ქვიზი N5

1 რა არის ნონსი?

nonce არის 32-ბიტიანი (ან უფრო დიდი) ველი ბლოკის სათაურში, რომელსაც მაინერები ზრდიან ახალი ბლოკების მაინინგის დროს.

2 როგორ მუშაობს ჰეშირების ალგორითმი SHA-256?

ფართოდ გამოყენებული კრიპტოგრაფიული ჰეშის ფუნქცია, რომელიც აწარმოებს 256-ბიტიან (32-ბაიტი) ჰეშის მნიშვნელობას თვითნებური ზომის შეყვანის მონაცემებიდან. აი, როგორ მუშაობს SHA-256 ჰეშირების ალგორითმი. შეყვანის შეტყობინება ისეა შეფუთული, რომ მისი სიგრძე შეესაბამება 448 მოდულს 512. შიგთავსი შედგება ერთი "1" ბიტისაგან, რასაც მოჰყვება იმდენი "0" ბიტი, რამდენიც საჭიროა საჭირო სიგრძის მისაღწევად, და ბოლოს, სიგრძე ორიგინალური შეტყობინება ბიტებში დართულია 64 ბიტით. შეფუთული შეტყობინება დაყოფილია 512 ბიტიან ბლოკებად. ჰეშის ფუნქცია იწყება რვა 32-ბიტიანი ცვლადის ინიციალიზებით (ცნობილია როგორც "ჰეშ მნიშვნელობები") კონკრეტული მუდმივებით. ეს ჰეშის მნიშვნელობები, როგორც წესი, მიღებულია პირველი 8 მარტივი რიცხვის კვადრატული ფესვების წილადი ნაწილების პირველი 32 ბიტიდან. შეკუმშვის ფუნქცია თავის მხრივ მოქმედებს შეტყობინების თითოეულ ბლოკზე. ის იღებს მიმდინარე ბლოკს წინა ჰეშის მნიშვნელობებთან ერთად, როგორც შეყვანა და აწარმოებს ჰეშის მნიშვნელობების ახალ კომპლექტს, როგორც გამოსავალს. თითოეული ბლოკის დამუშავებამდე ბლოკი გაფართოვდება შეტყობინებების განრიგის მასივში 64 32-ბიტიანი სიტყვისგან. შეკუმშვის ფუნქცია შედგება მრავალი გამეორებისგან, თითოეული იყენებს ლოგიკური და არითმეტიკული ოპერაციების სერიას (როგორიცაა ბიტის ოპერაციები, დამატების მოდული 2^32 და ბრუნვა) ჰეშის მნიშვნელობების განახლებისთვის. ეს ოპერაციები აერთიანებს მიმდინარე ბლოკს წინა ჰეშის მნიშვნელობებთან ახალი ჰეშის მნიშვნელობების შესაქმნელად. ყველა ბლოკის დამუშავების შემდეგ, საბოლოო ჰეშის მნიშვნელობა მიიღება შეკუმშვის ფუნქციის ბოლო ოპერაციიდან მიღებული ჰეშის მნიშვნელობების შეერთებით.

რა არის ჰეშრეიტი (hashrate)?

ჰეშრეიტი ეხება გამოთვლით სიმძლავრეს ან სიჩქარეს, რომლითაც მაინინგ მოწყობილობების ქსელს შეუძლია შეასრულოს კრიპტოგრაფიული ჰეშის ფუნქციები წამში. ბლოკჩეინის ქსელების კონტექსტში, რომლებიც იყენებენ სამუშაოს დადასტურების (PoW) კონსენსუსის მექანიზმებს, როგორიცაა ბიტკოინი, ჰეშრეიტი არის ქსელის მთლიანი გამოთვლითი სიმძლავრის საზომი.

რამდენი გახდა მაინინგური ანაზღაურება 2020 წლის მაისიდან?

რით შევიდა ისტორიაში მაინინგური ფული Ghash ?

ბიტკოინის მაინინგის ისტორიაში მაინინგ აუზმა GHash.io (ასევე ცნობილი როგორც GHash.io ან უბრალოდ GHash) მნიშვნელოვანი ყურადღება და წინააღმდეგობა გამოიწვია 2014 წელს, როდესაც მოკლედ გადააჭარბა მთლიანი Bitcoin ქსელის ჰეშრეიტის 50%-ს.