as e:
        display_text(lcd, f"Error Signing Tx: {e}")
        print(f"Error: {e}")
        time.sleep(2)

def main_menu(wallet):
    menu_text = "UP: Show Address\nDOWN: Sign PSBT"
    display_text(lcd, menu_text)

    while True:
        if GPIO.input(KEY_UP_PIN) == 0:
            show_wallet_address(wallet)
            display_text(lcd, menu_text)
        elif GPIO.input(KEY_DOWN_PIN) == 0:
            sign_psbt(wallet)
            display_text(lcd, menu_text)
        time.sleep(0.1)

def main():
    if not request_pin():
        return

    wallet = create_or_load_wallet()
    if wallet:
        main_menu(wallet)
if __name__ == "__main__":
    main()
```