Univerza v Ljubljani
Fakulteta za računalništvo in informatiko

Matej Arčon

Tehnologija veriženja blokov

diplomsko delo

visokošolski študijski program
prve stopnje
računalništvo in informatika

Mentor: doc. dr. Tomaž Dobravec

Ljubljana, 2018

Besedilo je oblikovano z urejevalnikom besedil LaTeX.

Fakulteta za računalništvo in informatiko izdaja naslednjo nalogo:

Tematika naloge:

V diplomskem delu preglejte in podrobneje predstavite tehnologijo veriženja blokov. Osredotočite se tako na zgodovino nastanka kot tudi na uporabo tehnologije v sedanjosti. Predstavite arhitekturo, ki omogoča uporabo te tehnologije ter pripadajoče varnostne mehanizme. Opišite tudi nekaj primerov uporabe tehnologije veriženja blokov v sodobnih aplikacijah.

Zahvaljujem se mentorju, doc. dr. Tomažu Dobravcu, za pomoč pri sestavljanju diplomske naloge in družini, ki mi je omogočila študij ter me pri tem ves čas podpirala.

Kazalo

Povzetek

Naslov: Tehnologija veriženja blokov

Avtor: Matej Arčon

Tehnologija veriženja blokov je danes ena najodmevnejših novosti v svetu računalništva. Čeprav so izdelki, ki uporabljajo to tehnologijo, še v zgodnjih fazah razvoja, se zdi, da imajo velike možnosti za izboljšanje življenja ljudi na različnih področjih. Širši javnosti je najbolj znana uporaba veriženja blokov na finančnem področju, predvsem pri poslovanju s tako imenovanimi kriptovalutami, vendar ima lahko tehnologija veriženja blokov veliko širši obseg uporabe. V diplomski nalogi bi rad opisal, kako tehnologija deluje, kakšne spremembe prinaša trenutni infrastrukturi hranjenja podatkov, hkrati pa osvetlil, kakšne so možnosti uporabe tehnologije tudi na drugih področjih.

Ključne besede: veriženje blokov, kriptovalute, omrežje Bitcoin.

Abstract

Naslov: The blockchain technology

Avtor: Matej Arčon

The blockchain technology is one of the most hyped new computer technology of our time. Even though the products using the blockchain technology are still in their infancy it seems that the technology harnesses a lot of potential in various use cases. The public first heard of the blockchain technology by means of financial use cases, but the reach of the technology could be far greater. So the motivation behind my thesis is to present the workings of the blockchain technology, which innovations it brings to the way we collect data and show how the technology could be used for alternative use cases, not just in the area of financials.

Keywords: blockchain, cryptocurrency, Bitcoin network.

Chapter 1

Uvod

Ljudje se že od nekdaj povezujemo v večje skupnosti. Zaradi vse večje globalizacije je bilo potrebno ustvariti organizacijske sisteme, ki bi skrbeli za učinkovito delovanje velikih množic ljudi. Za te sisteme pa se je sčasoma pokazalo, da bolj služijo ljudem, ki te sisteme postavljajo, kot pa tistim, ki so del sistema in ki naj bi jim ti sistemi olajšali življenje. Zaradi tega se je določena skupina ljudi odločila, da poišče sistem, ki deluje v dobro uporabnika, ne glede na njegov socialni položaj, spol, nacionalnost, vero ali raso, in ki ne sloni na zaupanju v dobronamernost vpletenih v sistemu.

Rast prebivalstva je vplivala na kopičenje vedno večje količine podatkov tako o posameznikih kot tudi o razmerjih med njimi. To je sprožilo razvoj digitalnega hranjenja različnih podatkov in avtomatiziranje interpretacije podatkov v uporabne informacije. Sčasoma se je začela digitalizacija širiti na vse več področij človekovega vsakdanjika in pojavile so se ideje o digitalnem denarju.

Do sedaj najuspešnejša implementacija elektronskega denarja so kripto valute. Vendar pa le-te za svojo tehnično implementacije skrivajo veliko bolj daljnosežen potencial v obliki tehnologije veriženja blokov. Iznajdba tehnologije veriženja blokov je pokazala možnost za velike spremembe tako v svetu računalništva kot tudi družbe nasploh. Na krilih popularnosti kriptovalut je tudi zanimanje za tehnologijo veriženja blokov v kratkem času

skokovito naraslo.

Namen moje diplomske naloge je, predstaviti tehnologijo veriženja blokov, njene koncepte in implementacijo. Razlaga ozadja tehnologije se mi zdi pomembna, ker se je zaradi navala navdušenja nad njo le-to pozabilo podrobneje preučiti in začelo širiti napačne informacije ali jo omejevati zgolj na kriptovalute, namesto pogledati širše.

Chapter 2

Zgodovina in razlogi za nastanek tehnologije veriženja blokov

Tehnologija veriženja blokov je svojo prvo uporabo v praksi doživela s kriptovaluto bitcoin leta 2009, vendar pa so teoretični zametki tehnologije v glavah računalniških strokovnjakov doživeli rojstvo že v osemdesetih letih prejšnjega stoletja.

2.1 Subkultura *Cypherpunk*

Z razvojem in širjenjem računalnikov v vedno večje število področij človekovega vsakdanjika, se je med nekaterimi računalniškimi strokovnjaki pojavila bojazen, da bi lahko institucije in vladne organizacije s podatki, ki jih hranijo o posameznikih, ustvarile tako imenovani orvelijanski svet – svet v podobi distopične vizije ameriškega pisatelja Georga Orwella (predstavljene v romanu z naslovom 1984), ki mu vlada masovno nadziranje ljudi ter širjenje propagande in neresnic. Eden od prvih strokovnjakov, ki so bojazen izpovedali javnosti, je David Chaum, ki je leta 1985 objavil študijo z naslovom *Security without identification: Transaction systems to make Big Brother obsolete*, kjer predlaga uporabo kriptografskih metod za izmenjavo raznih podrobnosti

o transakcijah med posameznikom in institucijami, ki vračajo moč odločanja o meri lastne zasebnosti obema udeležencema v transakcijah. Prav tako je v študiji predstavil tudi idejo o elektronskem plačevanju [7]. Študija neuradno velja za navdih za začetek subkulture Cypherpunk. Nadalje se je subkultura razvijala preko komunikacije z uporabo poštnega seznama (ang. *mailing list*), začetega s strani Erica Hughesa, Timothyja Maya in Johna Gilmoreja. Z začetkom poštnega seznama se pojavi tudi termin cypherpunk, ki je skovanaka iz angleške besede za šifro *cipher* in imena umetniškega žanra *cyberpunk*, katerega zgodbe se večinoma dogajajo v distopični prihodnosti, ki je rezultat zlorabe visokotehnološkega napredka. Poštni seznam je samo med leti 1992 in 1994 nabral 700 naročnikov. Pripadnike subkulture *cypherpunk* druži zanimanje za kriptografijo, mišljenje, da bi moral posameznik imeti pravico do ohranjanja svoje zasebnosti in zavzemanje za preprečevanje nepotrebnega vmešavanja politike v različne poglede človekovega vsakdanjika. Na podlagi napisanega v njegovi študiji o bitcoinu je razvidno, da je Nakamoto določen del motivacije za razvoj omrežja bitcoin dobil od subkulture *cypherpunk* in z njimi deli določena prepričanja o pomembnosti ohranjanja zasebnosti ljudi s pomočjo kriptografije.

2.2 Omrežje bitcoin

Čas nastanka tehnologije veriženja blokov je vzporeden s časom nastanka ideje o kriptovaluti bitcoin. Ideja za omrežje je v javnost prvič prišla oktobra leta 2008 ob objavi študije z naslovom *Bitcoin: A Peer-to-Peer Electronic Cash System* [17]. Čeprav v študiji tehnologija veriženja blokov ni eksplicitno omenjena ali poimenovana s tem terminom, v splošnem velja, da je prav omrežje bitcoin prva praktična uporaba te tehnologije. Študija je podpisana z imenom Satoshi Nakamoto, vendar o identiteti skrivnostnega avtorja ali morebitne skupine avtorjev študije ni veliko znanega, razen kar je mogoče razbrati iz študije in objav na forumih o bitcoinu [6]. Znano je tudi, da je razvil prvi bitcoin odjemalnik Bitcoin Core, v katerega je dodajal popravke do verzije 0.3.9 [4]. Objava študije sovpada s časom začetka globalne finančne

krize, za katero mnogi menijo, da je bila posledica pomanjkljive regulacije centraliziranega finančnega sistema, ki je podvržen manipulacijam akterjev znotraj institucij [9]. Lahko sklepamo, da je enakega sentimenta tudi razvijalec bitcoin-a, saj je v tako imenovanem *"Genesis bloku"*, ki je prvi blok omrežja, zapisan tekst "03/Jan/2009 Chancellor on brink of second bailout for banks", kar je naslov članka v časopisu *The Times*, kjer je opisano, kako je bil britanski kancler Alistar Darling pripravljen z davkoplačevalskim denarjem reševati banke, ki so bile zaradi posojil v krizi. Razvidno je, da je med glavnimi razlogi za nastanek omrežja Bitcoin nezadovoljstvo z trenutnim finančnim sistemom in poskus ustvarjanja boljše alternative.

Figure 2.1: Naslovnica časopisa *The times* dne 3. januarja 2009.

2.3 Razlogi za nastanek omrežja bitcoin

Z branjem študije Nakamota dobimo vpogled v motivacijo za ustanovitev elektronskega denarnega sistema. Glavna skrb Nakamota je dejstvo, da us-

trezno delovanje trenutnega denarnega sistema temelji na zaupanju. Zaupanje ima zelo pomembno vlogo v socializirani družbi, saj se je družba razvila v takšno, kot je danes, pretežno zaradi zaupanja v sisteme, kot so politični sistem, bančni sistem in monetarni sistem [13]. Ker ljudje zaupajo v demokratski sistem, grejo na volitve in izvolijo svoje predstavnike. Prav tako nosijo denar v banke, ker jim zaupajo in ker zaupajo v to, da bodo banke z njihovim denarjem ravnale pošteno in njihovo imetje zavarovale. Nakamoto v študiji o omrežju Bitcoin razloži, da četudi trenutni sistem v principu deluje, ustvarjanje transakcij med dvema osebkoma temelji na zaupanju v tretje osebe oz. finančne institucije, kot so npr. banke, ki pa se v preteklosti niso izkazale kot najbolj zaupanja vredne in so velikokrat bile glavni vzrok za razne finančne krize in hiperinflacije valute [12]. Zaradi tega je Nakamoto ustvaril sistem, kjer izmenjava osebnih finančnih sredstev ni odvisna od zaupanja v tretjo osebo, temveč od udeležencev v omrežju, ki skrbijo, da so podatki v omrežju točni. Dodatna skrb Nakamota je varstvo osebnih podatkov in zasebnost, kateri Nakamoto posveti v študiji cel razdelek. Po raznih škandalih v zvezi z zlorabljanjem osebnih podatkov je prišlo do potrebe po vse večjem varovanju osebnih podatkov. Pri vsakem spletnem nakupu je potrebno prodajalcem zaupati veliko osebnih podatkov in potem zaupati, da podatkov ne bodo izrabili. Uporaba kriptovalute bitcoin zaradi uporabe kriptografije skuša čim bolj povečati mero zasebnosti in anonimnosti pri izmenjavi podatkov.

Chapter 3

Koncepti tehnologije veriženja blokov

V ospredju tehnologije veriženja blokov sta dva termina: "blok" in "veriženje". Blok je podatkovna struktura, ki hrani podatke. V primeru omrežja bitcoin so to podatki o transakcijah, ki se tičejo kriptovalute bitcoin, na splošno pa lahko v blok zapišemo poljubne podatke, kot so razne datoteke, GPS koordinate, podatki o stanju naprav interneta stvari in tako naprej.

Termin veriženje se nanaša na to, kako so bloki povezani med seboj. Veriženje najprej doseže, da je znano časovno zaporedje blokov. Za nek blok vemo, da je njegov predhodnik nastal časovno pred njim, naslednji blok pa časovno za njim. Vsak blok ima v glavi zapisano zgoščeno vrednost (ang. *hash*) prejšnjega bloka in njegovo višino, ki pove, kateri je po vrsti v verigi (prvi blok ima višino 0). Protokol omrežja je zasnovan tako, da je splošno veljavna veriga tista, ki je najdaljša. Lahko se zgodi, da sta po omrežju naenkrat poslani dve enako dolgi verigi. Vozlišče tako naprej računa zgoščeno vrednost za tisto verigo, ki jo je prejelo najprej, vseeno pa shrani tudi drugo verigo oziroma drugi blok, v primeru da postane alternativna veriga tista, ki je najdaljša.

Tehnologija veriženja blokov je relativno sveža in še vzhajajoča tehnologija v svetu računalništva, o kateri se širi marsikatera polresnica, zato bom v tem

poglavju nanizal koncepte, ki združeni delajo tehnologijo veriženja blokov različno od preteklih tehnologij, kako so ti koncepti tehnično implementirani in kakšne prednosti prinašajo v primerjavi z ostalimi tehnologijami.

3.1 Decentralizacija

Decentralizacija je način ustvarjanja organizacijske strukture obratno od centralizacije. Če centralizacija pomeni, da je organizacijska kontrola strukture dodeljena eni točki ali centru, je decentralizacija pomikanje te kontrole na skupino enakovrednih točk. Večina sistemov, s katerimi imamo interakcijo in vplivajo na naše življenje kot posameznika, je centraliziranih. Takšen je npr. bančni sistem s centralnimi bankami, korporativni sistem z upravnimi odbori, politični sistem s parlamenti itn. Čeprav niso centralizirani sistemi sami po sebi nič slabega, vseeno obstajajo področja, katerim bolj služi decentraliziran kot pa centraliziran strukturni model.

Decentralizacija je pri veriženju blokov omogočena z pomočjo omrežja oblike vsak z vsakim (ang peer to peer network). Vsako tako imenovan vozlišče (ang. *node*) prejema transakcije, in ko je blok transakcij sestavljen, ga razpošlje vsem članom omrežja. Ostala vozlišča nato preverijo, ali so vse transakcije v bloku veljavne. Če so transakcije v bloku veljavne in je tudi struktura bloka pravilna, potem blok sprejmejo kot nadaljevanje verige in takoj začnejo zbirati nove, še nepotrjene transakcije, in začnejo ustvarjati nov blok vrh zadnjega bloka. Z decentralizacijo odstranimo potrebo po zaupanju v institucije, kot so banke, ki so se v preteklosti večkrat izkazale kot ne preveč zaupanja vredne in bolj zagrete za lasten dobiček kot pa za ustvarjanje kvalitetne storitve za stranke. V decentraliziranemu sistemu ni več potrebno zaupanje v nekoga, da bo ravnal je moralno in socialno koristno, ker za integriteto podatkov skrbijo vozlišča omrežja.

Tudi če je neka organizacija zagotovo vredna zaupanja, še vedno centralizirana struktura dopušča možnost, da z vdorom v centralno vozlišče pride do neavtoriziranega spreminjanja podatkov s strani zlonamerne osebe, kar je zaradi množice podatkov včasih zelo težko odkriti. V decentraliziranem

omrežju vsako polno vozlišče hrani kopijo najdaljše verige blokov, ki služi kot javna glavna knjiga (ang. *public ledger*) in v primeru, da zlonameren napadalec vdre v eno od vozlišč in spremeni podatke, potem to vozlišče nima več veljavne verige, kar je preverljivo z preverbo verige, ki jo hranijo druga vozlišča. Mehanizem je tako veliko bolj varen, saj ni enotne točke napada. Poleg tega so decentralizirane glavne knjige tudi bolj odporne proti napadu za zavrnitev storitve (ang. *Denial of service attack* ali DOS), ker če postane eno od vozlišč nedelujoče, je na voljo še veliko drugih, na katere se lahko obrneš, tako da decentralizirane aplikacija deluje naprej nemoteno ali z manjšo upočasnjenostjo.

3.2 Psevdonimnost

Živimo v časih, ko je vedno več govora o pomembnosti posameznikove zasebnosti. Razne korporacije in vladne organizacije imajo ob porasti uporabe digitalnih orodij, kot so socialna omrežja, v lasti vedno več osebnih podatkov in načinov nadziranja ljudi. Te podatke, za katere se marsikdo ne zaveda, da jih z uporabo socialnih omrežij in brskanja po spletu pušča za sabo, je s pomočjo nove tehnologije mogoče izrabljati za marsikatere namene, kot je na primer vplivanje na volilce [5].

S pomočjo tehnologije veriženja lahko veliko naših podatkov obdržimo zase ali vsaj omejimo dostop do njih. Vseeno izvajanje transakcij z uporabo tehnologije veriženja blokov ni popolnoma anonimna v dobesednem pomenu. V resnici je psevdonimna, kar pomeni, da so za transakcijami psevdonimi, ki jim pravimo naslovi. Če pride do tega, da se razve kdo stoji za psevdonimom, je vse, kar je nekdo počel za psevdonimom povezano z njim [16]. Znotraj omrežja, vsaj dokler naši naslovi niso povezani z našo identiteto, lahko pošiljamo in sprejemamo transakcije, ne da bi ljudje vedeli, kdo stoji za temi transakcijami. Da je naslov težje povezati z osebo, Nakamoto priporoča, da se za vsako transakcijo uporablja drugi naslov [17].

3.3 Transparentnost

Besedo transparentnost največkrat slišimo iz ust politikov v zvezi s proračuni, gospodarskimi načrti, državnimi trošarinami in podobnim. Transparentnost v takšnem kontekstu pomeni zmožnost dostopa in pregleda različnih podatkov kot je na primer kako neka entiteta porablja denar, kako je nekaj zasnovano itn.

Z uporabo tehnologije veriženja blokov in kriptovalut je takšno transparentnost mogoče doseči, saj so podatki o vseh transakcijah v omrežju dostopni vsem udeležencem omrežja. Če na primer ustvariš fundacijo za dobrodelne namene, lahko do neke mere spremljaš, kaj ta fundacija počne s sredstvi. Ker je v njihovem interesu, da so videti institucija z integriteto in vredni zaupanja, lahko omrežju razkrijejo svojo identiteto in pustijo odprt dostop za pregledovanje porabe zbranega denarja in na tak način dokazujejo svojo legitimnost. Transparentnost je koristna še za marsikatero uporabo (več o tem v poglavju o domenah uporabe tehnologije blockchain).

3.4 Nespremenljivost blokov

V preteklosti je bilo že več poskusov implementacije načina elektronskega plačevanja (Hashcash-a denial of service counter-measure, Blind signatures for untraceable payments). Največji problem pri implementiranju sistema elektronskih plačil je predstavljalo iskanje učinkovitega načina za preprečevanje dvojnega porabljanja sredstev (ang. *double spend problem*), saj je pri elektronskem denarju ponarejanje in zavajanje lažje kot pri papirnatem. Z nespremenljivostjo blokov se rešimo tega problema in valuto je zelo težko večkrat porabiti. Prav tako je pomembno, da se človek, ki nekaj plača, ne premisli, potem ko dobi dobrino. Prodajalec, preden pošlje dobrino, počaka nekaj potrjenih blokov in po nekaj potrjenih blokih je lahko prepričan, da je plačilo prejel in ga ni mogoče preklicati, razen če on tako hoče (tako, da pošlje vsoto transakcije nazaj plačniku, prej potrjene transakcije ne more spremeniti).

Chapter 4

Arhitektura veriženja blokov

Omrežja, ki temeljijo na veriženju blokov, imajo obliko omrežja vsak z vsakim. V takšni obliki omrežja so vsi udeleženci odjemalci in strežniki hkrati. Vsi udeleženci v omrežju so enakovredni, kar pomeni, da ne obstaja entiteta z dodatnimi privilegiji. Verigi blokov se dodaja bloke tako, da ko miner uspešno zrudari blok, ga pošlje vozliščem, ki so povezana z njim in ta vozlišča razpošljejo blok naprej po omrežju.

Omrežij, ki uporabljajo tehnologijo veriženja blokov, je veliko in število še raste. Zaradi tega se lahko arhitekture različnih verig blokov med seboj bolj ali manj razlikujejo. Ker je omrežje Bitcoin prvo delujoče omrežje, na ramenih katerega so zrasla ostala omrežja verig blokov, bom v tem poglavju opisal arhitekturo omrežja bitcoin, katerega bistven namen je hranjenje podatkov o kriptovaluti Bitcoin.

4.1 Vozlišče

Vsak udeleženec v omrežju je vozlišče. Poznamo dve vrsti vozlišč:

- polna vozlišča (ang. *full node*) in
- lahka vozlišča (ang. *light node*).

4.1.1 Polna vozlišča

Polna vozlišča so računalniki, ki so del omrežja verige blokov in imajo na disku shranjeno celotno verigo blokov. Tako imajo dostop do celotne zgodovine blokov, ki so bili potrjeni s strani omrežja. Naloga polnih vozlišč, je da skrbijo za validacijo blokov, kar pomeni, da če neko zlonamerno vozlišče po omrežju pošlje verigo z lastnim blokom, ki se ne drži pravil protokola ali vsebuje transakcije, ki se ne držijo pravil, vozlišče take verige ne sprejme kot ustrezne in je ne pošlje naprej ostalim udeležencem v omrežju. Prav tako je polno vozlišče obvezno za rudarjenje valute omrežja, ni pa obvezno, da polno vozlišče rudari.

4.1.2 Lahka vozlišča

Lahka vozlišča nimajo shranjene celotne verige blokov. Namesto tega imajo shranjene samo določene bloke oz. transakcije, ki se tičejo transakcij, ki jih lahko vozlišče izvaja. Navadno so lahka vozlišča samo denarnice, ki delujejo tako, da ko nekdo želi izvesti transakcijo z nekom, denarnica pregleda pri enem ali več polnih vozliščih zgodovino transakcij pošiljatelja valute, da preveri, ali ima zagotovo v lasti določeno količino sredstev, ki jih želi poslati.

4.2 Transakcije

Transakcije znotraj omrežja verige blokov so podatkovne strukture, ki hranijo podatke o prenašanju vrednosti med različnimi naslovi. V primeru kriptovalut je vrednost, ki se prenaša preko transakcij, količina valute, ki jo pošiljatelj pošilja prejemniku. Vse transakcije so javno dostopne in jih je mogoče pregledati z uporabo tako imenovanega raziskovalca blokov (ang. *block explorer*). Raziskovalec blokov v resnici dešifrira zapise transakcij v omrežju v človeško berljiv zapis.

4.2.1 Verifikacija transakcij

Preden odjemalec omrežja Bitcoin doda transakcijo v bazen transakcij preveri ali transakcija sledi določenim pravilom. Če transakcija ne sledi pravilom

protokola (ang. *protocol rules*), potem jo vozlišče označi kot neveljavno in je ne vstavi v bazen transakcij.

Vozlišča omrežja preverjajo, ali so transakcije v skladu z več določenimi pravili. Med temi pravli so:

- transakcija mora biti sintaktično pravilna,
- vhodi in/ali izhodi transakcije ne smejo biti prazni,
- v vhodih so lahko samo izhodi, ki niso še postavljen kot vhod v katero drugo, še nepotrjeno transakcijo,
- transakcija ne sme že obstajati v enemu od blokov glavne verige blokov,
- seštevek vrednosti izhodov ne sme preseči seštevka vrednosti vhodov.

Če nekdo ustvari blok s transakcijo, ki je neveljavna, se pravi krši eno od pravil protokola, potem postane tudi blok neveljaven in posledično ostali udeleženci v omrežju verige, ki vsebuje tak blok, ne bodo sprejeli.

4.2.2 Bazen transakcij

Bazen transakcij (ang. *transaction pool* ali *mempool*) je prostor v delovnem pomnilniku (ang. *random acess memory* - RAM) naprave za rudarjenje, ki je dodeljen za shranjevanje transakcij, ki jih vozlišče prejme od omrežja. Vse veljavne transakcije se najprej shranijo v bazen transakcij. Iz tega bazena transakcij nato rudarji pobirajo transakcije in jih ustavljajo v bloke. Še nepotrjene transakcije, se pravi take, ki še niso vstavljene v noben potrjen, blok ostanejo v bazenu transakcij in so na voljo za dodajanje v naslednji blok. Če je v navodilih protokola verige blokov določen najmanjši strošek na transakcijo, se transakcije, ki nimajo zapisanih dovolj velikih stroškov, sploh ne uvrstijo v bazen transakcij in so ignorirane. Pride tudi do primera, ko za transakcije še ni bilo najdenih vseh neporabljenih izhodov, ki so navedeni v vhodih transakcije. Takšni transakciji rečemo osirotela transakcija (ang. *orphan transaction*). Določene implementacije vozlišč imajo tudi posebej ločen bazen samo za osirotele transakcije.

4.2.3 Struktura transakcij

Transakcije morajo imeti standardizirano strukturo, da jih lahko različne naprave in programi ustrezno preberejo in razumejo. Seznam polj in njihov namen lahko najdemo v tabeli 3.1.

Neobdelana transakcija izgleda takole(odebeljeni del je odklepajoča skripta transakcije):

0100000001fe0548c09e6893b51b2e2462db63ca44c51e3d468538664cdad9787 e57c9f45e
670000008a47@**304402207ed5ee2f7c5dcf02e05cd00ba815 732ab36c427736d2f
23fbed8ef0ef5c531280220115d427f3c032c6efd281c49a 62344ed09169b7d7a9
7dd3c4a4a7ef9c22524c3014104dab8b2cd8e167637fd17 36422f12497a8aba24
7ac8020cdcd6e198a83fd3291870356ab3a8dbe790e8afa bce817b28c73db73cc
6b5c3bab2aabf191a32699f67**@ffffffff0200000000000 00000306a2e6483dbfed18981cc
16d3cd5f008417fd5e4749f9766e11e0d212bb d8cd73cd26255d30facfb820a423432ec5c929
3615000000000000001976a9149d3 3d96b9e10f7e9920731a5fd996af98a9928e788ac00000000

Tako pa izgleda ista transakcija v človeško berljivi obliki (zapisana v formatu JSON): .


```
{
 "txid": "bf587fa387cdd7715e2397cb7b0993d7c37f0aa04c4b26
 3552e5fe378b7819b3",
 "hash": "bf587fa387cdd7715e2397cb7b0993d7c37f0aa04c4b26
 3552e5fe378b7819b3",
 "version": 1,
 "size": 280,
 "vsize": 280,
 "locktime": 0,
 "vin": [
  {
   "txid": "5ef4c9577e78d9da4c663885463d1ec544ca63db6224
   2e1bb593689ec04805fe",
   "vout": 103,
                "scriptSig":
                 "304402207ed5ee2f7c5dcf02e05cd00ba815732
```

```
                ab36c427736d2f23fbed8ef0ef5c531280220115
                d427f3c032c6efd281c49a62344ed09169b7d7a9
                7dd3c4a4a7ef9c22524c3[ALL]
                04dab8b2cd8e167637fd1736422f12497a8aba24
                7ac8020cdcd6e198a83fd3291870356ab3a8dbe7
                90e8afabce817b28c73db73cc6b5c3bab2aabf19
                1a32699f67",

              "sequence": 4294967295
            }
        ],
"vout": [
            {
              "value": 0.00000000,
              "n": 0,
              "scriptPubKey": {
                "asm": "OP_RETURN
                 6483dbfed18981cc16d3cd5f008417fd5e4749f97
                 66e11e0d212bbd8cd73cd26255d30facfb820a423
                 432ec5c929",
                "hex":
                 "6a2e6483dbfed18981cc16d3cd5f008417fd5e474
                 9f9766e11e0d212bbd8cd73cd26255d30facfb820a
                 423432ec5c929",
                "type": "nulldata"
               }
            },
            {
             "value": 0.00005430,
             "n": 1,
             "scriptPubKey": {
              "asm":"OP_DUP OP_HASH160
               9d33d96b9e10f7e9920731a5
               fd996af98a9928e7 OP_EQUALVERIFY OP_CHECKSIG",
              "hex":
               "76a9149d33d96b9e10f7e9920731a5fd996af98a992
               8e788ac",
              "reqSigs": 1,
```

```
        "type": "pubkeyhash",
        "addresses": [
         "1FLDCfr9iG7n6bAdGsqBXmhaLgC4aSze72"
        ]
       }
      }
     ]
}
```

polje	namen
txid	Identifikator transakcije
version	Različica transakcij. Prva različica transakcij ima polje nastavljeno na 1, transakcije naslednjih različic imajo večje število.
size	Velikost transakcije v bajtih.
locktime	Polje, v katerega zapišemo zaporedno številko najzgodnejšega bloka, v katerega želimo, da se transakcija zapiše.
vin	Skupina polj, ki se tičejo vhodov (opisano v podrazdelku Vhodi).
vout	Skupina polj, ki se tičejo izhodov (opisano v podrazdelku Izhodi).

Table 4.1: Polja transakcije.

Izhodi

Najbolj osnovni gradniki transakcij so neporabljeni izhodi (ang. *unspent outputs* ali kratica *UTXO-unspent transaction output*), ki so reference na nedeljivo količino valute bitcoin. Protokol bitcoin v resnici nima nikjer zapisanega finančnega stanja posamezne denarnice. Namesto tega denarnica v ozadju preišče omrežje in spravi skupaj vse neporabljene izhode, ki jih je mogoče porabiti z zasebnim ključem, ki ga hrani denarnica. V drugih

besedah so neporabljeni izhodi povezani z zasebnim ključem, porabi pa se jih lahko, samo če imamo pravi zasebni ključ. Transakcije je tako način prenosa možnosti porabe neporabljenih izhodov. Kdor ima možnost porabe izhoda, je tako rekoč lastnik tega izhoda. Tabela 3.2 prikazuje polja znotraj strukture polja `vout`.

polje	**namen**
value	Količina valute bitcoin.
scriptpubkey	Skripta, ki opisuje pogoje, ki morajo biti zadovoljeni za prevzem lastništva valute (podrobneje o tem v podrazdelku Zakljepajoče in odklepajoče skripte).

Table 4.2: Polja izhodov transakcije

Vhodi

V polju `vin` najdemo strukturo, ki hrani podatke o vhodih transakcije. Ko želiš nekomu poslati določeno količino valute bitcoin, se v vhod transakcije vstavi identifikator neporabljenega izhoda, ki ga je moč porabiti z zasebnim ključem iz denarnice. Če je količina željenega prenosa valute manjša od vsakega posameznega neporabljenega izhoda, ki si ga lastiš, se kot vhod v transakcijo vstavi enega od izhodov z večjo količino valute bitcoin, razlika (ang. *change*) pa se kot dodaten izhod prenese nazaj v tvojo denarnico. Če je količina željenega prenosa večja kot vsak posamezni neporabljen izhod v tvoji denarnici, se tvori tako imenovana večvhodna transakcija (ang. *multi-input transaction*), ki vsebuje več vhodov, sestavljenih iz neporabljenih izhodov iz denarnice. Poleg neporabljenih izhodov je v vhodih mogoče videti tudi referenco na prejšnjo transakcijo, v kateri se pojavi neporabljen izhod. Tabela 3.2 prikazuje polja znotraj strukture polja `vin`.

polje	namen
txid	Referenca transakcije, ki hrani neporabljen izhod, ki bo služil kot vhod nove transakcije
vout	Zaporedno število izhoda znotraj transakcije z identifikatorjem txid
scriptsig	Podpis zaklepajoče skripte (podrobneje o tem v podrazdelku Zakljepajoče in odklepajoče skripte).

Table 4.3: Polja vhodov transakcije

4.2.4 Abstrakcije transakcijskih podatkov

Tako imenovani raziskovalci verig blokov (ang. block explorer) na podlagi surovih podatkov o transakcijah omrežja izpeljejo še dodatne podatke, ki sicer niso shranjeni del transakcij, so pa pomembni za uporabnike omrežja.

Stanje na računu

V omrežju bitcoin nikjer ne zasledimo koncepta stanja računa (ang. *balance*). Raziskovalci verige blokov in denarnice podatek o stanju izračunajo tako, da za poljuben javni naslov preiščejo vso zgodovino transakcij, da najdejo katere neporabljene izhode lahko odklene lastnik javnega naslova. Seštevek vrednosti neporabljenih izhodov je stanje na računu.

Transakcijski stroški

Vsaka transakcija ima zapisane tudi transakcijske stroške, ki jih določi pošiljatelj valute. Stroški so, poleg nagrade, ki jo dobijo z rudarjenjem, še ena spodbuda, za rudarje, ki potrjujejo in verificirajo bloke. Ko bo celoten nabor valute bitcoin (21 miljonov) zrudarjen, bodo rudarji za spodbudo k verifikaciji blokov prejemali samo transakcijske stroške. Hkrati transakcijski stroški služijo tudi kot preganjanje zapolnjevanja omrežja z nepotrebnimi transakcijami [2], saj so transakcije z višjimi stroški s strani rudarjev prej izbrane iz nabora transakcij.

Denarnice s kriptovalutami same po sebi izračunajo stroške transakcije na podlagi velikosti transakcije (v bajtih) in mediane velikosti transakcije v določenem dnevu. Če transakcije sestavljaš ročno, se pravi brez pomoči denarnice, lahko sam nastaviš poljubno vrednost stroška transakcije (0 ali več). Vseeno je priporočeno, da so transakcijski stroški višji od 0, saj višina stroškov vpliva na to, koliko hitro bojo rudarji transakcijo vstavili v blok. Določeni protokoli imajo tudi nastavljeno najnižjo vrednost stroškov in v primeru, da ima transakcija nižje stroške od minimalnih, potem ni kandidat za vstavljanje v blok.

Naslovi prejemnika in pošiljatelja

Prav tako kot stanje računa tudi naslovi pošiljateljev in prejemnikov niso takoj razvidni iz transakcij. Naslov pošiljatelja raziskovalec blokov pridobi iz vhodov transakcije, kjer so zapisani neporabljeni izhodi pošiljatelja, iz izhoda pa je mogoče ekstrahirati pošiljateljev naslov. Naslov prejemnika raziskovalec ekstrahira iz izhodov transakcije. Lahko pa se zgodi, da se prejemnik odloči, da si drobiž pošlje na nek drugi naslov. V tem primeru se lahko samo ugiba, kateri izhod je namenjen prejemniku transakcije in kateri je naslov, ki ga je zbral prejemnik za nakazilo drobiža.

Količina poslanega denarja

Količina poslanega denarja je še en podatek, ki ga ne najdemo neposredno v transakciji. Podatek se izračuna kot razliko med seštevkom količine valute v vhodih in količino drobiža, se pravi izhoda poslanega na pošiljateljev naslov. Ampak kot že napisano, je mogoče, da si pošiljatelj drobiž pošlje na nek drug naslov in v tem primeru ni mogoče določiti kateri delež gre na naslov, ki ni v lasti pošiljatelja valute in kateri delež je drobiž, ki gre na naslov pošiljatelja valute.

4.3 Blok

Bloki, ki se povezujejo v verige, imajo določeno strukturo. Sestavljeni so iz glave bloka, kjer so shranjeni metapodatki o bloku, ter transakcij. V

glavi bloka so zapisani metapodatki o bloku. Ti podatki so zgoščena vrednost prejšnjega bloka, koren *merkle* drevesa (drevo vsebuje zgoščene vrednosti transakcij), časovni žig (ang. *timestamp*), *nonce*, podatek o težavnosti rudarjenja bloka.

- Zgoščena vrednost prejšnjega bloka, potrebna za evidentiranje, kateri blok je prejšnji oz. kateri je starš trenutnega bloka.
- Koren merkle drevesa, ki skrajša čas preverjanja, ali je iskana transakcija prisotna v bloku.
- Časovni žig se uporablja kot sredstvo za variranje zgoščene vrednosti bloka in hkrati služi kot zapis za vednost, koliko časa je preteklo za rudarjenje zadnjih 2016 blokov. Če so bili zminirani prehitro se težavnost miniranja poveča.
- Nonce je naključno število, ki služi kot parameter za vhod zgoščevalne funkcije v postopku iskanja dokazila o delu.
- Podatek o težavnosti rudarjenja je določeno število v šestnajstiškem formatu.

4.4 Ključi in naslovi

Lastništvo valute in dokazovanje identitete dokazujemo z zasebnimi ključi. V primeru valut lahko nekdo določene unspent output-e porabi samo, če k transakciji priloži zasebni ključ, ki potem ta sredstva odklene.

Pri pošiljanju podatkov lahko dokažemo svojo identiteto z zasebnimi ključi, ker se pričakuje, da imamo zasebni ključ samo mi. Istovetnost se preverja s pomočjo kriptografije javnih ključev ali asimetrične kriptografije. Zasebni ključ generiramo z močnim generatorjem naključnih števil. Ko imamo zasebni ključ, iz njega izpeljemo javni ključ s pomočjo algoritma ECDSA [2]. Ko pošiljamo podatke, jih prej vstavimo v zgoščevalno funkcijo skupaj z zasebnim ključem. Temu postopku rečemo tudi digitalno podpisovanje. Da smo

pošiljatelji mi, je mogoče dokazati z našim javnim ključem, ki je dostopen vsem. Ni pa mogoče s pomočjo javnega ključa priti do zasebnega ključa.

Iz zasebnega ključa nato izpeljemo naš naslov. Bitcoin protokol za to uporablja dva kriptografska protokola: SHA-256 in RIPEMD160. Najprej zasebni ključ vstavi v SHA-256, nato pa še v RIPEMD. Nato število zakodira z uporabo BASE58Check, ki 160 bitov dolg izhod funkcije RIPEMD spremeni v 58-mestno kombinacijo števk in črk, kar naredi naslov bolj berljiv od 256 oz. 160 mestnega števila [2].

Chapter 5

Varnostni mehanizmi tehnologije veriženja blokov

Pri načrtovanju zanesljivega načina izmenjave podatkov, ne glede na to ali so to finančni podatki ali zasebni pogovori, je eden najpomembnejših vidikov varnost prenašanja in hranjenja teh podatkov. Cilj ustvarjalca omrežja Bitcoin je bil ustvariti sistem izmenjave, ki ne temelji na zaupanju v tretjo osebo, zato da je izvajanje transakcij med dvema osebama pravično. Takšen sistem je skušal doseči z uporabo kriptografije, vede o matematičnih tehnikah za dosego informacijske varnosti in skrivanje podatkov ter teorije iger (ang. *game theory*), študije matematičnih modelov pri strateških interakcijah. V tem poglavju bom opisal, kakšni so varnostni mehanizmi sistema brez zaupanja in kako ti mehanizmi dosegajo koncepte, opisane v prvem poglavju.

5.1 Zgoščevalne funkcije

Zgoščevalne funkcije (ang. *hash function*) so orodja za zgoščevanje podatkov, ki vhodne podatke poljubne dolžine spremenijo v izhodne podatke točno določene dolžine. Izhodi 8-bitne zgoščevalne funkcije so dolgi 8 bitov oz. v splošnem n-bitna zgoščevalna funkcija ustvari izhode, dolge n bitov. Tehnologija veriženja blokov uporablja tako imenovane kriptografske zgoščevalne funkcije, ki imajo sledeče lastnosti:

1. Težko je najti dva različna vhoda, ki imata enako zgoščeno vrednost.
2. Za dano zgoščeno vrednost je neizvedljivo ugotoviti kakšen bi moral biti vhod v zgoščevalno funkcijo, ki bi generiral to zgoščeno vrednost.
3. Iz zgoščene vrednosti neznanega vhoda je neizvedljivo, da bi našli nek drugi vhod, ki generira enako zgoščeno vrednost kot ta neznani vhod.

Omrežja, ki temeljijo na tehnologiji veriženja blokov, se naslanjajo na to, da zgoščevalne funkcije, ki jih uporabljajo za delovanje omrežja, dosegajo te lastnosti. Na kakšen način je veriženje blokov odvisno od teh lastnosti, bo predstavljeno v naslednjih razdelkih poglavja.

Še ena zelo uporabna lastnost dobrih zgoščevalnih funkcij, ki se je poslužuje tehnologija veriženja blokov, je, da dva minimalno različna vhoda v zgoščevalno funkcijo generirata zelo različni zgoščeni vrednosti. Tako je tudi zelo majhna sprememba bloka hitro razvidna in z lahkoto opažena, kar je predvsem uporabno, da se prepreči nedovoljeno spreminjanje podatkov verige blokov.

5.2 Asimetrična kriptografija in podpisovanje transakcij

Eno najpomembnejših področij, ki omogočajo koncept veriženja blokov je področje asimetrične kriptografije. V to področje spadajo algoritmi, ki za varnost prenosa podatkov skrbijo z uporabo zasebnega in javnega ključa (v angleški literaturi zasledimo tudi termin public key cryptography). Zaradi transparentne narave veriženja blokov namen uporabe asimetrične kriptografije ni za skrivanje vsebine sporočil, temveč se pri tehnologiji veriženja blokov uporablja za dokazovanje:

- verodostojnosti transakcij oz. da se transakcija ni spreminjala med pošiljanjem po omrežju,
- da je pošiljatelj transakcije pravi in da je on ustvaril transakcijo ter
- da je pošiljatelj resnično lastnik neporabljenih izhodov (v primeru kriptovalut je to količina valute).

Vse prejšnje alineje pa so dokazljive samo v primeru, da je zasebni ključ dostopen samo pravemu lastniku, kar pomeni, da je potrebno ključ skriti. Če se zlonamerna oseba posluži nekega zasebnega ključa, lahko z njim podpisuje transakcije in odklepa neporabljene izhode. Tako se lahko pretvarja, da je nekdo drug in sodeluje v omrežju v njegovem imenu ter celo porabi celotno zalogo kriptovalute, ki jo zasebni ključ zaklepa.

5.2.1 Podpisovanje sporočil

Pošiljanje transakcij s pomočjo asimetrične kriptografije deluje tako, da ko pošiljamo sporočilo, ne glede na to, ali je sporočilo transakcija za pošiljanje kriptovalute ali kakšen drugi podatek, to sporočilo najprej digitalno podpišemo z našim zasebnim ključem. S tem dosežemo, da je prejemnik sporočila lahko prepričan, da je sporočilo prišlo od nas, vsaj v primeru, da imamo samo mi dostop do našega zasebnega ključa in da ni nihče spreminjal sporočila, preden je prišlo do prejemnika. V ta dejstva je lahko prepričan, ker bi v nasprotnem primeru, ko bi poskusil sporočilo dešifrirati z našim javnim ključem, ki ga pošljemo nekodiranega zraven sporočila, sporočilo bilo nesmiselno, saj kriptografske funkcije delujejo tako, da se ob že zelo majhni spremembi sporočila zgoščena vrednost tega sporočila popolnoma spremeni in je po dešifriranju nesmiselna.

5.2.2 Zasebni ključ

Zasebni ključ je naključno število, katerega dolžina je odvisna od implementacije digitalnega podpisovanja. V primeru omrežja bitcoin je dolžina zasebnega ključa 256 bitov, veljaven zasebni ključ pa je število med 1 in $1.158 * 10^{77} - 1$ [2].

Da ustvarimo dober zasebni ključ, potrebujemo dober generator naključnih števil (ang. random number generator – RNG) z visoko entropijo. Pri ustvarjanju zasebnega ključa se večkrat zanašamo na vir entropije, ki je neponovljiv. Spletna stran bitadress.org na primer za vir entropije uporablja odčitke pozicij kazalca računalniške miške in uporabniku naroči, naj nekaj časa premika miško po zaslonu. Ko imamo vir zadovoljivo visoke entropije, nam ostane

samo, da ustvarimo 256 bitov dolgo število, in če je število v razponu veljavnih ključev, potem imamo ustvarjen naš zasebni ključ, ki ga lahko uporabimo za ustvarjanje javnega ključa in digitalnih podpisov v omrežju bitcoin.

Ustvarjanje zasebnega ključa

Za prikaz ustvarjanja zasebnega ključa za omrežje Bitcoin bom uporabil funkcije iz python knjižice Pybitcointools, ki je dostopna preko javne domene na naslovu https://github.com/vbuterin/pybitcointools. Čeprav je razvoj knjižnjice razvijalec opustil, je med več pregledanimi knjižnjicami najbolj pregledna kar se tiče prikaza konceptov preko programske kode.

```
def random_key():
    entropy = os.urandom(32) \
        + str(random.randrange(2**256)) \
        + str(int(time.time() * 1000000))
    return sha256(entropy)
```

Kodni izsek 4.1: Funkcija za ustvarjanje naključnega zasebnega ključa.

Funkcija `random_key` na podlagi entropije ustvari 256 bitov dolgo naključno število, potrebno pa je tudi preveriti, ali je ključ v razponu veljavnih zasebnih ključev, se pravi ali je manjši od števila$1.158 * 10^{77} - 1$.

```
import bitcoin

def valid_private_key(priv_key):
    decoded_priv_key = bitcoin.decode_privkey(priv_key, 'hex')
    if decoded_priv_key > 0 and decoded_priv_key < bitcoin.N:
        return True
    else:
        return False


priv_key = ''
while not valid_private_key(priv_key):
```

```
priv_key = bitcoin.random_key()

print(priv_key)
```

Kodni izsek 4.2: Funkcija za preverjanje, ali je ustvarjen zasebni ključ znotraj intervala dovoljenih zasebnih ključev.

Primer veljavnega zasebnega ključa je:

d98f52c952cbc4a84b74dec8ba20035d64873c3b11cae23f5dc556c7a3493314

5.2.3 Javni ključ

Medtem ko je treba zasebni ključ skrbno varovati, saj z njim podpisujemo digitalna potrdila, je lahko javni ključ znan komurkoli, ne da bi to vplivalo na varnost komunikacije. To zagotavlja narava asimetrične kriptografije, saj uporablja enosmerne kriprografske funkcije, da iz zasebnega ključa ustvari javnega, kar pomeni, da je iz javnega ključa neizvedljivo izračunati zasebni ključ. Za pretvorbo zasebnega ključa v javnega veliko implementacij veriženja blokov uporablja funkcije, ki temeljijo na eliptičnih krivuljah. Od implementacije do implementacije veriženja blokov se razlikuje izbira eliptične krivulje. V primeru omrežja bitcoin se uporablja krivulja imenovana secp256k1 in algoritem ECDSA. Točke, ki so del krivulje, zadostujejo sledeči enačbi:

$$y^2 \bmod p = (x^3 + 7) \bmod p$$

pri čemer neznanki x in y predstavljata koordinati točke, mod p (operacija za izračun ostanka po celoštevilskem deljenju z primarnim številom p) pa pove, da je krivulja definirana v končnem polju primarnega reda p (kjer je p $= 2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1$). Slika 4.1 prikazuje približen izgled krivulje secp256k1.

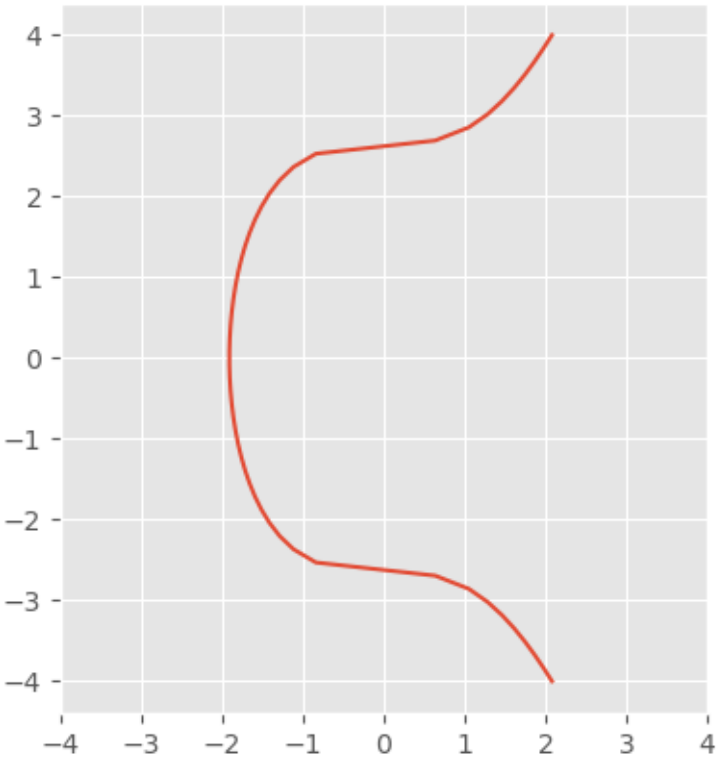

Figure 5.1: Približek izgleda eliptične krivulje secp256k1.

Javni ključ se s pomočjo krivulje ustvari tako, da generatorsko točko (ang. *generator point*), ki je samo prej izbrana točka na krivulji, pomnožimo z zasebnim ključem. V matematični formuli ta operacija izgleda takole:

$$K = k * G$$

kjer je K javni ključ, k zasebni ključ in G generatorska točka (množenje točke s številom je, v primeru algoritma ECDSA, v resnici samo ponavljajoče prištevanje točke same sebi, vzdolž krivulje). Iz zasebnega ključa ustvarjen javni ključ je reprezentiran z predpono 04 in dvema 256 bitnima številoma, ki predstavljata x in y koordinati točke na eliptični krivulji. Večinoma pa se javne ključe shranjuje v stisnjeni obliki, kjer je del ključa samo ena od

koordinat, saj matematična narava krivulj omogoča, da lahko na podlagi ene od koordinat izračunamo še drugo [2].

Ustvarjanje javnega ključa

```
priv_key = 'd98f52c952cbc4a84b74dec8ba20035d64873c3b1
1cae23f5dc556c7a3493314'

public_key = bitcoin.fast_multiply(bitcoin.G,
bitcoin.decode_privkey(priv_key))
```

Kodni izsek 4.3: Funkcija za izpeljavo javnega ključa iz zasebnega ključa (bitcoin.G predstavlja generatorsko točko).

5.2.4 Zakljepajoče in odklepajoče skripte

Prenos lastništva izhodov se izvede s pomočjo programskih skript. Skripte, uporabljane v omrežju Bitcoin, so napisane v skriptnem jeziku, ki je bil zasnovan posebej za namen omrežja kriptovalute. Skriptni jezik se preprosto imenuje *Script*. Jezik *Script* je skriptni jezik, ki se zapisuje v obrnjenem poljskem zapisu in temelji na uporabi skladov. Jezik *Script* ni Turingovo poln, kar pomeni, da ne zmore izračunati vsega in uporabljati določenih funkcij, kot to zmore večina modernih jezikov. Omejenost zmožnosti jezika je načrtno zasnovana, saj z manjšanjem zmožnosti manjšaš tudi možnost napak v kodi, in ker je jezik omejen, je tudi manj možnosti, da programer po nesreči vnese ranljivosti v skripte.

Del vhodov transakcije so odklepajoče skripte (ang. *scriptSig* ali *unlocking script*). Odklepajoča skripta vsebuje digitalni podpis in prejemnikov javni ključ. Pošiljatelj vzame transakcijo, ki vključuje neporabljen izhod, ki ga želi odkleniti, jo združi z prejemnikovim javnim ključem in digitalno podpiše s svojim zasebnim ključem. Ta podpis je potreben, da se odklene zaklepajoča skripta (ang. *scriptPubKey* ali *locking script*) omenjenega

neporabljenega izhoda. Poleg podpisa je v odklepajoči skripti še prejemnikov javni ključ.

Zaklepajoča skripta, ki je del vsakega izhoda, je poenostavljeno povedano pogojni stavek, zapisan v jeziku *Script*, ki ob izpolnjenemu pogoju, se pravi, da je digitalni podpis odklepajoče skripte ustrezen, odklene neporabljen izhod in zmožnost odklepanja izhoda prenese na prejemnika. Naslednjič, ko bo prejemnik želel izhod porabiti, bo to lahko storil, samo če bo v odklepajočo skripto ustavil digitalni podpis, ustvarjen s svojim zasebnim ključem.

Primer izvedbe odklepajoče in zaklepajoče skripte

Sliki 4.2 in 4.3 za boljše razumevanje grafično prikazujeta, kako odklepajoča skripta odklene zaklepajočo skripto.

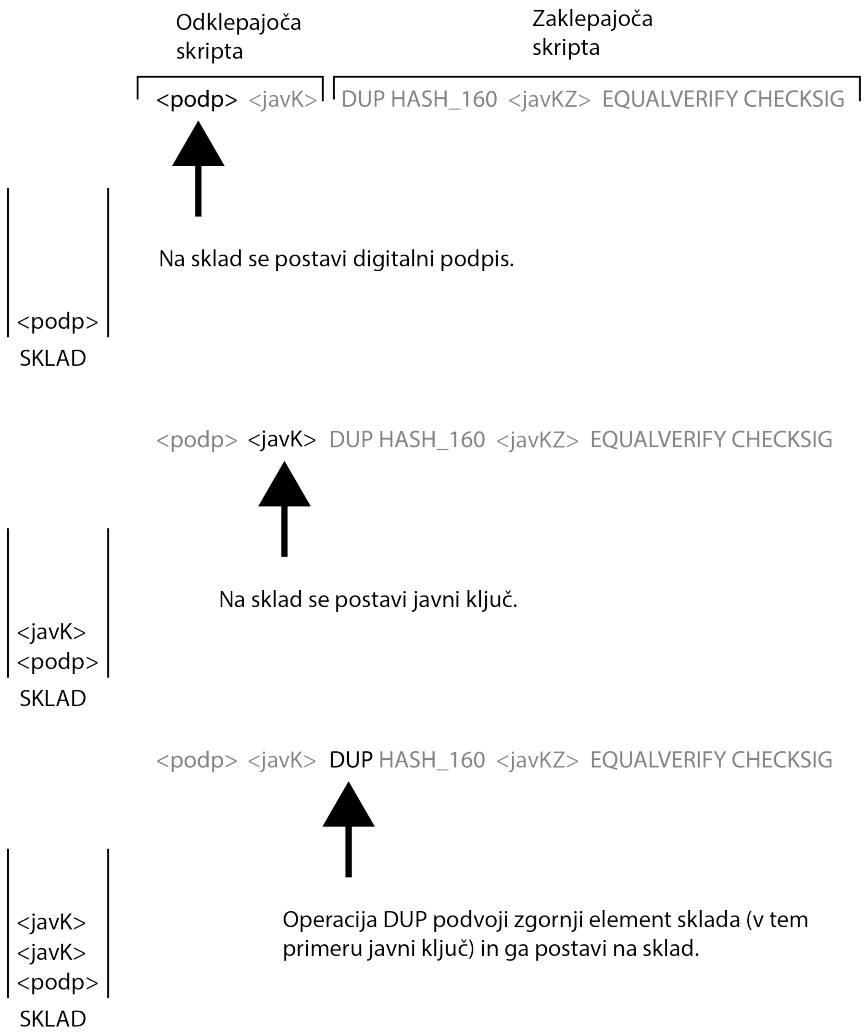

Figure 5.2: Grafični prikaz izvajanja odklepajoče in zaklepajoče skripte (<podp> predstavlja digitalni podpis pošiljatelja, <javK> predstavlja javni ključ prejemnika, <javKZ> predstavlja zgoščeni javni ključ prejemnika, puščica pa predstavlja izvajalni kazalec (ang. *execution pointer*, v skladu pa je rezultat po izvajani operaciji).

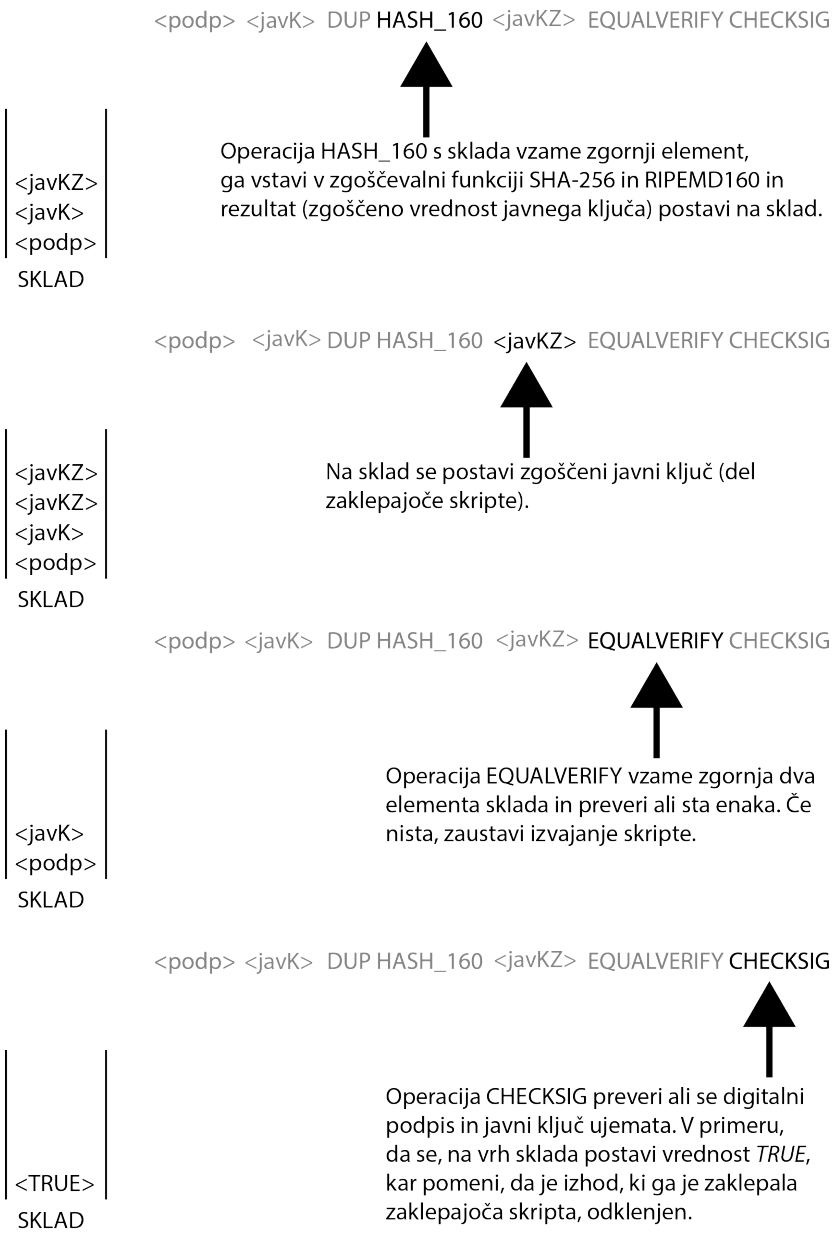

Figure 5.3: Grafični prkaz izvajanja odklepajoče in zaklepajoče skripte (drugi del)

Prikazana transakcija je tipa *P2PKH* (ang. *Pay to public key hash*), ki je najbolj pogosto uporabljen tip transakcije v omrežju Bitcoin (obstajajo tudi bolj zapletene transakcije, ki pa so redkejše in mejijo na pametne

pogodbe). Kot že povedano, skriptni jezik Script za izvajanje računskih operacij uporablja sklade. Skripte se sicer po omrežju prenašajo v obliki šestanjstiških števil.

5.3 Doseganje decentraliziranega konsenza

Decentraliziran sistem hranjenja podatkov, ki uporablja tehnologijo blokov, ne temelji na zaupanju. Namesto tega je za potrjevanje verodostojnosti blokov vzpostavljen mehanizem, ki otežuje spreminjanje ali brisanje vsebine blokov. Ko govorimo o decentraliziranemu konsenzu, imamo v mislih konsenz o tem, katera glavna knjiga oz. veriga blokov je pravilna. Splošno velja, da je pravilna veriga blokov tista, ki je najdaljša, se pravi tista, ki ima največ potrjenih blokov. Mehanizmov za potrjevanje blokov in doseganje konsenza je več, najbolj uporabljana mehanizma v omrežjih z verigo blokov sta dokazilo o delu (ang. *proof of work*) in dokazilo o deležu (ang. *proof of stake*).

5.3.1 Dokazilo o delu

Dokazilo o delu je prvi mehanizem potrjevanja blokov, ki ga uporablja tudi prva praktična implementacija tehnologije veriženja blokov – omrežje bitcoin. Iskanje tega dokazila dela imenujemo rudarjenje, polno vozlišče, ki išče dokaz dela, pa rudar. Postopek iskanja dokaza o delu v omrežju bitcoin je sledeč: polno vozlišče, ki rudari valuto omrežja iz bazena transakcij zbere transakcije in jih postavi v blok. Po tem ko zbere transakcije in bloku doda metapodatke (poglavje 2), kot prvo transakcijo bloka ustvari še tako imenovano coinbase transakcijo, s katero na svoj račun pošlje nagrado za svoje rudarjenje. Coinbase transakcija skupaj z metapodatki bloka in transakcijami omrežja tvorijo kandidatni blok. Blok je samo kandidatni, ker mora rudar nato še poiskati dokaz o delu. Dokaz o delu išče z uporabo zgoščevalne funkcije SHA-256 (ang. *secure hash algorithm 256*). SHA-256 je kriptografski algoritem iz družine SHA, ki ustvarja izhode, dolžine 256 bitov. Rudar kot vhod v funkcijo SHA-256 ustavi zaglavje bloka in naključno število (ang. *nonce*), potem pa preveri, ali je rezultat zgoščevalne funkcije število, ki je

manjše od števila, ki predstavlja težavnost rudarjenja. Če je število večje od težavnosti rudarjenja, rudar spremeni naključno število in ponovno izračuna zgoščeno vrednost. Težavnost rudarjenja se spreminja glede na računsko moč celotnega omrežja. V protokolu omrežja je zapisano, da naj bi med potrditvami blokov poteklo približno 10 minut, za kar omrežje poskrbi samo, tako da vsakih 2016 blokov preveri, ali je v povprečju med dvema potrditvama blokov poteklo 10 minut (oz. 20160 minut). V primeru, da je razvidno, da se bloki potrjujejo z večjo hitrostjo se težavnost preračuna na novo in tako poskrbi, da se bloke ponovno potrjuje na 10 minut. Nasprotno se težavnost zmanjša, če je za potrjevanje blokov potrebno več kot 10 minut. S takšno povprečno hitrostjo ustvarjanja blokov se bo rudarjenje zadnjega bitcoina končalo približno leta 2140, saj je število možnih kovancev v obtoku omejeno (razlogi za to so opisani v poglavju 5 pod razdelkom kriptovalute). Ko bo celotna količina bitcoinov v obtoku, bodo rudarji kot nagrado za rudarjenje pobirali samo stroške transakcij. Ko rudar dobi ustrezen dokaz o delu, blok razpošlje po omrežju. Vsako vozlišče tudi samo preveri, ali je dokazilo o delu ustrezno. V primeru je dokazilo o delu v skladu s protokolom omrežja, blok sprejme kot nadaljevanje najdaljše verige in začne iskati dokazilo o delu za nov blok s še nepotrjenimi transakcijami. Rudar bloka tako pobere nagrado, ki jo je mogoče porabiti šele čez 100 potrjenih blokov. Nagrada deluje kot spodbuda k rudarjenju (ang. *incentive*), saj rudarji v zameno za porabo električne energije, ki je potrebna za ohranjanje delujočega omrežja, dobijo plačilo. Količina nagrade se razpolavlja vsakih 210.000 blokov ali povprečno vsaka 4 leta. Tako je v prvem letu rudar za vsak potrjen blok prejel 50 bitcoinov, danes (leta 2018) pa jih prejme 12,5.

5.3.2 Dokazilo o deležu

Alternativa iskanju dokazila o delu za potrebe potrjevanja blokov je potrjevanje blokov z uporabo dokazila o deležu. V omrežju, kjer se konsenz o najdaljši verigi dosega z iskanjem dokazila o deležu v potrjevanju novega bloka, sodeluje več naključno izbranih imetnikov valute omrežja. Imetniki

valute, ki so v procesu potrjevanja imenujemo potrjevalci (ang. *validator*). Potrjevalci pred začetkom potrjevanja bloka pošljejo v omrežje posebno transakcijo s katero zaklenejo določen delež (ang. *stake*) njihovega imetja. Nato sledi potrjevanje ustreznosti bloka. Če je blok ustrezen in sledi protokolu omrežja, potrjevalci bloka poleg svojega zastavljenega deleža prejmejo tudi nagrado kot spodbudo k temu, da delujejo pošteno in v dobro omrežja. Če se razve, da blok, na katerega je potrjevalec zastavil delež premoženja, krši pravila protokola, potem potrjevalec to imetje izgubi. Zaradi morebitne izgube premoženja je potrjevalcu v interesu, da ne goljufa in se drži pravil omrežja [18].

Za določanje, kdo bo potrjevalec naslednjega bloka obstaja, več algoritmov, ki delujejo na naključni izbiri. Tak način izbire potrjevalcev omogoči večjo decentraliziranost omrežja, medtem ko pri potrjevanju blokov z dokazilom o delu, mero decentraliziranosti maje dejstvo, da ima večjo možnost, da bo blok potrdil, tisti, ki ima v lasti več računske moči, se pravi tisti, ki ima več denarja za nakup večje količine in zmožnejše strojne opreme.

Poleg večje decentraliziranosti omrežja, potrjevanje blokov na podlagi dokazila o deležu omogoča tudi manjšo porabo električne energije. Pri potrjevanju z dokazilom o delu se za potrjevanje blokov troši veliko električne energije, ki je potrebna za napajanje naprav, ki izvajajo zgoščevalne funkcije. Posledično rudarji z manjšo računsko močjo, ki večinoma ne uspejo dovolj hitro najti dokazila o delu in zaradi tega ne prejmejo nagrade, ne uspejo pokriti stroškov električne energije in se odločijo rudarjenje zaustaviti, rezultat pa je še večja decentraliziranost omrežja.

Chapter 6

Domene uporabe tehnologije veriženja blokov

Eden od namenov te diplomske naloge je, prikazati potencial tehnologije veriženja blokov za razvoj različnih aplikacij in kako lahko le-ta izboljša trenutne implementacije orodij in sredstev, ki jih, čeprav o njih ne razmišljamo veliko, uporabljamo vsakodnevno. Ideja o tehnologiji veriženja je v javnost prišla preko kriptovalute bitcoin, kmalu pa so strokovnjaki ugotovili, da se lahko v teoriji tehnologija uporablja na veliko področjih in ne samo na finančnem. Ustvarjalec omrežja Bitcoin je namreč z vpeljavo dokazila o delu in spodbud dobil rešitev za več kot 40 let star problem z imenom "problem bizantinskih generalov" [15], ki opisuje težave pri doseganju konsenza v distribuiranih sistemih. Rešitev tega problema je povzročila pravo revolucijo in vsesplošno navdušenje ter porast idej za vpeljavo tehnologije veriženja blokov v čim več delov področij človekovega vsakdanjika. Tehnologija veriženja blokov je sicer še v začetni fazi razvoja, zato je marsikatera rešitev, ki jo vsebuje, še nedodelana. V nadaljevanju poglavja bom opisal nekaj domen uporabe, za katere menim, da bi s pravo praktično implementacijo lahko bile koristne. Začnem z opisom populariziranih kriptovalut, ki se do določene mere držijo tudi v praksi, nato nadaljujem z drugimi domenami uporabe, ki se mi zdijo zanimive. V vsakemu razdelku skušam prikazati, kateri problemi

bi bili rešeni z uporabo veriženja blokov.

6.1 Kriptovalute

Kriptovalute so prva domena uporabe veriženja blokov in najverjetneje tudi najpomembnejša. Živimo v svetu, v katerem je denar zelo pomembna stvar in posledično je za povprečnega človeka ene največjih skrbi, kako denar pridobiti in kako pridobljeni denar shraniti. Za hranjenje denarja se ljudje že dolga leta zanašamo na banke ter na državne vlade, ki naj bi skrbele, da državna valuta obdrži svojo vrednost. Kot pa opazi tudi ustvarjalec omrežja Bitcoin Satoshi Nakamoto, je v zgodovini veliko primerov, ko so vlade in banke z denarjem in valuto upravljale nepremišljeno, škodo teh dejanj pa so v največji meri čutili navadni ljudje. Prav ta nepremišljenost institucij, ki naj bi bile zaupanja vredne, je Nakamota napeljala k iznajdbi valute, ki naj bi odvzela kontrolo iz rok teh institucij in jo položila v roke ljudi. Sad tega kripto-anarhističnega nazora je bila prva kriptovaluta bitcoin. Poleg omenjenih problemov z manipuliranjem vrednosti valut imajo običajne vladno izdane in centralizirane valute še druge probleme, ki jih v vsakdanjem življenju redko opazimo. Eden od problemov je višina stroškov transakcij. Težo tega problema še posebej občutijo ekonomski migranti, ki iz razvijajoče države migrirajo v tujo deželo z željo po zaslužku in nato svojim družinam pošiljajo denar v matično državo, pri čemer v primeru afriških držav, stroški transakcije dosegajo v povprečju 9,4 procenta za pošiljanje 200 dolarjev [14]. Pri pošiljanju kriptovalut geografska pozicija ne igra vloge. Sicer imajo tudi kriptovalute svoje probleme s transakcijskimi stroški [3], vendar razvijalci kriptovalut za te probleme iščejo in razvijajo rešitve, medtem ko za banke transakcijski stroški predstavljajo skoraj polovico zaslužka [10].

6.1.1 Denarnice

Uporaba kriptovalut je tehnično precej zahtevna. Za ustvariti ključe in naslove ter sestaviti transakcije je potrebno veliko tehničnega znanja in razumevanja konceptov. Zaradi tega je, da bi se uporaba kriptovalut čimbolj razširila, bilo

potrebno ustvariti vmesnik, ki bi čim bolj skril zahtevnost uporabe kriptovalut in jih naredil dostopne povprečnemu človeku z malo tehničnega znanja. Rešitev so denarnice. Denarnice so programska oprema, ki služi velikemu številu uporab v zvezi s kriptovalutami. Med drugim poskrbijo za:

- ustvarjanje zasebnega in javnega ključa ter naslova,
- strukturiranje transakcij,
- računanje stroškov za pošiljanje transakcij in
- varno hranjenje zasebnega ključa.

Razvijalcem denarnic je tako kot uporabnikom bistvenega pomena, da je interakcija s programsko opremo čim lažja in je hranjenje kriptovalut čim bolj varno. Poznamo več različnih vrst denarnic, ki prinašajo različno mero varnosti in enostavnosti uporabe.

Namizne denarnice

Namizne denarnice (ang. *desktop wallet*) so programska oprema, ki se izvajajo in hranijo ključe na namiznih računalnikih. Spadajo tudi v podskupino vročih denarnic (ang. *hot wallets*), ki se od hladnih denarnic (ang. *cold wallets*) razlikujejo v tem, da so povezane z internetom, ko podpisujejo transakcije. Zasebni ključ se shrani na trdem disku računalnika, zato je podvržen zlonamernim poskusom kraje preko računalniških virusov in ostale škodljive programske opreme. Primer popularne namizne denarnice je Electrum, ki ponuja vse možnosti, ki bi si jih uporabnik želel, da jih denarnica ponuja. Z denarnico Electrum kreiramo zasebni ključ in pripadajoče podključe in naslove (več o tem v razdelku o HD denarnicah), plačujemo in prejemamo plačila (tudi preko kod QR) ter pregledamo zgodovino transakcij, ustvarjenih z denarnico. Denarnica Electrum podpira tudi obnovitev zasebnega ključa z uporabo mnemotehnike [11], s katero lahko na podlagi 12 angleških besed (ki si jih moramo zapisati in skrbno shraniti) preko mnemotehničnega algoritma izračunamo naš zasebni ključ, v primeru da ga izgubimo. Prav tako podpira tudi zavarovanje zasebnega ključa z geslom.

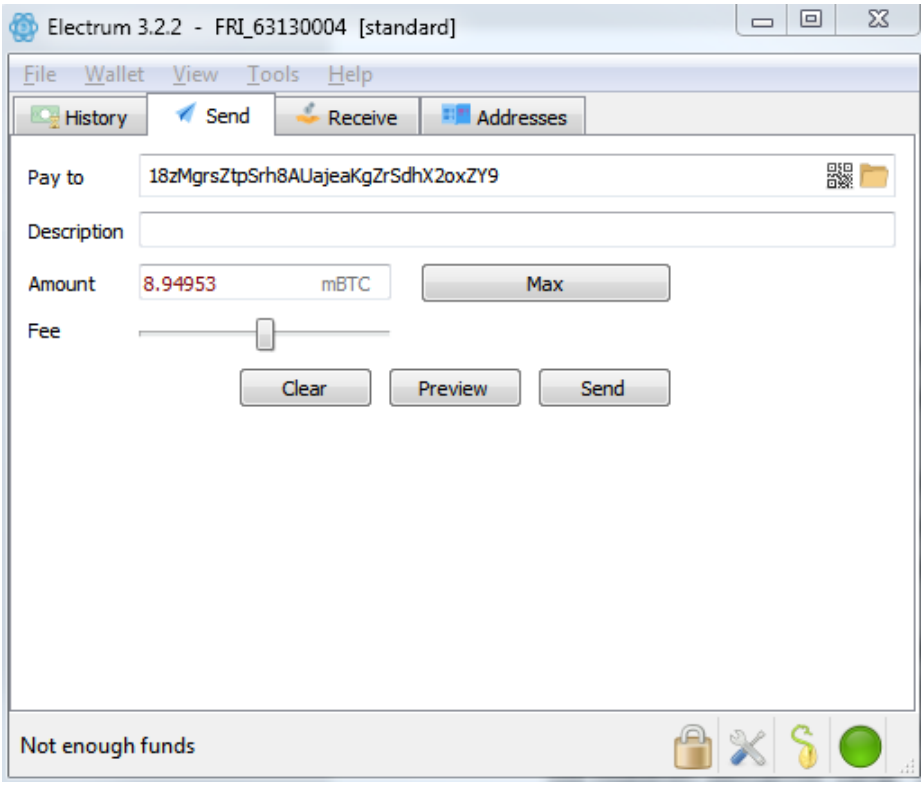

Figure 6.1: Zaslonska slika denarnice Electrum.

Mobilne denarnice

Mobilne denarnice uporabljamo na mobilnih napravah, kot so pametni telefoni in tablice. Odlikuje jih izjemna enostavnost namestitve in uporabe. Poleg tega da tako kot namizne denarnice tudi mobilne spadajo pod vroče denarnice, je njihova dodatna ranljivost, da je mobilne naprave lažje izgubiti ali nam jih ukradejo. V takem primeru, če denarnica ni zavarovana z geslom, lahko najditelj naprave sprazni celotno denarnico, tako, da kriptovaluto pošlje na svoj naslov. Zaradi teh pomanjkljivosti se uporabnikom odsvetuje hranjenje večje zaloge kriptovalut v mobilnih denarnicah. Ena za uporabo bolj enostavnih mobilnih denarnic za kriptovaluto bitcoin na operacijskem sistemu Android se imenuje *Bitcoin Wallet*. Denarnica ob namestitvi ustvari bitcoin zasebni naslov, z njo pa je mogoče še pošiljati in prejemati valuto bitcoin ter spremljati zgodovino transakcij. Mobilne denarnice za prejemanje

in plačevanje s kriptovaluto večinoma uporabljajo kode QR, s katerimi je mogoče ustvariti tudi zahtevke za plačilo, ki dovoljujejo, da plačnik s svojo napravo samo skenira kodo QR, da se ustvari transakcija, ki prenese zahtevano količino valute na prejemnikov račun.

Figure 6.2: Zaslonska slika denarnice *Bitcoin Wallet*.

Strojne denarnice

Med varnejše vrste denarnic spadajo strojne denarnice. Strojne denarnice so naprave, ki same generirajo zasebni ključ in ga hranijo samo znotraj naprave. Posledično je digitalne podpise mogoče ustvariti samo z uporabo strojne denarnice. Ker strojne denarnice spadajo pod hladne denarnice, se zasebni ključ nikoli ne znajde v medmrežju kot tudi ne na trdem disku kakšne druge naprave, ki ni strojna denarnica. Zaradi tega je kraja zasebnega ključa neizvedljiva, razen če si nekdo prilasti strojno denarnico in geslo, ki zaklepa

strojno denarnico. Običajno so naprave manjše velikosti, z nekaj gumbi za potrjevanje transakcij in so primerne za prenašanje v žepu. Največji tržni delež na trgu strojnih denarnic imata denarnici Trezor (slika 5.3) in Ledger Nano S. Obe denarnici imata manjši zaslon in dva gumba. Zaslon se uporablja za preverjanje, da je prejemnikov naslov pravi in da je količina poslane valute ustrezna, z gumboma pa bodisi potrdimo transakcijo ali jo zavrnemo. Za določitev naslova prejemnika in željene količine valute, ki jo želimo poslati ter izbor valute (strojne denarnice običajno podpirajo več različnih valut), pa se uporablja programska oprema, ki spominja na namizne denarnice.

Figure 6.3: Strojna denarnica Trezor.

Papirnate denarnice

Papirnate denarnice so vrsta hladne denarnice. Ustvarimo jih tako, da naključno ustvarjen zasebni ključ in pripadajoči naslov natisnemo na papir, običajno skupaj s kodo QR (ang. *quick reponse*) dveh števil zasebnega ključa. Ta vrsta denarnice bolj kot na denarnico spominja na sef. Če so do sedaj omenjene denarnice primerne za pošiljanje in prejemanje kriptovalut, se

papirnate denarnice pretežno uporabljajo za varno hranjenje valute. Hkrati predstavljajo tudi način hrambe zasebnega ključa, ki ni odvisen od strojne ali programske opreme, kar pomeni, da so odporne proti raznim nesrečam, kot so nenamerni izbris ključa, napaka trdega diska in podobno.

Figure 6.4: Primer papirnate denarnice za valuto ether.

6.1.2 Deterministične denarnice

Ali je denarnica deterministična ali nedeterministična je odvisno od tega, na kakšen način ustvarja zasebne ključe. Ob nastanku omrežja Bitcoin so se uporabljale nedeterministične denarnice, ki zasebni ključ ustvarijo na podlagi naključnosti in za vsak nov zasebni ključ za uporabijo novo seme (ang. *seed*). Zaradi tega je, če ustvarjamo več zasebnih ključev, kar je priporočljivo, potrebno za vsakega ustvariti novo varnostno kopijo (ang. *backup*) ali ga dodati k varnostni kopiji skupaj z ostalimi ključi. Če se zgodi, da pozabimo ustvariti kopijo enega od ključev in ta ključ ponesreči zgubimo, je vsebina, ki jo ključ hrani, za vedno izgubljena. Za rešitev te težave in poenostavitev življenja uporabnikov denarnic so se strokovnjaki na področju veriženja blokov domislili rešitve v obliki hierarhično determinističnih denarnic ali HD denarnic (ang. *hierarchical deterministic wallet – HD wallet*). Standard o HD denarnicah je zapisan v predlogu o izboljšavi bitcoina številka 39 [23] (ang. *BIP – Bitcoin Imporvement Proposal*).

Ustvarjanje glavnega ključa in otrok

HD denarnice na podlagi enega semena ustvarijo podaljšan ključ (ang. *extended key*). Za seme se uporabi naključno število variabilne dolžine (med 126 in 512 biti), ustvarjeno z uporabo mnemotehnike, ki običajno uporablja 12 ali 24 naključno izbranih besed. Ko imamo seme, ga vstavimo v zgoščevalno funkcijo HMAC-SHA512, ki ustvari 512-biten izhod, ki predstavlja podaljšan ključ. Levih 256 bitov podaljšanega ključa je glavni zasebni ključ (ang. master private key), desnih 256 bitov pa glavna verižna koda (ang. *master chain code*). Iz glavnega zasebnega ključa je nato z algoritmom ECDSA mogoče izpeljati tudi glavni javni ključ (ang. *master public key*). Podaljšani ključi (glavni ključ in verižna koda) služijo kot vhod v funkcije za ustvarjanje otrok ključev (ang. *child key derivation function*. Funkcije za ustvarjanje otrok ključev za vhod sprejmejo indeks otroka, verižno kodo starša in glavni ključ starša, na izhodu pa ustvarijo zasebni ključ otroka in verižno kodo otroka, ki lahko nato ustvarjajo še nadaljnje generacije otrok ključev. Če za vhod v funkcijo za ustvarjanje otrok ključev, poleg verižne kode in indeksa otroka, vstavimo javni ključ namesto zasebnega, dobimo na izhodu samo javni ključ otroka, kar je uporabno, ko hočemo na strežniku ustvarjati javne ključe, ne želimo pa izpostaviti zasebnega ključa.

Prednosti HD denarnic

HD denarnice imajo več prednosti:

- Hraniti je potrebno samo en zasebni ključ, na podlagi katerega se izpeljejo otroci ključa (ang. *child keys*). Če se denarnica okvari ali jo izgubimo, je tako za obnovo ključa potrebna samo ena varnostna kopija oziroma ena kombinacija besed za mnemotehniko.

- Organizacija ključev je lažja (za podjetja se lahko kreira otroka ključa za vsak oddelek).

- Za primere, ko je potrebno ustvarjati transakcije z veliko različnimi osebami (npr. spletna trgovina) in potrebujemo več različnih naslovov,

ni potrebno zasebnega ključa hraniti na strežniku in ga na tak način izpostaviti možnosti kraje.

6.2 Pametne pogodbe

Drugo za kriptovalutami najbolj zanimanje vzbujajoče področje, primerno za uporabo tehnologije veriženja blokov, je področje pametnih pogodb. Idejo o pametnih pogodbah si je v 90-ih letih prejšnjega stoletja zamislil računalničar in pravnik Nick Szabo [21]. Pametne pogodbe so zapisane v računalniškem jeziku, kar pomeni, da ne dopuščajo prostora za človeško interpretacijo. Tako kot je v pogodbi zapisano, tako se bo vse tudi izvedlo. Poleg tega so tudi avtomatizirane, zaradi česar so ljudje, ki sodelujejo v pogodbi, lahko prepričani, da bodo pogoji, zapisani v pogodbi, do potankosti držali. Koncepti, kot sta neizbrisljivost in decentraliziranost, delajo tehnologijo veriženja blokov trenutno najprimernejšo platformo za hranjenje in izvajanje pametnih pogodb. Za pogodbe je pomembno, da so organi, ki uveljavljajo pogoje pogodb, nepristranski, za kar je omrežja veriženja blokov, če so dovolj decentralizirana, mogoče trditi. Poleg tega je tudi potrebno, da so pogodbe trdne in se jih ne da zlahka preklicati ali spreminjati, kar omogoča omrežje veriženja blokov. Za pametne pogodbe je omrežje Bitcoin precej neprimerno. Sicer je v bitcoinovem skriptnem jeziku *Script* mogoče implementirati tudi pametne pogodbe, vendar se zaradi okorne narave jezika ob bolj zapletenih pogodbah s kompleksnejšimi pogoji, uporaba omrežja Bitcoin za pametne pogodbe ne obnese. Zaradi tega so se razvila še druga omrežja veriženja blokov, ki so primernejša za pisanje in izvajanje pametnih pogodb. Najbolj znano takšno omrežje je Ethereum.

6.2.1 Omrežje Ethereum

V omrežju Ethereum ima vsako vozlišče omrežja tudi svoj Ethereum navidezni stroj (ang. *Ethreum virtual machine*). Ta navidezni stroj omogoča, da vozlišča izvajajo programe v programskem jeziku *Solidity*. *Solidity* je programski jezik, podoben programskemu jeziku JavaScript, ustvarjen in op-

timiziran za potrebe omrežja Ethereum. Pametne pogodbe, napisane v programskem jeziku *Solidity*, so deterministične, kar pomeni, da ob enakih vhodnih parametrih pridejo do enakega rezultata, neodvisno od operacijskega sistema in strojne opreme računalnika, ki program izvaja.

6.3 Dobavna veriga in informacijski sistemi

Tehnologija veriženja blokov prinaša v informacijske sisteme overitev informacij, transparentnost in nespremenljivost podatkov. Informacijski sistemi v dobavni verigi imajo opravka z velikim številom podatkov, nadzorniki dobavnih verig pa računajo na to, da so podatki točni, saj točnost podatkov velikokrat vpliva na dobiček oziroma izgubo podjetja. Poleg prednosti, ki jih tehnologija veriženja blokov prinaša podjetjem, obstajajo tudi prednosti za stranke podjetij, kot je npr. sledenje izvora prehrambenih izdelkov [22]. Z uporabo pametnih pogodb lahko zahtevamo, da razne organizacije, ki skrbijo za kvaliteto in potrjujejo izvor izdelkov, na vsakem koraku oskrbovalne verige, s podpisom z zasebnim ključem, jamčijo, da vse poteka po standardih, vsi tej podatki, pa so transparentni in preverljivi.

6.3.1 Pravična trgovina

Tehnologija veriženja blokov je idealen sistem za vzpostavitev pravične trgovine (ang. *fair trade*) [19]. Vzpostavitev informacijskega sistema, ki deluje na sistemu veriženja blokov, bi omogočila bolj pošteno plačevanje dobrin, ki prihajajo iz držav v razvoju, saj bi lahko pridelovalec spremljal potovanje njegove dobrine po oskrbovalni verigi in preveril, za koliko se končni izdelek, narejen iz njegove dobrine, prodaja, na podlagi tega pa določal ceno, po kateri svojo dobrino prodaja dobaviteljem. Prav tako lahko tudi kupci preverjajo, koliko proizvajalci izdelkov plačujejo pridelovalce, in se odločajo, ali želijo kupiti izdelke proizvajalcev, ki do pridelovalcev niso pravični.

6.3.2 Sledenje pošiljkam

Računalniško podjetje *IBM* in eno večjih logističnih podjetij textitMaersksta združili moči in na podlagi tehnologije veriženja blokov razvili platformo

za digitalizirano sledenje pošiljkam, imenovano *TradeLens*[1]. Platforma za vzvod uporablja distribuirano omrežje veriženja blokov, da zbira podatke iz veliko različnih entitet in vsem udeležencem omrežja omogoča pregled teh podatkov v realnem času. Platforma je še v fazah razvoja in čas bo pokazal, koliko je uporabna in kakšna je mera pridobitve pri logističnih podjetjih in strankah teh podjetij.

6.4 Pametna mesta

Ob porastu uporabe pametnih telefonov, ki imajo dostop do interneta in lahko po omrežju pošiljajo razne podatke, pridobljene z raznimi senzorji, se je začelo vedno večje razpravljanje o konceptu interneta stvari (ang. *Internet of Things*). Poleg vsem poznanih pametnih telefonov, internet stvari zavzema tudi ostale naprave z dostopom do interneta, ki pošiljajo podatke v omrežje in uporabljajo informacije, pridobljene z interneta, za bolj optimalno delovanje. Tako smo s časom doživeli tudi rojstvo idej o pametnih hišah in nato še pametnih mestih. Termin pametno mesto je zelo ohlapen in ima več definicij[8]. V grobem velja, da pametno mesto tehnologijo uporablja na pameten način, kar pomeni, da pridobljene podatke interpretira v povprečnemu človeku razumljive informacije, ki jih lahko uporablja tako, da mu izboljšajo življenje. Pametno mesto naj bi zavzemalo omrežje med seboj povezanih senzorjev (luči, termometrov, barometrov, senzorjev premikanja itd.), ki v realnem času procesirajo podatke in jih interpretirajo v informacije, uporabne na različnih področjih mesta (npr. spremljanje financ, prevozništvo, ohranjanje čistega okolja ipd.). Velikokrat se pri definiciji pametnega mesta omenja tudi izmenjava informacij med različnimi področji, ki vplivajo druga na drugo, npr. vpliv vremena na prevozništvo. Ob vnašanju interneta stvari v človekov vsakdanjik, se vedno pojavlja vprašanje, kako vzpostaviti sistem, ki ni le učinkovit, ampak tudi varen pred zlonamernimi poseganji in lažnimi informacijami ter upošteva tudi posameznikovo zasebnost. Ob prihodu tehnologije veriženja blokov bi se tem problemom lahko izognili, saj lahko posameznikovo zasebnost ohranjamo preko psevdonimnosti in zagotavljamo integriteto po-

datkov z uporabo zasebnih ključev. Zaradi transparentnosti podatkov pa lahko učinkovitost mesta raziskujejo tudi vladno neodvisni organi, kar bi povečalo decentraliziranost in potrebo po zaupanju v institucije [20].

Chapter 7

Zaključek

V diplomski nalogi sem skušal kar se da objektivno prikazati ozadje tehnologije veriženja blokov. Naštel sem prvine, ki tehnologijo odlikujejo in jo delajo drugačno od trenutno ustaljenih tehnologij. Z opisom kriptografskih algoritmov, ki se jih veriženje blokov poslužuje, sem prikazal še, kako so pri tehnologiji obljubljene funkcionalnosti tudi implementirane. Moj namen je bil prikazati, da možnost uporabe tehnologije veriženja blokov niso zgolj kriptovalute in da ima tehnologija širok potencial.

Kot vsaka tehnologija tudi ta ni brez pomanjkljivosti, vendar ker spada med tehnologije v razvoju, strokovnjaki redno razvijajo izboljšave. V prostoru veriženja blokov najdemo tako ljudi, ki so optimistični, da bo tehnologija veriženja blokov spremenila svet na bolje, kot udi skeptike, ki mislijo, da je povzdigovanje tehnologije samo marketinška prevara. Realnost je, da je v tako zgodnji fazi razvoja težko reči karkoli dokončnega, ni pa mogoče zanikati, da so se s prihodom te tehnologije načela marsikatera vprašanja o kvaliteti trenutnih tehnologij in o tem, kakšna bi lahko bila tehnologija v prihodnosti. Čeprav veriženje blokov najverjetneje ne bo izrinilo vseh trenutnih tehnologij, kot nekateri napovedujejo, vseeno izgleda, da bo prodrlo v določena področja ali vsaj odprlo vrata naslednji generaciji tehnologij.

Bibliography

[1] Maersk and ibm unveil first industry-wide cross-border supply chain solution on blockchain. Dosegljivo: `https://www-03.ibm.com/press/us/en/pressrelease/51712.wss`, 2017. [Dostopano: 25.8. 2018].

[2] Andreas M Antonopoulos. *Mastering Bitcoin: Programming the open blockchain*. O'Reilly Media, Inc., 2017.

[3] Leonid Bershidsky. Bitcoin's high transaction fees show its limits. Dosegljivo: `https://www.bloomberg.com/view/articles/2017-11-14/bitcoin-s-high-transaction-fees-show-its-limits`, 2017. [Dostopano: 23.8. 2018].

[4] Matthew Boesler. How 9 countries saw inflation evolve into hyperinflation. Dosegljivo: `https://www.businessinsider.com/worst-hyperinflation-episodes-in-history-2013-9`, 2015. [Dostopano: 11.8. 2018].

[5] Carole Cadwalladr. I made steve bannon's psychological warfare tool': meet the data war whistleblower. Dosegljivo: `https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump`, 2018. [Dostopano: 8.8. 2018].

[6] Phil Champagne. The book of satoshi: The collected writings of bitcoin creator satoshi nakamoto. *E53*, 2014.

[7] David Chaum. Security without identification: Transaction systems to make big brother obsolete. *Communications of the ACM*, 28(10):1030–1044, 1985.

[8] Annalisa Cocchia. Smart and digital city: A systematic literature review. In *Smart city*, pages 13–43. Springer, 2014.

[9] James Crotty. Structural causes of the global financial crisis: a critical assessment of the 'new financial architecture'. *Cambridge journal of economics*, 33(4):563–580, 2009.

[10] Robert DeYoung, Tara Rice, et al. How do banks make money? the fallacies of fee income. *Economic Perspectives-Federal Reserve Bank of Chicago*, 28(4):34, 2004.

[11] Marek Palatinus et al. Mnemonic code for generating deterministic keys. Dosegljivo: `https://github.com/bitcoin/bips/blob/master/bip-0039.mediawiki`, 2013. [Dostopano: 24.8. 2018].

[12] Cointelegraph guest author. History of cryptocurrency, part i: From bitcoin's inception to the crypto-boom. Dosegljivo: `https://cointelegraph.com/news/history-of-cryptocurrency-from-bitcoins-inception-to-the-crypto-boom`, 2013. [Dostopano: 8.8. 2018].

[13] Yuval Noah Harari. *Sapiens: kratka zgodovina človeštva*. Mladinska knjiga, 2014.

[14] Dan Kopf. Remittances to africa cost far too much—more competition would change that. Dosegljivo: `https://qz.com/africa/1272445/remittances-sending-cash-to-africa-is-most-expensive-says-world-bank/`, 2018. [Dostopano: 23.8. 2018].

[15] Leslie Lamport, Robert Shostak, and Marshall Pease. The byzantine generals problem. *ACM Transactions on Programming Languages and Systems (TOPLAS)*, 4(3):382–401, 1982.

[16] Malte Moser. Anonymity of bitcoin transactions. *Department of Information Systems, WWU Münster*, 2013.

[17] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. Dosegljivo: `https://bitcoin.org/bitcoin.pdf`. [Dostopano: 28.8. 2018].

[18] James Ray. Proof of stake faqs. Dosegljivo: `https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump`, 2018. [Dostopano: 20.8. 2018].

[19] Laura T Raynolds. Re-embedding global agriculture: The international organic and fair trade movements. *Agriculture and human values*, 17(3):297–309, 2000.

[20] Jianjun Sun, Jiaqi Yan, and Kem ZK Zhang. Blockchain-based sharing services: What blockchain technology can contribute to smart cities. *Financial Innovation*, 2(1):26, 2016.

[21] Nick Szabo. Smart contracts: building blocks for digital markets. *EXTROPY: The Journal of Transhumanist Thought,(16)*, 1996.

[22] Feng Tian. An agri-food supply chain traceability system for china based on rfid & blockchain technology. In *Service Systems and Service Management (ICSSSM), 2016 13th International Conference on*, pages 1–6. IEEE, 2016.

[23] Pieter Wuille. Hierarchical deterministic wallets. Dosegljivo: `https://github.com/bitcoin/bips/blob/master/bip-0032.mediawiki`, 2012. [Dostopano: 24.8. 2018].