УНИВЕРЗИТЕТ У БЕОГРАДУ
МАТЕМАТИЧКИ ФАКУЛТЕТ

МАСТЕР РАД

Криптографија у систему Биткоин

Аутор:
Војислав Станковић

Ментор:
проф. др. Миодраг Живковић

Чланови комисије:
проф. др. Саша Малков
проф. др. Филип Марић

Београд, 2022

Садржај

Страна

1 Увод **1**

2 Криптографски елементи **2**
2.1 Шифарски системи са јавним кључем 2
2.2 Криптографија са елиптичким кривама 4
2.3 Елиптичке криве у коначном пољу 6
2.4 Дигитални потписи и алгоритам ECDSA 7
2.4.1 Начин рада са дигиталним потписима 7

3 Кључеви и адресе **9**
3.1 Дигитални потписи и дигитални новац 9
3.2 Приватни и јавни кључеви 9
3.3 Биткоин адресе 10
3.3.1 Кодови Base58 и Base58Check 11
3.3.2 Формати кључева 11
3.4 Посебне варијанте кључева и адреса 14
3.4.1 Шифровани приватни кључеви (BIP-38) 14
3.4.2 Pay-to-Script Hash (P2SH) и Multisig адресе 14
3.4.3 Персонализоване адресе 14
3.4.4 Папирни нованици 15

4 Новчаници **17**
4.1 Преглед технологија реализације нованика 17
4.1.1 Недетерминистички новчаници 17
4.1.2 Детерминистички новчаници 17
4.1.3 ХД новчаници (BIP-32 и BIP-44) 18
4.1.4 Лозинке и мнемонички кодови (BIP-39) 19
4.1.5 Препоруке за употребу биткоин новчаника 20
4.2 Детаљи реализације речника 20
4.2.1 Мнемоничке кодне речи (BIP-39) 20
4.2.2 Креирање ХД новчаника на основу мнемоника . . . 21

5 Сигурност биткоина **22**
5.1 Сигурносни принципи 22
5.2 Препоруке за постизање сигурности корисника 22
5.2.1 Физичко чување биткоина 23
5.2.2 Хардверски новчаници 23
5.2.3 Разноврсност чувања 24

5.2.4 Уравнотежење ризика 24
5.2.5 Вишеструки потписи 25

6 Анализа имплементације новчаника у језику Пајтон 26
6.1 Генерисање почетне вредности и главног кључа 26
6.2 Генерисање хијерархије кључева 28
6.3 Прављење и потписивање трансакције 29

7 Закључак 32

Литература 33

1 Увод

Биткоин је први пут представљен 2008. године у раду [1], као децентрализована валута која се може слати другим корисницима преко мреже Биткоин, у којој су трансакције аутентиковане од стране чворова и забележене у ланцу блокова.

Сатоши Накамото је први решио проблем двоструке потрошње кроз децентрализован систем, без посредовања финансијских институција и централних банака, и због тога је биткоин остао најзначајнија међу криптовалутама.

Биткоин новчаници, за разлику од обичних новчаника, не чувају саму валуту, већ приватне кључеве и адресе. Валута је записана у ланцу блокова и кључ доказује власништво над валутом, те даје могућност потрошње исте. Губитак кључа значи губитак приступа средствима, стога је неопходно кључ што боље заштити од губитка, али и крађе.

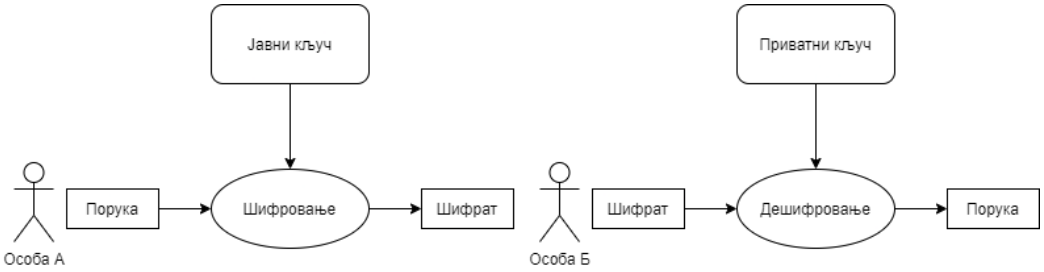
У овом раду су описани основни криптографски елементи система Биткоин, креирање кључева и адреса као и њихово чување у новчанику. Обрађени су сигурносни принципи као и препоруке за постизање што веће сигурности корисника система. У последњем поглављу садржана је анализа имплементације пара новчаника, развијених у сврху овог рада, са циљем демонстрације употребе система.

2 Криптографски елементи

Криптографија се користи у заштити података и комуникације. Како би се заштитили подаци могуће их је шифровати неким алгоритмом шифровања. Алгоритам шифровања се уобичајено састоји од низа трансформација над подацима које зависе од кључа. Кључ одређује које ће се трансформације користити код шифровања и дешифровања. Када се исти кључ користи и за шифровање и за дешифровање, говоримо о симетричном шифарском систему. Подаци су на овај начин заштићени од свих особа које немају кључ. Уколико се неко домогне кључа и зна алгоритам шифровања, може да прочита шифровану поруку, или да је чак замени другом поруком коју је сам шифровао. Тиме се нарушава поверљивост и аутентичност података.

2.1 Шифарски системи са јавним кључем

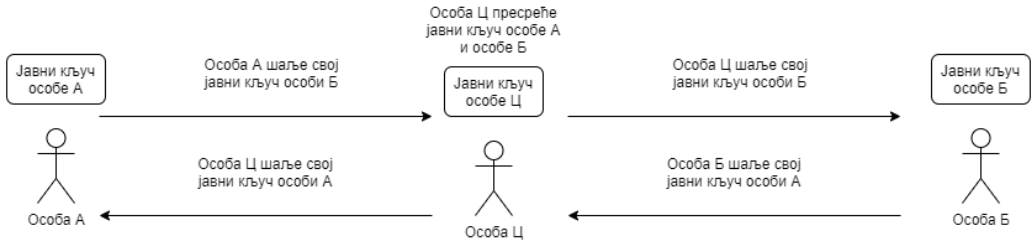
Асиметрични шифарски системи подразумевају коришћење два кључа, за разлику од симетричних шифарских система код којих суштински постоји само један кључ. Свака особа која учествује у конверзацији генерише пар кључева - приватни и јавни кључ, који су повезани. Приватни кључ се користи се за дешифровање, он се чува у тајности. Јавни кључ се користи за шифровање података. Њега власник може слободно поделити са свим учесницима у комуникацији и због тога се асиметрични шифарски системи још називају и шифарски системи са јавним кључем. Уколико особа А жели да пошаље шифровану поруку особи Б, она је шифрује јавним кључем особе Б. Особа Б онда искористи свој приватни кључ како би дешифровала поруку особе А (погледати слику 1). Уколико постоји особа Ц која прислушкује комуникациони канал, она може да пресретне поруку, али не може ефективно да одреди приватни кључ на основу јавног [2] (под условом да примењени систем са јавним кључем није лош).



Слика 1: Комуникација у шифарском систему са јавним кључем

Иако не постоји ефективан начин за одређивање приватног кључа на основу јавног, шифарски систем са јавним кључем је подложан "нападу човека у средини" (енгл. *Person-in-the-Middle attack*).

Пример 2.1 *Уколико особа Ц контролише комуникациони канал између особе А и особе Б, она може да пресретне размену јавних кључева и да се уметне у комуникацију између особа А и Б (погледати слику 2)*



Слика 2: Напад човека у средини

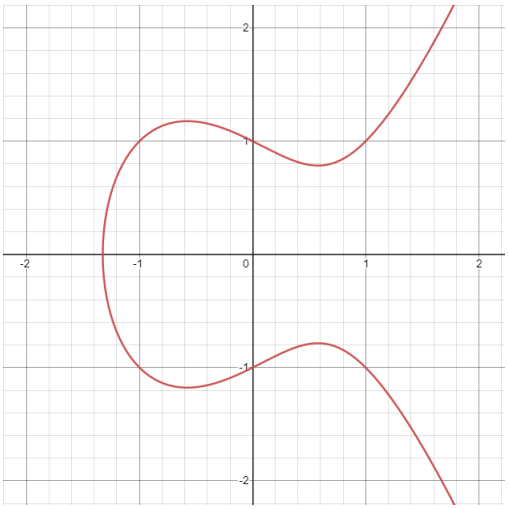
Особа Ц задржава јавне кључеве особа А и Б, а њима прослеђује свој јавни кључ. Уколико особа А жели да пошаље поруку особи Б, она је шифрује јавним кључем који је добила кроз комуникациони канал, не знајући да је то јавни кључ особе Ц. Особа Ц сада лако може да дешифрује поруку особе А. Особа Ц може да измени садржај поруке особе А (делимично или потпуно), шифрује је јавним кључем особе Б који је задржала, и прослеђује поруку особи Б. Особа Б дешифрује поруку мислећи да је стигла од особе А. Уколико особа Б жели да одговори особи А, понавља се описана процедура у обрнутом смеру.

Ова ситуација је могућа ако протокол не обезбеђује аутентикацију пошиљаоца поруке. Једна последица овог напада је да подаци постају доступни особи Ц којој нису првобитно намењени, али постоје и озбиљније

последице. Рецимо да су у примеру са слике 2 особа А и Б размењивали банковне рачуне. Особа Ц може особама А и Б проследити свој банковни рачун и на тај начин их опљачкати.
Од описаног напада се може одбранити уколико се размена јавних кључева одвија лично или кроз сигуран комуникациони канал, или уколико постоји сертификационо тело за валидацију јавних кључева [2].

2.2 Криптографија са елиптичким кривама

Елиптичка крива је скуп тачака (x, y) над пољем које задовољавају једначину $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$. Без губитка општости једначина се може записати у облику $y^2 = x^3 + a_4x + a_6$, то јест $y^2 = x^3 + Ax + B$ (на слици 3 приказан је пример графика елиптичке криве над пољем реалних бројева). То су криве чији су коефицијенти $a_1 = a_2 = a_3 = 0$, оне су симетричне у односу на x-осу и називају се Вајерштрасове криве [3]. У криптографији се често користе елиптичке криве над коначним пољем у овом упрошћеном облику.



Слика 3: Елиптичка крива: $y^2 = x^3 - x + 1$

Размотрићемо најпре сабирање тачака елиптичке криве над коначним пољем. Нека су дате две тачке са различитим x координатама, $P(x_p, y_p)$ и $Q(x_q, y_q)$. Збир тачака $P+Q$ тачака P и Q се дефинише као симетрична тачка у односу на x-осу пресечној тачки елиптичке криве и праве која пролази кроз тачке P и Q.

Нека су $P(x_p, y_p)$ и $Q(x_q, y_q)$ две тачке са различитим x координатама на елиптичкој кривој једначине $y^2 = x^3 + Ax + B$. Нека је $y = kx + n$ једначина праве која пресеца криву у тачкама P и Q. За њу важи:

$$k = \frac{y_q - y_p}{x_q - x_p} \qquad n = y_p - kx_p$$

Једначина $y = kx + n$ је дакле:

$$y = \frac{y_q - y_p}{x_q - x_p} \cdot x + \left(y_p - \frac{y_q - y_p}{x_q - x_p} \cdot x_p \right)$$

Нека тачка $R = (x_r, y_r)$ представља трећу тачку пресека праве и елиптичке криве. Како су тачке P и Q познате, тачка R се израчунава као решење система

$$y = kx + n$$
$$y^2 = x^3 + Ax + B$$

Елиминацијом y добија се кубна једначина по x:

$$x^3 - k^2x^2 + Ax - 2kxn + B - n^2 = x^3 - k^2x^2 + (A - 2kn)x + B - n^2 = 0$$

Дељењем кубног полинома квадратним полиномом $(x-x_p)(x-x_q)$ добија се линеарни полином $(x - x_r)$. Тиме се добија да су координате (x_r, y_r) тачке R једнаке:

$$x_r = \left(\frac{y_q - y_p}{x_q - x_p} \right)^2 - x_p - x_q$$
$$y_r = \frac{y_q - y_p}{x_q - x_p}(x_p - x_r) - y_p$$

Уколико важи $P = Q$, операција сабирања је уствари операција дуплирања тачака: $P + P = 2P$. Праву кроз тачке P и Q замењује тангента на криву у тачки P. Како важи $x_p = x_q$ и $y_p = y_q$, коефицијент правца k не можемо рачунати по претходној формули због дељења са нулом. У коначном пољу једначина тангенте на криву у тачки одређује се на исти начин као и над пољем реалних бројева, рачунањем првог извода у задатој тачки криве.

$$(y^2 = x^3 + Ax + B)/\frac{\partial y}{\partial x}$$
$$2y\frac{\partial y}{\partial x} = 3x^2 + A$$
$$k = \frac{\partial y}{\partial x} = \frac{3x^2 + A}{2y}$$

Слободан члан n се рачуна по претходној формули, стога се једначина праве записује као:

$$y = \frac{3x_p^2 + A}{2y_p}(x - x_p) + y_p$$

Елиминацијом y као и у претходном случају добија се кубна једначина по x. Двоструки корен те једначине је x_p, па се дељењем кубног полинома са $(x - x_p)^2$ добија линеарни полином, чијим се изједначавањем са нулом добијају координате тачке R:

$$x_r = \left(\frac{3x_p^2 + A}{2y_p}\right)^2 - 2x_p$$

$$y_r = \frac{3x_p^2 + A}{2y_p}(x_p - x_r) - y_p$$

Неутрал у односу на сабирање је *бесконачно удаљена тачка* $(0, 1, 0)$, у ознаци $\varnothing$. Она представља замишљену тачку сусрета свих вертикалних правих и криве у бесконачности. Важи:

$$P + \varnothing = \varnothing + P = P$$
$$P + (-P) = \varnothing$$
$$\varnothing + \varnothing = \varnothing$$

Инверз тачке $P(x, y)$ је тачка $-P = P(x, -y)$. Одузимање се своди на сабирање са инверзном тачком.

2.3 Елиптичке криве у коначном пољу

Коначна поља $\mathbb{F}_q$ су поља која садрже коначни број елемената и подржавају операције сабирања и множења и за које важи закон дистрибутивности. Елиптичке криве које се користе у криптографији се најчешће дефинишу над два типа коначних поља где је $q = p$ (p је прост број) или $q = 2^m$ [3].

У систему биткоин користи се елиптичка крива над коначним пољем облика $\mathbb{F}_p$ где је p фиксирани прост број. Коначно поље $\mathbb{F}_p$ се дефинише као поље са p елемената $\{0, 1, \ldots, p-1\}$. Елементи скупа $\{0, 1, \ldots, p-1\}$ су бројеви добијени као остатак при дељењу са бројем p. Ако се приликом извршења неке операције над $\mathbb{F}_p$ добије резултат r који није у скупу $\{0, 1, \ldots, p-1\}$, r се замењује својим остатком $r \pmod p$ по модулу p.

Пример 2.2 *За коначно поље* $\mathbb{F}_{23}$ *резултат операције* $15 + 22 = 14$, *јер је* $37 \pmod{23} = 14$.

Операција одузимања над коначним пољем $\mathbb{F}_p$ се дефинише као операција супротна операцији сабирања. Ако су $P, Q \in \mathbb{F}_p$ онда је разлика $P - Q = R$ где је $R \in \{0, 1, \ldots, p-1\}$ остатак при дељењу $P - Q \pmod{p}$.

Пример 2.3 *За коначно поље* $\mathbb{F}_{23}$ *резултат операције* $15 - 22 = 16$, *јер је* $7 \pmod{23} = 16$.

Операција множења над коначним пољем $\mathbb{F}_p$ се дефинише као множење по модулу p. Ако су $P, Q \in \mathbb{F}_p$ онда је производ $P \cdot Q = R$ где је $R \in \{0, 1, \ldots, p-1\}$ остатак при дељењу $P \cdot Q \pmod{p}$.

Пример 2.4 *За коначно поље* $\mathbb{F}_{23}$ *резултат операције* $15 \cdot 22 = 8$, *јер је* $330 \pmod{23} = 8$.

Над коначним пољем $\mathbb{F}_p$ елиптичка крива (у Вајештрасовом запису) задаје се једначином облика $y^2 = x^3 + Ax + B$. Скуп тачака у коначном пољу $\mathbb{F}_p$ које припадају елиптичкој кривој је група G са операцијом сабирања тачака. За групу G кажемо да је циклична уколико је свака тачка на кривој неки умножак kG тачке G, *генератора*.

2.4 Дигитални потписи и алгоритам ECDSA

Дигитални потписи у систему биткоин се користе примарно за потписивање трансакција. Када корисник жели да изврши трансакцију он мора да докаже да има право да потроши средства. Дигитално потписивање се састоји из две процедуре: креирања потписа на основу приватног кључа помоћу алгоритма потписивања и верификације потписа на основу трансакције и јавног кључа.

Ако Алиса жели да пошаље Бобану један биткоин, она мора да потпише трансакцију својим приватним кључем. Да не би њен приватни кључ био видљив учесницима који валидирају трансакцију Алиса користи дигитални потпис приватним кључем како би доказала власништво. Учесници мреже који валидирају трансакцију утврђују исправност потписа на основу њеног јавног кључа.

2.4.1 Начин рада са дигиталним потписима

Дигитални потпис помоћу елиптичке криве (енгл. *Elliptic Curve Digital Signature Algorithm, ECDSA*) се састоји од два алгоритма:

- Алгоритам потписивања трансакције приватним кључем то јест дигиталним потписом. Резултат је пар приватног/јавног кључа у ознаци (r, s).

- Алгоритам верификације потписа трансакције на основу јавног кључа.

Алгоритам потписивања као улаз прима трансакцију и приватни кључ и генерише две вредности, R і S. Прво се рачуна вредност R одабиром псеудо-случајног броја k и његовим множењем G, где је G генератор групе; R је x координата производа: $(x, y) = kG$. Затим се рачуна вредност S изразом

$$S = k^{-1}(H + R \cdot a) \pmod{p}$$

где је H хеш вредност трансакције, a приватни кључ коришћен при потписивању, а p ред генератора G у групи тачака криве.

Верификација потписа је поступак инверзан операцији потписивања. Резултат верификације је тачка P на елиптичкој кривој. Верификација потписа се врши помоћу израза:

$$P = S^{-1} \cdot H \cdot G + S^{-1} \cdot R \cdot A$$

где је A јавни кључ. Уколико је координата x тачке P једнака R, порука је верификована.

3 Кључеви и адресе

Један од основних услова које протокол Биткоин мора да испуни је омогућавање доказивања власништва над биткоинима. Доказ о власништву заснива се на претходно поменитум елементима: приватни кључ, дигитални потпис и биткоин адреса. Биткоин адреса се користи за примање биткоина од других корисника.

3.1 Дигитални потписи и дигитални новац

Алгоритам Биткоин користи елиптичке криве у криптографском алгоритму потписивања и верификације трансакција. Особа која поседује приватни кључ контролише износ у биткоинима и може се сматрати његовим власником. Власник биткоина свој кључ чува у *новчанику* о коме ће бити више речи у поглављу 4. Основна "операција" са биткоинима јесте трансакција, тј. слање или примање износа у биткоинима. Сваку трансакцију треба верификовати како би се утврдило да корисник стварно поседује износ који шаље. У систему Биткоин верификација трансакције базирана је на децентрализованој мрежи.

3.2 Приватни и јавни кључеви

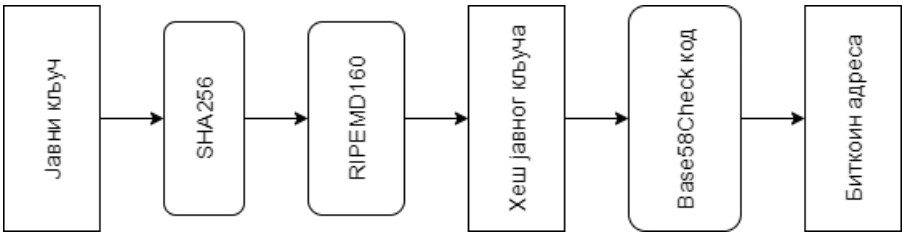
Систем Биткоин подразумева коришћење пара кључева, приватног и јавног. Приватни кључ се први генерише и он се користи за потписивање трансакције којом се преноси биткоин другом кориснику. Јавни кључ K је тачка на кривој која се добија множењем генератора G са приватним кључем k: $K = kG$ (приватни кључ је број који је најчешће случајно генерисан). Након генерисања јавног кључа од њега се хеширањем добија биткоин адреса. Одређивање приватног кључа на основу јавног је тежак проблем, еквивалентан решавању проблема дискретног логаритма за елиптичке криве [3].
Крива која се користи у стандарду је увек иста, $y^2 = x^3 + 7$. Њена структура није одабрана насумично као што је често случај са елиптичким кривама, него је осмишљена да омогући ефикасну брзину израчунавања [4]. Тачка генератор G у коначном пољу $\mathbb{F}_p$, $p = 2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1$, која се налази на елиптичкој кривој одређена је стандардом secp256k1. Пошто је тачка G увек иста и јавни кључ који се генерише на основу неког одређеног приватног кључа ће увек бити исти.

3.3 Биткоин адресе

Код обичних валута банковни рачун корисника представљен је низом цифара и користи се за уплату валуте на рачун. Биткоин адреса функционише на сличном принципу, али има неколико разлика.

- Банковни рачун је везан за особу или компанију и банка има увид о учесницима у трансакцији, док у биткоин систему учесници у валидирању трансакције виде само биткоин адресе.
- Банка додељује број рачуна кориснику, док биткоин адресу генерише сам корисник.
- Биткоин адреса није трајна као број банковног рачуна већ је пожељно да се користи само за једну трансакцију.
- Новац на банковном рачуну може да контролише банка, док је приватни кључ који је везан за биткоин адресу искључиво у власништву корисника.

Биткоин адреса се добија хеширањем јавног кључа алгоритмом хеширања. Функција која се користи у систему је *SHA* (енгл. *Secure Hashing Algorithm*), која се користи у композицији се алгоритмом *RIPEMD* (енгл. *RACE Integrity Primitives Evaluation Message Digest*).



Слика 4: Генерисање биткоин адресе

Јавни кључ K (добијен корацима описаним у тачки 3.3.2) се прво хешира помоћу *SHA256*[5], чиме се добија хеш величине 256 бита. Затим се резултат помоћу хеш функције *RIPEMID160*[6] мапира у хеш величине 160 бита. Резултат двоструког хеширања кључа K се даље прослеђује алгоритму кодирања *Base58Check*, чији је резултат биткоин адреса (слика 4).

3.3.1 Кодови Base58 и Base58Check

Алгоритам кодирања Base64 претвара бинарни у текстуални запис, који разликује велика и мала слова. Овај корак је неопходан да би олакшао читљивост од стране корисника или превазишао проблем слања бинарног записа преко интернета [7]. Код Base64 користи алфанумеричке карактере A–Z, a–z, 0–9 и симболе + и /. Код Base58 се користи са намером да се смањи могућност грешке при коришћењу биткоин адреса и избацује из употребе симболе + и / као и број 0 и слова O, I (велико латинично слово И), l (мало латинично слово л). У случају папирних новчаника (видети одељак 3.4.4) кључ обично прекуцава корисник или се користи софтвер за оптичко препознавање карактера и човек или софтвер могу направити грешку у препознавању записа наведених карактера.

Као додатни ниво заштите од грешака у препознавању записа, уведен је формат кодирања Base58Check који садржи контролни збир на крају записа. Контролни збир се изводи из хеша Base58 записа. Ако желимо да проверимо да ли је запис исправно прочитан, израчунаћемо контролни збир и упоредити га са контролним збиром на крају записа, ако нису исти дошло је до грешке.

У систему Биткоину код Base58Check такође садржи префикс који означава тип записа, и користи се за препознавање различитих формата.

Тип	Хексадекадни префикс	Base58Check префикс
Биткоин адреса	0x00	1
Pay-to-Script-Hash адреса	0x05	3
Биткоин тестнет адреса	0x6F	m или n
WIF кључ	0x80	5, K, или L
BIP-38 кодирани приватни кључ	0x0142	6P
BIP-32 продужени јавни кључ	0x0488B21E	xpub

Табела 1: Примери формата записа адреса и кључева

3.3.2 Формати кључева

У оригиналном формату приватни кључ и јавни кључ су представљени у бинарном запису као број од 256 бита (32 бајта). Међутим, они могу бити представљени на више начина, у зависности од сврхе за коју се користе. Различите репрезентације кључа се називају формати. Поједине формате (бинарни, хексадекадни) користи искључиво софтвер и не приказују се кориснику, док се поједини формати као што је WIF користе

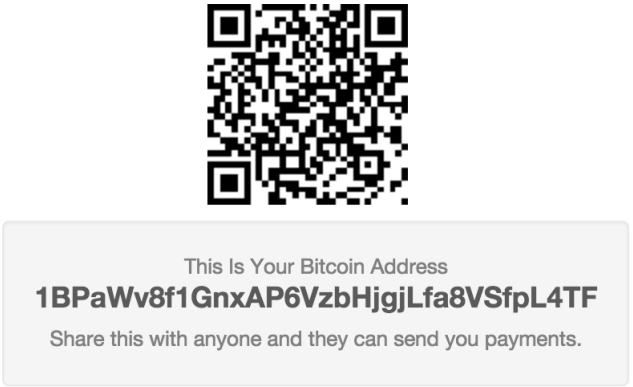
за преношење кључева између новчаника.
Најчешће коришћени формати приватних кључева поред оригиналног су:

- Хексадекадни
- Base58 WIF (Wallet Import Format)
- Мини приватни кључ
- Приватни кључеви BIP38 заштићени шифром (више у одељку 3.4.1)

Хексадекадни кључ је величине 32 бајта и се састоји од 64 карактера хексадекадног записа. Пример:

$$a1a41b0a7a496ca0c6d326a5654cebbf9ad64f946f24a29fe7883632e9c3b23f$$

Base58 WIF је формат који се најчешће користи за репрезентацију приватних кључева као и у баркод и QR код репрезентацијама адреса [8], слика 5 приказује пример QR кода за биткоин адресу. Формат Base58 WIF користи Base58Check кодирање и има заштиту од грешака у транскрипцији. На почетак сваког кључа се додаје префикс 5 за Base58 WIF формат, K или L за компресовани Base58 WIF формат.



Слика 5: Пример QR кода за биткоин адресу

Компресовани јавни кључеви су уведени како би се смањила величина трансакција и сачувала меморија на чворовима који чувају ланац блокова. Већина трансакција чувају у себи и јавни кључ, који се користи за валидацију величине је 520 бита, што када се помножи са хиљаде трансакција које се обаве дневно доводи до значајне количине података коју

треба чувати на чвору. Јавни кључ је тачка (x, y) на кривој $y^2 = x^3 + 7$ из одељка и свака координата је величине 256 бита. Уколико знамо x координату, y координату можемо израчунати решавањем једначине $y^2 \pmod{p} = (x^3 + 7)$. Стога је могуће чувати само x координату јавног кључа и добити на уштеди меморије од 50%.

Компресовани приватни кључеви су приватни кључеви из којих се могу изводити само компресовани јавни кључеви. Супротно имену они су заправо за један бит дужи од кључа у обичном Base58 WIF формату због контролног бита $0x01$ који се додаје на крај хексадекадног записа који означава да је кључ компресован.

Процес генерисања WIF приватног кључа је следећи:

1. На хексадекадни запис кључа додаје се префикс $0x80$ за *mainnet* или $0xef$ за *testnet* мрежу

   $80a1a41b0a7a496ca0c6d326a5654cebbf9ad64f946f24a29fe7883632e9c3b23f$

2. На крај хексадекадног записа се додаје контролни бит $0x01$ ако кључ треба компресовати

3. Затим се примењује SHA-256 хеширање на тако проширеном кључу; добијени хеш

   $e1a97a60ea26c55dca54790dcac2db1bbd9a2db78f7f75e4c9139ceb490dd14d$

4. Применом SHA-256 хеширања на хеш из корака 3 добија се хеш

   $620c220e750eaac119b253ad9b24c890761948c01c8393c1e5f0d8debca074be$

   од кога се узимају прва 4 бита као контролни збир $620c220e$

5. Додавањем контролног збира из корака 4 на кључ из корака 1 добија се хексадекадни запис кључа

   $80a1a41b0a7a496ca0c6d326a5654cebbf9ad64f946f24a29fe7883632e9c3b23f620c220e$

6. Хексадекадни запис из корака 5 се затим кодира Base58Check кодом и добија се кључ

   $5k3uv5maroerdev5oumitprw42lgda4czdjqy9dc378tw9ccggd$

3.4 Посебне варијанте кључева и адреса

Постоје неки интересантни формати кључева и адреса, као и начини да се они чувају. Један од формата адреса су скрипте за плаћање. Скрипте су у суштини листе инструкција које описују начин на који се врши трансакција за одређену адресу. Интересантан начин чувања кључева је шифровати их неком фразом.

3.4.1 Шифровани приватни кључеви (BIP-38)

Важно је истаћи да формати кључева не шифрују кључеве већ само олакшавају коришћење истих. Уколико би корисници желели да додатно осигурају своје кључеве од хакера или од крађе, морали би их шифровати на неки начин. Обичан корисник би морао да поседује велико техничко знање како би то извео исправно. Стога је BIP-38 [9] увео могућност шифровања приватних кључева. BIP-38 подразумева шифровање кључа, уобичајено у формату Base58 WIF, AES блок шифром AES256. Функција AES256Encrypt прима као улаз лозинку коју корисник зада у формату 256 битне фразе. Резултат је кључ који почиње префиксом 6P ради назначавања новчанику да кључ прво треба да се дешифрује функцијом AES256Decrypt и пребаци у формат Base58 WIF. Шифровани приватни кључеви омогућавају кориснику додатни степен заштите од крађе или доспећа кључа у посед трећег лица услед губитка кључа. Ово је нарочито корисно код папирних новчаника о којима ће бити више речи у одељку 3.4.4.

3.4.2 Pay-to-Script Hash (P2SH) и Multisig адресе

Код обичних биткоин адреса које почињу бројем 1 најчешћи тип трансакције је *плаћање ка хешираном јавном кључу* (енгл. *Pay to pubkey hash*, *P2PKH*). За валидирање овог типа трансакције неопходан је потпис поруке и хеш јавног кључа. За разлику од обичних биткоин адреса, посебне биткоин адресе које почињу бројем 3 користе тип трансакције *плаћање ка хешираној скрипти* (енгл. *Pay to script hash*, *P2SH*). Да би се валидирала трансакција овог типа потребне су додатне операције које се дефинишу при креирању адресе.

3.4.3 Персонализоване адресе

При генерисању валидне биткоин адресе може да се деси да она садржи смислен низ карактера. Уколико би корисник желео да има адресу која има неку кључну реч (нпр. $1MatfBG314....$) у називу, не постоји

могућност да утиче на то у самом процесу генерисања адресе. Како би направио персонализовану адресу корисник мора да генерише приватни кључ, изведе јавни кључ на основу приватног, генерише биткоин адресу и понавља поступак док не добије адресу жељеног облика. Сложеност процеса генерисања адресе је велика и тежина зависи од дужине речи коју корисник жели да адреса садржи.

Дужина	Жељена реч	Просечно време претраге
1	1M	<1 милисекунде
2	1Ma	50 милисекунди
3	1Mat	<2 секунде
4	1Matf	1 минут
5	1MatfB	1 сат
6	1MatfBG	2 дана
7	1MatfBG3	3-4 месеца
8	1MatfBG31	13-18 година
9	1MatfBG314	800 година

Табела 2: Време потребно за налазак адресе у односу на дужину појма

На основу података из табеле 2 види се да је узалудно тражити адресе са жељеном речју дужом од 6-7 речи. Могуће је превазићи ову препреку и користити сајтове за проналажење адресе помоћу више рачунара али то није препоручљиво из безбедносних разлога. Треће лице које генерише адресу може задржати приватни кључ везан за њу и тиме преузети власништво над средствима. Важно је напоменути да биткоин адресе (укључујући и персонализоване адресе) не треба поново користити након употребе у трансакцији [10] због очувања приватности трансакције.

По питању безбедности, персонализоване адресе су у суштини обичне биткоин адресе, али могу потенцијаљно да изазову један безбедносни проблем. Било ко може да направи адресу са одређеним бројем истих почетних карактера. Уколико корисник рецимо адресу за уплату подели на неком сајту и користи само њу уместо генерисања нове адресе за сваку трансакцију, треће лице са приступом сајту би могло да подметне своју адресу уместо оригиналне адресе и тако преусмери средства себи.

3.4.4 Папирни нованици

Папирни новчаници нису ништа друго до приватни кључеви записани на папирном медијуму. Поред кључева могу бити складиштене и адресе

ради удобности коришћења, како би се новчаници лакше идентификовали. Чување адреса није неопходно јер могу бити генерисане на основу кључа. Ефикасан начин чувања кључева је у формату QR кода ради лакшег импортовања у клијентске апликације (видети пример на слици 6). Папирни новчаници могу представљати безбеднији начин чувања кључева него чување на рачунару или у хардверским уређајима, уколико се правилно чувају. Препорука је да се кључеви и адресе генеришу на рачунару који није прикључен на интернет и да се штампају на уређају који такође није прикључен на интернет. Новчаник је најбоље чувати у сефу отпорном на ватру. Како би се додатно заштитили од крађе, кључеве је могуће прво трансформисати у неки од формата описан у одељку 3.3.2. Најчешће се кључеви шифрују неком фразом помоћу шеме BIP-38 објашњене у одељку 3.4.1.

Слика 6: Пример папирног нованика у QR формату који садржи биткоин адресу и приватни кључ

4 Новчаници

Биткоин новчаник служи сличној сврси као и електронски новчаник, омогућава извршавање долазних и одлазних трансакција. Разлика је у томе што биткоин новчаник не чува биткоине него кључеве и адресе корисника. У зависности од типа медијума новчаник може бити физички и електронски. Посебан подтип електронског новчаника је веб новчаник. Веб новчаник не чува кључеве него их чува и складишти код трећег лица.

4.1 Преглед технологија реализације нованика

Као што је наглашено, новчаници не чувају износ који корисник поседује. Величина износа се чува у ланцу блокова који чува податке о трансакцијама за сваку адресу. Новчаници омогућују примање средстава на адресе које садрже и плаћање ка адресама помоћу приватних кључева које чувају. Уколико новчаник има приступ ланцу блокова, он може и да прикаже кориснику баланс његових средстава. Новчаник може да генерише нове приватне кључеве који одређују адресе за уплату ка кориснику. Новчаници се разликују по начину чувања кључева и деле се на недетерминистичке и детерминистичке новчанике.

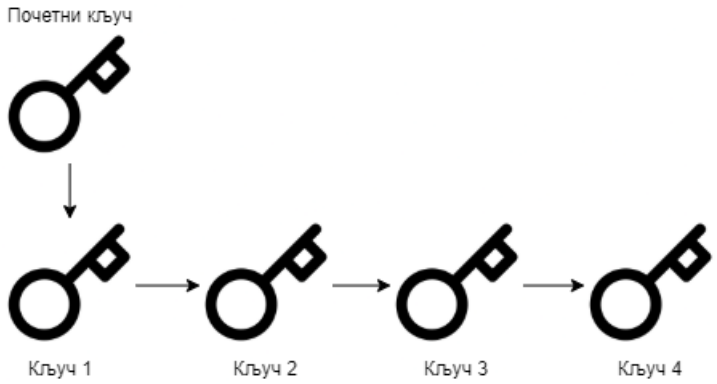
4.1.1 Недетерминистички новчаници

Новчаник складишти приватне кључеве и адресе. Према оригиналној имплементацији пожељно је генерисати пар (кључ, адреса) за сваку трансакцију коју корисник жели да обави, било да је то слање или примање. Када неко пошаље средства на неку од адреса корисника (садржаних у новчанику), корисник ту адресу не би требало поново да користи [10]. Ово доводи до нагомилавање кључева и адреса које је потребно чувати у новчанику. Такође је неопходно правити резервне копије свих кључева који се налазе у новчанику, што може бити захтевно са повећањем броја кључева. Овакви типови новчаника који чувају случајно генерисане кључеве се називају недетерминистичким новчаницима.

4.1.2 Детерминистички новчаници

Мана недетерминистичких новчаника јесте неефикасно чување и прављење резервних копија, јер је са сваким додавањем кључа у новчаник неопходно поновно прављење резервне копије целог новчаника. Величина копије расте са бројем кључева. Ово може бити веома неефикасно

уколико се користе хардверски или папирни новчаници. Како би се то превазишло, могуће је користити новчанике који уместо генерисања новог кључа за сваку трансакцију користе главни (мастер) кључ. Тај кључ је заправо почетна вредност (енгл. *seed*) на основу које се генеришу кључеви који се складиште у новчанику. Сваки нови кључ је генерисан на основу претходног и формира се ланац као на слици 7. Овакви новчаници се називају детерминистички новчаници. При прављењу резервне копије или пребацивању у други новчаник довољно је користити само почетни кључ, јер је на основу њега могуће реконструисати све изведене кључеве.



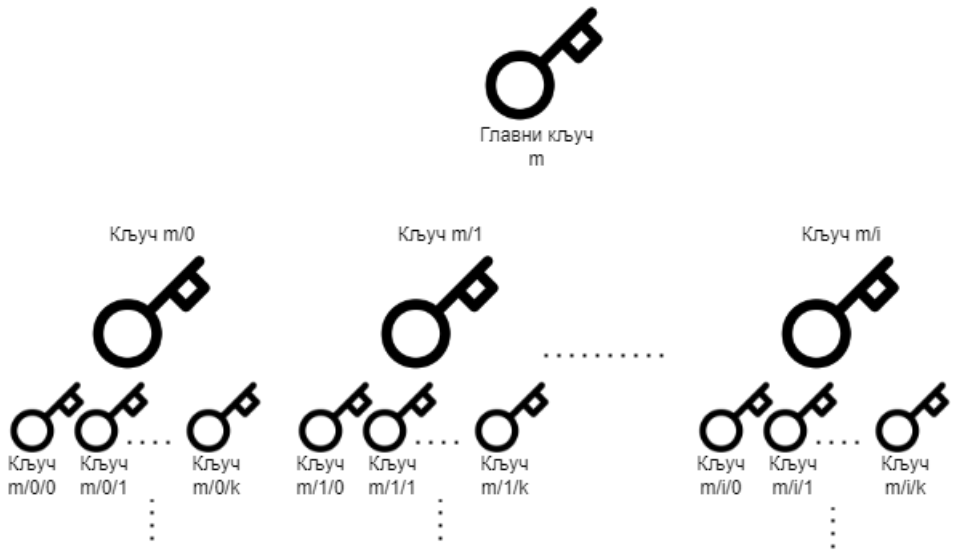
Слика 7: Изглед ланца кључева у детерминистичком новчанику

4.1.3 ХД новчаници (BIP-32 и BIP-44)

Хијерархијски детерминистички новчаници (енгл. *Hierarchical Deterministic wallets - HD wallets*, у даљем тексту ХД новчаници) су детерминистички новчаници код којих се уместо ланца формира хијерархијска структура кључева. Структура која се користи за имплементацију хијерархије је стабло. Предност стабла у односу на ланац кључева је првенствено практичније коришћење. Најчешћи пример где је ово корисно је у случају компанија, где сваку грану може да контролише одређени одељак фирме. ХД новчаници су детерминистички новчаници типа 2, који омогућују потпуно одвајање креирања јавних и приватних кључева, што доводи до повећане сигурности. Постоје два различита стабла за приватне и јавне кључеве који се креирају из јединственог главног кључа. Слика 8 приказује структуру ХД новчаника. Сваки ниво може да садржи максимално $2^{32}-1$ кључева, где је опсег $[0, 2^{31}-1]$ резервисан за приватне, а опсег $[2^{31}, 2^{32}-1]$ је резервисан за јавне кључеве. Хијерархија у теорији може да садржи бесконачан број нивоа, али у пракси

је тај број ограничен меморијом новчаника.

Иако пружају многе погодности, у тренутку њиховог стварања није било могуће пребацивање кључева из новчаника једног типа имплементације у други. Стандард BIP-32 [11] је развијен у ту сврху и предлаже детаљну спецификацију новчаника и дефинише структуру хијерархије. Стандард BIP-43 [12] је уведен да исправи мане стандарда BIP-32 и предложи коришћење првог слоја хијерархије за одређивање сврхе новчаника. Сврха новчаника може бити само за примање, плаћање или оба. Стандард BIP-44 [13] представља надоградњу стандарда BIP-43 и уведен како би се омогућило коришћење хијерархије новчаника са више налога и употреба новчаника за друге крипто валуте.



Слика 8: Хијерархија кључева: i/k индекс $[0, 2^{32} - 1]$

4.1.4 Лозинке и мнемонички кодови (BIP-39)

Бирање јаке лозинке из које се генерише главни кључ је веома важан корак при коришћењу ХД новчаника. У оригиналној имплементацији ХД новчаника лозинка је у бинарној или хексадекадној имплементацији и као таква није згодна за људску употребу и пребацивање у друге новчанике. Стандард BIP-39 предлаже начин генерисања лозинки на основу речи енглеског језика коришћењем мнемоничких кодова [14]. Стандард BIP-39 садржи списак од 2048 речи енглеског језика, тако да свака реч замењује 12 бита лозинке. Могуће је да човек одабере одређен број речи као лозинку или да новчаник насумично одабере речи. Број речи који се сматра довољним за остваривање добре безбедности је 12. Број комби-

нација са 12 речи је 2048^{12} што се може пребацити у основу 2, тј. 2^{132}, што је слично јачини приватног кључа (128 бита) [15]. Мана стандарда BIP-39 је коришћење фиксног скупа речи, јер може олакшати упад неовлашћеним лицима [16].

4.1.5 Препоруке за употребу биткоин новчаника

Како је технологија напредовала, временом су дефинисани стандарди који су постали широко прихваћени. Стандарди примарно служе да олакшају коришћење, повећају компатибилност, сигурност и флексибилност.
Неки од стандарда су:

- Мнемоничке кодне речи (засноване на препоруци BIP-39)
- ХД новчаници (засновани на препоруци BIP-32)
- Вишенаменска структура ХД новчаника (заснована на препоруци BIP-43)
- Новчаници који подржавају више налога и више валута (засновани на препоруци BIP-44)

Ови стандарди су прихваћени и користе се у имплементацији великог броја софтверских и хардверских новчаника што доприноси компатибилности између њих. Могуће је прекопирати мнемоник из једног новчаника и пребацити у други, а да притом остану сачуване све трансакције, кључеви и адресе.

Међу софтверским новчаницима који користе поменуте стандарде су Breadwallet, Copay, Multibit HD, и Mycelium, а од хардверских новчаника Keepkey, Ledger, и Trezor.

4.2 Детаљи реализације речника

У овом одељку обрадићемо стандарде мнемоничких кодних речи и ХД новчаника заснованих на мнемоницима.

4.2.1 Мнемоничке кодне речи (BIP-39)

Мнемоничке кодне речи су низ речи које кодирају случајно одабрани број, који се користи као главни кључ детерминистичног новчаника. Лозинка је довољана за поновно креирање главног кључа и помоћу њега

поново креира новчаник и све изведене кључеве. Апликација за креирање новчаника која имплементира детерминистички новчаник са мнемоничким кодним речима приказује кориснику низ од 12 до 24 речи при првом креирању новчаника. Тај низ речи је резервна копија новчаника и користи се опоравак и поновно креирање свих кључева у истом или било ком компатибилном новчанику. Мнемоничке кодне речи олакшавају корисницима да направе резервне копије новчаника, јер су лаке за читање и транскрипцију у поређењу са насумично одабраним низом бројева. Пример низа од 12 речи, редослед речи је битан: *van episode hotel digital soup situate surprise language salt elbow churn alpha.*

Мнемоничке кодне речи су дефинисане у препоруци BIP-39 [14]. Важно је напоменути да је BIP-39 само једна од примена стандарда са мнемоничким кодним речима. Постоје други стандарди који користе другачије низове речи, које користи новчаник Electrum и настали су пре стандарда BIP-39. Стандард BIP-39 је предложила компаније која је направила хардверски новчаник Trezor и није компатибилан са имплементацијом новчаника Electrum. Стандард BIP-39 је у међувремену добио подршку индустрије и постао де факто индустријски стандард.

4.2.2 Креирање ХД новчаника на основу мнемоника

ХД новчаник аутоматски генерише мнемоничке кодне речи коришћењем стандардизованог процеса дефинисаног у препоруци BIP-39. Новчаник почиње од извора ентропије (случајно одабраног низа бројева) и мапира га у низ речи:

- Прављење ентропије величине 128 до 256 бита
- Прављење контролног збира ентропије на основу првих 32 бита његовог хеша SHA256
- Додавање контролног збира на крај ентропије
- Подела низа у делове од 11 бита
- Мапирање сваке 11-битне вредности у реч из предефинисаног BIP-39 речника од 2048 речи
- Мнемонички код је добијени низ од 12 до 24 речи

5 Сигурност биткоина

Биткоине је, као и остале скупоцености, неопходно чувати од лица која желе да их украду. За разлику од физичких скупоцености које не могу да се дуплирају, биткоин може да се обезбеди прављењем копије. Приватни кључ представља доказ о поседовању биткоина и биткоине може потрошити само особа која поседује приватни кључ. Уколико се приватни кључ изгуби, губи се и приступ самим биткоинима. Приватни кључ је представљен низом битова и може се обезбедити прављењем резервне копије (енгл. *backup*) као и сваки други фајл. Прављење копије не значи да човек поседује више биткоина, јер када се приватни кључ једном искористи за потписивање трансакције, не може се поново употребити за трошење истих биткоина. Стога је неопходно размотрити како складиштити приватне кључеве и како их правилно обезбедити.

5.1 Сигурносни принципи

Сигурност система биткоин је заснована на разлици у односу на традиционални банкарски систем. Банкарски систем је централизован и сви подаци се чувају у самој банци. Уколико би треће лице доспело у посед броја банковног рачуна и пин кода, оно би могло да лиши купца свих његових средстава. Из тог разлога банкарски систем се ослања на разне сигурносне принципе укључујући и криптографију како би се спречио упад неовлашћеног лица у систем.

Због начина на који је биткоин систем имплементиран, није потребно користити шифровање за чување ланца блокова, свако има приступ бази података. Чињеница да је систем децентрализован има веома битну последицу, а то је померање имплементације сигурности са система на корисника система. Кориснику без техничког знања ово може представљати препреку и постоје препоруке за постизање сигурности обрађене у одељку 5.2.

Предлог за унапређивање протокола биткоина (енгл. *Bitcoin Improvement Proposal*, BIP[1]) је документ који обично састављају људи који раде на развоју биткоина. То су обично људи који унапређују Bitcoin Core.

5.2 Препоруке за постизање сигурности корисника

Према истраживању института Cane Island [17] сваке године 4% биткоина се неповратно губи због губитка приступа.

[1]Више о самим предлозима може се пронаћи на линку BIP

5.2.1 Физичко чување биткоина

Због лакоће употребе корисници често бирају да своја средства чувају у новчаницима који имају интернет конекцију ради комуникације са биткоин системом. Корисници могу с правом бити скептични према овом начину чувања средстава, јер је сваки уређај прикључен на интернет подложан неовлашћеним упадима и треба га додатно обезбедити. Ипак, приватни кључеви нису ништа друго до веома дугачки бројеви и као такви могу да се чувају и на физичком медијуму. Тај медијум може бити папир или USB-стик. Ти кључеви нису конектовани на интернет, па стога није неопходно користити шифровање, али су подложни крађи или губитку, па се стога се морају прикладно обезбедити. Кључеви на оваквом типу складишта пре коришћења прво морају да се учитају у новчаник. Уколико се као медијум користи папир, препорука је кључеве претходно шрифровати 3.4.4. Није препоручљиво чувати средства искључиво у оваквим типовима новчаника[18].

5.2.2 Хардверски новчаници

Хардверски новчаници су офлајн физички уређаји специјализовани за чување кључева. Разликују се од обичних физичких медијума, јер имају могућност потписивања трансакција. То се постиже тако што обично комуницирају са клијентским софтвером на рачунару, најчешће путем УСБ конекције. Изглед самог новчаника је прилично једноставан, новчаник поседује мали екран на ком приказује детаље трансакције и дијалоге. Уз то поседује обично неколико дугмића за слање команди, као што су прихватање или одбијање трансакције. Примери хардверских новчаника су Ledger и Trezor (слика 9). Кориснику се препоручује да поред хардверског новчаника направи додатне резервне копије кључева. Ledger и Trezor омогућавају прављење резервне копије, јер су засновани на технологији детерминистичких новчаника.

Слика 9: Хардверски новчаници Ledger и Trezor

5.2.3 Разноврсност чувања

Људи често наводе децентрализован систем за обраду трансакција као предност биткоина у односу на банку, али често држе сва своја биткоин средства на једном централизованом месту, у једном новчанику. Како би се осигурали да чак и случају крађе кључа или губитка истог не изгубе сва своја средства, корисницима се препоручује да своје кључеве распореде на више новчаника. Пожељно је да новчаници буду различитих типова (онлајн, мобилни, десктоп, хардверски) и од различитих произвођача. Пример губитка средстава чуваних на једном месту је Џејмс Хауелс (James Howells) који је својих 8000 биткоина (вредност 184 милиона америчких долара на дан 4.08.2022.) чувао на хард диску који случајно бацио у смеће када је чистио стан.

5.2.4 Уравнотежење ризика

Корисницима се препоручује равнотежа између ризика од крађе и ризика од губитка кључа. У јулу 2011. године Стефан Томас (Stefan Thomas) је својих 7002 биткоина (вредност 162 милиона америчких долара на дан 4.08.2022.) чувао на виртуалној машини чији су подаци обрисани након ажурирања система виртуалне машине. Поседовао је и две резервне копије. Једну је чувао онлине на Dropboxu, а другу на шифрованом хард диску IronKey. Онлајн копија је изгубљена када је случајно прегажена другим подацима. Такође је изгубио шифру за хард диск IronKey, коју је чувао на комаду папира. IronKey корисницима даје десет покушаја пре него што подаци буду изгубљени; Стефану је остало још 2 покушаја [19].

5.2.5 Вишеструки потписи

Слично принципу дељеног банковног рачуна, где је потребан потпис оба власника (нпр. мужа и жене) да би се подигла средства, систем Биткоин подржава захтевање више дигиталних потписа ради верификовања трансакције. Ова пракса се посебно препоручује власницима више биткоина или власницима биткоина у корпоративној средини. Препорука је да се кључеви чувају децентрализовано, како би били отпорни на нападе хакера, или да би један власник био спречем да потроши сва средства без знања осталих власника. Број потписа који тренутно могу да се користе за трансакцију која захтева вишеструке потписе је 3, због имплементације скрипти које се користе за креирање биткоин трансакција [20].

6 Анализа имплементације новчаника у језику Пајтон

За потребе рада имплементирана су два новчаника: хладни хијерархијски детерминистички новчаник и обичан новчаник.

Хладни новчаник је задужен за генерисање и чување приватних кључева. Он није конектован на интернет ради заштите приватних кључева, стога он не може бити коришћен за проверу стања нити трошење средстава.

За те потребе је имплементиран новчаник који ће само да чува адресе (без кључева) и он има приступ интернету. Адреса је довољна да се утврди висина износа на датој адреси, као и прављење непотписане трансакције за трошење средстава. Ту трансакцију мора да достави хладном новчанику ради потписивања трансакције приватним кључем. Када добије потписану трансакцију, онда је доставља на биткоин мрежу преко биткоин чвора на који је прикључен. Када ова трансакција буде верификована од стране рудара, новац је успешно пребачен.

6.1 Генерисање почетне вредности и главног кључа

Генерисање мнемоничких кодних речи описано је у одељку 4.2.2. Сегмент кода *entropy_to_words(entbytes)* дефинише генерисање мнемоничких кодних речи на основу низа случајно генерисаних бројева. Као улаз прима ентропију величине 16 бајтова, то јест 128 бита. Скраћенице коришћене ради читљивијег кода: *ent-entropy*, *cs-checksum*, *m-mnemonic*.

```
words = entropy_to_words(os.urandom(16))

def entropy_to_words(entbytes,wordlist=wordlist_english):
  if(len(entbytes) < 4 or len(entbytes) % 4 != 0):
    raise ValueError("Not a multiple of 4 bytes")
  entropy_size=8*len(entbytes)
  csint,checksum_size = entropy_cs(entbytes)
  entint=int(binascii.hexlify(entbytes),16)
  mint=(entint << checksum_size) | csint
  mint_num_words=(entropy_size+checksum_size)//11

words = mnemonic_int_to_words(mint,mint_num_words,wordlist)
return ' '.join(words)
```

Прво проверавамо да ли је прослеђен бинарни кључ. Након тога се

генерише контролни збир величине једног бајта, помоћу алгоритма за хеширање *SHA256* . Сегмент кода *entropy_ cs(entbytes)* дефинише генерисање контролног збира на основу ентропије.

```
def entropy_cs(entbytes):
  entropy_size=8*len(entbytes)
  checksum_size=entropy_size//32
  hd=hashlib.sha256(entbytes).hexdigest()
  csint=int(hd,16) >> (256-checksum_size)
  return csint,checksum_size
```

Контролни збир се додаје на почетак ентропије и дели се у 11-битне сегменте. Сваки од сегмената се мапира у реч из фиксиране листе речи помоћу метода *mnemonic_ int_ to_ words*.

```
def mnemonic_int_to_words(mint,mint_num_words,wordlist=
    ↪ wordlist_english):
  backwords=[wordlist[(mint >> (11*x)) & 0x7FF].strip() for x
    ↪ in range(mint_num_words)]
  return backwords[::-1]
```

Након што је формирана листа речи она се смешта у новчаник. Препорука је направити више резервних копија ових речи на више различитих медијума.

Затим се мнемоници користе за генерисање почетне вредности за главни кључ помоћу методе *mnemonic_ to_ seed(words)* из библиотеке *cryptos*.

```
seed = cryptos.mnemonic_to_seed(words)
```

Главни кључ се генерише помоћу методе *bip32_ master_ key* која као аргументе прима почетну вредност као и назнаку да ли је кључ за *TESTNET* или *MAINNET* мрежу.

```
extended_private_key = cryptos.bip32_master_key(seed,
    ↪ TESTNET_PRIVATE)
```

За генерисање биткоин адреса потребан је јавни кључ, који се генерише на основу приватног помоћу методе *bip32_ privtopub*.

```
extended_public_key = cryptos.bip32_privtopub(
    ↪ extended_private_key)
```

Наредни сегмент кода демонстрира генерисање листе речи, почетне вредности, главног кључа и њему одговарајућег јавног кључа користећи претходно дефинисане методе:

```
def create_new_master_key():
  words = entropy_to_words(os.urandom(16))
  seed = cryptos.mnemonic_to_seed(words)
  extended_private_key = cryptos.bip32_master_key(seed,
    ↪ TESTNET_PRIVATE)
  extended_public_key = cryptos.bip32_privtopub(
    ↪ extended_private_key)
```

6.2 Генерисање хијерархије кључева

Након што смо генерисали главни кључ можемо да на основу њега формирамо изведене кључеве. Метода *bip32_ ckd* као аргумент прима родитељ кључ и индекс (редни број кључа у хијерархији) и враћа изведени приватни кључ на нивоу $+1$ са датим индексом. Главни кључ је једини на нивоу 0, стога сви кључеви изведени директно из њега су на нивоу 1. Сваки изведени кључ може се користити као кључ за извођење нових кључева. Уколико је индекс већи од 2^{31} а мањи од $2^{32} - 1$ онда је кључ који се генерише јавни. Скраћеница *ckd* потиче од *child key derivation*.

```
derived_private_key = cryptos.bip32_ckd(extended_private_key,
    ↪ 0)
derived_public_key = cryptos.bip32_ckd(extended_public_key, pow
    ↪ (2, 31)+1)
```

Када имамо изведени јавни кључ можемо га прекопирати у новчаник који је конектован на интернет и њега користимо за прављење биткоин адресе за примање новца. Приватни кључеви остају у офлајн новчанику и користе се за потписивање трансакција при потрошњи средстава.

Пошто сваки родитељ може да чува $2^{32} - 1$ кључева, што је 4 милијарде кључева, неопходно је имплементирати навигацију кроз кључеве. Као што је приказано на слици 8, сваки кључ има ознаку нивоа и индекса, које користимо да бисмо пронашли кључ који ће се користити за потписивање трансакције.

У наставку је приказан главни кључ као и један изведени кључ на основу насумично одабраног низа речи *"use public drive sad truck cheap bike common cherry leaf loan famous"*.

```
Master private key:
    ↪ tprv8ZgxMBicQKsPdzUr6bSTGyAFPoTCqBpguNcVLb97CTznsUbbYL27
    ↪ -h4pAyqzrHX9iLqd9vAQvivpZZ4pqunYjwgvYZ9uDz5BrNcZPjTtStfU
Master public key:
    ↪ tpubD6NzVbkrYhZ4XTWdzF73gNpMxpy8zX1bUgDGd7BQcjoBhxrNAiqh
    ↪ -sZS39wocXVYFiAg1e9jj7nPvcfDrcbRXHkVqCEQnMcy9fzaiEkVAYua
Derived private key:
    ↪ tprv8bgUhDHmUGJuBKSgHitTax1d9pHdeEYLTPLTqypHK93rhhdGZsJJ
    ↪ -Sxu2LTovCbrC8cJNp7soguFzDvaMHmynNLBS2EkQuUUMDgfh4WtYYwi
Derived public key:
    ↪ tpubD8NWqdKsGyTbs3hEvzCg8asWdcscoa5XK94yiUToUR6PuXnp76up
    ↪ -hY9Gd3cqtuHuR3NXnj84KM2ZNt2Yng1fxW1VYfMHAQoh91snDEBtraA
```

6.3 Прављење и потписивање трансакције

Онлајн новчаник се прво конектује на чвор Биткоин тестнет мреже са којим комуницира ради провере стања, креирања и верификације трансакција. За потребе апликације на рачунару је покренут цео чвор са целокупном историјом трансакција. На чвор се конектујемо методом *NetworkAPI.connect_to_node* библиотеке *bit* са назнаком да је мрежа на коју се конектујемо Тестнет мрежа, како бисмо могли да користимо тест биткоине.

```
node = NetworkAPI.connect_to_node(user='user', password='
    ↪ password', host='localhost', port=18332 , use_https=
    ↪ False, testnet=True)
```

Након што је конекција са чвором оспособљена, могуће је проверити стање средстава, као и слати новац. Пошто онлајн новчаник не чува приватни кључ, за слање новца прво је потребно направити непотписану трансакцију и проследити је хладном новчанику. Затим хладан новчаник потписује трансакцију одговарајућим приватним кључем и враћа потписану трансакцију онлајн новчанику. Онлајн новчаник потписану трансакцију шаље чвору где трансакција бива верификована. Након што је трансакција верификована средства на адреси се умањују за потрошену суму и тиме је процес слања средстава завршен.

Наредни сегмент кода демонстрира прављење непотписане трансакције:

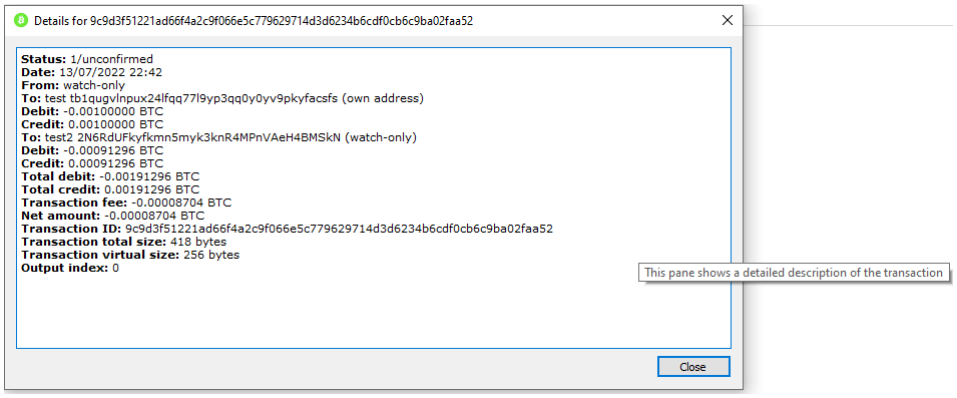
```
def create_raw_transaction(my_address, destination_address,
    ↪ amount):
  version = VERSION_1
  lock_time = LOCK_TIME
  outputs = construct_outputs([(destination_address, amount)])
  inputs = []
  for unspent in node.get_unspent_testnet(my_address):
    script_sig = b''  # empty scriptSig for new unsigned
    ↪ transaction.
    tx_id = hex_to_bytes(unspent.txid)[::-1]
    tx_index = unspent.txindex.to_bytes(4, byteorder='little')
    amount = int(unspent.amount).to_bytes(8, byteorder='little'
    ↪ )
    sequence = unspent.sequence.to_bytes(4, byteorder='little')
    inputs.append(TxIn(script_sig, tx_id, tx_index, amount=
    ↪ amount, segwit_input=unspent.segwit, sequence=sequence))

  tx_unsigned = TxObj(version, inputs, outputs, lock_time)
  print(version, inputs, outputs, lock_time)

create_raw_transaction("2N6JuNZ5HbpbVbtc5vxmzaDzsWpfkCFqZqY", "
    ↪ 2MsNZDZSqpfbm74M9wu9i9gXDPAYQYhJSKg", 80000)
```

Све методе које су коришћене су методе библиотеке *bit.transaction*.

За потписивање трансакције користи се метода *transaction.sign_tx*. Подразумева се да смо претходно пронашли приватни кључ којим треба потписати трансакцију. Након што имамо потписану трансакцију шаљемо је на мрежу ради верификације.

```
tx_signed = transaction.sign_tx(private_key, tx_unsigned,
    ↪ unspents)
node.broadcast_tx_testnet(tx_signed)
```

Тестнет мрежа захтева 6 потврда како би трансакција била верификована. Слика 10 приказује прозор са детаљима трансакције као и статус верификације.



Слика 10: Статус верификације трансакције, прва потврда од неопходних 6

7 Закључак

У овом раду приказана је имплементација Хијерархијског детерминистичког новчаника као и технологије и криптографски принципи на којима је заснован систем Биткоин. Овај тип новчаника пружа висок ниво безбедности, где чак иако нападач доспе у посед једног приватног кључа, он не може да приступи осталим кључевима на истом нивоу хијерархије, нити изнад, већ само кључевима који су из њега изведени.

Хијерархијски детерминистички новчаници су значајни по томе што могу да садрже више валута, не само биткоине, где свака грана може да буде засебна валута. Због значаја система Биткоин коришћени су биткоини, али будући радови могу унапредити апликацију тако што ће омогућити коришћење осталих валута подржаних од стране коришћених библиотека, као што су Доџкоин (енгл. *Dogecoin*) и Лајткоин (енгл. *Litecoin*).

Литература

[1] Satoshi Nakamoto. "Bitcoin: A Peer-to-Peer Electronic Cash System". У: *Cryptography Mailing list at https://metzdowd.com* (мар. 2009.).

[2] Richard A. Mollin. *RSA and Public-Key Cryptography*. Chapman и Hall/CRC, 2002. ISBN: 978-1584883388.

[3] Darrel Hankerson, Alfred Menezes и Scott Vanstone. *Guide to Elliptic Curve Cryptography*. Springer, 2004. ISBN: 978-0-387-21846-5.

[4] Daniel R. L. Brown. *Standards for Efficient Cryptography SEC 2: Recommended Elliptic Curve Domain Parameters*. on-line на: `https://www.secg.org/sec2-v2.pdf`. 2010.

[5] Henri Gilbert и Helena Handschuh. *Security Analysis of SHA-256 and Sisters*. Springer, Berlin, Heidelberg, 2004. ISBN: 978-3-540-24654-1.

[6] Hans Dobbertin, Antoon Bosselaers и Bart Preneel. *RIPEMD-160:A Strengthened Version of RIPEMD*. Springer, Berlin, Heidelberg, 2005. ISBN: 978-3-540-49652-6.

[7] Andreas M. Antonopoulos. *Mastering Bitcoin: Programming the Open Blockchain*. O'Reilly Media, Inc., 2014. ISBN: 978-1491954386.

[8] *Wallet import format*. on-line на: `https://en.bitcoin.it/wiki/Wallet_import_format`.

[9] Mike Caldwell и Aaron Voisine. *Passphrase-protected private key*. on-line на: `https://github.com/bitcoin/bips/blob/master/bip-0038.mediawiki`. 2012.

[10] *Address reuse*. on-line на: `https://en.bitcoin.it/wiki/Address_reuse`.

[11] Pieter Wuille. *Hierarchical Deterministic Wallets*. on-line на: `https://github.com/bitcoin/bips/blob/master/bip-0032.mediawiki`. 2012.

[12] Marek Palatinus и Pavol Rusnak. *Purpose Field for Deterministic Wallets*. on-line на: `https://github.com/bitcoin/bips/blob/master/bip-0043.mediawiki`. 2014.

[13] Marek Palatinus и Pavol Rusnak. *Multi-Account Hierarchy for Deterministic Wallets*. on-line на: `https://github.com/bitcoin/bips/blob/master/bip-0044.mediawiki`. 2014.

[14] Marek Palatinu, Pavol Rusnak, Aaron Voisine и Sean Bowe. *Mnemonic code for generating deterministic keys*. on-line на: `https://github.com/bitcoin/bips/blob/master/bip-0039.mediawiki`. 2013.

[15] *Seed phrase*. on-line на: https://en.bitcoin.it/wiki/Seed_phrase.

[16] Thomas Voegtlin. *Electrum Seed Version System*. on-line на: https://electrum.readthedocs.io/en/latest/seedphrase.html#motivation. 2017.

[17] Cane Island Alternative Advisors LLC. *There Will Never Be More Than 14 Million Bitcoins*. on-line на: https://static1.squarespace.com/static/5d580747908cdc0001e6792d/t/5e98dde5558a587a09fac0cc/1587076583519/research+note+4.17.pdf. 2020.

[18] *Storing bitcoins: Bad wallet ideas*. on-line на: https://en.bitcoin.it/wiki/Storing_bitcoins#Bad_wallet_ideas.

[19] New York Times. *Lost Passwords Lock Millionaires Out of Their Bitcoin Fortunes*. on-line на: https://www.nytimes.com/2021/01/12/technology/bitcoin-passwords-wallets-fortunes.html?auth=link-dismiss-google1tap.

[20] Pedro Franco. *Understanding Bitcoin: Cryptography, Engineering and Economics*. Wiley, 2014. ISBN: 978-1-119-01916-9.