FERIT
FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA
I INFORMACIJSKIH TEHNOLOGIJA **OSIJEK**

LABORATORIJSKA VJEŽBA 2

Izrada jednostavne kriptovalute

Sadržaj

1. Uvod

U ovoj laboratorijskoj vježbi baviti ćemo se izradom jednostavne kriptovalute. Kao što već znamo, kriptovaluta je podatak. Ovaj podatak je zaštićen kriptografijom koja ga čini otpornim na krivotvorenje ili dvostruku potrošnju. Umjesto na centralnim serverima banaka, podaci su distribuirani među korisnicima koje nazivamo čvorovima (eng. node). Izmjenu podataka bez centraliziranog tijela među korisnicima izvodimo u obliku blockchaina koji spada u DLT tehnologije (eng. distributed ledger technologies). Zapravo, možemo reći da je blockchain zapravo knjigovodstveni zapis kriptovalute. U njemu su zabilježena kretanja kriptovaluta između adresa.

2. Potrebna predznanja

U prethodnoj laboratorijskoj vježbi, naučili ste koristiti Base58, SHA256 i generiranje javnog i privatnog ključa. U ovoj vježbi će vam to biti potrebno. Primjer rješenja prethodnih laboratorijskih vježbi dan je niže.

2.1. Base58 node.js rješenje

```
const bs58 = require('bs58');
// Define the text to encode
const textToEncode = "FERIT";
// Encode the text using Base58
const encodedText = bs58.encode(Buffer.from(textToEncode));
// Display the encoded text
console.log(`Encoded text: ${encodedText}`);
// Decode the encoded text back to the original text
const decodedText = Buffer.from(bs58.decode(encodedText)).toString('utf-8');
// Display the decoded text
console.log(`Decoded text: ${decodedText}`);
```

2.2. SHA256 node.js rješenje

```
const { createHash } = require('crypto');

function hash(string) {
  return createHash('sha256').update(string).digest('hex');
}
console.log(hash('FERIT'));
```

3. Osnovna terminologija

Osnovni pojmovi vezani za kriptovalute u ovoj laboratorijskoj vježbi su transakcija, blok, blockchain i novčanik tj. wallet. Ukoliko radimo u nekom od objektno orjentiranih jezika, njih možemo predstaviti klasama.

3.1. Transakcija

Transakcija je osnovna jedinica u kriptovaluti. Transakcija se odnosi na prijenos jedne kriptovalute s jednog računa na drugi račun u mreži. Svaka transakcija u kriptovaluti mora biti autentična, potvrđena i verificirana.

3.2. Blok

Blok se odnosi na grupu transakcija koje se nalaze u blockchainu. Svaki blok u blockchainu ima jedinstveni identifikator i sadrži informacije o svim transakcijama koje su unutar tog bloka. Blokovi se povezuju jedan za drugim kako bi se stvorio blockchain.

3.3. Wallet (novčanik)

Novčanik je jedinstvena adresa dizajnirana za prihvaćanje kriptovalute. Možete to zamisliti kao adresu e-pošte. Svaki blockchain ima jedinstvenu vrstu novčanika, a većina njih trenutno je nekompatibilna jedna s drugom (npr. nije moguće poslati Bitcoin na Ethereum adresu).

Svatko može slobodno imati koliko god adresa želi, a osim ako korisnik ne pogriješi ili adresu ne objavi javno, adresu je nemoguće povezati s njegovim pravim identitetom. Svatko može vidjeti koliko novca svaka adresa ima jer je na većini blockchaina stanje svačije adrese javno. Ako novčanik u kripto carstvu zamislimo kao sandučić e-pošte, svatko ga može čitati, ali samo vlasnik može slati e-poruke ili odgovarati na njih. Metoda kojom se koristi novac na adresi je potpisivanje izjave - takozvana transakcija - da se novac prenosi s adrese A na adresu B pomoću privatnog ključa, koji je niz brojeva i slova koji se ne mogu pogoditi. Nakon toga, blockchainu se šalje zahtjev za potvrdu kako bi ga mogli vidjeti svi ostali korisnici. Točnije, novac u kriptovalutama zapravo ne putuje; umjesto toga, adresa koja je posljednja navedena u blockchainu kao vlasnik određenog iznosa određene valute smatra se vlasnikom te valute.

Novčanik služi kao sigurno mjesto za pohranjivanje i čuvanje kriptovaluta. Svaki novčanik ima svoje karakteristike i značajke, ovisno o platformi na kojoj se nalazi. Na primjer, neki novčanici su online, dok su drugi offline ili "hladni", što znači da se ne povezuju s internetom. Ovi offline novčanci su sigurniji, jer su manje podložni hakiranju ili krađi od online novčanika.

3.4. Blockchain

Chain, ili blockchain, je tehnologija koja se koristi za pohranu podataka o svim transakcijama u kriptovaluti. Svaki novi blok koji se dodaje u blockchain povezuje se s prethodnim blokovima u lancu. To stvara neprekidni lanac blokova koji sadrži sve transakcije u kriptovaluti. Svaka promjena u jednom bloku utjecat će na sve buduće blokove u lancu.

4. Zadatak

Kreirati jednostavnu kriptovalutu. Možete koristiti programe i alate koje želite. Preporuka je kreirati 4 klase (Transakcija, Wallet, Blok i Blockchain). Transakcija mora sadržavati količinu kriptovalute, adresu pošiljatelja te adresu primatelja.

Blok možemo predstaviti spremištem unutar kojeg je spremljena barem jedna transakcija. Osim prvog, odnosno Genesis bloka, svaki blok sadrži hash vrijednost prethodnog bloka. Također, blok mora imati vremensku oznaku svoga nastanka kao i vlastitu hash vrijednost. Koristiti SHA256 kod iz prethodne vježbe.

Blockchain zapravo prima svaki novonastali blok. Nove blokove možete dodavati u blockchain koristeći push funkciju.

Novčanik odnosno wallet ima dva svojstva – private i public key. Za ovo možete koristiti kod iz prethodne vježbe.

Instancirajte tri walleta sa imenima profesor, student, cryptowhale. Sa sva tri walleta je potrebno poslati nekom drugom walletu određeni iznos kriptovalute.

Za kraj zadatka, ispišite Blockchain.

4.1 Primjer ispisa blockchaina (bez adresa walleta):


```
"blockchain": [
        {
            "index": 0,
            "timestamp": "15.3.2023.",
            "data": "Genesis blok",
            "previousHash": "",
            "hash":
"1f5d7072bd3a521117ccde5da7d9bfb300ba21e9cbc32dfb90c45cacfd4ba020"
        },
        {
            "index": 1,
            "timestamp": "16.3.2023.",
            "data": {
                "sender": "Profesor",
                "recipient": "Student",
                "quantity": 25
            },
            "previousHash":
"1f5d7072bd3a521117ccde5da7d9bfb300ba21e9cbc32dfb90c45cacfd4ba020",
            "hash":
"c7bfd299ec25f58c15d5b84eb6460042829a51c2e1be2f3261c51839de06f4ae"
        },
        {
            "index": 2,
            "timestamp": "17.3.2023.",
            "data": {
                "sender": "Student",
                "recipient": "Cryptowhale",
                "quantity": 34
            },
            "previousHash":
"c7bfd299ec25f58c15d5b84eb6460042829a51c2e1be2f3261c51839de06f4ae",
            "hash":
"af00e280872546c5a347f0c47bdcc7630c3dd3d3027ce081c076219ffef56b8a"
        },
        {
            "index": 3,
            "timestamp": "18.3.2023",
            "data": {
                "sender": "Cryptowhale",
                "recipient": "Profesor",
                "quantity": 34
            },
            "previousHash":
"af00e280872546c5a347f0c47bdcc7630c3dd3d3027ce081c076219ffef56b8a",
            "hash":
"37aec5892ba45a1771d9c5cd5467b57520318a209b2e791f1d4a826f826ee1dc"
        }
    ]
}
```