Hardver za rudarenje kriptovaluta

Matijević, Marko

Sveučilište u Rijeci – Odjel za informatiku

Preddiplomski jednopredmetni studij informatike

Marko Matijević

Hardver za rudarenje kriptovaluta

Završni rad

Mentor: dr. sc. Miran Pobar dipl.ing.el.

Rijeka, 20.09.2018.

Sažetak

U ovom završnom radu obrađen je pojam hardvera za rudarenje kriptovaluta. Nakon uvoda u prvom poglavlju opisana je prva kriptovaluta „Bitcoin“. U drugom poglavlju objašnjen je protokol „Blockchain“ na koji Bitcoin funkcionira. U trećem poglavlju opisane su transakcije, te posao rudara u bitcoin mreži. U četvrtom poglavlju je opisana povijest hardvera, te detaljan opis hardvera ovisno o generaciji. U zadnjem poglavlju je opisan suvremeni hardver te najbolje rješenje za Bitcoin i Ethereum, drugu najvrjedniju kriptovalutu.

Ključne riječi

Kriptovaluta, Bitcoin, Blockchain, Satoshi Nakamoto, SHA256, Proof-of-work, hash, rudarenje, hardver, CPU, GPU, FPGA, ASIC, Ethereum

Sadržaj

1. Uvod

Kriptovaluta je digitalni novac koji funkcionira na temelju kriptografskih algoritama. Rudarenje je postupak koji u decentraliziranoj valuti omogućuje postizanje konsenzusa kod svake promjene koje se izvode na blockchain mreži. Rudar za posao rješavanja kriptografkih problema koji omogućuje rad decentralizirane valute dobivaju nagradu u toj valuti. Jedno od zanimljivih stvari u Blockchainu je da svatko može postaviti svoje računalo kako bi se usredotočio na kriptografske zagonetke kao način za osvajanje nagrada. U ovom seminaru detaljnije se obrađuje prva kriptovaluta, Bitcoin, izum Satoshija Nakamota koji je zaslužan za cijeli decentralizirani sustav valute. Kroz godine, rješavanje kriptografskih zagonetka postalo je teže. Kriptovalute su tako napravljene ako ih što više ljudi rudari, težina za pronalazak bloka postaje veća. Rudari su ti koji su zaslužni za rad Bitcoin mreže. Na povećanje težine je i utjecala cijena kriptovaluta, te su se i hardveri mijenjali ovisno o težini samih zagonetaka. U seminarskom radu opisan je i povijesni razvoj hardvera koji prati razvoj Bitcoina i ostalih kriptovaluta te danas najkorištenija sredstva koja se koriste za rudarenje.

2. Bitcoin

Bitcoin je nova valuta (kriptovaluta) koja je kreirana 2009. godine, samo nekoliko mjeseci nakon financijske krize 2008. godine. Bitcoin je posve virtualan za razliku od tradicionalnih valuta. Ona isključivo postoji na Internetu kao otvorena mreža računala. Sastoji se od tehnologija i zbirke koncepata koje čine osnovu sustava digitalnog novca. Jedinice valute pod nazivom „Bitcoin“ koriste se za pohranu i prijenos vrijednosti među sudionicima u Bitcoin mreži. Svaki Bitcoin korisnik sa pristupom na Internet može komunicirati pomoću Bitcoin protokola, iako se mogu koristiti i druge transportne mreže. „Bitcoin protocol stack“ tzv. Blockchain, dostupan kao open source softver može se izvoditi na širokom rasponu računalnih uređaja, uključujući smartphone, tablete, te prijenosna računala, čineći tehnologiju lako dostupnom. Korisnici mogu prenijeti Bitcoin putem mreže kako bi učinili gotovo sve što se može učiniti s konvencionalnim valutama npr. kupnja i prodaja robe, slanje novca fizičkim ili pravnim osobama.

Bitcoinova tehnologija se temelji na enkripciji i digitalnom potpisu kako bi se osigurala sigurnost mreže. Korisnici Bitcoina posjeduju ključeve koji im omogućavaju dokazivanje vlasništva u transakcijama u bitcoin mreži, otključavanje vrijednosti za trošenje, te prijenos ka novom primatelju. Ti se ključevi pohranjuju u digitalni novčanik na korisničkom računalu. Jedini preduvjet za potrošnju Bitcoina je ključ koji otključava transakciju i stavlja potpunu kontrolu u ruke korisnika. Bitcoin sam po sebi je potpuno distribuiran sustav, peer-to-peer sustav takav da ne sadrži središnjeg poslužitelja ili točku kontrole. Kupovina, prodaja i razmjena Bitcoina i ostalih valuta se vrši na specijaliziranim mjenjačnicama za digitalne valute.

Autor Bitcoina poznat je pod pseudonimom S.N. S tim se nadimkom predstavljao njegov originalni osnivač na forumima kako bi pomogao vodičima glavnih razvojnih programa za održavanje i podržavanje izvornog koda. Iako nitko ne može potvrditi njegov identitet, vrijednost njegovog rada je vidljiva u tome tako da je Bitcoinov izvorni kod testiran, te da je isprogramiran bez ikakvih prijavljenih ozbiljnih bugova.

Bitcoin protokol sadrži ugrađene algoritme koji kontroliraju složenost funkcije rudarenja. Složenost problema kojeg rudari rješavaju da bi se blok transakcija uspješno potvrdio je osmišljena tako da svakih 10 minuta netko uspije potvrditi blok neovisno koliko je rudara uključeno. Svake četiri godine prepolovi se brzina stvaranja novih Bitcoina te se na taj način osigurava ukupan broj Bitcoina na 21 milijun. Taj broj će biti dostignut 2032. godine. Trenutna vrijednost Bitcoina iznosi 6500$ i na dnevnoj bazi je podložna promjenama vrijednosti.

2.1. Transakcije

Transakcija je prebacivanje vrijednosti između dva digitalna novčanika koji se potom registriraju u Blockchain, odnosno sustav umreženih blokova. Bitcoin novčanik sadrži dio podataka koji je tajan i on se naziva privatni ključ ili sjeme, a njime se potpisuju transakcije potvrđujući matematički dokaz koji povezuje ključ i vlasnika novčanika. Jednom kada je transakcija izdana više se ne može promijeniti, te upravo u toj situaciji važnu ulogu ima potpis. Transakcije na Blockchain mreži su javne, a vidjeti se može čitava povijest procesiranih transakcija, čak i onih prvih.

U praksi, ako osoba A želi poslati Bitcoinove osobi B, mora imati digitalni novčanik koji u sebi sadrži privatni ključ koji dopušta kreiranje kriptografskog potpisa. Osoba A unosi iznos Bitcoinova koji se želi poslati osobi B. Osoba B daje javni ključ (adresu digitalnog novčanika) osobi A kako bi prebacio određeni iznos.

Za mogućnost izvršenja transakcija određenog iznosa Bitcoina iz jednog digitalnog novčanika (engl. wallet) na drugi,potrebne su tri stvari:

- Adresa ili javni ključ (engl. Public Key),
- privatni ključ (engl. Private Key) i
- kriptografski potpis.

Adresa je definirana kao bankovni račun. Dolazak do adrese je vrlo jednostavan, potrebno je samo otići na za to predviđene pružatelje, te se adresa postavi u nekoliko sekundi. Bitcoin adresa je identifikator 26-35 alfanumeričkih znakova, počevši od broja 1 ili 3, što predstavlja moguću destinaciju za plaćanje Bitcoina. Svatko od korisnika Bitcoina može generirati adrese bez ikakvih troškova. Na primjer, koristeći Bitcoin Core[1], imate odabir kreiranja nove adrese, te vam program dodijeli novokreiranu adresu. Također je moguće dobiti Bitcoin adresu koristeći račun na mjenjačnici za kriptovalute ili putem digitalnog novčanika. Bitno je za istaknuti kako jedan korisnik može koristiti i imati više adresa.

Privatni ključ je dio podataka koji ostaje tajan, te dokazuje pravo prebacivanja Bitcoinova s novčanika pomoću kriptografskog potpisa. Kada se stvori nova Bitcoin adresa, ona dolazi uz privatni ključ koji je matematički povezan s tim brojem računa. Privatni ključevi Bitcoina obično sadrže 51 znak i počinju s brojem 5. Ti privatni ključevi se spremaju na osobnom računalu. U slučaju korištenja softverskog ili web novčanika tada se spremaju na serveru.

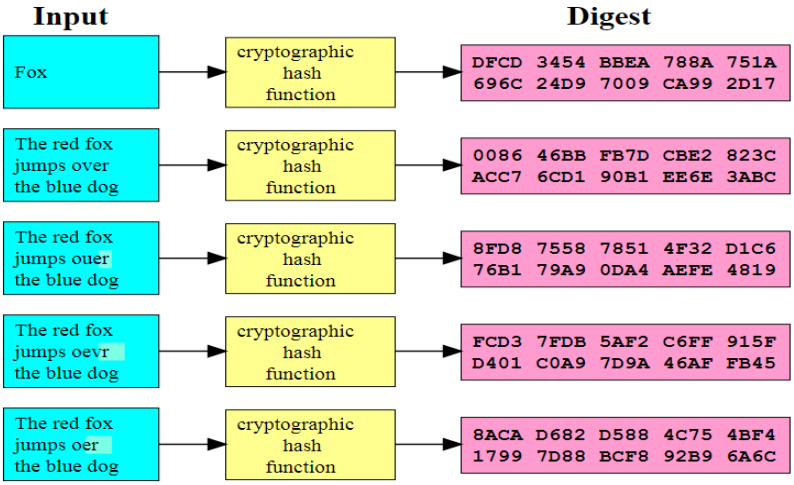
Kriptografski potpis matematički je mehanizam koji omogućuje vlasniku da dokaže svoje vlasništvo određene adrese, odnosno novčanika. U trenutku kada Bitcoin softver potpiše transakciju pripadajućim privatnim ključem, cjelovitoj Bitcoin mreži je omogućen prikaz potpisa koji odgovara izvršenoj transakciji, ali privatni ključ koji zaštićuje račun je nemoguće vidjeti.

Kriptografska hash funkcija preuzima ulazne podatke koji mogu biti bilo koje veličine i pretvaraju ih u relativno kompaktan niz iz kojeg je nemoguće otkriti izvorne podatke. Najmanjim promjenama na ulaznim podacima u hash funkciju, vrijednost hasha se potpuno mijenja (slika 1). Na Slici 1 prikazana

[1] Bitcoin Core je besplatan i open-source softver koji služi kao Bitcoin čvor i pruža digitalni novčanik za Bitcoin koji u potpunosti provjerava plaćanja

je hash funkcija koja uzima ulazni skup znakova (naziva se ključ) i mapira ga na vrijednost određene duljine. (Technopedia - Hash function)

Ako se napravi isti hash od različitih ulaznih podataka dolazi do sudara ili kolizije. Budući da su Bitcoin adrese uglavnom slučajni brojevi, moguće je, iako malo vjerojatno, da dvije osobe neovisno proizvode istu adresu. Ako se to dogodi, onda izvorni vlasnik adrese i vlasnik adrese kreiran sudarom mogu potrošiti novac poslan na tu adresu. Ako biste namjerno pokušali napraviti sudar, trebalo bi 2^{107} puta dulje generirati istu Bitcoin adresu nego stvoriti blok. (Stack exchange)



Slika 1 Hash funkcija (https://en.wikipedia.org/wiki/File:Cryptographic_Hash_Function.svg)

Blockchain Bitcoina koristi SHA256 kao temeljnu kriptografsku hash funkciju. **SHA-256** je sigurna kriptografska hash funkcija koja ulazni podatak pretvara u 256-bitni broj i može izračunati pomoću softvera ili učinkovitije pomoću hardvera. Kako bi se potvrdila autentičnost i vjerodostojnost transakcije, ona prolazi kroz proces verifikacije za kojeg su zaslužni rudari, a zajednici je taj proces poznat pod nazivom rudarenje. Kod rudarenja Bitcoina, rudari traže vrijednost niza bitova, tzv. nonce, koji skupa s blokom transakcija daje hash vrijednost koja ima određena unaprijed zadana svojstva. Izračunavaju hash vrijednost za milijune ulaznih vrijednosti u sekundi, u potrazi za dobitnim rezultatom hasha. Svaki pokušaj ponovnog dobivanja hash-a inkrementira se nonce. Kada se nonce inkrementira, dobiveni hash je potpuno drugačiji od prethodnog hasha. To daje rudaru još jednu priliku za pronalaženje hash vrijednosti koja je niža od objavljene razine težine. (Caetano, 2015)

Bitcoin protokol organiziran je na način kojem je potrebno otprilike 10 minuta da bi se rudario svaki blok (ujedno je to vrijeme potrebno za verifikaciju transakcije). Taj postupak se naziva potvrda (engl. confirmation) određene transakcije. Uzimajući u obzir ovaj razlog, kada se Bitcoin šalje na mjenjačnice ili se kupuje preko trgovina koje odobravaju Bitcoinove kao način plaćanja, te je česti slučaj čekanja na odobrenje transakcije, što u prosjeku zahtijeva nekoliko potvrdi (2-3) i 30-60 min čekanja. (Hrvatski Bitcoin Portal - rudarenje)

U prosjeku Bitcoin procesira oko 7 transakcija po sekundi, što ga čini sporim u odnosu na Ethereumovih 15, Ripple-ovih 1500 i Vizinih koja ima čak 24000 transakcija u sekundi. Tipična naknada za transakciju iznosi 0.0001 Bitcoin (0.63 dolara). Za usporedbu, osoba koja prebacuje 100 dolara vrijednosti s kreditnom karticom, trošak bi iznosio 3.37 dolara. Dok bi transakcija slične vrijednosti Bitcoina koštala najviše 0.63 dolara – čime bi kreditne kartice bile nešto više od 5 puta skuplje za tu transakciju. (Hayes)

2.2. Blockchain

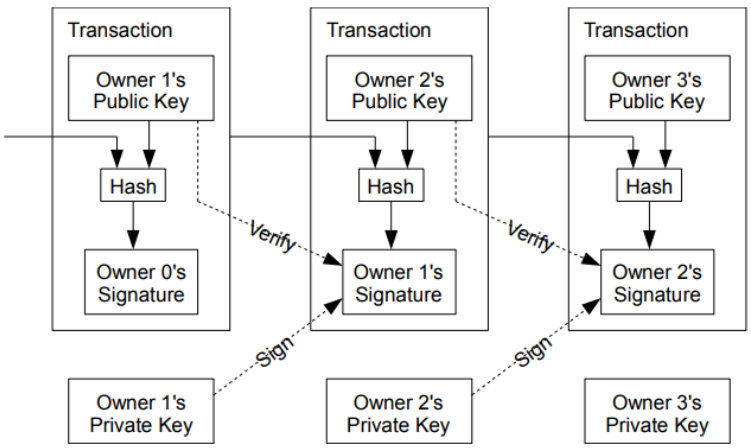
U slučaju Bitcoina, međusobnim natjecanjem računala diljem svijeta „rudare“ Bitcoin.
Bitcoin se sastoji od 3 stvari:

- Protokol (ili skup pravila) koji definira kako mreža treba raditi,
- softverski projekt koji implementira taj protokol i
- mreža računala i uređaja koji rade s programom koji koristi protokol za kreiranje i upravljanjem Bitcoin valutom.

Rudarenje je definirano u protokolu, implementirano u softveru i bitna je funkcija u upravljanju Bitcoin mrežom. Transakcije su najvažniji dio Bitcoin sustava. Sve ostalo u Bitcoin mreži osmišljeno je kako bi se osiguralo da se transakcije mogu stvoriti, potvrditi i konačno dodati u globalnu knjigu transakcija Blockchain. Transakcije su podatkovne strukture koje kodiraju prijenos vrijednosti između sudionika u Bitcoin sustavu. Svaka transakcija je javni unos u Bitcoinovoj knjizi knjigovodstva s dvostrukim unosom, Blockchainom. (Nakamoto)

Rudarenje provjerava transakcije, sprječava dvostruku potrošnju, prikuplja transakcijske naknade. Također potvrđuje transakcije ocjenjujući ih protiv transakcija koje su se dogodile prije. Transakcije ne mogu potrošiti nepostojeće ili već potrošene Bitcoinove. Bitcoinovi se šalju do valjanih adresa, te je važno pridržavati se svih pravila koje definira protokol. Rudari provjeravaju blokove proizvedene od strane drugih rudara kako bi dopustili cijeloj mreži da nastavi s izgradnjom na Blockchainu. (Sterry, 2012)

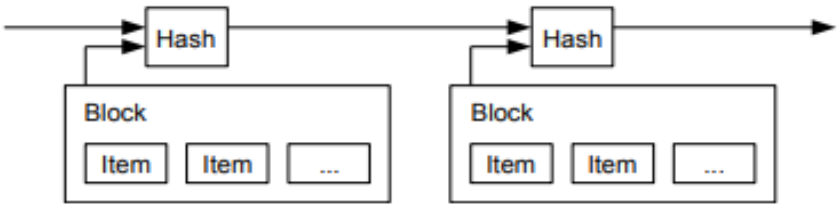
Na Slici 2 vidimo kako Bitcoin definira svoju valutu kao lanac digitalnih potpisa. Svaki vlasnik prenosi novac slijedećem vlasniku sa digitalnim potpisom hasha prethodne transakcije, javnim ključem slijedećeg vlasnika. Primatelj može potvrditi potpise kako bi potvrdio lanac vlasništva. Problem je da primatelj ne može potvrditi da li je jedan od vlasnika dvaput potrošio novac. Zajedničko je rješenje uvesti pouzdano središnje tijelo koji provjerava transakcije za duplu potrošnju. Nakon svake transakcije, novac mora proći središnje tijelo kako se novac ne bi dvostruko utrošio. Problem s ovim rješenjem je da sudbina cijelog novčanog sustava ovisi o onome tko upravlja središnjim tijelom. (Nakamoto)



Slika 2 Opis transakcije u Blockhainu (https://bitcoin.org/bitcoin.pdf)

2.2.1. Timestamp Server / General ledger

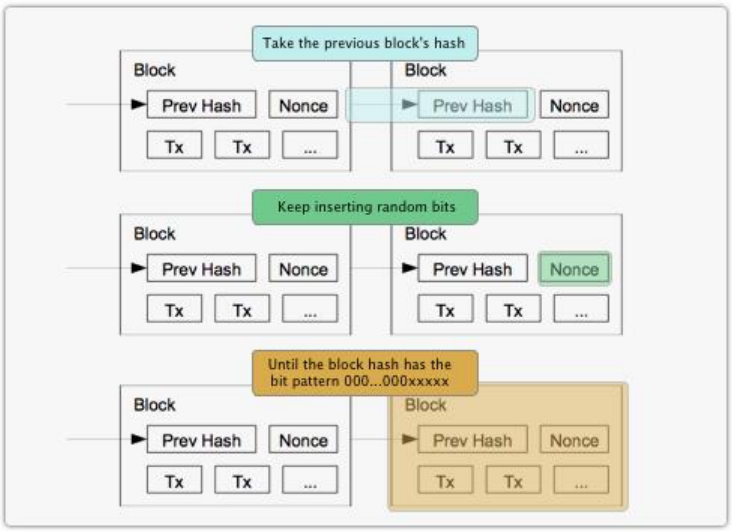
Kod Bitcoina je problem riješen tako da su sve transakcije javne, te je postoji povijest reda u kojem su transakcije primljene tzv. Server vremenskih oznaka(engl. „Timestamp server“). Slika 3 prikazuje vremensku oznaku servera i ona funkcionira tako da se uzme hash iz bloka predmeta koji trebaju dobiti vremensku oznaku, te se taj hash rasprostranjeno izdaje. Svaka vremenska oznaka obuhvaća prethodnu vremensku oznaku u svom hashu, stvarajući lanac, a svaka dodatna vremenska oznaka je pojačana od prethodne. (Nakamoto)



Slika 3 Timestamp server (https://bitcoin.org/bitcoin.pdf)

2.2.2. Proof-of-work

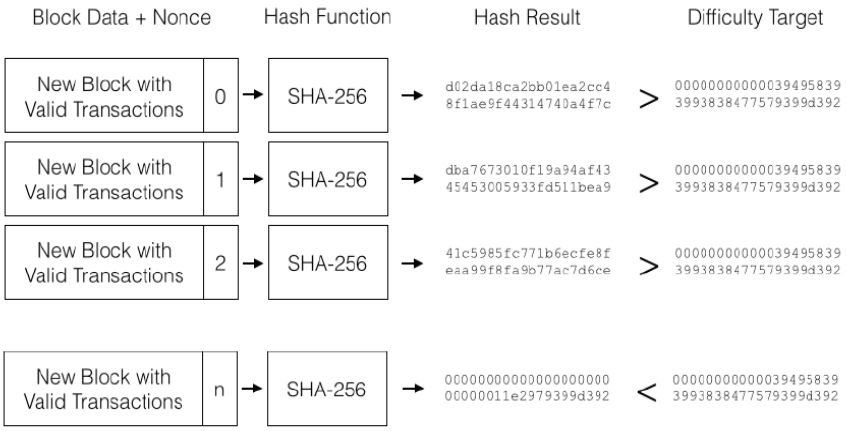
Da bi se implementirala vremenska oznaka na peer-to-peer osnovi, mora se koristiti sustav Dokaz o radu (engl. proof-of-work). Dokaz o radu uključuje skeniranje vrijednosti kad je hashirana, npr. sa SHA-256, tada hash počinje sa brojem od nula bitova. Na Slici 4 vidljivo je da se za vremensku oznaku uzima hash iz prijašnjeg bloka, te se provodi dokaz o radu. Prilikom tog procesa povećava se nonce u bloku, sve dok se ne pronađe vrijednost koja hashu iz bloka daje potrebne bitove nula. (Nakamoto)



Slika 4 Proof-of-work (https://crobitcoin.com/wp-content/uploads/2014/02/bitcoin-diagram-490-1.png)

Nonce u bloku Bitcoina je 32-bitno (4 bajta) polje, čija je vrijednost namještena od rudara, tako da je hash blok manji ili jednak trenutnom cilju mreže. Ostala polja ne smiju se mijenjati, jer imaju određeno značenje. Svaka promjena podataka u bloku (kao što je nonce), učinit će blok hash potpuno drugačijim. Budući da se vjeruje da je nemoguće predvidjeti koja će kombinacija bitova

rezultirati pravim hashom, puno različitih nonce vrijednosti se pokušava, a hash se ponovno obrađuje za svaku vrijednost, dok se ne pronađe hash manji ili jednak trenutnom cilju mreže. Potreban cilj je također predstavljena kao poteškoća, pri čemu veća težina predstavlja niži cilj. Budući da ovaj iterativni izračun zahtijeva vrijeme i resurse, prikaz blokova sa ispravnom nonce vrijednošću predstavlja dokaz rada. (Bitcoinwiki - Nonce)



Slika 5 Povećavanje nonce-a za stvaranje hasha do pronalaska rješenja. (Learning Bitcoin – Richard Caetano)

Na Slici 5 prikazani su podatci o bloku, koji se sastoje od valjanih transakcija i nonce a, raspršeni su mnogo puta dok se ne pronađe hash vrijednost koja je manja od razine težine. Vidljivo je da se isti podaci iz bloka koriste s inkrementiranim hashom kako bi se izračunala hash vrijednosti. Koristeći „brute force“ [2] pristup, rudari čini mnoge milijune pokušaja da pronađu n, nonce koji proizvodi dobitni hash rezultat. (Caetano, 2015)

2.2.3. Decentralizirani konsenzus

Blockchain nije stvorio središnji autoritet, već ga samostalno sastavlja svaki čvor u mreži. Svaki čvor u mreži, djelujući na informacije prenesene preko nesigurnih mrežnih veza, može doći do istog zaključka i sastaviti kopiju iste javne knjige kao i svi ostali. Glavni izum Satosha Nakamota je decentralizirani mehanizam za nastupanje konsenzusa. Konsenzus se ne postiže eksplicitno - nema izbora ili fiksnog trenutka kada se dogodi konsenzus. Umjesto toga, konsenzus je izmišljena tvorevina asinkrone interakcije tisuća nezavisnih čvorova gdje svi slijede jednostavna pravila.

Sva svojstva Bitcoina, uključujući valutu, transakcije, plaćanja, sigurnosni model koji ne ovise o središnjem autoritetu, proizlaze iz ovog izuma. Bitcoinov de-centralizirani konsenzus proizlazi iz interakcije četiri procesa koji se neovisno događaju na čvorovima preko mreže:

- Nezavisna provjera svake transakcije, po svakom punom čvoru
- nezavisno sakupljanje transakcija u nove blokove zajedno s prikazanim računanjem kroz „Dokaz o radu“,
- nezavisna provjera novih blokova po svakom čvoru i sklapanje u lanac i
- neovisni izbor, po svakom čvoru, lanca s najraširenijim računanjem pokazan kroz „Dokaz o radu“. (Antonopoulos)

[2] „Brute force“ algoritam služi za pronalaženje djelitelja prirodnog broja n da bi mogli nabrojati sve cijele brojeve od 1 do n i provjeriti da li svaki od njih dijeli n bez ostatka. (Wikipedia - Brute force search)

2.3. Rudarenje

Korisnici šalju Bitcoinove međusobno preko cijele Bitcoin mreže. Nužno je vođenje evidencije o transakcijama kako bi svaki pojedini korisnik imao uvid u količini novaca koje posjeduje. Bitcoin mreža radi na način da se u određenom periodu sakupe sve transakcije i stavljaju u Blockchain. Posao rudara je zapisivanje i potvrđivanje transakcija u „General ledger“ (glavnu knjigu), a za nagradu rudar dobije svotu Bitcoina.

Glavna knjiga je dugi lanac blokova koji se koristi za provjeru transakcija napravljene u bilo kojem vremenu između Bitcoin adresa. Nakon izrade transakcijskog bloka , on se dodaje u Blockchain, što stvara listu svih ikad napravljenih transakcija na Bitcoin mreži koja je dostupnima svima koji žele znati što se događa u mreži na https://blockexplorer.com/. (Hrvatski Bitcoin Portal - rudarenje)

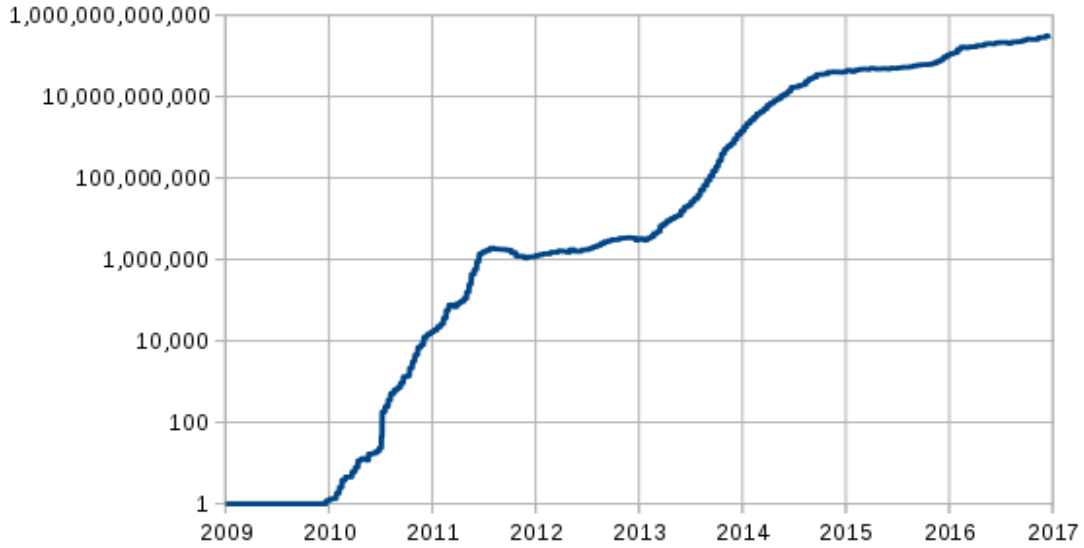
Nakon kreiranja transakcijskog bloka, rudari ga postavljaju u proces obrade. Rudari uzimaju informacije iz bloka i primjenjuju hash funkciju. Zajedno sa blokom, taj hash je pohranjen na kraju Blockchain-a. Međutim, rudari koriste hash zadnjeg bloka pohranjenog u Blockchain-u, jer je hash svakog bloka napravljen od hash bloka prije njega pa taj blok postaje digitalni pečat. To potvrđuje da je taj blok i svaki slijedeći legitiman, jer ukoliko bi se mijenjalo, promjena je vidljiva. Prilikom pokušaja krivotvorenja transakcije mijenjajući već pohranjen blok u Blockchain-u, doći će do promjene hasha tog bloka. Ako se provjerava autentičnost bloka pomoću hash funkcije, tada se dolazi do otkrića da je hash drugačiji od već pohranjenog bloka u Blockchain-u. Dolazi se do spoznaje da je blok krivotvoren. Hash svakog bloka koristi se za stvaranje slijedećeg bloka u Blockchain-u i mijenjanjem jednog bloka izazvala bi se promjena sljedećeg bloka.

Mijenjanjem bilo kojeg bloka prouzrokuje se lančana reakcije koja bi se protezala do kraja lanca. Prilikom uspješnog kreiranja hasha, rudari dobivaju 25 Bitcoina, lanac blokova se ažurira i svi na mreži budu obaviješteni. To je jedan od načina da se potakne rudare da nastave rudariti i da transakcije funkcioniraju. No, Bitcoin mreža je učinila stvari težima, jer bi inače svi stvarali svake sekunde tisuće hasheva, a svi Bitcoinovi bili bi „iskopani“ u par minuta. Zato je Bitcoin protokol otežao situaciju pomoću dokaza rada. Bitcoin protokol ne prihvaća bilo kakav hash, nego zahtjeva da hash ima određeni broj nula (0) na početku. Ne možemo znati kako će hash izgledati prilikom stvaranja, ali svaki put prilikom dodavanja novog komadića podatka, hash će poprimiti drugačiji oblik. Unutar transakcijskog bloka rudarima nije dopušteno mijenjati podatke, ali su obavezni mijenjati podatke tijekom korištenja kako bi kreirali drugačiji hash. Radnju izvode nasumično, koristeći drugi dio podataka zvan nonce. Kako bi se stvorio hash, nonce se koristi s transakcijskim podatcima. Nonce se kako bi stvorio hash se koristi s transakcijskim podatcima. Nonce se mijenja ako hash ne odgovara formatu i cijela stvar se ponavlja. Za pronalazak odgovarajućeg nonce-a potrebno je mnogo pokušaja, zbog čega na mreži svi rudari rudare u isto vrijeme istu stvar tj. zarađuju Bitcoinove.
(Hrvatski Bitcoin Portal - rudarenje)

2.3.1. Hash rate i težina rudarenja

Hash je izlaz hash funkcije, kako što se odnosi na Bitcoin, Hash rate je brzina kojom računalo izračunava operaciju u Bitcoinovom kodu. Što je veći hash rate, u rudarenju povećava vašu priliku za pronalaženje slijedećeg bloka i primanje nagrade. Jednostavno rečeno, hash rate može se definirati kao brzina kojom određeni stroj za rudarenje radi. Hash rate izračunava se u hashevima u sekundi (h/s). Neki od uobičajenih pojmova upotrebljavaju mega, giga i tera, ovisno o broju hasheva. Na primjer, stroj s brzinom od 60 hasheva u sekundi će napraviti 60 pretpostavki u sekundi kada pokušava riješiti blok. Kilohash (KH/s) koristi se za 1000 hasheva, megahash.a (M /s) za 1000 kilohash, terahash (TH/s) za 1000 megahash i petahash (PH /s) za 1000 terahash. (Buybitcoinworldwide - Hash rate)

Kako se povećava konkurencija za nagradu za blok, povećat će se broj rješenja pronađenih do teškog računalnog problema. S više rudara koji traže rješenje, prosječna brzina mogla bi postati manja od predviđene brzine od jednog novog bloka svakih 10 minuta. Kako bi se to izjednačilo, izračunava se razina težine i prilagođava se svakih 2016 blokova. Izračun uzima u obzir transakcije u posljednja 2 tjedna kako bi stvorili ciljanu težinu. Ako je prosjek manji od prosjeka 10 minuta, težina se povećavam, a ako je iznad, težina se smanjuje. (Caetano, 2015)



Slika 6 Relativna težina rudarenja od 2009. do 2015. (https://en.wikipedia.org/wiki/File:Difficulty.svg)

Pomoću mjere težine, rudar može napraviti neka osnovna predviđanja o tome koliko mnogo računalnih snaga će biti potrebno za miniranje jednog Bitcoina. (Caetano, 2015)

Ovo su neke činjenice vezano za Bitcoin proces rudarenja:

- Približno svakih 10 minuta, pronađena je nagrada za blok
- Svaka dva tjedna podešava se stupanj težine
- Svake četiri godine, nagrada za blok je prepolovljena
- Pronaći će se samo 21 milijun Bitcoina
- 99% Bitcoina biti će rudareno do 2032. godine

Oko 2015. godine, više od 60% svih Bitcoina rudareno je, a trenutačna nagrada za blokiranje postavljena je na 12.5. (Bitcoin Block Reward Halving Countdown)

3. Povijesni razvoj hardvera

Sa osnovnim znanjem o Bitcoin rudarenju, može se jasnije razumjeti njegov razvitak u posljednjih 9 godina. U počecima, rudarenje je uključivalo rješavanje kriptografskih problema, koji su se zbog svojih nižih razina težine mogli riješiti sa procesorom osobnog računala. Međutim, kako se broj transakcija i ljudi povećao u mreži, pojačala se procesna snaga potrebna za rudarenje. Kad god mreža otkrije da se snaga obrade od strane rudara poveća, isto se događa da se zadrži konstanta stvaranja bloka za 1 blok svakih 10 minuta. Ako uzmemo u obzir Mooreov zakon, znamo da su procesori dužni postati učinkovitiji tijekom određenog vremena, što je potaknulo razvoj posebnih uređaja za rudarenje tzv. hardver za rudarenje kriptovaluta. Najbitnija 3 čimbenika za hardver su:

1. Hash rate,
2. potrošnja električne energije i
3. cijena hardvera.

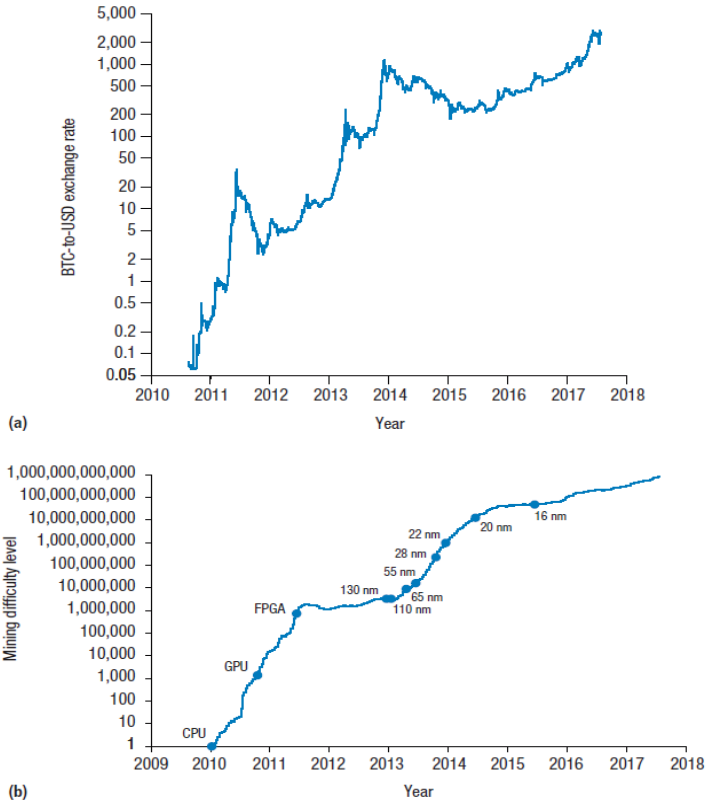
Hash rate je broj izračuna koji hardver može izvesti u jednoj sekundi. Hash rate je ključni aspekt hardvera. Što je veći, to je veća vjerojatnost da možete riješiti složene matematičke izračune i dobiti BTC nagradu.

Potrošnja električne energije je bitan faktor rudarenja. Naravno, što je moćniji hardver, to je veći trošak energije koji se očekuje. Međutim, neka su rješenja troškovno učinkovitija od drugih. Na primjer, da li prihod od rudarstva nadoknađuje račune za struju, provjeri li se potrošnja električne energije u wattima.

Cijena definira količinu uloženih sredstava u hardver. Očekivanje velike zarade i bogatstva na Bitcoinu sa jeftinim rudarskim hardverom malo je vjerojatna. Ulaganje u hardver predstavlja veće mogućnosti zarade, no povrat uloženog novca ipak se očekuje u nešto duljem vremenskom intervalu.

Na Slici 7, graf b prikazuje težinu rudarenja kroz povijest. Početna težina 1 odgovara četiri do osam jezgri opće namjene koje pokreću „nonce search“ algoritam, koji ispituje oko 7 milijuna dvostrukih SHA funkcija[3] po sekundi. U srpnju 2010. godine hash rate ukupne mreže je dosegla 850 miljardi (6 exahasheva po sekundi). Zaradom od jednog bloka odgovara oko 271 dvostrukih SHA-256 hashova, impresivna količina izračuna jer svaki dvostruki hash je sam po sebi nekoliko tisuća operacija. (Taylor, 2017)

[3] Kada hash funkcija proizvodi isti izlaz za dva različita ulaza, to se zove sudar. Neophodno je izbjegavati sudare kako bi se zajamčio integritet podataka. Ako dva dijela podataka proizvode isti hash, onda se može zamijeniti drugom, što dovodi do sloma kontinuiteta. U praksi, Bitcoin zapravo koristi dvostruku SHA265 hash funkciju kako bi se smanjila vjerojatnost sudara. (The Evolution of the Cryptographic Hash Function in Blockchains)

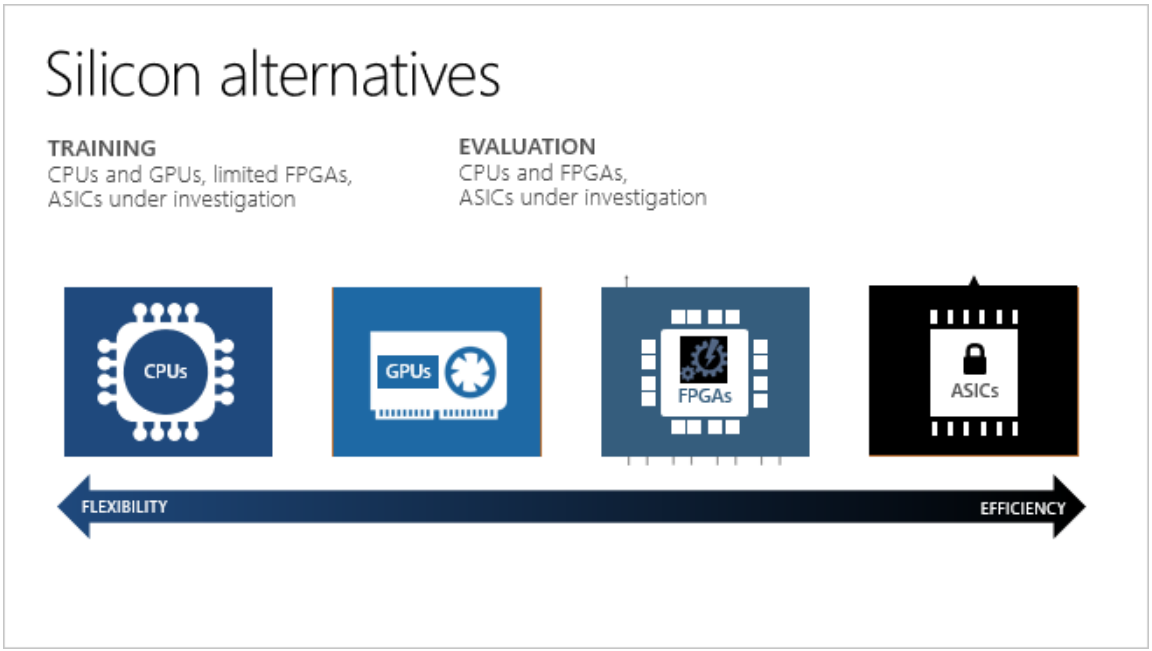


Slika 7 cijena i težina rudarenja Bitcoina kroz povijest (The evolution of Bitcoin hardware, Taylor)

Na povećanje težine u rudarenju utječu porast tečaja, koji može pokriti troškove više hardverskih sklopova odjednom. Softver i hardver za rudarenje se stalno poboljšavaju. Pad težine je često puta paralelan sa „puknućem balona“ tzv. nagli pad cijene Bitcoina. U takvim slučajevima vrijednost Bitcoina nije opravdala operativne troškove za manje učinkovite rudare, a njihovi korisnici su prekinuli s radom.

Najraniji oblik rudarenja Bitcoina bio je uz pomoć CPUa računala. Prvi softver za rudarenje je objavio Satoshi Nakamoto koji je dopusti korisnicima da održavaju mrežu. Točke na grafu b pokazuju kad je uvedena nova Bitcoin oprema za rudarenje. Prvi javno dostupni GPU rudar baziran na CUDA tehnologiji pojavio se u rujnu 2010. godine, mjesec dana nakon što je izašao je OpenCL rudar. Ubrzo nakon toga, u studenom 2010. godine pojavila se mogućnost grupnog rudarenja (engl.„pool mining“) koji omogućava većoj grupi rudara da zajedno rudare i podjele nagradu srazmjerno. Grupno rudarenje se u kratkom roku povećao na tisuće članova, dajući korisnicima male, ali česte isplate svakih nekoliko mjeseci, umjesto velikih 50 ili 25 Bitcoinova. Do tog vremena, rudarenje bloka bilo je ekvivalentno nekoliko mjeseci računanja za jednog korisnika GPU rudara. (Taylor, 2017)

FPGA (engl. Field Programmable Gate Array) rudari pratili su GPU rudarenje. Takvo hardversko rješenje sadržava posebne programibilne integrirane sklopove s ciljem rudarenja Bitcoi-a. Uvođenjem FPGA rudara, CPU i GPU rudarenje postali su zastarjeli, jer se nisu mogli natjecat s radom FPGA rudara. Nažalost vijek FPGA sklopova bio je kratkotrajan sve dok se nije Application Specific Integrated Circuits (ASICs) pojavio na tržište. ASIC rudari s klijentskim čipovima pružili su daleko veću izvedbu od bilo kojeg drugog rudarskog hardvera dostupnog.



Slika 8 Prikaz mining hardvera u odnosu na fleksibilnost i efikasnost (https://docs.microsoft.com/en-us/azure/machine-learning/service/media/concept-accelerate-with-fpgas/azure-machine-learning-fpga-comparison.png)

Na Slici 8 Prikazan je odnos fleksibilnosti i efikasnosti hardvera .Kada je u pitanju fleksibilnost, središnje jedinice za obradu (CPU) su iznimno fleksibilne i dizajnirane su za rukovanje širokim rasponom računalnih scenarija tako da mogu pronaći u širokom rasponu uređaja poput stolnih računala, prijenosnih računala, tablet računala, pametnih telefona, televizora i dronova. Grafičke jedinice za obradu (GPU-ovi), kao što naziv implicira, optimalni su za obradu slika, animacija i videozapisa. Uz GPU-ove gubi se dio fleksibilnosti procesora, ali se povećava učinkovitost i performansa prilikom obrade. FPGA imaju konfigurabilne logičke blokove povezanih preko programibilnih međusobnih veza, koji omogućuju programiranje FPGA-ja za specifične aplikacije. Posljednje, ali ne manje važno, su ASIC-ovi. Specifičan integrirani krug specifičan za aplikaciju (ASIC) je sklop prilagođen za određenu upotrebu, a ne namijenjen za opću namjenu. Na primjer, čip koji je dizajniran za specifičnu uporabu na visokoučinkovitom trgovanju na financijskim tržištima je ASIC. To će raditi bolje od čipova opće namjene za visoke frekvencije trgovanja, ali neće biti dobri za bilo što drugo. Sposobnost reprogramiranja logike FPGA je različit kada ih uspoređujete s ASIC-ovima, CPU-ovima i GPU-ima koji drže istu logiku od kada su proizvedeni.

3.1. Prva generacija hardvera - CPU

Prijelaz iz jednostavnog preglednog članka (engl. whitepaper) u nešto stvarno je trenutak kada je tvorac Satoshi Nakamoto proizveo što je danas poznato kao „genesis block“. Genesis block je naziv za prvi Bitcoin blok transakcija, generiran s CPU-om. Samo tjedan dana nakon, Satoshi je najavio puštanje Bitcoin verzije 0.1 na kriptografsku mailing listu[4].

[4] Članak o bitcoin v0.1 od samog tvorca Satoshija Nakamota
https://www.mail-archive.com/cryptography@metzdowd.com/msg10142.html

U samim početcima rudarenja koristio se CPU. Tako se u par dana sa Pentium 4 ili sličnim procesorom moglo zaraditi 100 ili 200 Bitcoinova. Oni su hashirali između 1 i 2 MH/s za korištenih 50 Watta, 0.04MH/watt. Zarada dobivena u to vrijeme najviše je ovisila o vrsti procesora.

Tablica 1 Usporedba CPU-a u prvoj generaciji hardvera za rudarenje

Ime modela	Broj jezgri	Frekvencija (Ghz)	Brzina rudarenja (MH/s)	Prosječna snaga rada (watt)
Intel(R) Core(TM) i3 M350	2	2.27	1.48	35
Intel(R) Core(TM) i5 CPU M 450	2	2.40	1.80	35
AMD Athlon 64 X2 Dual Core Processor 4400+	2	2.30	2.09	65
Intel(R) Celeron(R) E3300	2	2.50	2.20	65
Intel (R)Pentium(R) Dual-Core E5400	2	2.70	2.27	65
Athlon 64 X2 5000+	2	2.30	2.31	65
AMD Athlon(tm) II X2 240e Processor	2	2.80	2.70	45
AMD Athlon(tm) 64 X2 Dual Core Processor 6000+	2	3.00	2.81	89
Intel Xeon E5430	4	2.66	3.04	80
AMD Phenom X4 9650	4	2.30	4.90	95
Intel(R) Xeon(R) E5520	4	2.27	6.50	80
Intel(R) Xeon(R)E5530	4	2.40	7.13	80
Intel(R) Core(TM) i7 980x	6	3.33	25.00	130
Intel(R) Core(TM) i7 990x	6	3.46	33.0	130

Izvor: (Bitcoin forum) **,** (Intel - Product specifications) i (CPU Benchmark)

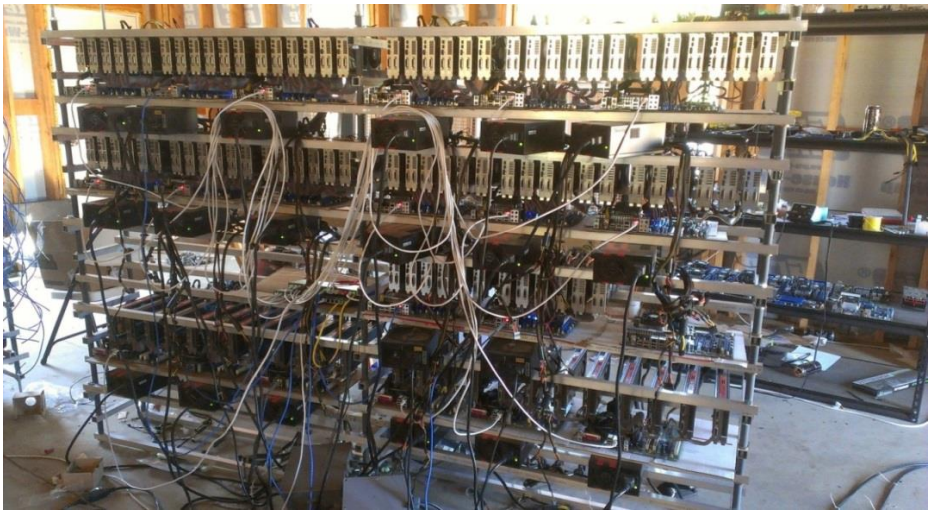
U Tablici 1. prikazane su različite vrste CPU-a koji su se koristili u razdoblju od 2009. do 2010. godine. Opisane su osnovne specifikacije svakog CPU-a, te njihova brzina rudarenja. Ako se koristio Core i7 990x, najbolji u klasi, dobilo se 33 MH/s. S time završava prva generacija hardvera za rudarenje.

3.2. Druga generacija hardvera- GPU

Druga generacija rudara uglavnom se sastoji od grafičkih kartica. Grafička kartica u računalu prikazuje sliku na zaslonu monitora. Bio to program, tekst ili igra, ona je zaslužna za prikaz na zaslonu. Grafička kartica dolazi kao zaseban dio ili je integrirana na matičnoj ploči. Putem sabirnice povezana je računalom. Grafičke kartice opremljene su snažnim grafičkim procesorima,koji brojem tranzistora i svojom snagom obrađivanja gotovo nadmašuju centralne procesore (CPU) nekog računalnog sustava. Intenzivna konkurencija značila je brzo zastarivanje CPU-a, što je navelo rudare traženje bržeg načina rudarenja Bitcoina. U obzir je uzet GPU koji do tada nije korišten za rudarenje. Ti čipovi su napravljeni za obradu video efekata. Bili su sveprisutni na računalima jer su potrebni za prikazivanje 3D grafike i vizualnih efekata. U usporedbi sa CPU-ovima, GPU-ovi su brži za izvršavanje ste operacije na velikom broju podataka. Bitcoin rudarenje zahtijeva ponovljene izračune hasha, kako bi se pronašlo rješenje. Zbog toga su GPU-ovi prikladniji za rudarenje od procesora. Za razliku od CPU rudarenja koji je u osnovi jedan uređaj, GPU rudarenje može sadržavati niz hardvera koji su povezani s matičnom pločom. To je poznato kao GPU „mining rig“.

Slika 9 Mining rig (http://www.coinminingrigs.com/wp-content/uploads/2017/08/6-gpu-ethereum-mining-rig-running-amd-rx-480-gpus.png)

Na Slici 9 prikazan je primjer jednog mining rig-a sa šest GPU-a spojenih na matičnu ploču. Matične ploče u prosjeku dolaze sa 2,3 ili naviše 4 PCI Express utora veličine (x16), te još 2 ili 3 manja (x8, x4, x1). Za rudarenje su potrebni svi utori, uključujući x1 utore. Kako bi se mogli iskoristiti, potreban je „PCIe riser“. Oni dozvoljavaju da se grafičke kartice odmaknu od matične ploče, te da se na jednu matičnu ploču spoji onoliko grafičkih kartica koliko postoji PCI Express utora na matičnoj ploči. To su dodatci koji se sastoje od jednog PCI Express konektora x1 veličine (na matičnoj ploči njega spajamo u PCIe port) i pločice sa PCI Express utorom x16 veličine, koju na željeno mjesto postavimo i na nju utaknemo GPU. Za napajanje pogona svih GPU-ova preporučuje se korištenje visokoučinkovitog izvora napajanja. Preporučuju se modeli sa certifikatima 80 PLUS Titanium, Platinum, Gold, Silver, Bronze. Da bi sustav imao povećan protok zraka koristi se „open air frame“.



Slika 10 Rudarska farma (https://securityxt.com/wp-content/uploads/2018/07/what-are-big-crypto-miners-called-main.jpeg)

Najuspješnije Bitcoin rudarske operacije su preseljene u skladišne prostore s velikim volumenom zraka za hlađenje i jeftine industrijske snage. Na Slici 10 prikazan je podatkovni centar, tehnički opremljen za rudarenje Bitcoina ili drugih kriptovaluta, tzv. Rudarska farma (engl. Mining farm). Jedan od glavnih resursa u koji rudar mora uložiti je električna energija. Ona je također faktor rizika, budući da rudarenje zahtijeva trajni izvor napajanja od 24 sata dnevno. Osim toga, veliki broj procesora zahtijeva odgovarajući sustav hlađenja i ventilacije.

Tablica 2 Usporedba GPU-a u drugoj generaciji hardvera za rudarenje

Ime modela	Graphics clock (Mhz)	DRAM (MB)	Brzina rudarenja (MH/s)	Prosječna snaga rada (Watt)
NVidia GeForce 8800 GTS	513	640	16.8	135
Nvidia GTS450	783	1024	32.2	106
NVidia GTX260	576	896	37.5	182
ATI Mobility Radeon HD 5650	550	1024	48	35
ATI Radeon HD5570	650	1024	59	39
ATI Radeon HD4870	750	512	78	150
2x NVidia GeForce GTX 460 SLI	675 (x2)	1024 (x2)	102	160 (x2)
ATI Radeon HD5850	725	1024	236	151
ASUS ATI Radeon HD5870	850	1024	299	188

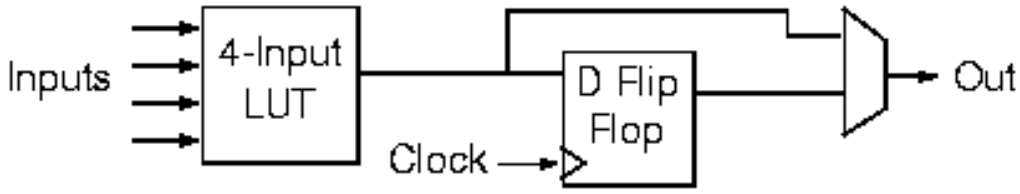
Izvor: (Bitcoin forum) **,** (Intel - Product specifications) **i** (CPU Benchmark)

U Tablici 2. možemo vidjeti da tipičan AMD-ov GPU pokazuje veću produktivnost rudarenja nego popularni nVidia kada usporedimo frekvenciju 'Gh /s' s vrijednošću '$'. Upravo zbog toga AMD GPU-ovi i dalje su popularni u rudarenju.

3.3. Treća generacija hardvera – FPGA

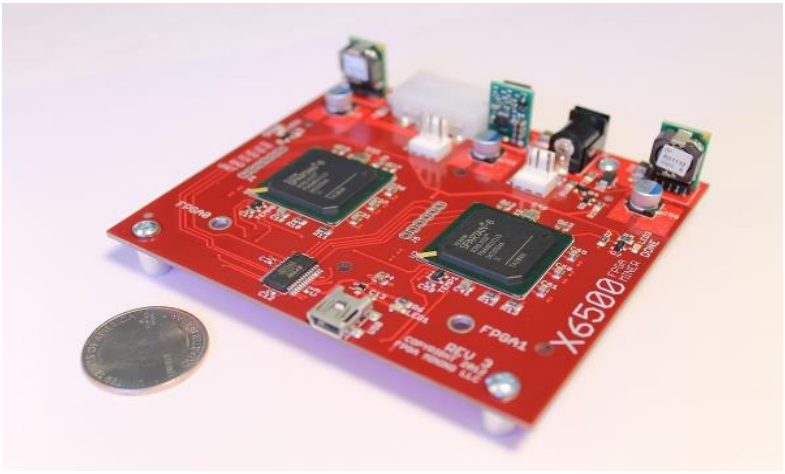
Težina rudarenja se nastavila podizati. U lipnju 2011. godine uvođenjem FPGA u Bitcoin rudarenje, označio se prijelaz s hardvera koji se mogu koristiti za svakodnevne primjene potrošača na specijalizirani hardver koji se mogu koristiti za brže rudarenje Bitcoina.

FPGA (engl. field-programmable gate array) je poluvodički uređaj koji se sastoji od mnogih logičkih blokova s konfigurabilnim međusobnim vezama. To je integrirani krug dizajniran za konfiguraciju sa strane potrošača nakon proizvodnje. Konfiguracija FPGA općenito se definira korištenjem jezika opisnog hardvera (VHDL).



Slika 11 Struktura logičkog bloka FPGA (http://www.eecg.toronto.edu/~vaughn/challenge/fpga_arch.html)

Na Slici 11 vidimo glavnu komponenta FPGA, a to je logički blok. Logički blokovi sposobni su djelovati kao jednostavna logička vrata, kao što su AND i XOR. Osim logičkih vrata, postoje usmjeravajući kanali koji se pokreću između svakog logičkog bloka. Ovi kanali se mogu programirati i omogućuju različitim logičkim blokovima međusoban razgovor. Milijuni logičkih blokova su replicirani u mreži kroz čip. Oni se provode u tablici za pretraživanje (engl. Lookup Table) koja se obično sastoji od četiri ulazna pin-a. Tablica za pretraživanje ima mali komad memorije koji je programiran za izlaznu logiku ovisno o ulazu. Svaka Tablica ima samo jedan izlaz. Izlaz se zatim može pohraniti u flip-flopu kako bi se očuvale vrijednosti tijekom satnih ciklusa ili se može pokrenuti na druge tablice pretraživanja za daljnju implementaciju logike. Kanali usmjeravanja, koji se odvijaju između logičkih blokova, koriste se za povezivanje različitih tablica zajedno. Kanali usmjeravanja kontroliraju se blokovima koji kontroliraju veze između žica za prijelaz. Te veze omogućuju ogromnu količinu konfigurabilne logike koja FPGA omogućuje da provede funkcionalnost. Na Slici 12 prikazan je primjer jednog od FPGA rudara. (FPGA Architecture for the Challenge)



Slika 12 FPGA X6500 Rev. 3 (http://fpgamining.com/assets/images/x6500_rev3_angle_a.jpg)

FPGA su dobri u procesiranju SHA-256 rotacije po konstanti i operacijama s bitovima, ali ne s 32-bitnim operacijama. Tipični FPGA rudar replicirao je više SHA-256 funkcija i odmotao (engl.unroll-ao)[5] ih. Sa potpunim odmotavanjem, modul je stvorio različite hardvere za 64 hash runde, od kojih je svaki bio odvojen od registara cjevovoda (engl. pipeline). Ti registri su sadržavali izlaz hash funkcije kao i 512-bitni blok koji se hashirao. Stanje za ispitivanje nonce-a se nastavlja niz cjevovodom. Jedan stupanj po ciklusu, dopuštajući za propusnost jednog ispitivanja nonce (hash) po ciklusu. Hakeri su razvili prilagođene ploče koje su smanjile nepotrebne troškove zbog RAM-a i I / O-a , a koje su usredotočene na pružanje dovoljne snage i hlađenja. Ove ploče dosegle su 215 MH/s stope s Spartan XC6SLX150 dijelovima. Quad-chip ploče razvijene su kako bi smanjile izradu ploče, montažu i troškovima materijala dosegnuvši 860 MH/s na 216 MHz i 39 W, te imaju cijenu od 1.060 dolara. Kansas-based BFL je ponudio ne-open source verziju za $ 599 sa sličnim performansama od 830 MH/s. BFL je na svim računima najuspješniji komercijalni dobavljač FPGA rudara. FPGA-ovi su imali poteškoća s konkurencijom po cijeni po GH/s s velikim brojem GPU-ova koji su bili na naprednijim procesnim čvorovima i prodavani na maloprodajnim mjestima kao što su Newegg. Međutim, FPGA je bio pet puta više energetski učinkovit nego GPU, pa čak i nakon ukupnog troška vlasništva (TCO) nakon godinu ili dvije. Ipak, vladavina FPGA rudara bila je kratka jer su ASIC-ovi stigli ubrzo nakon toga, pružajući narudžbe velikih troškova i poboljšanja energetske učinkovitosti. (Taylor, 2017)

Tablica 3 Usporedba FPGA-a u trećoj generaciji hardvera za rudarenje

Ime modela	Brzina rudarenja (MH/s)	Prosječna snaga rada (Watt)	Cijena ($)
Bitcoin Dominator X50000	100	6.8	440
BitForce SHA256 Single	832	80	599
Butterflylabs Mini Rig	25,200	1250	15295
Icarus	380	19.2	569
ModMiner Quad	800	40	1069
X6500 FPGA Miner	400	17.2	550

Izvor (Bitcoin.it - Mining hardware comparison)

Danas FPGA mogu izvoditi mnoge različite aplikacije. FPGA-i imaju veliki kapacitet za proces paralelizacije i cjevovoda. Često se koriste kao periferne jedinice na CPU-ovima kako bi izvršili specifične procese sa kojima CPU-ovi imaju problema s rukovanjem. Glavni problem s ovim uređajem bio je prilično velika cijena (gotovo 30% veća), te odnos performansi/troškovima je bio manji u usporedbi s GPU rudarima. Rudarenje kriptovaluta pomoću FPGA nije trajalo jako dugo i uskoro je zamijenio ASIC, nova generacija hardvera koji je bio posebno namijenjen rudarenju.

[5] smanjiti broj ciklusa sata koji su potrebni za izvršenje SHA256 hash računanja sa uvođenjem više krugova SHA256 funkcija kompresije kombinacijskom logikom (Naik)

3.4. Četvrta generacija hardvera – ASIC

ASIC („Application – Specific Integrated circuit“) je specijaliziran integrirani krug koji je samo namijenjen za rudarenje Bitcoina. Oni su dizajnirani za jednu jedinu svrhu i funkcioniraju isti za cijeli operativni život. Sa svojim performansama nadilazi CPU, GPU i FPGA uređaje, uz relativno nisku potrošnju energije. Njegova logička funkcija ne može se mijenjati na bilo što drugo jer je njegov digitalni krug sastavljen od trajno spojenih vrata i flip-flopova u siliciju. Logička funkcija ASIC-a određena je na sličan način kao u slučaju FPGA, koristeći jezike opisane hardvera kao što su Verilog ili VHDL. Razlika u slučaju ASIC je da je rezultirajući krug trajno uvučen u silicij, dok je u FPGA sklop napravljen povezivanjem brojnih konfigurabilnih blokova. Kako su veličine značajki smanjene i dizajnirani alati tijekom godina poboljšani, maksimalna složenost (i stoga funkcionalnost) koja je moguća u ASIC-u je narasla sa 5,000 logičnih vrata na više od 100 milijuna. Moderni ASIC često uključuju cijele mikroprocesore, memorijske blokove, uključujući ROM, RAM, EEPROM, flash memoriju i ostale velike građevne blokove. (Singh)

Premda neki ASIC uređaji podržavaju dvije kriptovalute (Litecoin i Bitcoin), takvi modeli posjeduju 2 ASIC čipa npr. Greedseed 5-Chip. Druge kriptovalute npr. Ethereum, nije moguće rudariti pomoću ASIC-a. Temeljni problemi ASIC uređaja su visoka cijena, teška dobavljivost, te njihovo korištenje u kućnim uvjetima. To je zato jer ih najveći igrači na polju kriptovaluta ponajviše kupuju, tj. oni koji sastavljaju rudarske farme i koji mjesečno na struju troše stotine tisuće dolara, ali istovremeno zarađuju milijunske iznose.

3.4.1. Prva generacija ASIC-a

Godine 2012. na tržište su došle 3 tvrtke sa ASIC Bitcoin rudarima: Butterfly Labs, ASICMiner i Avalon. Dizajn je bio temeljen na FPGA rudarima. ASIC je donio ogromne prednosti nad prethodnim uređajima, no naglasak je bio na što brži početak uporabe, koja nužno nije morala biti optimalna, te da se izrade što je brže moguće.

Butterfly labs nakon uspjeha od svojih FPGA rudara, prvi su objavili svoju ASIC liniju proizvoda.
Tvrtka je u lipnju 2012. godine uzimala prednarudžbe za 3 tipa ASIC rudara:

- Jalapenos 4,5 GH/s ($149,00),
- Single SC 60 GH/s ($1.299,00) i
- Mini Rigs 1500 GH/s ($30.000,00).

Slika 13 ASIC Bitcoin Miner - Butterfly Labs Jalapeño (https://fs.bitcoinmagazine.com/img/images/butterfly-labs-ships-first-finished-asic-for-re.original.jpg)

Na Slici 13. Prikazan je jedan od tri tipa rudara – „Butterfly Labs Jalapeño„. Po tim cijenama ASIC rudari su mogli generirati 20 do 50 puta više Bitcoina po uloženom dolaru u odnosu na GPU. Čip u sva 3 proizvoda sadržavao je 16 dvostrukih SHA-256 hash cjevovoda. Butterfly labs planirao je studeni 2012. kao datum lansiranja na tržište, no raspored je više puta odgođen radi usporavanja i kašnjenja iz ASIC proizvodnje, te radi pakiranja. Trebalo je skoro godinu dana da se narudžbe pošalju. Glavni uzrok toga bio je da je sam čip trošio 4 do 8 puta više snage nego što se očekivalo, što je zahtijevalo redizajn svih ASIC uređaja. (Taylor, 2017)

ASICMiner je osnovan početkom srpnja 2012. godine, nakon što su Butterfly Labs počeli preuzimati prednarudžbe za svoje ASIC rudare. Glavna motivacija bila je spriječiti da Butterfly Labs bude jedini Bitcoin ASIC dobavljač i, te da ne kontrolira Blockchain. ASICMinerov pristup bio je posve drukčiji od Butterfly Labs-a. U početku je bilo namijenjeno da se ne prodaje hardver, nego da se pokrene ASIC podatkovni centar koji bi rudario Bitcoin u ime dioničara. Ovaj pristup, vjerojatno prvi ASIC-ov „cloud“ (hr. oblak), uklonio je potrebu za isporuku hardvera korisnicima. U nedostatku prepoznavanja imena Butterlfy Labs-a, ASICMiner je prikupljao sredstva preko bitcointalk.org foruma[6] i nekih foruma na kineskom jeziku. Tvrtka je pažljivo naznačila svoj plan za razvoj 130 nm ASIC Bitcoin rudara za svoj oblak i odgovorila na stotine pitanja od strane internetske zajednice u pogledu svog poslovnog modela, tehničkih odluka i financijske pouzdanosti. U kolovozu 2012. godine prikupili su 160.000,00 dolara preko online burze GLBSE. Dana 28. prosinca tvrtka je objavila fotografije svojih čipova – prvog ASICMinera na bitcointalk.org forumu. Do 31. siječnja 2013. ASICMiner je imao 64 ploče s čipovima i imali su cilj dostići do 800 ploča. Do 14. veljače imali su 2-TH /s rudara. Tijekom vremena ASICMiner je imao poteškoća prilagodbom podatkovnog centra, te je počeo prodavati hardver. Najprije su prodali ploče iz podatkovnog centra, no kasnije su razvili prijenosni USB disk sa jednim ASIC-om, „Block Erupterom“ kao što možemo vidjeti na Slici 14. (Taylor, 2017)

[6] https://bitcointalk.org/index.php?topic=99497.0

Slika 14 ASICMiner Block Erupter USB 330MH/s Sapphire Rudar (https://i1.wp.com/www.altcointoday.com/wp-content/uploads/2014/11/USB-block-erupter-miners.jpg?resize=828%2C500)

Dionice ASICMiner dosegle su 4 Bitcoina u listopadu 2013. godine, što znači 40 puta povratak investicije početnim ulagačima. Od triju navedenih tvrtki, ASICMiner je bio najinovativniji u isprobavanju novih proizvoda i poslovnih modela.

Avalon je također osigurao financiranje putem prednarudžba preko online trgovine. Ključni osnivač N.G. Zhang je uspostavio svoj ugled dizajniranjem vrhunske Bitcoin FPGA ploče, Icarusa. Avalon je usredotočen na izradu 110-nm čipa za izvedbu dvostrukog SH-256 cjevovoda. Kao ASICMiner, Avalon ima sjedište u Shenzhen, Kini. Tvrtka je imala prednarudžbu od 300 uređaja, od kojih je svaki koštao $1.299,00 ili 108 Bitcoina (2012. godine), a istodobno je hashao 66 GH/s na 600W. Dana 30. siječnja 2013. godine, razvojni programer Bitcoina, Jeff Garzik postao je prvi kupac u povijesti koji je primio ASIC mining rig, kojeg možemo vidjeti na Slici 15 i koji je zaradio oko 15 Bitcoina prvog dana. Avalon je ponudio pošiljku od 600 ASIC rudara za 75 Bitcoinova 2. veljače (1.600,00 dolara) i 25. ožujka (5.500,00 dolara). U kratkom roku su bili rasprodani. Avalon je slijedio prodaju direktnih čipova, prodavši više od 100 pošiljka od 10.000 čipova za 780 BTC po pošiljci, odnosno oko 78.000 dolara. (Buterin)

Slika 15 Avalon ASIC Bitcoin Rudar (https://fs.bitcoinmagazine.com/img/images/avalon-ships-bitcoins-first-consumer-asics.original.png)

3.4.2. Druga generacija ASIC-a

Slijedeća generacija ASIC-a razlikuje se od prošle na nekoliko načina. ASIC-ovi prve generacije dokazali su svoju vrijednost u Bitcoin rudarenju tako što su potakli investitore za ulaganje u ASIC rudare. Novi ASIC rudari morali su pobijediti prethodnu generaciju u troškovima, izvedbi i energetskoj učinkovitosti, te ostati ispred sve većih razina težine. Ove uzastopne generacije imale su dva moguća izvora inovacija: bolju arhitekturu i naprednije procesne čvorove.

BitFury je sa dizajnerom čipova Valery Nebesny sredinom 2013. godine dostigao 55nm, najboljom u klasi, potpuno prilagođenom implementacijom superiornijom od 28nm dizajna, dosežući 0,8 W po GH/s i 2,5 GH/s po čipu. Za razliku od većine ostalih arhitektura koje su odmotali dupli SHA-256 BitFury je koristio hasheve koje se ponavljaju na mjestu.

KnCMiner sa sjedištem u Švedskoj dosegla je 28 nm do listopada 2013. godine. Nedugo zatim, iz San Francisca, **Hash Fast** i **Austin CoinTerra8** također su izašli s 28-nm implementacijama. Ovi ASIC rudari bili su puno isplativiji od BitFury čipova, ali energetska učinkovitost je zapravo bila gora: veća od 1.1 W po GH / s. **BFL**, **Spondoolies** i **Bitmain** također su implementirali 28-nm rudare, usmjeravajući se na učinkovitost energije koja odgovara ili premašuje BitFury-ove dizajne, na 0,7 W po GH /s. Na Slici 16 prikazan je Bitmain-ov Antminer S1 180 GH/s. Postoje dokazi da su 21 tvrtke dostigle 22 nm oko prosinca 2013. godine, no detalji su usko čuvane tajne. (Taylor, 2017)

Slika 16 Bitmain Antminer S1 (https://i0.wp.com/betbybitcoin.com/wp-content/uploads/2016/12/ANTMINER-S1.jpeg?resize=700%2C466)

3.4.3. Treća generacija ASIC-a

Treća generacija ASIC rudara su tvrtke koje su preživjele ASIC rati i napredovale do 20 nm i 16 nm čipova. Dva glavna javno poznata natjecatelja su BitFury i Bitmain , koji imaju 16-nm čipove. Implementacije obje tvrtke se odvajaju pri jako niskim naponima. BitFury rudari premašuju 0,07 W po GH / s, što je 100 puta energetski učinkovitije od prvog 130-nm ASIC rudara i 8000 puta energetski učinkovitiji od GPU rudara. Nekoliko postojećih Bitcoin rudarskih tvrtki sada razvija svoje ASIC-ove i stvorilo je ASIC podatkovne centre za oblak u područjima s niskim troškovima energije i hlađenja.
Na primjer, BitFury optimizira svoje čipove za uporabu u novim hlađenim centrima u Republici Gruziji, Finskoj i Islandu. Ujedinjeni ASIC i podatkovni centar prevladavaju u industriji iz tri razloga:

1. ASIC i podatkovni centar mogu se kodirati. Time se eliminira potreba brige o različitim okruženjima kupca (temperatura, carinska certifikacija, kompatibilnost od 220 V / 110 V, postavljanje i tehnička podrška, isporuka i vraćanja, jamstva itd.), omogućavanje novih troškova, energetske učinkovitosti i optimizacije performansi.
2. Vrijeme za pokretanje ASIC-a je znatno skraćeno ako se proizvod ne mora pakirati, otkloniti i dostaviti kupcu, što znači da čipovi mogu ranije početi s hashiranjem. To je osobito važno kada se hash rate cjelokupne mreže povećava eksponencijalno, a najveći dio profita se zaradi u ranoj životnoj fazi stroja.
3. Izmjene ASIC čipa točno u skladu s obećanom energetskom učinkovitošću i specifikacijama performansi prije nego što se dostave do klijenta odgađa ASIC implementaciju i smanjuje životni vijek ASIC-a. (Taylor, 2017)

Tablica 4 Usporedba ASIC-a u četvrtoj generaciji hardvera za rudarenje

Ime modela	Brzina rudarenja (GH/s)	Prosječna snaga rada (Watt)	Brzina rudarenja po prosječnoj snazi rada (GH/W)	Cijena ($)
ButterFly labs Jalapenos	4.5	30	0.15	149
ButterFly labs Single	60	300	0.2	1299
ButterFly labs[7] Mini Rigs	500	2400	0.208	30000
ASICMiner BE100	0.33	2	0.336	40
Avalon ASIC Miner A3256	0.295	1.947	0.15	1299
KnCMiner Mercury	100	250	0.4	1995
CoinTerra TerraMiner IV	1600	2100	0.76	1500
BFL Monarch 700GH/s	700	490	1.428	1379
Spondooliestech	1400	1250	1.12	2845

[7] Zbog prije opisanog problema sa ButterFly Lab-om povećala se prosječna snaga rada za 75% i smanjila brzina rudarenja za 75%

SP10 Dawson				
AntMiner S1	180	360	0.5	299

Izvor: (List of Bitcoin mining ASICs) i (Mining hardware comparison)

Tablica 4 prikazuje različite rudare kroz tri generacije ASIC-a. Budući da Bitcoin rudarenje povećava popularnost i da je Bitcoinova cijena rasla, tako je narasla i vrijednost ASIC Bitcoin rudarskog hardvera. Kako se Bitcoin rudarski hardver koristi za osiguranje Bitcoinove mreže, Bitcoinova težina raste. To ga čini nemogućim da se profitabilno natječu bez Bitcoin ASIC rudara. Štoviše, ASIC tehnologija postaje brža, učinkovitija i produktivna, tako da zadržava ograničenja onoga što čini najbolji Bitcoin hardver za rudarenje.

4. Suvremeni hardver za rudarenje

U početcima nije bio potreban poseban hardver za rudarenje Bitcoina jer je težina rudarenja bila niska, a i nagrada za blok je bila veća. Kroz godine pojavio se veliki broj ostalih kriptovaluta, te se težina samog Bitcoina povećala, paralelno se unaprjeđivao hardver za rudarenje. U današnje vrijeme mora se uzeti u obzir težina, jer neće svaki hardver rudariti kriptovalute, a pritom donijeti zaradu.

4.1. Rudarenje Bitcoina

Kako bi se počelo s rudarenjem Bitcoina, potreban je ASIC, koji je posebno izrađen za tu svrhu. CPU, GPU i FPGA ne pokazuju dobru produktivnost rudarenja pored ASIC-a, pa je zato upravo on danas najkorišteniji pri rudarenju Bitcoina. Budući da je popularnost rudarenja velika svatko želi nabaviti ASIC kako bi rudario, no oni mogu biti skupi i veoma teški za naći. U većini slučajeva mora se nabaviti kvalitetno napajanje kako bi se osigurala maksimalnu učinkovitost.

Tablica 5 Razlika najkorištenijih hardvera za rudarenje Bitcoina u 2018.

Ime modela	Brzina rudarenja (TH/s)	Prosječna snaga rada (Watt)	Cijena ($)
Pangolin Whatsminer M10	33	2145	1888
GMO Miner B3	24	1950	1999
Innosilicon T2 Turbo	24	1980	1950
Antminer S9 Hydro	18	1728	745
DragonMint T1	16	1480	999
Antminer S9j	14.5	1350	689
Antminer S9	14	1372	659
Antminer R4	8.7	845	1100
Antminer T9+	10.5	1332	399
Antminer S7	4.7	1300	199

Izvor: (Best Bitcoin Mining Hardware (September 2018))

U Tablici 5 prikazana su najbolja Bitcoin ASIC rudara u 2018. godini što se tiče cijene, potrošnje i brzine rudarenja.

4.2. Rudarenje Ethereuma

Ethereum koristi Etash algoritam koji najviše podržava GPU rudarenje na tržištu kriptovaluta. Trenutno je algoritam iza mnogih kriptovaluta poput Ethereum classic, Musicoin, Pirl, Ubiq. Veoma bitne činjenice o Ethereumu su sljedeće:

1. Ethereum se planira prebaciti na alternativni oblik za određivanje rudarske moći. Dokaz o ulozi (ili PoS u kratkom) navodi da što više posjedujete određenu kriptovalutu, to je veća rudarska moć koju imate u svojoj mreži.
2. Prilikom gledanja kriptovalute bazirane na Ethash algoritmu mora se provjeriti DAG (Directed Acyclic Graph). On se pohranjuje u VRAM GPU-a. Kako bi moglo rudariti kriptovalutu, vaš GPU mora imati dovoljno prostora za pohranu DAG-a. Trenutno se rudari s Ethereum karticama koje imaju najmanje 3 GB-a VRAM-a. DAG se povećava svakih 30000 Ethereum blokova. Dok Ethereum rudarenje trenutno nije moguć s 2 GBkartice, moguće je rudariti druge novčiće kao što je Ubiq sa 2 gigabajt kartice.

AMD kartice su gotovo uvijek prikladnije za početnike u smislu cijene jer su osnovne rudarske kartice AMD-a koštale gotovo dvije trećine cijene nego konkurentne Nvidia kartce. Međutim, Nvidia kartice gotovo se uvijek lakše koriste, konfiguriraju i overclockiraju. Dakle, Nvidia kartice ne zahtijevaju više vremena učenja kako konfigurirati kartice, flash bios ili undervolt.
AMD kartice također nisu tako snažne kao Nvidia kartice. Jedna od najvažnijih prednosti Nvidijinih kartica jest ta da su one mnogo bolje od drugih algoritama. Dok su AMD kartice učinkovitije na algoritmima Ethash i Cryptonight,. Nvidia kartice su ih pobijedile na većini drugih algoritmima. (Best Ethereum mining hardware, 2018)

Tablica 6 prikazuje AMD-ove i Nvidia kartice za rudarenje Ethereuma pomoću Ethash algoritma. Vrijednosti u tablici variraju ovisno o kojem se modelu grafičke kartice govori, te da li je proizvođač Nvidia ili AMD, ili druga kompanija koja dorađuje originalne kartice (ASUS,GIGABYTE itd..)

Tablica 6 Usporedba GPU-a za rudarenje Ethereuma u 2018. godini

Ime modela	Brzina rudarenja (MH/s)	Prosječna snaga rada (Watt)	VRAM (GB)	Cijena ($)
AMD RX570	20-30	80-200	4/8	300-400
AMD RX580	20-30	100-250	4/8	450-550
AMD Radeon RX Vega	30-45	150-250	8	800-1000
NVidia GTX 1060	18-25	60-150	3/6	400-550
NVidia GTX 1070	25-32	150-225	8	750-950
NVidia GTX 1080ti	35-40	150-250	11	1200-1500

Izvor: (Best Ethereum mining hardware, 2018)

Zaključak

Izum Satoshija Nakamota 2009. godine promijenio je svijet. Izmislio je novi izgled digitalnog novca u kojem se miče glavni posrednik, banka. Blockchain je platforma na koji Bitcoin funkcionira. On koristi računalnu opremu korisnika, te sa njihovom snagom obrade čuva sigurnost mreže tako što validira transakcije. Te transakcije su sporije u odnosu na kreditne kartice, ali je njihov trošak je znatno niži. Za nagradu, rudare nagrađuje s Bitcoinom. No, ta se nagrada s vremenom smanjivala, jer je validacija transakcija otežana zbog veličine aktivnih korisnika, stoga se i računalna oprema razvijala paralelno.

U početku se moglo rudariti pomoću procesora iz osobnog računala i tada se najviše moglo rudariti i do sto Bitcoina dnevno. U kratkom roku rudari su shvatili da se može efikasnije rudariti pomoću grafičkih kartica. Polako se fleksibilnost CPU-a i GPU-a pretvorio u funkcionalnost putem FPGA sklopova i ASIC rudara koji su bili namijenjeni samo za rudarenje. U zadnjem poglavlju objašnjeno je rudarenje Bitcoina i Ethereuma, te je doveden zaključak da nisu samo ASIC uređaji jedini izbor za rudarenje u 2018 godini.

Danas je rudarenje Bitcoina i ostalih kriptovaluta skupa investicija, a ne osigurava povrat uloženog novca. Bitcoin je nova kriptovaluta sa kojom svatko može započeti sa rudarenjem. Postoji nekoliko razloga zašto možete rudariti: za profit, osiguravanje mreže ili samo za stjecanje tehničkog iskustva.

Popis literature

Best Ethereum mining hardware. (2018). Dohvaćeno iz https://99bitcoins.com/best-ethereum-mining-hardware/

Antonopoulos, A. M. (n.d.). *Mastering Bitcoin.*

Best Bitcoin Mining Hardware (September 2018). (n.d.). Dohvaćeno iz https://www.anythingcrypto.com/guides/best-bitcoin-mining-hardware-2018

Bitcoin Block Reward Halving Countdown. (n.d.). Dohvaćeno iz www.bitcoinblockhalf.com

Bitcoin forum. (n.d.). Dohvaćeno iz https://bitcointalk.org/index.php?topic=1628.25;wap2

Bitcoin.it - Mining hardware comparison. (n.d.). Dohvaćeno iz https://en.bitcoin.it/wiki/Mining_hardware_comparison

Bitcoin.it - Nonce. (n.d.). Dohvaćeno iz https://en.bitcoin.it/wiki/Nonce

Bitcoinwiki - Nonce. (n.d.). Dohvaćeno iz https://en.bitcoinwiki.org/wiki/Nonce

Block explorer. (n.d.). Dohvaćeno iz https://blockexplorer.com/

Buterin, V. (n.d.). *Avalon Ships Bitcoin's First Consumer ASICs*. Dohvaćeno iz https://bitcoinmagazine.com/articles/avalon-ships-bitcoins-first-consumer-asics-1358905223/

Buybitcoinworldwide - Hash rate. (n.d.). Dohvaćeno iz https://www.buybitcoinworldwide.com/mining/hash-rate/

Caetano, R. (2015). *Learning Bitcoin.*

CPU Benchmark. (n.d.). Dohvaćeno iz https://www.cpubenchmark.net/

Enciklopedija.hr - Javne knjige. (n.d.). Dohvaćeno iz http://www.enciklopedija.hr/natuknica.aspx?id=28835

FPGA Architecture for the Challenge. (n.d.). Dohvaćeno iz http://www.eecg.toronto.edu/~vaughn/challenge/fpga_arch.html

Hayes, A. (n.d.). *How Much Cheaper are Bitcoin Fees than Credit Card Fees?* Dohvaćeno iz https://www.investopedia.com/news/how-much-cheaper-are-bitcoin-fees-credit-card-fees/

Hrvatski Bitcoin Portal - rudarenje. (n.d.). Dohvaćeno iz https://crobitcoin.com/bitcoin/rudarenje-mining/

Intel - Product specifications. (n.d.). Dohvaćeno iz https://ark.intel.com/

List of Bitcoin mining ASICs. (n.d.). Dohvaćeno iz https://en.bitcoin.it/wiki/List_of_Bitcoin_mining_ASICs

Mining hardware comparison. (n.d.). Dohvaćeno iz https://en.bitcoin.it/wiki/Mining_hardware_comparison

Naik, R. P. (n.d.). *Optimising the SHA256 Hashing Algorithm.* Dohvaćeno iz http://www.nicolascourtois.com/bitcoin/Optimising%20the%20SHA256%20Hashing%20Algorithm%20for%20Faster%20and%20More%20Efficient%20Bitcoin%20Mining_Rahul_Naik.pdf

Nakamoto, S. (n.d.). *Bitcoin: A Peer-to-Peer Electronic Cash System.* Dohvaćeno iz https://bitcoin.org/bitcoin.pdf

Singh, R. (n.d.). *FPGA Vs ASIC: Differences Between Them And Which One To Use?* Dohvaćeno iz https://numato.com/blog/differences-between-fpga-and-asics/

Stack exchange. (n.d.). Dohvaćeno iz How to deal with collisions in bitcoin adresses: https://crypto.stackexchange.com/questions/33821/how-to-deal-with-collisions-in-bitcoin-addresses

Sterry, D. R. (2012). Introduction to Bitcoin Mining.

Taylor, M. B. (2017). *The Evolution of Bitcoin Hardware.* Dohvaćeno iz https://ieeexplore.ieee.org/document/8048662/

Technopedia - Hash function. (n.d.). Dohvaćeno iz https://www.techopedia.com/definition/19744/hash-function

The Evolution of the Cryptographic Hash Function in Blockchains. (n.d.). Dohvaćeno iz https://medium.com/shokone/hash-no-not-that-kind-the-crypto-kind-2e8bf616aa24

Wikipedia - Brute force search . (n.d.). Dohvaćeno iz https://en.wikipedia.org/wiki/Brute-force_search

Popis slika

Popis tablica