Kako i zašto funkcioniše blockchain?

Seminarski rad u okviru kursa
Tehničko i naučno pisanje
Matematički fakultet

Lazić, Jovana
kontakt email adresa autora

Nikić, Ognjen
kontakt email adresa autora

Nešković, Ognjen
mi22009@alas.matf.bg.ac.rs

Sekešan, Pavle
kontakt email adresa autora

31. oktobar 2022.

Sažetak

U radu su sažeto iznete osnove kriptografije potrebne za razumevanje i implementaciju blokčejna. Ukratko je predstavljena istorija blokčejna, kao i glavne ideje potrebne za realizaciju blokčejna koji se nalazi iza jedne od najpoznatijih kriptovaluta - Bitcoin. Dopuniti kasnije...

Sadržaj

1 Uvod

Napisati uvod - ukratko nešto o istoriji blokčejna, čemu služi, zašto je koristan, pomenuti osnovne ideje koje se koriste (heširanje, merkle stabla, asimetrična kriptografija (digitalni potpisi) itd.) Ovako treba da citiramo stvari [1]

2 Kriptografske osnove

2.1 Kriptografske heš funkcije

Napisati ovaj subsection

2.2 Asimetrična kriptografija

Napisati ovaj subsection

3 Blokčejn

3.1 Blokovi

Napisati ovaj subsection - apstraktnije opisati pojam bloka u blokčejnu generalno (ne samo kod bitkojna), način za postizanje konsenzusa (proof of work, proof of stake,...), forkovi

3.2 Decentralizacija

Napisati ovaj subsection - opisati kako blokčejn koristi peer to peer mrežu, sa konkretnim primerom (na primer kako bitkojn radi broadcast ili šta već), prednosti i mane decentralizacije generalno - double spending ako neko ima preko 51%, itd.

4 Bitkojn (Bitcoin)

4.1 Transakcije

Napisati kako se realizuju transakcije u bitkojnu, u suštini transakcije definišu šta je digitalni coin

4.2 Blokčejn

Objasniti timestamp server i proof of work sekcije iz bitcoin rada

4.3 Distribuirana mreža

Objasniti Network i incentive sekcije iz bitcoin rada

4.4 Optimizacija memorije

Objasniti upotrebu merkle stabla, full node, pojednostavljenu verifikaciju ako neko nije full node itd.

5 Primene

5.1 Kriptovalute

Napisati ovaj subsection

5.2 Pametni ugovori

Napisati ovaj subsection - pomenuti eth pošto btc nije turing complete

6 Diskusija

Napisati ovaj subsection - pomenuti prednosti i mane kriptovaluta, moguće napade na blokčejn 51% i druge koji zahtevaju manje od toga, pojavu centralizacije u formi mining poolova, nešto iz ekonomije?, privatnost, kriminal itd.

7 Zaključak

Napisati ovaj subsection

Literatura

[1] A. M. Turing. On Computable Numbers, with an application to the Entscheidungsproblem. *Proceedings of the London Mathematical Society*, 2(42):230–265, 1936.