ELEKTROTEHNIŠKI VESTNIK 82(1-2): 1–7, 2015
IZVIRNI ZNANSTVENI ČLANEK

Računanje kriptografskih valut z GPE

Luka Sedmak, Tomaž Dobravec

Univerza v Ljubljani, Fakulteta za računalništvo in informatiko, Tržaška 25, 1000 Ljubljana, Slovenija
E-pošta: sedmak@gmail.com, tomaz.dobravec@fri.uni-lj.si

Povzetek. Na področju sodobnih financ in bančništva se je razvila močna koncentracija kapitala v peščici finančnih središč. Kot alternativa takšni centralizaciji so se začele uporabljati umetne deregulirane ter popolnoma distribuirane kriptografske valute. Njihova zasnova deluje na principu peer-to-peer omrežja, v katerem se s kriptografskimi funkcijami skupinsko nadzorujejo transakcije in ustvarjanje same valute, kar omogoča transparentnost ter hkrati anonimnost ter varnost. Za pridobivanje kriptografskih valut smo sestavili napravo, ki z izkoriščanjem velike količine ter hitrosti pomnilnika na grafičnih karticah s posebno programsko opremo potrjuje transakcije v omrežju in nam s tem ustvarja majhen delež valute za nagrado. Opisali bomo lastnosti različnih kriptovalut, razložili metode maksimizacije dobička ter opisali uporabljeno strojno opremo. Predstavili bomo tudi algoritem za potrjevanje transakcij in prikazali vpliv konfiguracijskih parametrov na končno hitrost preračunavanja.

Ključne besede: kriptografske valute, kriptografske funkcije, anonimnost, transparentnost, distribuirana valuta, dereguliranost, bitcoin, scrypt

Calculating the cryptographic currencies using GPUs

In the field of modern finance, a concentration has developed in a handful of financial institutions. As an alternative to such centralization, deregulated and fully distributed synthetic currencies have been introduced. They are designed as a peer-to-peer network, where by using cryptographic functions, transactions and creation of the currency are controlled, which allows for full transparency along with an anonymity and security. To obtain some cryptographic currencies, we assembled a device that uses a large amount of the fast memory on video cards by running a special software which confirms transactions in the network. Using this device, we collected a small amount of the currency as a reward. In the paper we describe characteristics of various cryptocurrencies, explain the methods for maximizing the profit, describe the hardware used, present characteristics of various cryptocurrencies, introduce methods for maximizing the profit and describe the hardware used. We also explain the algorithm used to validate the transactions and show the impact of the configuration parameters on the resulting hashing speed.

1 UVOD

Skozi zgodovino smo ljudje iz prvotne blagovne menjave fizičnih dobrin najprej prešli na monetarni sistem z denarno menjavo v obliki srebrnih in zlatih kovancev, nato pa so začele nastajati prve osnovne banke. Z njimi so se prvič v zgodovini pojavile tudi razne denarne mahinacije, ki so že takrat aktivno vplivale na oblikovanje takratnega sveta. Pozneje se je z uvedbo tiskanja denarja in nato borz ter delniških trgov dokončno ustvaril ekosistem moči kapitala, katerega niti držijo v rokah finančne elite. Takšna ureditev je postopoma privedla do situacije, ko je moč nad koordiniranjem tako rekoč celotnega svetovnega kapitala v realnem času skoncentrirana v rokah nekaj finančnih institucij in ko sta denar in ravnanje z njim postala popolnoma abstrakten pojem.

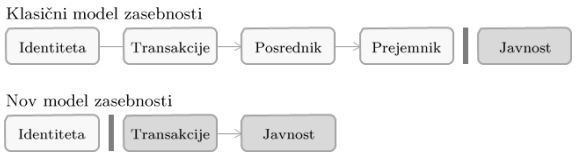
V želji po neodvisnosti finančnega prometa od bank in drugih finančnih institucij so se kot eden od mehanizmov za dosego cilja razvile kriptografske valute [1], [2]. Idejna zasnova kriptografskih valut temelji na principu peer-to-peer elektronskega denarja, ki omogoča plačevanje neposredno med uporabniki mimo sistema finančnih institucij. Glavna knjiga vseh transakcij se sproti osvežuje pri vseh uporabnikih hkrati in se kodira tako, da onemogoča reverzibilnost transakcij. Kriptografija z uporabo kombinacije zasebnih in javnih ključev pa omogoča varnost in identifikacijo uporabnikov. Tak sistem zagotavlja decentralizacijo, saj je distribuiran med vsemi uporabniki omrežja, hkrati s popolno anonimnostjo pa tudi transparentnost transakcij, ki niso reverzibilne in so vse zapisane v skupni glavni knjigi. Potrjevanje transakcij in hkrati nastajanje same valute v sistemu se izvaja s t. i. 'rudarjenjem', ki bo tudi podrobneje opisano v poznejših poglavjih tega članka.

Ena ključnih prednosti kriptografskih valut in hkrati velik trn v peti svetovnim oblastem je odsotonost regulacije z ukrepi kakršnihkoli finančnih ali vladnih avtoritet, ki je onemogočena zaradi anonimne in distribuirane narave sistema, katerega ideologija je razvidna iz slike 1.

2 KRIPTOGRAFSKE VALUTE

Prve ideje o digitalni valuti so nastale že leta 1998 na Cypherpunks mailing listi v obliki umetnih valut,

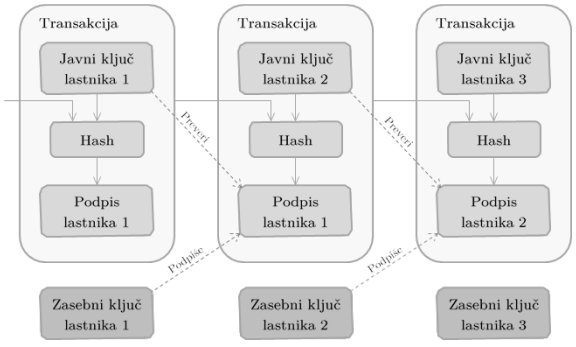
Prejet 16. december, 2014
Odobren 12. januar, 2015



Slika 1: Ideološki pristop k zasebnosti

ki bi s kriptografijo nadzirale svoj nastanek in vse transakcije. Po številnih razpravah in dopolnitvah je deset let pozneje nekdo pod psevdonimom Satoshi Nakamoto izdal tehnično specifikacijo ter dokaz teoretične pravilnosti delovanja koncepta prve prave kriptografske valute imenovane Bitcoin. Bitcoin je trenutno glavna in svetovno najbolj znana kriptografska valuta in njeni osnovni principi delovanja so bili temelj za izpeljavo vseh drugih novih kriptovalut. Kot prva formalna valuta svoje vrste je od leta 2009 do danes prebrodila nemalo težav, vendar se je zaradi pametnih potez razvijalcev in hitrih popravkov obdržala in pridobila na razpoznavnosti.

Tehnično ozadje Bitcoina v osnovi temelji na verigi blokov, glavni knjigi v kateri se verižno nalagajo bloki potrjenih transakcij, in na digitalnem podpisovanju transakcij. Elektronska valuta je definirana v obliki verige digitalnih podpisov [3] oziroma drevesa vseh transakcij med lastniki v času od nastanka do zadnje transakcije, sama po sebi pa kot entiteta ne obstaja. Vsaka transakcija vsebuje številko pošiljatelja, prejemnika, znesek poslane valute in nekaj kontrolnih parametrov. Pošiljatelj prenese valuto prejemniku tako, da zgoščeno vrednost (angl. hash) ene prejšnjih transakcij, poslanih njemu, skupaj z javnim ključem prejemnika digitalno podpiše s svojim zasebnim ključem in jo pošlje naprej. Potek podpisovanja transakcij je prikazan na sliki 2.



Slika 2: Podpisovanje transakcij

Ko pošiljatelj izvede transakcijo, je ta poslana vsem uporabnikom v omrežju ter čaka na potrditev. Potrjevanje transakcij se izvede s t. i. 'rudarjenjem' (kar je tudi glavna funkcija naprave, opisane v poznejšem poglavju). Rudarji so uporabniki omrežja, ki beležijo vse v omrežje prihajajoče transakcije in jih zbirajo v tekoči blok v obravnavi, tega pa poskušajo potrditi pred drugimi uporabniki. Pri tem nenehno izvajajo operacije algoritma, ki deluje takole: vzamemo *vse podatke še nepotrjenih transakcij* **T**, *zgoščeno vrednost podatkov zadnjega bloka* v verigi blokov **B** ter *naključno vrednost* **N** in nato s pomočjo kriptografske funkcije `sha-256(T,B,N)=zgoščena vrednost` iščemo takšno vrednost **N**, da funkcija vrne `zgoščeno vrednost`, ki se začne z določenim številom ničel v vodilnih bitih. Število zahtevanih ničel tako pomeni zahtevnost rudarjenja. Treba je povedati, da je uspeh tu v popolnosti odvisen od naključnosti. Uporabnik, ki mu prvemu uspe najti pravo vrednost, zbere vse nepotrjene transakcije v blok. Bloku nato doda zgoščeno vrednost prejšnjega bloka ter izračunano `zgoščeno vrednost` z začetnimi ničlami (kot dokaz opravljenega dela, angl. proof-of-work) in ga pošlje v verigo blokov. Tako je potrdil oziroma 'zapečatil' blok in je nagrajen z deležem na novo nastale valute. Potrjeni blok se nemudoma doda na konec verige blokov in nove prihajajoče transakcije se že obravnavajo kot del novega bloka v obdelavi. Omrežje vedno obravnava kot veljavno tisto verigo blokov, ki je najdaljša. Torej, če več kot en uporabnik v natanko istem času potrdi blok, se veriga blokov razveji, toda pozneje eden od repov prehiti preostale in ti nato odmrejo. Zahtevnost rudarjenja se v protokolu dinamično prilagaja glede na število uporabnikov v omrežju in njihovo izmerjeno računsko moč, upoštevajoč pravilo, da se en blok transakcij v omrežju potrdi v približno desetih minutah.

Z namenom, da bi zmanjšali naključno komponento rudarjenja ter zagotovili redne in pravično razdeljene nagrade pri rudarjenju, so se uporabniki začeli povezovati v t. i. bazene (angl. poole). V bazenih več uporabnikov prispeva svojo računsko moč za potrjevanje trenutnega bloka. Ob uspehu je nagrada razdeljena mednje glede na njihov prispevani delež, upravljavec bazena pa običajno pobere majhno provizijo. Namesto da bi en uporabnik poizkušal srečo več let in upal na veliko povračilo, lahko redno in z gotovostjo dobiva manjše delčke nagrade. Princip se je izkazal za zelo uspešnega in tako dandanes rudarjenje bolj znanih valut v celoti poteka v različnih manjših ali večjih bazenih.

Kmalu zatem, ko je Bitcoinu v svetu zrasla prepoznavnost ter seveda vrednost, so druga za drugo začele prihajati nove kriptografske valute. Vse temeljijo na enaki ideološki in tehnološki zasnovi, vsaka pa tako ali drugače poizkuša dopolniti funkcionalnost ali odpraviti hibe začetnika. Glavna 'hiba' Bitcoina se skriva v dejstvu, da je izvajanje funkcije SHA-256 mogoče zelo učinkovito realizirati s pomočjo aplikacijsko specifičnih integriranih vezij oziroma računalnikov ASIC [4], kar je pripeljalo do masovne izdelave le-teh in s tem dviga zahtevnosti za potrjevanje blokov na smrtnikom popolnoma nedosegljivo raven. Da bi se temu izognili, so načrtovalci novih valut za potrjevanje blokov začeli uporabljati algoritme, ki jih je težje ali manj smotrno implementirati z računalniki ASIC.

Večina na novo nastalih kriptovalut zdaj uporablja

algoritem Scrypt za potrjevanje svojih transakcij. Scrypt je v letu 2009 zasnoval Colin Percival, da bi ustvaril časovno in strojno čim zahtevnejši šifrirni mehanizem, ki bi napadalcem popolnoma izničil rentabilnost napada s finančnega vidika [5]. Algoritem uporablja kombinacijo sekvenčno spominsko izjemno zahtevnih funkcij in tako za hitro izvajanje potrebuje velike količine zelo hitrega pomnilnika, ki pa je drag in težko dobavljiv. Tako so z uporabo Scrypta namesto SHA-256 za svoj algoritem proof-of-work nove valute omejile eksponentne rasti zahtevnosti ter ohranile bolj distribuirano in raznoliko mrežo uporabnikov, ki rudarijo.

Prva takšna alternativna valuta je bila Litecoin. Projekt je bil vnaprej objavljen in nato splavljen oktobra 2011 [6]. Po zasnovi je neposredna kopija Bitcoina in se od njega razlikuje le po krajšem času potrjevanja bloka, večjem končnem številu kovancev in seveda uporabi algoritma Scrypt za potrjevanje transakcij. Litecoin je kot prva kriptovaluta Scrypt hitro pridobil na popularnosti in večina uporabnikov, ki je rudarila na domačih računalnikih, se je pridružila njim bolj prijaznemu omrežju. Skladno s tem je rasla tudi vrednost in tako je v letu 2013 Litecoin presegel kapitalizacijo trga v vrednosti milijarde ameriških dolarjev. Še ena izmed zanimivih kriptovalut Scrypt je Dogecoin, ki se je sprva začel kot šala na spletnih forumih z idejo lahko pridobljive valute, ki bi bila zelo razširjena, imela naključne nagrade za potrditve blokov ter delovala kot mehanizem za 'dajanje napitnine' avtorjem internetnih vsebin, ki se uporabnikom zdijo uporabne. Sprva valute nihče ni jemal resno, toda njena popularost se je razširila kot virus in je presegla število transakcij vseh kriptovalut skupaj. Dogecoin razvijalci so znani tudi po nenavadnih načinih promocije valute, kot so recimo sponzorstvo jamajškega moštva za bob, poslikavo celotnega dirkalnega avtomobila NASCAR z maskoto valute in dobrodelno gradnjo vodnjaka s pitno vodo v Keniji. Na trgu obstaja še veliko drugih kriptovalut Scrypt, vsaka s svojimi posebnostmi, prednostmi in slabostmi.

V iskanju optimalne zasnove kriptovalute, ki bi kljubovala vsem v praksi odkritim pomanjkljivostim današnjih, so se razvile tudi različne kombinacije in variacije uporabe kriptografskih funkcij in algoritmov:

- X11 (cryptcoin, darkcoin) – 11 kriptografskih funkcij, prepletenih med seboj,
- Keccak (maxcoin) – NIST je izbral Keccak kot zmagovalca na tekmovanju za implementacijo SHA-3 [7],
- Scrypt-N (execoin, vertcoin) – Scrypt z dodanim parametrom N, ki progresivno skozi čas povečuje samo spominsko zahtevnost algoritma,
- Grøstl (diamondcoin) – Grøstl, kandidat za SHA-3 s strani študentov danske DTU in TU Graz [8].

Razprava o tem, katera zasnova je najboljša, ostaja odprta, saj razvijalci tako algoritmov kot novih valut poudarjajo negativne lastnosti svojih tekmecev, definitivno pa se razvoj celostno odvija v pravo smer in zato lahko v prihodnosti pričakujemo čedalje bolj izpopolnjene rešitve.

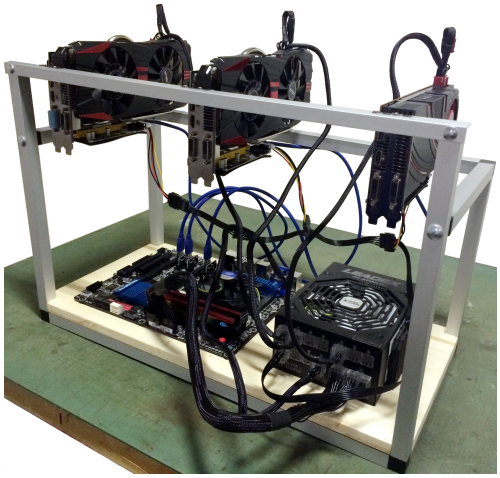
3 IMPLEMENTACIJA RUDARJA

Za potrjevanje blokov transakcij in s tem pridobivanje določene kriptografske valute smo sestavili napravo oz. rudarja, ki za delovanje uporablja hitrost in količino grafičnega pomnilnika na več grafičnih karticah visokega cenovnega razreda in v ta namen uporablja specializirano programsko opremo. Pri sestavi rudarja moramo premišljeno izbrati, kateri del sistema bomo uporabljali za potrjevanje transakcij (CPE, GPE, drugo), kako bo strojna oprema nameščena in hlajena in kateri tip algoritma proof-of-work najbolj ustreza naši konfiguraciji. Nato izberemo optimalen operacijski sistem in ustrezno programsko opremo, ki bo operacije izvajala, in se odločimo, katero valuto bomo rudarili ter kateremu poolu se bomo pridružili. V našem primeru smo se odločili za poganjanje algoritma Scrypt na GPE in uporabili naslednje komponente:

- Matična plošča je bila poleg zahteve po visoki kakovosti materiala skrbno izbrana tako, da se na njej nahajajo osnovne kontrole kot so gumb za vklop/izklop, reset gumb, gumb za ponastavitev CMOSa in LED indikator statusa sistema za preprostejše upravljanje. Prav tako smo zavoljo elegantnosti potrebovali podporo diskom mSATA.
- Procesorska moč je za rudarjenje z GPE irelevantna lastnost, zato je bil izbran najcenejši procesor, ki ustreza podnožju LGA 1155 na naši matični plošči.
- Za disk smo izbrali disk mSATA SSD, ki se vstavi v matično ploščo, za priklop ne potrebuje nikakršnih kablov ali vodil in je tako rekoč neviden. Hkrati s svojimi 120 GB prostora zadostuje za namestitev dveh sodobnih operacijskih sistemov.
- Velikost pomnilnika je odmerjena tako, da pri rudarjenju visoka konkurenčnost niti v kombinaciji s porabo operacijskega sistema ne doseže omejitve sistema.
- Napajalnik je poleg grafičnih kartic v tem primeru najpomembnejša komponenta sistema. Zagotavljati mora izjemno stabilno napajanje pri konstantni visoki porabi energijsko požrešnih grafičnih kartic. Po izčrpni raziskavi smo skrbno izbrali napajalnik višjega kakovostnega razreda, s praktično neobstoječim nihanjem napetosti na 12V tračnici ter več kot 92-odstotno učinkovitostjo pri polni obremenjenosti.
- Grafične kartice vse izhajajo iz vrha ponudbe družine Radeon izdelovalca AMD, ki se od svojih NVIDIinih tekmic razlikujejo po arhitekturni zasnovi senčilnikov in so pri karticah primerljivega ranga tudi do trikrat hitrejši pri rudarjenju. V osnovi so si sorodne, vse so zgrajene okoli AMDjevega 28nm Hawaii-Pro procesorja in imajo na vezju 4GB

GDDR5 pomnilnika. Prvotni namen je bil uporabiti štiri identične grafične kartice, a to ni bilo mogoče zaradi tedanjih razmer na trgu. Uporabili smo dve kartici ASUS DirectCU II R9 290 in eno referenčno kartico Gigabyte R9 290.

- Poleg skrbnega izbora strojne opreme je bilo treba za doseganje optimalnih rezultatov zasnovati in izdelati posebno ohišje, ki omogoča postavitev uporabljenih komponent tako, da se zagotovi največja mogoča pretočnost zraka in odvajanje toplote. Za doseganje zadovoljivih temperatur je bilo nujno grafične kartice ločiti od matične plošče in jih locirati čim bolj razpršeno v zračnem prostoru. Za ta namen smo uporabili posebne podaljške PCI-e vodil matične plošče, imenovane USB PCI-e 'riserji'. USB riserji so sodobna različica starih riser kartic, ki so se včasih uporabljale v starih strežniških ohišjih za priklop dodatnih kartic kadar je primanjkovalo prostora, le da tu za pretok podatkov med dvignjenim vezjem in PCI-e vodilom na matični plošči skrbi podatkovni kabel USB 3.0. S pomočjo riserjev in natančnega načrtovanja smo zasnovali in sestavili optimalno ogrodje za namestitev naše strojne opreme. Končni rezultat si lahko ogledamo na sliki 3.



Slika 3: Naprava za rudarjenje

Za operacijski sistem smo si prvotno izbrali posebej za rudarjenje prilagojeno distribucijo Linuxa Cryptoslax, ki temelji na ogrodju distribucije Slackware, vsebuje pa zgolj module, potrebne za rudarjenje ter se ob nalaganju v celoti zapiše v sistemski pomnilnik. Konfiguracija kljub prizadevnemu prilagajanju in preizkušanju različnih opcij ni dajala pričakovanih rezultatov, zato smo se iz nezaupanja v neuradno in relativno nepreverjeno distribucijo odločili za drugačen pristop. Na rudarja smo vzporedno namestili operacijski sistem Microsoft Windows 7 in Linux distribucijo Slackware 14.1 in na obeh naložili enake gonilnike ter programsko opremo za rudarjenje.

Izmed obstoječih programov, ki implementirajo rudarjenje kriptografskih valut s pomočjo algoritma Scrypt proof-of-work smo izbrali CGMiner [9], katerega avtor je Con Kolivas in je eden od dveh najbolje poznanih in pogosto uporabljanih programov za rudarjenje s pomočjo grafičnih kartic. Zavoljo boljše konfigurabilnosti smo uporabili različico iz posebne veje razvoja CGMinerja. CGMiner s pomočjo knjižnice ADL in okolja OpenCL v gonilnikih za grafične kartice omogoča podrobno upravljanje le-teh in opazovanje le-teh med rudarjenjem. Z uporabo programskih vmesnikov kriptografskih valut komunicira v njihovih omrežjih po zapovedanih protokolih, omogoča pa tudi priključevanje k bazenom in preklapljanje med njimi.

Na vse kartice smo namestili posebej spremenjen neuraden BIOS, ki s kalibracijo krmilnika grafičnega pomnilnika zmanjša čas med cikli in s tem latenco pri komunikaciji jedra s pomnilnikom. Optimizirana je tudi učinkovitost regulatorja napetosti, kar omogoča stabilnejše delovanje ter doseganje višjih frekvenc delovanja pri nižjih privzetih napetostih. Pri obeh operacijskih sistemih smo uporabili uradne grafične gonilnike AMD Catalyst 13.12, ki dajejo optimalne rezultate. Novejša različica gonilnikov Catalyst 14.1 in njihovi nasledniki imajo hroščato implementacijo okolja OpenCL in knjižnice ADL, kar se kaže v slabših zmogljivostih pri rudarjenju. Pri testiranju smo ugotovili, da so zmogljivosti na operacijskem sistemu Windows 7 pri rudarjenju ob enakih nastavitvah vedno za okoli 5% boljše od tistih na Linuxu. Krivdo za to verjetno lahko pripišemo slabše optimiziranim grafičnim gonilnikom za operacijski sistem Linux.

CGMiner prek konfiguracijskih datotek `.conf` omogoča zelo širok nabor nastavitev grafičnih kartic in upravljanje vsake kartice posebej. Tako je med drugim mogoče nastavljati hitrosti delovanja ventilatorjev, frekvence delovanja jedra in pomnilnika, privzeto voltažo na vezju in podobno. Spodaj je prikazana vsebina naše končne konfiguracije, ki daje dobre in stabilne rezultate skupaj z razlago pomembnejših parametrov in argumentacija uporabljenih vrednosti:

- `"gpu-threads":"1"` Število glavnih niti rudarskega procesa na kartico. Po naših ugotovitvah sta edini realno uporabni vrednosti 1 ali 2, meritve pa pokažejo, da je bolje imeti eno nit z višjo intenziteto rudarjenja kot dve vzporedni manj intenzivni niti.
- `"lookup-gap":"2"` Velikost presledka pri shranjevanju podatkov v beležniški pomnilnik med izvajanjem funkcije Salsa20/8 [10]. Vrednost 1 bi pomenila vseh 1024 vrednosti hkrati shranjenih v pomnilniku, pri vrednosti 2 shranimo vsako drugo, pri 3 vsako tretjo in tako naprej. Pri bolj gosto shranjenih podatkih je potrebnega manj preračunavanja manjkajočih delov in s tem manj ciklov procesne enote. Tako je v primeru zelo velikega beležniškega

pomnilnika optimalno izbrati nič presledka in nasprotno, pri visoki frekvenci procesorja in manjšega beležniškega pomnilnika bolje izbrati večji presledek. Za naše grafične kartice je optimalen izbor hramba vsake druge vrednosti.

- `"gpu-engine": "1025:947,1025:947,1065:947"` Nastavitev višine frekvenc delovanja grafičnega jedra po karticah, ločenih z vejico. Delovna frekvenca med rudarjenjem je z dvopičjem ločena od ponastavitvene frekvence, na katero se vrnemo po končanem rudarjenju. Tukaj se referenčna kartica izkaže veliko bolj dovzetna za navijanje, saj kartici ASUS ne zmoreta dolgotrajnega stabilnega delovanja pod obremenitvijo na frekvencah, višjih od 1025 MHz, medtem ko kartica Gigabyte v dobrih razmerah stabilno prenese tudi frekvence, višje od 1075 MHz. Ta 5-odstotna razlika v hitrosti procesorskega takta se prevede tudi v 5-odstotno razliko v hitrosti računanja zgoščenih vrednosti. Teoretični optimum, ki bi ga dosegli pri frekvenci 1100 MHz in s tem popolni zasičenosti pomnilnika bi znašal 2560 * 1100 * 0.352 (nominalna učinkovitost Hawaii jeder) = 991232 zgoščenih vrednosti oziroma približno 991000 zgoščenih vrednosti na sekundo.
- `"gpu-memclock": "1400:1250,1400:1250,1400:1250"` Nastavitev višine frekvenc delovanja grafičnega pomnilnika po karticah, ločenih z vejico. Delovna frekvenca med rudarjenjem je z dvopičjem ločena od ponastavitvene frekvence, na katero se vrnemo po koncu rudarjenja. Za pomnilnik izdelovalca Elpida so priporočene optimalne frekvence delovanja med 1375 MHz in 1450 MHz. Tako latenca kot pasovna širina, ki sta potrebni za optimalno zasičenost, sta na voljo že pri 1400 MHz in nadaljnje višanje frekvence le še slabša rezultate.
- `"thread-concurrency":"20481"` Mogoče število konkurenčnih operacij za vsako nit. V teoriji je optimalno izbrati čim višji večkratnik števila pretočnih procesorjev na kartici, s katerim še lahko izvajamo operacije in mu prištejemo ali odštejemo 1. Po izčrpnem testiranju smo si izbrali vrednost 20481, kar je 2560 * 8 + 1. Pri računanju zgoščenih vrednosti z dvema ali več glavnimi nitmi je ta vrednost občutno nižja.
- `"xintensity":"400"` Količina dela, ki ga grafična kartica mora opraviti, preden lahko vrne svoje rezultate. Optimalna vrednost je tik pod mejo preobremenjenosti kartice. Podana vrednost se zmnoži s številom pretočnih procesorjev na kartici, da dobimo število grafičnih niti. Ugotovili smo, da se ob vrednostih nad 400 hitrost računanja zgoščenih vrednosti spreminja minimalno in dokaj naključno, čeprav je končna zmogljivost kartic pred preobremenitvijo presegla 1500 * 2560 = 4194304 grafičnih niti.
- `"cl-filename":"kalroth"` Prilagojeno jedro grafičnega gonilnika. Prilagojena jedra vsebujejo različne optimizacijske prijeme pri implementaciji algoritma Scrypt proof-of-work, kot je recimo razvijanje zank, drugačna definicija podatkovnih struktur, alternativen način preverjanja pogojev, spremenjen ritem oddajanja deležev in podobno. Izkaže se, da so izboljšave rezultatov nekonsistentne in se razlikujejo od ene fizične kartice do druge. Tako na primer isto jedro, ki nam na eni kartici ASUS izboljša hitrost računanja zgoščenih vrednosti za 2%, na drugi rezultat poslabša za 3%. O enakih ugotovitvah poročajo tudi drugi, ki si prizadevajo za tak način optimizacije.

4 MERITVE

V specifikacijah kartic je navedena poraba energije pri polni obremenitvi za kartici ASUS 300 W, za Gigabytovo pa kar 600 W. Zadnje se izkaže za pretirano, saj v praksi med rudarjenjem kartica porabi približno 356 W elektrike in v kombinaciji s porabo vseh drugih komponent v sistemu skupna poraba ne preseže 1050 W, kar je razvidno iz slike 4. Takšen rezultat potrjuje optimalno izbiro uporabljenega napajalnika.

(a) Ena kartica (b) Dve kartici (c) Vse kartice

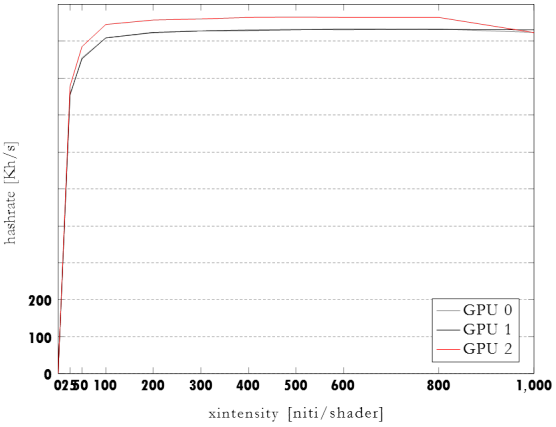
Slika 4: Poraba elektrike med rudarjenjem

Še ena zanimiva lastnost je kakovost ASIC GPE jedra, ki nakazuje, v kolikšni meri napetost ‘pušča’ skozi jedro. Višja vrednost kakovosti jedra ASIC v tem primeru (ne vedno) pomeni višjo stopnjo uhajanja in s tem slabše predispozicije za doseganje nizkih temperatur ob obremenitvi v normalnih okoliščinah. Pri karticah R9 290 praviloma variira med 60 in 100 %. Glede na naše meritve je referenčna kartica Gigabyte v rangu nizko ‘puščajočih’ primerkov z 71.4 %, medtem ko sta obe kartici ASUS na tem področju manj učinkoviti pri 84.8 %.

Večina konfiguracijskih parametrov, ki zagotavljajo optimalne rezultate pri računanju zgoščenih vrednosti, je pridobljena z dolgotrajno metodo poizkusov in napak, ker so rezultati naključni ali pa so ti rezultati linearno vezani na frekvenco delovanja jedra grafičnih kartic. Zato sta od poprej že podrobno opisanih parametrov, ki so se izkazali za optimalne, za grafični prikaz za-

nimiva le `xintensity` ter `thread-concurrency`. Pri meritvah spodaj prikazanih rezultatov so vsi drugi parametri nastavljeni na poprej že opisane vrednosti, ki zagotavljajo optimalno delovanje.

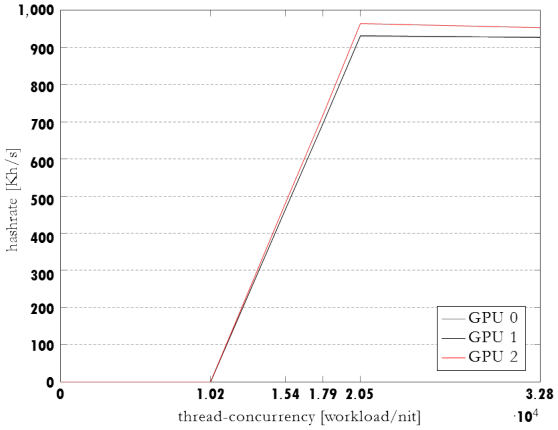
Ko postopoma povečujemo `xintensity` opazimo, da se hitrost računanja zgoščenih vrednosti hitro poveča do neke sprejemljive vrednosti, optimum pa je dosežen pri `xintensity = 400`. Pri tej vrednosti je hitrost tudi stabilna. Če `xintensity` še naprej povečujemo, povprečna hitrost računanja sicer ostane enaka, a med rudarjenjem čedalje bolj niha, nato pa začne po `xintensity = 800` počasi padati. Graf vidimo na sliki 5.



Slika 5: Graf hitrosti računanja zgoščenih vrednosti v odvisnosti od xintensity

Na sliki 6 vidimo, da se tudi pri višanju parametra `thread-concurrency` hitrost računanja zgoščenih vrednosti hitro dvigne, pride do optimuma in nato začne počasi padati. Treba je povedati, da so sicer same številke hitrosti računanja zgoščenih vrednosti že pri `thread-concurrency = 5120` blizu 930 Kh/s, toda z odstotkom sprejetih deležev blizu 0 %. Podobno je pri naslednjih vrednostih, ki smo jih tukaj za namen bolj realnega prikaza obtežili z njihovimi odstotki sprejetih deležev.

Tabela 1 prikazuje povprečne rezultate rudarjenja v bazenu v enakem časovnem obdobju pri uporabi različnih prilagojenih jeder gonilnikov. Pri tem spremljamo povprečno hitrost preverjanja zgoščenih vrednosti na sekundo, delovni obseg WU oziroma število poslanih preverjenih deležev bloka, ki ga potrjujemo, delovno uporabnost WUE oziroma odstotek poslanih deležev ki so bili sprejeti kot pravilni, odstotek napak po karticah R in temperaturo posameznih kartic med delovanjem. Pri interpretaciji tabele je treba biti pozoren na to, da večje število poslanih deležev ali pa najvišja povprečna hitrost računanja zgoščenih vrednosti ni nujno najboljši rezultat, saj sta pri potegovanju za nagrado pomembna odstotek sprejetih deležev WUE in odstotek napak R. Iz tabele je razvidno, da različne optimizacije jedra ne prinašajo ponovljivih in uniformnih izboljšanj



Slika 6: Graf hitrosti računanja zgoščenih vrednosti v odvisnosti od thread-concurrency

rezultatov pri hitrosti računanju zgoščenih vrednosti.

	GPU0	**GPU1**	**GPU2**	Poročilo
CGMiner Kalroth	931 Kh/s WU 830 R 3.8% 66°C 88°C VRM	935Kh/s WU824 R 2.5% 69°C 89°C VRM	966 Kh/s WU 874 R 3.0% 79°C 61°C VRM	2832 Kh/s WU 2528 WUE 88.6% 5.7/min
Zuikkis	915 Kh/s WU 807 63°C 79°C VRM		956 Kh/s WU 835 78°C 60°C VRM	CRASH WUE 85.3
SternStunde	928 Kh/s WU 833 R 2.5% 65°C 86°C VRM	920 Kh/s WU 833 R 4.4 % 67°C 87°C VRM	965 Kh/s WU 879 R 0.7% 78°C 60°C VRM	2813 Kh/s WU 2545 WUE 88.5% 9.48/min
Lantis	934 Kh/s WU 685 R 0% 65°C 86°C VRM	931 Kh/s WU 615 R 0% 68°C 87°C VRM	965 Kh/s WU 1000 R 3.5% 78°C 60°C VRM	2830 Kh/s WU 2363 WUE 81.7% 9.13/min
Kombinacija	925 Kh/s WU 831 R 1.7% 64°C 85°C VRM	940 Kh/s WU 860 R 1.5% 67°C 86°C VRM	966 Kh/s WU 843 R 2% 78°C 60°C VRM	2831 Kh/s WU 2531 WUE 88.6% 5.68/min

Tabela 1:: Primerjava zmogljivosti rudarjenja med prilagojenimi jedri

5 Sklep

Opisali smo ideološko in tehnično ozadje zasnove ter delovanja kriptografskih valut, predstavili njihove prednosti, slabosti in ranljivosti. Uspešno smo sestavili in skonfigurirali napravo za potrjevanje blokov transakcij kriptografskih valut, ki to počne s pomočjo algoritma Scrypt proof-of-work. Podrobno smo predstavili uporabljeno strojno opremo, načrt naše naprave in konfiguracijo strojne opreme. Predstavili smo tudi uporabljeno programsko opremo, konfiguracijo le-te ter razložili in argumentirali izbrane nastavitve ter pokazali izsledke meritev učinkovitosti sestavljene naprave. Ugotovili smo, da smo se s pomočjo naše konfiguracije

pri eni od grafičnih kartic zelo približali teoretičnemu maksimumu zmogljivosti, medtem ko nas je pri preostalih dveh ovirala napaka izdelovalca v zasnovi kartic, zaradi katere se je na njih pregreval regulator napetosti. Ugotovili smo tudi, da poseganje v jedrno implementacijo algoritma Scrypt proof-of-work z namenom optimizacije ne daje konsistentnih in sledljivih rezultatov. Podrobnejša razlaga tehnologij in algoritmov opisanih v tem članku, ter nekaj zanimivih informacij o področju kriptovalut najdemo v diplomskem delu avtorja [11]. Treba je povedati, da je bila naša naprava aktualna in dobičkonosna v času sestavljanja ter testiranja, zdaj pa je zastarela in se namesto grafičnih sistemov za potrjevanje transakcij večinoma uporabljajo sistemi ASIC s strojno realizacijo algoritmov.

Vsekakor so kriptovalute zanimivo in razvijajoče se področje. Rudarjenje se je v dveh letih razvilo v svetovno manijo. Od začetkov rudarjenja na centralnih procesnih enotah domačih računalnikov smo prišli najprej do specializiranih domačih rudarskih naprav, kot je opisana v tem članku, in končno do specializirane strojne implementacije potrjevalnih algoritmov na računalnikih FPGA in ASIC. Masovna proizvodnja zadnjih je dvignila zahtevnosti tako visoko, da je rudarjenje postalo dobičkonosno le še za lastnike celih hangarjev takšnih računalnikov, ki za napajanje potrebujejo moč prave male elektrarne. K temu sta delno pripomogli tudi konsolidacija in stabilizacija cene Bitcoina, ki trenutno znaša tretjino vrednosti tiste pred enim letom. Tako je recimo decembra 2013 dnevni donos naše naprave, katere največja moč računanja zgoščenih vrednosti je okoli 2,8Mh/s, znašal približno $60/dan, v času pisanja tega članka pa le še $0,30/dan. Za doseganje istih donosov bi trenutno potreboval sistem ASIC z močjo okoli 800Mh/s, ki pa ni dobavljiv in katerega cena bi znašala okoli 9000 ameriških dolarjev. Pri tem je seveda treba upoštevati tudi razpolovne dobe nagrad za potrjene bloke in volatilnost vrednosti valut. Položaj se v svetu kriptografskih valut izjemno hitro spreminja in tako rekoč nemogoče je predvideti prihodnost. Tako so zdaj glavni igralci v tem segmentu prav prvotni snovalci in izdelovalci vezij ASIC, ki posameznih naprav ne prodajajo več končnim uporabnikom, temveč sami postavljajo svoje centre za rudarjenje in nato po načelu oblačnih storitev oddajajo moč računanja zgoščenih vrednosti končnim uporabnikom. Zaradi ekološke in ekonomske smotrnosti ti centri temeljijo na področjih s čim cenejšo električno energijo, kar posledično ustvarja centralizacijo sistema, proti kateri se je Satoshi Nakamoto tako vneto boril.

Kljub vsemu so možnosti za razvoj kriptografskih valut in uporabo le-teh v vsakdanjem življenju tako rekoč neskončne. Rast števila uporabnikov, trgovcev in tržne kapitalizacije so indikatorji, ki kažejo na dolgoročno stabilizacijo in sprejetje kriptografskih valut. Manjša je tudi volatilnost vrednosti, kar posledično vodi v večje zaupanje pri uradnih institucijah ter državah. Z malo sreče in pravilnim ravnanjem odgovornih bi v daljni prihodnosti lahko prišlo do fuzije kriptografskih valut in uradnih denarnih valut ali celo popolne nadomestitve zadnjih.

LITERATURA

[1] Financial Action Task Force (FATF), *Virtual currencies: key definitions and potential AML/CFT risks*, FATF Report June, 2014

[2] R. Ali, J. Barrdear, R. Clews, J. Southgate, *Innovations in payment technologies and the emergence of digital currencies*, Bank of England Quarterly Bulletin Q3, 2014

[3] S. Nakamoto, *Bitcoin: A peer-to-peer electronic cash system*, https://bitcoin.org/bitcoin.pdf, 2008

[4] L. Dadda, M. Macchetti, J. Owen, *An ASIC design for a high speed implementation of the hash function sha-256 (384, 512)*, In Proceedings of the 14th ACM Great Lakes symposium on VLSI, pages 421–425 ACM Press April, 2004

[5] C. Percival, *Stronger key derivation via sequential memory-hard functions*, http://www.tarsnap.com/scrypt/scrypt.pdf, 2009

[6] C. Lee, *Litecoin*, https://litecoin.info/litecoin.pdf, 2011

[7] The National Institute of Standards and Technology (NIST), *Third-round report of the sha-3 cryptographic hash algorithm competition*, http://nvlpubs.nist.gov/nistpubs/ir/2012/NIST.IR.7896.pdf, 2012

[8] P. Gauravaram, L. R. Knudsen, K. Matusiewicz, C. Rechberger, M. Schlaeffer, S. S. Thomsen, F. Mendel *Grøstl - a SHA-3 candidate*, http://www.groestl.info/groestl.pdf, 2011

[9] C. Kolivas, *CGMiner - The combined CPU, GPU, FPGA, and ASIC miner for bitcoin, litecoin, and altcoins written in C*, https://github.com/ckolivas/cgminer, 2011

[10] D. J. Bernstein, *The salsa20 family of stream ciphers*, http://cr.yp.to/snuffle/salsafamily-20071225.pdf, 2011

[11] L. Sedmak, *Računanje kriptografskih valut z GPE*, Fakulteta za računalništvo in informatiko, 2014

Luka Sedmak je diplomiral s področja informatike na Fakulteti za računalništvo in informatiko Univerze v Ljubljani. Njegovi interesi so predvsem na področjih informacijske varnosti, kriptografije in računalniških omrežij.

Tomaž Dobravec je docent na Fakulteti za računalništvo in informatiko Univerze v Ljubljani, kjer sodeluje v pedagoškem procesu na področjih programiranja, algoritmov in operacijskih sistemov. Raziskovalno se ukvarja z razvojem in analizo algoritmov, s teorijo programskih jezikov in z vzporednim računanjem.