VARNOSTNI VIDIK TEHNOLOGIJE BLOKOVNIH VERIG

Avtor: Vinko Klemenčič
Visoka šola za poslovne vede

Povzetek

Članek opisuje glavne gradnike blokovnih verig. Razvoj in pomembnost zgoščevalnih funkcij, ki so alfa in omega te tehnologije. Preprosti primer le te in glavne značilnosti, katere mora vsaka kripto zgoščevalna funkcija zagotavljati. Primeri ranljivosti najbolj poznanih blokovnih verig, kripto valut predvsem primata, Bitcoin omrežja. Spoznanja, da večja omrežja zagotavljajo večjo varnost, da rudarjenje in dokaz dela ni brezmiselna potrata električne energije. Privatni ključi oziroma elektronske denarnice, ponujajo ustrezno zaščito, če se jih ustrezno uporablja. Varnost v velikih blokovnih omrežjih je vredna zaupanja, vedno pa bodo ostajala manjša tveganja za manjše gradnike omrežja (določene uporabnike na določenem področju), največja nevarnost pa seveda tiči v nepoznavanju in tako nepravilnem ravnanju s privatnimi ključi oziroma elektronskimi denarnicami.

Ključne besede: blokovne verige, zgoščevalne funkcije, varnost blokovnih omrežij, rudarjenje kripto valut

Uvod

V članku si bomo na kratko pogledali osnovne pojme, ki se pojavljajo pod varnostjo blokovnih verig. Kaj je bistvo blokovne tehnologije, katera kriptografska načela so uporabljena, preprosti primeri načina delovanja le teh. Kaj so znane teoretične in praktične ranljivosti, največjih blokovnih omrežij, ki so dandanes še vedno kripto valute. Kako skrbimo za varnost uporabniki, oziroma kako uporabljamo elektronske denarnice, privatne ključe.

Princip delovanja blokovnih verig

Definicija blokovne verige

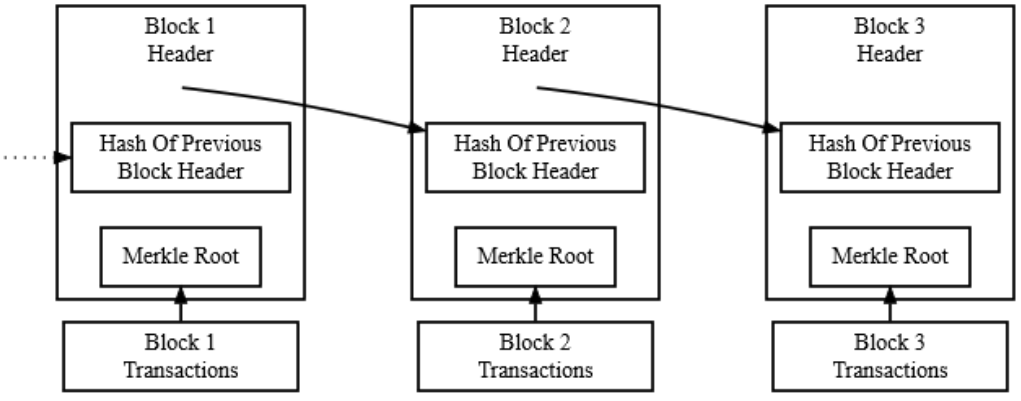
Blokovna veriga je preprosto povedano časovno žigosana serija nespremenljivih podatkov, ki jih upravlja gruča računalniških sistemov, ki niso v lasti posameznega subjekta. Vsak blok podatkov je zavarovan in povezan z drugim s pomočjo kriptografskih načel, ki jo imenujemo veriga.

Blokovno omrežje nima osrednje avtoritete gre za samo definicijo demokratičnega sistema. Ker gre za skupno in nespremenljivo bazo podatkov, so informacije v njej odprte za vse in vsakogar. Zato je vse, kar je zgrajeno na blokovni verigi, po svoji naravi pregledno in vsi vpleteni so odgovorni za svoja dejanja (Blockgeeks, 2020).

Tehnologija verige blokov

Veriga blokov, kot nam že ime pove so zaporedno vezani bloki, ki vsebujejo določene podatke, recimo transakcije. Vsak blok poleg primarnih podatkov nosi še zgodovino prejšnjih blokov v obliki zgoščene vrednosti (ang. hash), kot poenostavljeno za omrežje Bitcoin prikazuje slika 1. Zgoščene vrednosti se popolnoma spremenijo že ob najmanjši spremembi vhodnih podatkov. Zgoščena vrednost je neke vrste podpis podatkov oziroma žig, poljubne velikosti, kateri vrne vrednost konstantne dolžine. V verigi blokov so zgoščene vrednosti posameznega bloka praviloma unikatne, obstaja samo teoretična možnost zaradi ekstremno nizke verjetnosti, da bi se ponovila izračunana vrednost. Če je v bloku narejena najmanjša sprememba se spremeni tudi zgoščena vrednost bloka. Zgoščene vrednosti novo ustvarjenega bloka vsebujejo tudi zgoščeno vrednost prejšnjega bloka, to daje verigi blokov varnost (Burja, 2019).

Slika 6: Poenostavljena predstavitev blokovne verige omrežja Bitcoin (Bitcoin, 2020).



Šifrirni algoritmi in rudarjenje

Rudarjenje je postopek v katerem računalniki, grafične kartice ali za ta namen razviti stroji izvajajo računske kriptografske postopke (SHA256, Ethash, Zhash, Lyra2z, Hex, X16R, CNHeavy, ProgPow,..), s katerimi procesirajo nakazila in varujejo omrežje in skrbijo za soglasje in usklajenost vseh udeležencev sistema. Izraz »rudarjenje« je analogija rudarjenja zlata, ker je to hkrati tudi proces v katerem nastajajo novi kripto kovanci. Od kopanje zlata pa se rudarjenje kripto valut razlikuje po tem, da je delo, za katerega rudarji prejemajo nagrado, koristno za celotno omrežje, saj skrbi za njegovo celovitost in varnost. V nadaljevanju si bomo pogledali, primer kako izračunamo zgoščeno funkcijo in dokaz dela POW.

Zgoščevalne funkcije

Čeprav obstaja več različnih razredov kriptografskih zgoščevalnih funkcij, morajo imeti vse iste lastnosti. Na kratko si bomo pogledali te štiri lastnosti, ki jih mora imeti koristna kriptografska zgoščena funkcija.

Računsko učinkovita

V prvi vrsti morajo biti zgoščevalne funkcije računsko učinkovite. To je le izmišljen način, da lahko povemo, da morajo računalniki v izjemno kratkem času imeti možnost opravljanja matematičnega izračuna zgoščene funkcije. Ta zahtevana lastnost je verjetno očitna. Če bi navadni računalnik potreboval nekaj minut za obdelavo kriptografskih zgoščenih funkcij, to ne bi bilo zelo praktično. Da bi bile uporabne, morajo biti zgoščene funkcije računsko učinkovite. V resnici nas to ne skrbi več tako zelo, kot je bilo pred 40 ali 50 leti. Dandanes lahko povprečen domači računalnik obdela napredeno zgoščevalno funkcijo v le majhnem deležu sekunde.

Deterministična

Kriptografske zgoščene funkcije morajo biti deterministične. Z drugimi besedami, pri katerem koli enakem vnosu mora imeti zgoščena funkcija vedno enak rezultat. Če na vhod pripeljemo deset milijonov krat zapored enako vrednost, mora zgoščevalna funkcija ustvariti enako natančen rezultat deset milijonov krat. Tudi to je lahko precej očitno. Če bi kriptografska zgoščena funkcija proizvedla različne izhode ob vsakem vnosu istega vhoda, bi bila zgoščena funkcija naključna in zato neuporabna. Nemogoče bi bilo preveriti dotičen vhod, kar je celotna poanta zgoščevalnih funkcij - da bi lahko preverili, ali je zasebni digitalni podpis verodostojen, ne da bi imeli dostop do zasebnega ključa.

Odporna na razkrivanje vhodnih podatkov

Izhod kriptografske zgoščene funkcije ne sme razkriti nobenih informacij o vhodu. Pomembno je upoštevati, da lahko algoritmi kriptografskih mešanj prejemajo kakršne koli vnose. Vnos so lahko številke, črke, besede ali ločila. Lahko je posamezen znak, stavek iz knjige, stran iz knjige ali celotna knjiga. Vendar pa bo zgoščena funkcija vedno ustvarila izhod s fiksno dolžino. Ne glede na to, kakšen je vhod, bo izpis alfanumerična koda določene dolžine. Razmislimo, zakaj je to tako pomembno: če bi daljši vložek dal daljši izid, bi napadalci že imeli resno koristno informacijo, ko bi želeli razkriti privatno besedilo na vhodu. Če bi na primer vložek vedno dajal izhod 1,5-krat večji od njegove dolžine, bi zgoščena funkcija oddajala dragocene informacije hekerjem. Če bi hekerji videli izhod iz, recimo, 36 znakov, bi takoj vedeli, da je vnos 24 znakov. Namesto tega mora uporabna zgoščena funkcija skriti vse namige o tem, kako je morda izgledal vložek. Nemogoče je ugotoviti, ali je bil vnos dolg ali kratek, številke ali črke, parne ali neparne, naključne črke ali niz prepoznavnih besed. Poleg tega mora sprememba enega znaka v dolgem nizu besedila imeti za posledico radikalno drugačen zapis na izhodu.

Odpornost proti trkom

Končna lastnost, ki jo morajo imeti vse kriptografske zgoščevalne funkcije, je tista, ki je znana kot trčna odpornost. To pomeni, da mora biti zelo malo verjetno - z drugimi besedami, praktično nemogoče - najti dva različna vhoda, ki ustvarjata enak izhod. Kot je navedeno

zgoraj, so vhodi v zgoščevalno funkcijo lahko poljubne dolžine. To pomeni, da obstaja neskončno možnih vhodov, ki jih je mogoče vnesti v funkcijo. Vendar so izhodi določene dolžine. To pomeni, da obstaja končno število - čeprav izredno veliko število - izhodov, ki jih zgoščena funkcija lahko proizvede. Fiksna dolžina pomeni določeno število možnosti. Ker je število vhodov v bistvu neskončno, vendar so izhodi omejeni na točno določeno število, je matematična gotovost, da bo več izhodov ustvarilo isti izhod. Cilj je najti dva vhoda, ki ustvarjata enak izhod, tako astronomsko neverjeten, da bi bilo mogoče možnost takoj zavreči. Ne sme predstavljati realnega tveganja. Na tej točki se morda sprašujemo, kakšne neverjetne enačbe moramo imeti, da zagotovimo vse te štiri lastnosti. Odgovor je verjetno veliko preprostejši, kot si predstavljamo.

Kratek primer zelo enostavne enosmerne zgoščevalne funkcije

Zgoščevalne funkcije pogosto imenujemo enosmerne funkcije, ker glede na lastnosti, navedene zgoraj, ne smejo biti povratne. Če bi napadalec zlahka obrnil zgoščevalno funkcijo, bi bila ta popolnoma neuporabna. Zato kriptografija zahteva enosmerne zgoščevalne funkcije. Najboljši način za prikaz enosmerne funkcije je preprosta modularna funkcija, imenovana tudi modularna aritmetika ali taktna aritmetika. Modularne funkcije so matematične funkcije, ki poenostavljeno ustvarijo preostanek problema delitve.

Torej, na primer, 10 mod 3 = 1. To drži, ker je 10, deljeno s 3, 3 s preostankom 1. Prezremo, kolikokrat 3 preide v 10 (kar je 3 v tem primeru) in edini izhod je preostanek: 1.

Za funkcijo uporabimo enačbo X mod 5 = Y. Spodaj je slika, ki nam bo pomagala:

Slika 7: Primer vhodov in izhodov za funkcijo X mod 5 = Y (Komodoplatform.com, 2020).

INPUT (X)	OUTPUT (Y)
1	1
2	2
3	3
4	4
5	0
6	1
7	2
8	3
9	4
10	0
11	1
12	2
13	3
14	4
15	0

Verjetno lahko vsi opazimo vzorec. Za to funkcijo obstaja le pet možnih izhodov. V tem zaporedju se vrtijo v neskončnost. To je pomembno, ker sta tako zgoščena funkcija kot

izhod lahko javno objavljena, vendar se nihče ne bo mogel naučiti vašega vnosa. Dokler hranite številko, ki ste jo izbrali za X, skrivnost, napadalec tega ne more razbrati. Recimo, da je vaš vložek 27. To pomeni rezultat 2. Zdaj si predstavljajte, da svetu sporočite, da uporabljate zgoščevalno funkcijo X mod 5 = Y in da je vaš osebni izhod 2. Ali bi kdo lahko uganil vašo številko na vhodu? Očitno ne. Obstaja dobesedno neskončno število možnih vnosov, ki bi jih lahko uporabili za rezultat 2. Na primer, vaša številka bi lahko bila 7, 52, 3492 ali 23390787. Ali pa je lahko katerokoli drugo neskončno število od možnih vhodov. Dejstvo, ki ga moramo tukaj razumeti, je da so enosmerne zgoščevalne funkcije ravno to: enosmerne. Ni jih mogoče obrniti. Ko se ta ista načela uporabijo za veliko bolj izpopolnjeno zgoščevalno funkcijo in veliko večja števila, je nemogoče določiti vhodne vrednosti na podlagi izhoda. To je tisto, kar naredi kriptografsko zgoščevalno funkcijo tako varno in uporabno (Komodoplatform, 2020).

Dokaz dela (POW)

Rudarjenja POW se lahko loti vsak, ki ima ustrezno strojno in programsko opremo. Programska oprema za rudarjenje spremlja nova nakazila v vrstniškem omrežju in izvaja opravila za procesiranje in potrjevanje teh nakazil. Denarna motivacija za rudarjenje je, da rudarji prejmejo prispevke, ki jih uporabniki plačajo pri pošiljanju nakazil in nove kovance kriptovalute, ki nastanejo po vnaprej določenem redu. Nova nakazila se potrdijo na način, da jih rudarji vključijo v nov blok skupaj z matematičnim dokazom opravljenega dela na principu HashCash.

HashCash je kriptografski način dokaza dela, prvotno se je uporabil, kot proti ukrep pri onemogočanju storitev (DOS in DDOS) napadih in ukrep proti nezaželeni pošti (angl. SPAM). Dan danes se uporablja kot dokaz dela pri blokovnih verigah oziroma kripto valutah. Princip je sledeč, iščemo zgoščeno vrednost oziroma žig, za kriptirano vsebino pa naj si bo to zgoščena vrednost prejšnjega bloka in podatki o transakcijah ali kaj drugega, nato dodamo naključni niz ki ga npr. povečujemo za 1, da dobimo rešitev zgoščeno vrednost, ki ima določeno število ničel na začetku niza. Število zahtevanih ničel nam daje določeno zahtevnost več ničel moramo »uganiti« težja je težavnost, ali drugače rečeno moramo izračunati zgoščeno vrednost pod mejno vrednostjo številke, ki predstavlja težavnost. Za »ugibanje« zgoščenih vrednosti pride v poštev samo čista procesorska moč (angl. bruteforce). Pri SHA 256 je vseh možnih vrednosti žiga oziroma zgoščenih vrednosti $2^{256} - 1$, če predpostavimo da težavnost zahteva 20 začetnih ničel je to možnost 1 proti 2^{20} to je približno 1 proti milijon, z vsako dodatno ničlo se težavnost eksponentno povečuje. Statistično se lahko izračuna na koliko časa bo v povprečju izračunana zahtevana zgoščena vrednost glede na celotno procesorsko moč, ki računa ta problem. Tako se recimo določi na koliko časa se v povprečju rudari, oziroma najde nov blok. Če za primer vzamemo bitcoin omrežje se težavnost prilagodi na vsake 2016 blokov, kar pomeni približno na 2 tedna. Težavnost se poveča ali manjša glede na povprečni čas med bloki, če se ta čas zmanjša se težavnost poveča, če se pa ta čas poveča, se težavnost zmanjša. Cilj je, v povprečju 10 minut med bloki. Ko se zgoščena funkcija izračuna je za ostale soležnike v omrežju preprosto preveriti ali je res, ker preverjajo samo eno zgoščeno vrednost, ta pa se izračuna

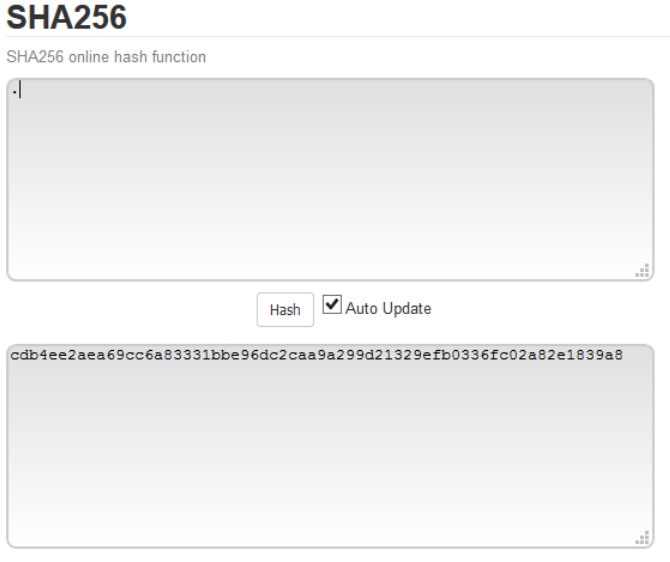
v rangu mili ali mikro sekunde, glede na moč današnjih procesorjev (Wikipedia, 2020), (Bitcoin, 2020).

Kot smo si pogledali je dokaz dela težavno opravilo, saj je edini način preizkušanje milijarde izračunov vsako sekundo. Ko vedno več ljudi rudari se povečuje težavnost računske operacije za tvorbo novih blokov, na ta način ostaja povprečni čas novega bloka približno enak, kot je zapisano v programski kodi kriptovalute (Bitcoin, 2020). To je tudi najkrajši čas na koliko se potrjujejo transakcije. Rudarji se zaradi velike težavnosti reševanja matematičnih operacij povezujejo v skupine (ang. Pools), ki potem s skupno računalniško močjo rešujejo operacije, morebitno nagrado pa si delijo po principu kolikor so vložili procesorske moči tolikšni procent nagrade dobijo.

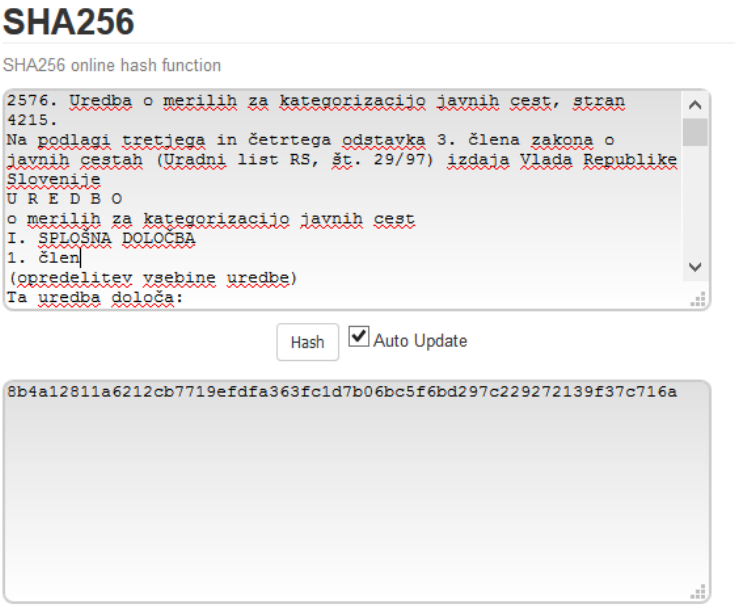
Šifrirni algoritem SHA-256

Zgoščena funkcija (ang. hash) je kot smo že omenili neke vrste podpis teksta ali datoteke. SHA-256 generira skoraj unikatni 256-bitni podpis (32 bajtni) za poljubni tekst. Dolžina zgoščene funkcije je vseskozi enaka neodvisno od dolžine teksta, kot je prikazano na spodnjih slikah. Zgoščena funkcija ni enkripcija, z nje ne moremo povrniti prvotnega teksta. Primerna je za primerjavo teksta z »originalno« verzijo (Movable-type, 2020).

Slika 8: Zgoščena funkcija SHA-256 na enem znaku ».« (Emn178.github, 2020).



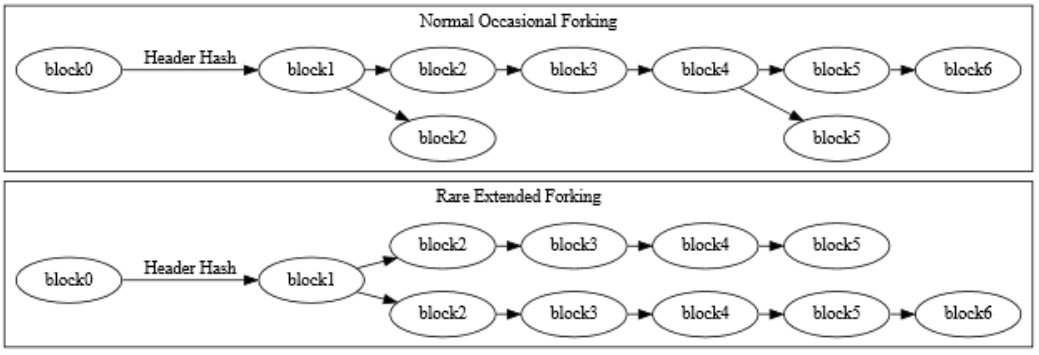
Slika 9: Zgoščena funkcija SHA-256 na daljšem tekstu (Emn178.github, 2020).



Dolžina blokovne verige in razdelitev le te (ang. forking)

Če tudi tu vzamemo za primer bitcoin omrežje, vsak rudar, ki uspešno izračuna zgoščeno vrednost, ki je pod potrebno mejno vrednostjo, doda nov blok v verigo. Blok dobi zaporedno številko od prvega izvornega bloka 0. Kot že vemo težavnost se prilagaja na vsakih 2016 blokov. Občasno pa se zgodi, da dva rudarja ob približno istem času najdeta ustrezen blok, tu se zgodi razdelitev omrežja (ang. fork). To ponazarja spodnja slika v zgornji polovici. Vsako vozlišče izbere, kateri blok bo sprejel, ker ni drugih pomislekov izberejo običajno prvi blok ki ga vidijo. Ko pa se ustvari naslednji blok, se ta pritrdi le na eno od »novih« vej omrežja, tu pa se izbere vejo, ki je močnejša, oziroma ima višjo težavnost (več rudarjev). Tako se blokovno omrežje nadaljuje po tej veji stranska pa zamre, nagrada za stranski blok pa je neuporabna, ker jo ne moremo nikjer zapraviti, ker se veriga pri tem bloku tudi konča (Bitcoin, 2020).

Slika 10: Razdelitev blokovnega omrežja (Bitcoin, 2020).



Drug primer, pa je prikazan na spodnjem delu zgornje slike, kjer določeni rudarji želijo vztrajati na »napačni« verigi. Na tak način delujejo tudi planirani razcepi blokovnih verig, kot je recimo Bitcoin Cash. V tem primeru večina rudarjev ostane zvesta originalni verigi Bitcoin, del pa jih vzporedno od določenega bloka dalje živi na novi verigi Bitcoin Cash verigi. Kot zanimivost če smo imeli kovance pred razdružitvijo verige, jih lahko sedaj zapravimo na obeh vejah (Bitcoin in Bitcoin Cash).

Napad 51% rudarske računske moči

51-odstotni napad je potencialni napad na blokovno omrežje, pri katerem lahko posamezen subjekt ali organizacija nadzoruje večino rudarske računske moči, kar lahko povzroči motnje v omrežju. V takem scenariju bi imel napadalec dovolj rudarske moči, da bi namerno izključil ali spremenil vrstni red transakcij. Prav tako lahko prekličejo transakcije, ki so jih opravili, ko imajo nadzor - kar bi povzročilo dvojno porabo. Uspešen večinski napad bi prav tako omogočil napadalcu, da prepreči potrjevanje nekaterih ali vseh transakcij (transakcija zavračanje storitve DOS) ali prepreči rudarjenje nekaterih ali vseh drugih rudarjev, kar ima za posledico rudarski monopol. Po drugi strani napad večine ne bi omogočil napadalcu, da preusmeri transakcije od drugih uporabnikov, niti ne prepreči, da bi se transakcije ustvarile in potrjevale v omrežje. Spreminjanje nagrade bloka, ustvarjanje kovancev iz nič in krajo kovancev, ki nikoli niso pripadali napadalcu, se prav tako štejejo za nemogoče dogodke.

Vprašajmo se kakšne so realne možnosti za 51% napad na blokovno omrežje. Ker blokovno omrežje vzdržuje distribuirana mreža vozlišč, vsi udeleženci sodelujejo pri doseganju konsenza. To je eden od razlogov, da so zelo varni. Večja kot je mreža, močnejša je zaščita pred napadi in korupcijo podatkov. Če vzamemo bitcoin omrežje je trenutna nagrada za blok 12.5 BTC, kar je trenutna tržna vrednost preko 100 000 ameriških dolarjev, tako se vsak dan priključijo novi rudarji, zaradi nenehnega tekmovanja je težavnost vedno višja če tudi so vse zmogljivejši čipi za računanje zgoščenih SHA256 funkcij. Konkurenčnost daje varnost. Zato je 51-odstotni napad na Bitcoin zaradi velikosti omrežja precej malo verjeten. Ko se bo blokovna veriga dovolj povečala, je verjetnost, da bo ena oseba ali skupina pridobila dovolj računalniške moči, da bi preplavila vse ostale udeležence, padla na zelo nizko raven.

Poleg tega spreminjanje prej potrjenih blokov postane vse težje, ko veriga raste, ker so bloki povezani s kriptografskimi dokazi. Iz istega razloga, več potrditev, ki jih ima blok, višji so stroški za spreminjanje ali razveljavitev transakcij. Zato bi uspešen napad verjetno lahko le za kratek čas spremenil transakcije nekaj zadnjih blokov.

Če gremo še dalje, si predstavljajmo scenarij, ko zlonamerna entiteta ne motivira dobička in se odloči, da bo napadla Bitcoin omrežje samo zato, da bi ga uničila, ne glede na stroške. Tudi če napadalcu uspe razbiti omrežje, bi bila Bitcoin programska oprema in protokol hitro spremenjena in prilagojena kot odgovor na ta napad. To bi zahtevalo, da bi ostala vozlišča omrežja dosegla soglasje in se dogovorila o teh spremembah, vendar bi se to v izrednih razmerah verjetno zgodilo zelo hitro. Bitcoin je zelo odporen na napade in velja za najbolj varno in zanesljivo kripto valuto, ki obstaja.

Čeprav je za napadalca precej težko pridobiti večinsko računalniško moč rudarjev v omrežju Bitcoin, to na manjših kripto valutah ni tako zahtevno. V primerjavi z Bitcoinom imajo altcoini sorazmerno nizko količino zahtevane rudarske moči, ki varuje njihovo blokovno verigo. Dovolj nizka, da omogoča 51% napad. Nekaj opaznih primerov kripto valut, ki so bile žrtve večinskih napadov, so Monacoin, Bitcoin Gold in ZenCash (Binance.vision, 2020).

Napad sebičnega rudarjenja

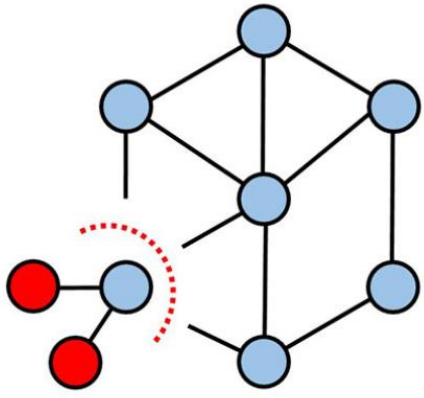
Sebični napad na rudarjenje, znan tudi kot napad zadržanega bloka, opisuje zlonamerni poskus diskreditacije integritete blokovnega omrežja. Sebični napadi rudarjenja se zgodijo, ko posameznik v rudarskem bazenu poskuša preprečiti, da se uspešno potrjen blok objavi v mrežo rudarskega bazena. Potem, ko sebični rudar »skrije« svoj uspešno izkopan blok rudarskemu bazenu, nadaljujejo z rudarjenjem naslednjega bloka, kar ima za posledico, da je sebični rudar pokazal več POW v primerjavi z drugimi rudarji v rudniškem bazenu. Sebični rudar bo vzdrževal svojo zasebno verigo in jo javno razkril oportunistično, da bi pridobil višje nagrade, ki bi jih običajno dodelili na podlagi njihovih dejanskih računskih prispevkov (Hashrate) v rudniškem bazenu. Več rudarjev v rudarskem bazenu lahko med rudarskim procesom sodeluje pri sebičnem rudarskem vedenju (Golden.com, 2020).

Napad osamitve vozlišč (ang. Eclipse attack)

Napad osamitve vozlišč je sredstvo za napad na decentralizirano omrežje, s katerim napadalec skuša izolirati in napasti določenega uporabnika, namesto da napade celotno omrežje. Uspešen napad Eclipse omogoča potencialno slabemu akterju, da izolira in pozneje prepreči, da bi njihov cilj dosegel resnično stanje blokovnega omrežja. Ta napad je mogoč, ker decentralizirano omrežje ne dovoli, da se vsa vozlišča hkrati povežejo z vsemi drugimi vozlišči v omrežju. Namesto tega se za učinkovitost vozlišče poveže z izbrano skupino drugih vozlišč, ki so nato povezana z lastno izbrano skupino. Na primer, Bitcoin vozlišče ima osem odhodnih povezav; Ethereum 13. Napadalec mora nadzorovati vsa ta vozlišča oziroma vse te povezave. Prizadevanje, ki je potrebno za dosego tega, se razlikuje glede na konstrukcijo, velikost in naravo omrežja.

Ko je zlonamerni akter žrtev izoliral tako, da je prevzel nadzor nad vsemi odhodnimi povezavami, jih lahko izkoristi tako, da na primer izvede napad dvojne porabe. Žrtev, bo ugotovila, da kovanci niso dosegli ciljni naslov šele, ko se bo sinhroniziral s pravim blokovnim omrežjem. Napadalec lahko uporabi to vrsto napada na blokovno verigo in »ugrabi« rudarsko moč izoliranega vozlišča (Radixdlt, 2020).

Slika 11: Osamitev vozlišč(a) (Radixdlt, 2020).



Elektronske denarnice, privatni ključi

Veliko pozornost je potrebno nameniti, tudi varovanju privatnih ključev oziroma uporabo elektronskih denarnic, za hrambo kripto kovancev.

Papirnata oblika denarnice, kjer natisnemo privatni ključ in naslov se dandanes smatra kot nevarna oblika zaradi veliko možnosti izgube sredstev (papir se zlahka uniči, pri tiskanju lahko pride do zlorabe, itd).

Eden od načinov hrambe privatnih ključev so tudi strojne denarnice, kjer strojna oprema skrbi za varnost privatnih ključev. Na spodnji sliki je en primer le te.

Slika 12: Strojna denarnica za kripto valute (Shop.ledger, 2020).

Najbolj razširjena pa je uporaba deterministčnih elektronskih denarnic, kot so Electrum, Mycelium, Armory. Tu uporabnik shrani oziroma si zapiše samo nekaj besed (seed), s pomočjo katerih lahko uporablja svojo denarnico oziroma regenerira privatni ključ s svojimi sredstvi.

Zaključek

Kar se tiče blokovnih verig se vse vrti okoli zgoščevalnih funkcij, ta revolucionarna kriptografska metoda zagotavlja varnost, kot jo poznamo. Seveda se z vsakim dnem povečuje računska moč, ki je na voljo za »brute force« napade a za zdaj se še ni bati, da bi to ogrozilo današnje blokovne verige.

Glede varnosti omrežja, pa obstaja več oblik napadov, kar pa je pogojeno z velikostjo omrežja, majhna omrežja so veliko bolj ranljiva kot velika. Pri velikih so ti napadi bolj teoretični, kot praktični, manjša pa so že bila deležna takih napadov.

Kot zadnje bi izpostavili problem privatnih ključev, katere je potrebno varovati. To je pa nekako tako, kot pri vseh stvareh pa naj si bo bančna kartica ali digitalno potrdilo, sistem omogoča načine, ki so zelo varni a za vsakim stoji človek in njegov način kako ga uporablja. Morebitno človeško neznanje ali pa ne posvečanje pozornosti varnemu ravnanju z še tako varno zasnovano tehnologijo, še vedno predstavlja največje varnostno tveganje.

Viri in literatura

Binance.vision. (Februar 2020). Pridobljeno iz Binance.vision: https://www.binance.vision/security/what-is-a-51-percent-attack

Bitcoin. (Februar 2020). Pridobljeno iz Bitcoin.org: https://bitcoin.org/en/blockchain-guide#proof-of-work

Bitcoin. (Februar 2020). Pridobljeno iz Bitcoin.org: https://bitcoin.org/en/blockchain-guide#block-height-and-forking

Bitcoin. (Februar 2020). Pridobljeno iz Bitcoin.org: https://bitcoin.org/en/blockchain-guide#introduction

Blockgeeks. (Februar 2020). Pridobljeno iz Blockgeeks.com: https://blockgeeks.com/guides/what-is-blockchain-technology/

Burja, A. (2019). Aplikacija za trgovanje na kriptoborzah. Ljubljana.

Emn178.github. (Februar 202j0). Pridobljeno iz Emn178.github.io: https://emn178.github.io/online-tools/sha256.html

Golden.com. (Februar 2020). Pridobljeno iz Golden.com: https://golden.com/wiki/Selfish_mining_attack

Komodoplatform. (Februar 2020). Pridobljeno iz Komodoplatform.com: https://komodoplatform.com/cryptographic-hash-function/

Movable-type. (Februar 2020). Pridobljeno iz Movable-type.co.uk: https://www.movable-type.co.uk/scripts/sha256.html

Radixdlt. (Februar 2020). Pridobljeno iz Radixdlt.com: https://www.radixdlt.com/post/what-is-an-eclipse-attack/

Wikipedia. (Februar 2020). Pridobljeno iz Wikipedia.org: https://en.wikipedia.org/wiki/Hashcash