ქვიზი N4

1. ვინ გამოიგონა "ჭკვიანი კონტრაქტები"?

ჭკვიანი კონტრაქტები გამოგონებული იქნა ნიკ საბოს მიერ 1990-იან წლებში.

2. როგორ ყალიბდება ბიტკოინის ქსელში ადრესაციის სისტემა?

1. გასაღების გენერაცია: ბიტკოინის ქსელში თითოეულ მომხმარებელს აქვს წყვილი კრიპტოგრაფიული გასაღები

2. მისამართის შექმნა: მისამართები მიღებულია საჯარო გასაღებიდან პროცესის გამოყენებით, რომელსაც ჰაშინგს უწოდებენ.

3. მისამართის გამოყენება: მისამართები გამოიყენება ტრანზაქციების გასაგზავნად და მისაღებად.

3. აღწერეთ გასაღებების გენერაციის პროცესი.

შემთხვევითი რიცხვების გენერაცია,

ელიფსური მრუდის გამრავლება,

წერტილის შეკუმშვა,

ჰეშირება და კოდირება,

მისამართის ფორმატი.

4. როგორ მუშაობს Base58 ალგორითმი?

Base58 კოდირება იყენებს 58 სიმბოლოს კომპლექტს, რომელიც არჩეულია სიმბოლოების გამოსარიცხად, რომლებიც შეიძლება გამოიყურებოდეს მსგავსად და გამოიწვიოს დაბნეულობა მაგალითად ასო O და ციფრი 0.

Base58 ში გადაყვანისას ჯერ ხდება მონაცემის კოდირება, შედეგის თითოეული ბაიტი განიხილება როგორც ციფრი.

წინა საფეხურიდან მიღებული დიდი მთელი რიცხვი იყოფა 58-ზე და დარჩენილი ნაშთი ჩაიწერება. ეს ნაშთი შეესაბამება Base58-ში კონკრეტულ სიმბოლოს. გაყოფა გრძელდება მანამ სანაბ ნაშთი ნული არ იქნება. ეს ნაშთები შემდგომ შებრუნებულად ჩაიწერება. ზოგჯერ დაშიფვრამდე ემატება პრეფიქსი, რომელსაც შეუძლია მიუთითოს კონტექსტი ან მონაცემების ტიპი.

5. რა არის "მემპული"?

Mempool არსებითად არის დროებითი საცავი დაუდასტურებელი ტრანზაქციებისთვის, რომლებიც გადაცემულია ქსელში, მაგრამ ჯერ არ არის შეყვანილი ბლოკში მაინერების მიერ. როდესაც მომხმარებელი იწყებს ტრანზაქციას, ის პირველად ვრცელდება ქსელის კვანძებში და ინახება მათ შესაბამის Mempool-ებში.