UNIVERZITET U KRAGUJEVCU

PRIRODNO-MATEMATIČKI FAKULTET

Uputstvo za Ethereum

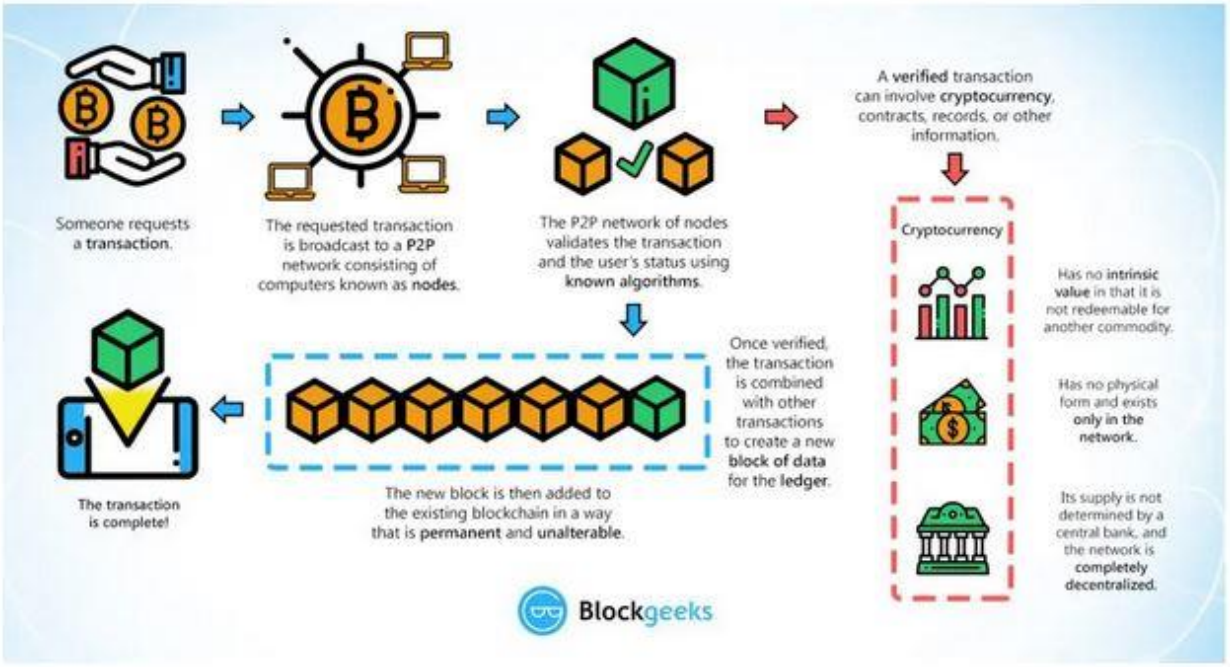
TechLab

Studenti	**Mentori**
Janko Radović 84/2018	Dr Boban Sojanović
Nikoleta Lešević 79/2018	Andreja Živić
Nikolija Mojsić 73/2017	Lazar Krstić
Nikola Jevremović 76/2018	Filip Bojović
David Dašić 62/2018	

Sadržaj

1.Šta je blockchain?

Blockchain je, najjednostavnije objašnjeno, kolekcija vremenski označenih nepromenljivih zapisa, kojima upravlja računarski klaster, ali ne poseduje nijedan od entiteta. Svaki blok podataka je osiguran i povezan sa ostalim blokovima korišćenjem kriptografskih principa.



1.1 Karakteristike

1. Decentralizacija – svaki blok u lancu sadrži replikaciju celog lanca, odnosno sve podatke.
2. Transparentnost – iako je identitet svakog člana osiguran, odnosno kriptovan, moguće je videti nečije transakcije ukoliko nam je nečija javna adresa poznata.
3. Nepromenljivost - ukoliko je nešto uneto u blockchain, to ne može biti izmenjeno.

2. Šta je Ethereum?

Ethereum je tehnologija (softver otvorenog tipa) koja omogućava slanje kriptovaluta bilo kome uz malu naplatu. Ethereum je zasnovan na blockchain tehnologiji, i omogućava kreiranje i održavanje decentralizovanih aplikacija.

Ethereum je zasnovan na ideji Bitcoin-a, uz par većih razlika.

I Bitcoin i Ethereum nam omogućavaju korišćenje digitalnog novca, bez plaćanja provajderima ili bankama. Međutim, Ethereum je moguće isprogramirati, tako da ima više namena, kao što su aplikacije za finansijske transakcije, igrice, aplikacije za glasanje, odnosno bilo koje aplikacije koje ne mogu da ukradu podatke ili da izvrše cenzuru.

2.1 Ethereum pametni ugovori

Pametni ugovori predstavljaju frazu koja se koristi za opis računarskog koda koji može olakšati razmenu novca, sadržaja, imovine, deonica ili bilo čega vrednog.

Kada se pokreće na blockchainu, pametan ugovor postaje samoupravni računarski program koji se automatski pokreće kada se ispune određeni uslovi.

Budući da pametni ugovori rade na blockhainu, oni rade tačno onako kako su programirani. bez ikakve mogućnosti cenzure, zastoja, prevare ili uplitanja treće strane.

2.2 Ethereum virtuelna mašina (EVM)

Osnovna inovacija Ethereuma, Ethereum Virtual Machine (EVM) predstavlja kompletan Turingov softver koji radi na Ethereum mreži. Omogućava svima da pokrenu bilo koji program, bez obzira na programski jezik, vreme i memoriju. Ethereum virtuelna mašina čini proces stvaranja aplikacije mnogo lakšim i efikasnijim. Umesto da se pravi potpuno originalni blockchain za svaku novu aplikaciju, Ethereum omogućava razvoj više različitih aplikacija na jednoj platformi.

2.3 Solidity

Solidity jeste jezik, koji se koristi za pisanje pametnih ugovora, koji kada se iskompajlira, generiše mašinski kod, koji se može pokrenuti na EVM.

Solidity je poprilično jednostavan jezik, bar što se tiče programiranja, i sintaksom podseća na JavaScript.

Ono što je potrebno postići pisanjem pametnog ugovora ovim jezikom, a što EVM zahteva, jeste determinizam.

Zbog toga Solidity ne poseduje implementaciju za funkciju random().

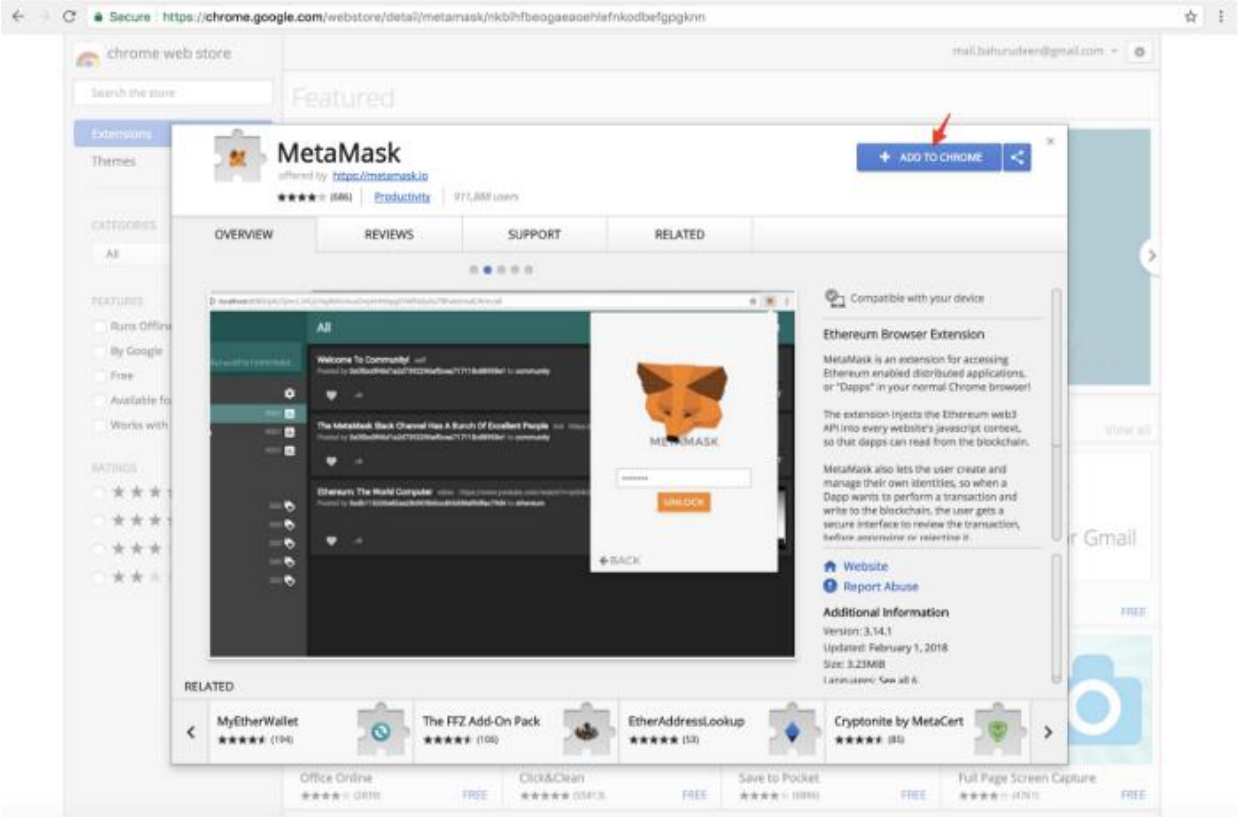
Zahtev za determinističkim pametnim ugovorima omogućava da mreža čvorova u blockchainu uvek može održati i potvrditi konsenzus o novim blokovima koji dolaze, kako bi nastavili da se izvode.

3.Potrebne instalacije

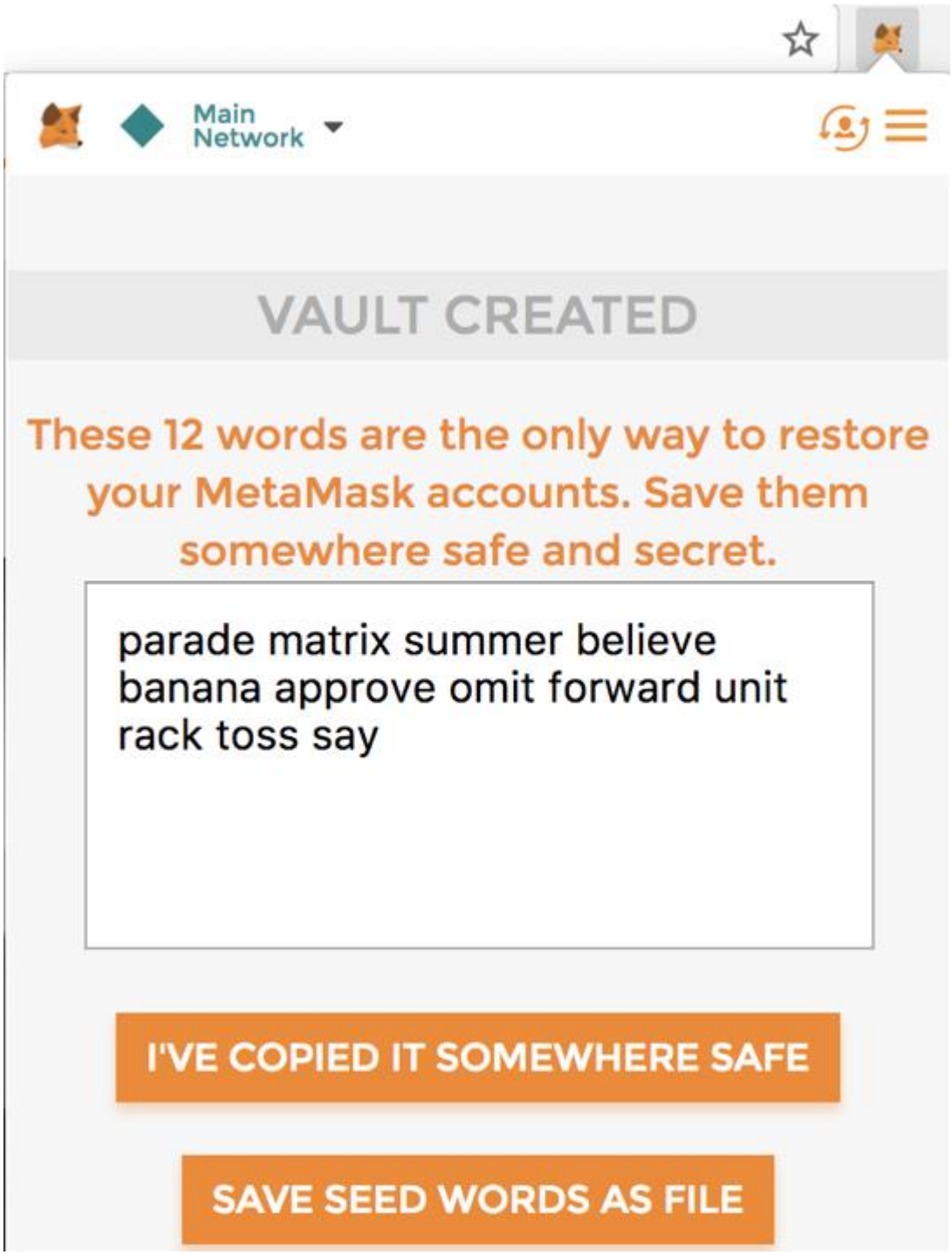
3.1Metamask

Metamask je GoogleChrome, Opera, Vivaldi, Firefox, ekstenzija koja omogućava jednostavnu komunikaciju sa Ethereum blockchainom.

Da biste dodali ekstenziju potrebno je otići na link https://chrome.google.com/webstore/search/metamask/nkbihfbeogaeaoehlefnkodbefgpgknn i kliknuti „ADD TO CHROME“.



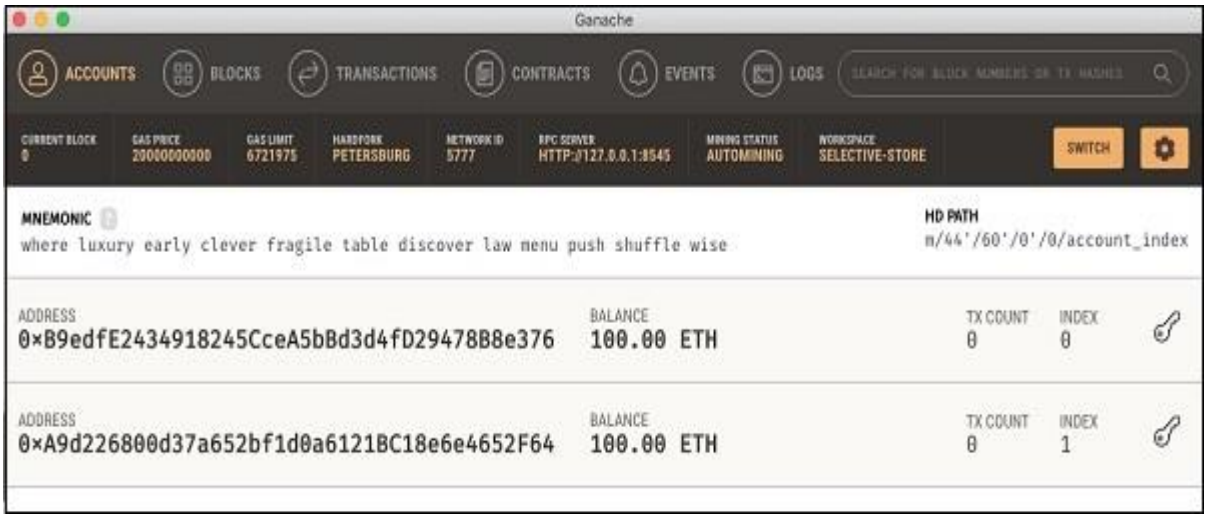
Prilikom setovanja metamask-a bitno je sačuvati na sigurnom ili zapamtiti 12-recnu frazu. 12-recna fraza(“seed“,“backup“) je jedinstven nasumično izabran set reči koji se dodeljuje prilikom kreiranja wallet-a.Ova fraza daje potpun pristup nalogu, zbog toga je vrlo vazno sačuvati je na sigurnom!



Nakon toga je kreirana nova Ethereum adresa.

3.2 Ganache

Ganache se koristi za postavljanje lokalnog Ethereum blokchaina za testiranje pametnih ugovora. Može se skinuti sa sledećeg linka: https://www.trufflesuite.com/ganache. Nakon pokretanja otvara se konzola slična ovoj na slici.



Konzola na slici prikazuje dva računa sa po 100ETH(Ether – valuta koja se koristi na za transakcije na Ethereum mrezi). Takodje se vidi da je broj transakcija nula za svaki račun, jer korisnik nije izvrsio nijednu transakciju.

3.3Rad sa flutterom

Potrebno je instalirati web3.dart paket. Potrebno je instalirati i http paket pošto njega koristi web3.dart. Da bi aplikacija mogla da koristi pametne ugovorne potrebno je generisati ABI, zbog toga je potrebno iskompajlirati pametni ugovor.Za kompajliranje se može koristiti truffle.