SVEUČILIŠTE U ZAGREBU
PRIRODOSLOVNO-MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Filip Maček

PAMETNI UGOVORI POMOĆU BLOCKCHAIN TEHNOLOGIJE

Diplomski rad

Voditelj rada:

prof.dr.sc. Luka Grubišić

Zagreb, kolovoz 2020.

Sadržaj

Uvod

Pametni ugovori naziv su za bilo kakav kompjutorski program ili transakcijski protokol koji automatski izvršava i kontrolira izvršavanje nekog ugovora i svih njegovih dijelova. Ideja je da su uvjeti ugovora kao i njegova etape izvršavanja potpuno prepušteni kompjutorskom kodu.

Glavna korisnost pametnih ugovora je u tome što se oni ne ovise o nikakvim sigurnim posrednicima ili arbitražama i svim troškovima koje takvo posredstvo nosi. Svi ostali problemi i prevare koji mogu nastati u izvršavanju ugovora također su izostavljeni jer se podrazumijeva da je kod tog ugovora napravljen u cilju obuhvaćanja svih mogućih događaja u stvarnom svijetu.

Još jedan važna odluka kod pametnih ugovora jest gdje će se taj program tj. ugovor izvršavati . Većina današnjih pametnih ugovora se izvršavaju na centralnim računalima onog jednog od sudionika tog ugovora. Ali idealni scenarij bi bio da se ugovor izvršava na serverima na kojima nitko od sudionika nema kontrola,a svi sudionica mogu vjerovati da se ugovor izvršiti po unaprijed određenim pravilima.

To dolazimo do blockchaina i jedan od mogućih rješenja gdje se taj programski kod pametnog ugovora može izvršavati. Trenutno je najveći blockchain i platforma za decentralizirano izvršavanje pametnih ugovora Ethereum.

U ovom diplomskom radu pokušat ćemo pokazati jednu moguću implementaciju i korisnost pametnih ugovora u stvarnom svijetu te ćemo pokušati pokazati kako se takva implementacija može natjecati sa sadašnjim modelom izvršavanja tih ugovora gdje velike korporacije ... TODO

Model i interakcija sa pametnim ugovorima na blockchainu je drugačiji nego današnje aplikacije koje u većini slučajeva komuniciraju sa svojim centralnim serverom pomoću API-ja (engl. Application programming interface).

Naša aplikacija je decentralizirana jer ne komunicira sa centralnim našim serverom nego se izvršava na svim kompjuterima na Ethereum blockchainu. Time naša aplikacija postaje „Dapp”, naziv koji se koristi za aplikacije tj. pametne ugovore koji se izvršavaju na Ethereum.

--- KRATAK OPIS APLIKACIJE I SVIH NJENIH DIJELOVA

Poglavlje 1

Uvod u blockchaina

1.1 Uvod

Kroz ovo poglavlje ukratko ćemo opisati glavne karakteristike i dizajn blockchain kao i njegovu povijest. Također značajna će nam biti i njegova motivacija i kakve pogodnosti blockchain donosi.

1.2 Povijest

Nakon izuma računala 1980-tih ljudi su se počeli pitati kakve su sve još inovacije moguće sa tim magičnim strojem koji su izumili. Tada su još to bila izolirana računala koja su slabo bila povezana. Ali i već tada su neki istaknuti stručnjaci počeli uviđati kako da povežu ta računala u jedan koherentan sustav ili mrežu. *David Chaum* je bio pionir u tom području, i on je već 1982. u svojoj doktorskoj disertaciji [1] počeo razmišljati kako organizacije koje međusobno ne vjeruju jedna drugoj, mogu zajedničkim snagama izgraditi i održavati siguran računalni sistem kojem svi mogu vjerovati. Uvidio je veliku potrebu u privatnom i javnom sektoru za takve sisteme. Kriptografskim tehnikama bilo bi moguće takav sistem ostvariti praktičnim, gdje bi se spremljeni i podaci u opticaju mogli biti zaštićeni mehanizmom sefa (*engl. vault*)
Kasnije, 1991. *Stuart Haber i W. Scot. Sornetta* iznose prvi dizajn kriptografski osiguranog lanca blokova u kojem se ne može manipulirati vremenskim oznakama. Godinu dana nakon u svoj dizajn unose novu inovaciju binarno hash stablo (*eng. Merkle Tree)*

Bibliografija

[1] David Lee Chaum, *Computer Systems Established, Maintained and Trusted by Mutually Suspicious Groups*, 1982. University of California, Berkley