2. prosojnica

Bitcoin je popularna kriptovaluta, katere namen je izničiti vpletenost tretjih oseb oz organizacij in omogočiti enostaven in hiter prenos valute širom sveta. Zaradi tega je postala ta kriptovaluta zelo priljubljena, saj promovira lastnost, da nobena vlada, podjetje in kakšna druga organizacija ne more vplivati na to koliko količine in vrednosti je v “obtoku”.

Vseeno pa je potrebno gledati na Bitcoin z malce rezerve, saj je ta valuta precej mlada in ima svoje pomanjkljivosti. Med drugim je zelo vprašljiva dejanska varnost valute, saj ima veliko ranljivosti ki ogrožajo ugled Bitcoin valute. Nekaj od teh ranljivosti so:

- omejitev hitrosti obdelovanja transakcij

- pomanjkanje podpore (premalo aplikacij za vsakdanjo uporabo)

- varnostne luknje, ki omogočajo zlorabo.

Na začetku je bila vrednost enega Bitcoina 6 centov, do danes pa je narasla na vrednost 2,390 ameriških dolarjev.

3. prosojnica

Vse izvedene transakcije se hranijo v verigi blokov (blockchain), ki je javno dostopna in preverljiva knjiga nakazil. Veriga zagotavlja, da je mogoče trošiti samo bitcoine, ki so dejansko v lasti plačnika in omogoča preverjanje stanj denarnic.

Vsak blok je sestavljen iz več nakazil, nakazilo pa predstavlja prenos bitcoinov iz ene denarnice v drugo. Vsako nakazilo mora biti podpisano s skrivnim ključem, ki ga hrani denarnica. Poleg avtentikacije podpis zagotavlja da nakazil ni mogoče kasneje spreminjati. Informacija o novem nakazilu oziroma transakciji je vedno poslana vsem zainteresiranim članom omrežja.

Zato, da je veriga blokov vredna zaupanja je potrebno vsako transakcijo overiti s potrditvijo omrežja, temu procesu pravimo rudarjenje (mining). Rudarji nakazila zberejo in jih zapakirajo v bloke, ki morajo zadoščati zelo strogim pravilom šifriranja, ki ji preverja omrežje. Bloke se overi tako, da se izračuna njihovo hash vrednost, zato da rudar ustreže zahtevam omrežja mora bloku transakcij dodati žeton (nonce). Iskanje žetona predstavlja glavnino dela, ki jo opravlja rudar. Ko rudar najde pravo vrednost objavi dokaz in ga skupaj z blokom doda v verigo. Za najdbo pravega žetona je nagrajen sz 25 novo ustvarjenimi bitcoini. Ta nagrada služi kot motivacija za izvajanje overjanja. Rudar v blok transakcij vključi transakcijo nagrade v svojo denarnico, kar onemogoča možnost da bi kdo ukradel njegovo opravljeno delo.(za posameznika)

Zato, da si rudarji povečajo možnost dobitka nagrade se združujejo v skupine poimenovane bazeni. V bazenu rudarjev imamo tako posamezne rudarje in enega administratorja, ki skrbi, da rudarji opravljajo delo in da je nagrada, ki jo dobi bazen pravično razdeljena med vse rudarje v bazenu.

4. prosojnica

V takšnih bazenih administratorji porazdeljujejo delo tako, da rudarjem pošljejo podpisan blok transakcij z razponom žetonov, ki jih morajo raziskati. Rudarji periodično pošiljajo preverjene žetone in izračunane hashe, ki predstavljajo delni dokaz o opravljenem delu (partial proof of work). Vsakič ko rudar poskuša najti delni dokaz ima možnost najdbe polnega dokaza, ki doprinese nagrado 25 bitcoinov. Administrator nato vknjiži blok, pobere nagrado in jo porazdeli med sodelujoče rudarje. Vsak rudar je nagrajen z deležem, ki je odvisen od količine delnih dokazov, ki jih pošlje administratorju. Administratorjev podpis v bloku zagotavlja, da noben izmed rudarjev ne more nagrado pobrati zase.

Rudar lahko pošilja vse delne dokaze in zakrije polne dokaze, čeprav nagrade ne more zahtevati zase, lahko na ta način od bazena dobiva deleže nagrade na račun drugih članov, kljub temu, da omrežju ne prinaša nobenih koristi. Takšen napad je poimenovan napad s prikrivanjem blokov. Trenutno je takšen napad nemogoče zaznati ali preprečiti.

Napad lahko izvede posamezen rudar, ali več rudarjev iz drugih bazenov. V primeru večjega napada, se lahko več rudarjev združi in skupaj napadejo enega ali več bazenov hkrati. Poznamo tudi sponzorirane napade, kjer neka tretja oseba investira v napadalca.

5. prosojnica

Napad s prikrivanjem blokov je lahko poguben za vse javno dostopne bazene rudarjev, ki omogočajo včlanitev nezanesljivih rudarjev. V času nastanka članka ni obstajal nobena dobra zaščita pred tem tipom napadov. V sorodnem delu je bila je opisana metoda za odkrivanje takih napadov. Administrator bi generiral opravilo za člana bazena, za katero ve da je rešitev poln dokaz o opravljenem delu. V primeru, da rudar ne posreduje rešitve se tako ujame v past. Slabost tega pristopa je ta, da od administratorja in poštenih rudarjev zahteva trošenje sredstev, ki bi jih lahko namenili rudarjenju. V drugem sorodnem delu, pa je kot rešitev predlagana dodatna nagrada za rudarja, ki najde poln dokaz.

Avtorji v članku predlagajo enostavno spremembo obstoječe sheme rudarjenja, ki bi preprečila napad tako s strani članov bazena kot tudi administratorja bazena.

6. prosojnica

V obstoječi shemi je poln dokaz hash vrednost, bloka in žetona , ki ima na najbolj pomembnih bitih z ničel. Delni dokazi o opravljenem delu pa so nizi, ki imajo z' začetnih ničelnih bitov, kjer je z' < z.

Delne dokaze rudarji pošiljajo administratorju, ki jih zbira in preverja. Administrator je odgovoren za določitev vrednosti z', ki mora biti taka, da lahko rudarji redno najdejo dokaz in hkrati ne presežejo računskih sposobnosti zaradi preverjanja.

Avtorji članka predlagajo sledečo spremembo Bitcoin sheme:

Administrator izbere vrednost z'. Bazen poleg tega določi še naključen niz bitov “s” in vrednost zadnjih z – z' najmanj pomembnih bitov hash vrednosti. Ta niz bitov poimenujemo r.

Bazen iz parametrov ustvari varnostno shemo com z ključem decom. Administrator pošlje shemo com vsem rudarjem, ključ pa hrani pri sebi in skrbi za to, da ostane tajen. Ko rudarji sestavijo blok vanj vključijo tudi shemo com in dolžino ciljne vrednosti delnega dokaza o opravljenem delu (z'). Rudarji administratorju posredujejo vse bloke, ki imajo hash vrednosti z z' začetnimi ničlami. Administrator prejme bloke in med preverjanjem išče takega, ki ustreza začetnim kriterijem. V primeru da najde takšen blok, ga posreduje Bitcoin sistemu skupaj z ključem. Ko vsa vozlišča v sistemu prejmejo blok in ključ, shemo odklenejo in preverijo, če ustreza kriterijem. Blok je sprejet, če je prvih z bitov hash vrednosti sestavljenih iz z' ničel in niza r.

V tej shemi rudarji ne morejo razlikovati med delnim in polnim dokazom dela. Ko se zamenja obdelovani blok mora administrator razkriti ključ s katerim rudarji preverijo svoje izračunane dokaze. Na ta način rudarjem odvzamemo sposobnost izvajanja dokazov, od administratorja pa zahtevamo dokazovanje poštenosti. Avtorji članka so dokazali, da ta shema ne vpliva na težavnost rudarjenja.

Zaključek

Za konec bi poudarili, da ta luknja še vedno obstaja in se la lahko uporabi za izvajanje drugih napadov, kot so dvojna uporaba bitcoinov. Prav tako se ta ranljivost še vedno raziskuje in zanjo išče rešitve.

To bi bilo iz naše strani vse.