Decentralizirane mjenjačnice na "blockchainu"

Bačić, Mateo

Sveučilište Jurja Dobrile u Puli

Fakultet Informatike

Mateo Bačić

Decentralizirane mjenjačnice na „blockchainu“

Završni rad

Pula, 2019.

Sveučilište Jurja Dobrile u Puli

Fakultet Informatike

Mateo Bačić

Decentralizirane mjenjačnice na „blockchainu“

Završni rad

JMBAG: 0112065913, redovni student

Studijski smjer: Informatika

Mentor: doc. dr. sc. Darko Etinger

Komentor: dr. sc. Nikola Tanković

Pula, rujan 2019.

IZJAVA O AKADEMSKOJ ČESTITOSTI

Ja, dolje potpisani Mateo Bačić, kandidat za prvostupnika informatike, smjera informatike ovime izjavljujem da je ovaj Završni rad rezultat isključivo mojega vlastitog rada, da se temelji na mojim istraživanjima te da se oslanja na objavljenu literaturu kao što to pokazuju korištene bilješke i bibliografija. Izjavljujem da niti jedan dio Završnog rada nije napisan na nedozvoljen način, odnosno da je prepisan iz kojega necitiranog rada, te da ikoji dio rada krši bilo čija autorska prava. Izjavljujem, također, da nijedan dio rada nije iskorišten za koji drugi rad pri bilo kojoj drugoj visokoškolskoj, znanstvenoj ili radnoj ustanovi.

Student

Mateo Bačić

U Puli, 23.9 , 2019 godine

Sadržaj

1. Uvod

„Blockchain“ tehnologija je tehnologija nastala na ideji da se stvori lanac blokova (ili blokova) koji su u određenom sustavu, gdje svaki novi blok ovisi o vrijednosti starijeg bloka, te se među njima razmjenjuju informacije. Svaki blok sadrži svoju kopiju svih relevantnih informacija koje sadrži te se tim načinom rada briše potreba za centraliziranom bazom podataka i entiteta koja mora vršiti kontrolu i nadziranje informacija. Prvi oblik „blockchain“ tehnologije je kao pojam poznat još od 90-ih godina, ali onakav oblik kakav danas poznajemo opisan je i definiran 2008. godine. Ta godina se smatra „blockchain“-ovim osnutkom, a nastao je tako što je osoba po pseudonimom Satoshi Nakamoto podigao web-stranicu bitcoin.org te na njoj predstavio svoj koncept. Već sljedeće godine rodio se „bitcoin“, u koji je implementiran „blockchain“ te se koristi kao glavna podloga za sve transakcije koje se odvijaju u mreži te su evidentirane u glavnu knjigu- „Ledger“. Način rada „blockchaina“ omogućuje da se nad zapisima ostvari maksimalna zaštita korištenjem kriptografskih funkcija. Unutar svakog lanca (chain) ili skupa blokova, svaki blok u sustavu unutar sebe sadrži ekvivalentne informacije, a taj način rada omogućen je pomoću algoritma od kojih su najpoznatiji „Proof of work“ i „Proof of stake“ o kojima se bude pričalo kasnije.

U današnje vrijeme, kad su računala postala neophodna za obavljanje mnogih poslovnih poteza i transakcija, boravište na mreži postala je većini osoba svakodnevnica. Samim time mrežom kola veliki broj informacija i podataka, što poslovnih što privatnih, te poslovanje preko mreže za sobom vuče određene rizike. Upravo zbog toga, važno je omogućiti da informacije kojima se koristimo kreću sigurnom mrežom te ih nitko ne može iskorištavati ili mijenjati, prije, za vrijeme ili nakon upisivanja.

Pojavom „blockchaina“ pojavila se šansa za velikom zaradom na novom tržištu. Samim time počele su se formirati centralizirane mjenjačnice koje su služile kao posrednik između prodavača i kupca. Centralizirane mjenjačnice kripto valuta su online platforme kojima se može kupovati i prodavati kripto valuta te omogućuju razmjenu između dvije različite kripto valute. Također uz centralizirane, počele su se razvijati i decentralizirane mjenjačnice koje nemaju posrednika odnosno autoriteta, nego se transakcije obavljaju u „nepouzdanom peer-to-peer“ (vršnjačkom) okruženju. Decentralizirane razmjene smanjuju rizik krađe hakiranjem razmjene te mogu spriječiti manipulaciju cijenama ili lažni volumen trgovanja i više su anonimne od razmjena koje implementiraju poznavanje zahtjeva kupaca. O obje vrste mjenjačnica, te njihovim prednostima i nedostatcima ćemo više saznati u nastavku.

2 Blockchain

2.1 Što je blockchain?

„Blockchain“ tehnologija je skupina blokova koji su nanizani i povezani u jednu cjelinu, ili lanac, te se u svakom od blokova nalazi niz zapisa odnosno informacija. Svaki blok se povezuje algoritmom koji koristi „hash“ funkciju (SHA256), koju je skoro nemoguće hakirati. Primjer „Bitcoina“ nam pokazuje kako korištenjem „hash“ funkcija i implementiranjem „blockchain“ tehnologije se stvorila prva kripto valuta koja ima sigurnosne transakcije bez korištenja centraliziranog autoriteta. Svaki blok u lancu ima određenu količinu podataka koje može pohraniti te kada se taj blok popuni stvara se novi koji se povezuje s prijašnjim i onim koji će bit stvoren u budućnosti. Takav način stvaranja blokova daje veliku razinu sigurnosti jer ukoliko netko želi mijenjati podatke u jednom bloku mora ih mijenjati u svim prijašnjim što je gotovo nemoguće. Kako smo ranije spomenuli, cijeli sustav temelji se na ideji ravnopravnih partnera (peer-to-peer). „Blockchain“ obilježavaju 4 funkcije koje korisnici mogu koristiti u sustavu a to su:

- Wallet (novčanik)
- Network routing (mrežno usmjeravanje)
- Mining (rudarenje)
- Održavanje blockchaina

2.1.1 Novčanik (Wallet)

Da biste olakšali trgovanje kripto valutama na centraliziranoj razmjeni, potreban je novčanik. Srećom, novčanici za razmjenu kripto valuta obično se automatski kreiraju kada se korisnički račun instalira na platformi. Novčanik s kripto valutama je mjesto na kojem se pohranjuje jedinstveni digitalni kod koji omogućuje pristup kripto tokenima. Oni djeluju više kao ključ koji otključava kripto valute spremljene u njihovom „blockchainu“. Ako se izgubi novčanik, kripto tokene se zapravo može obnoviti pomoću novog novčanika i jedinstvenih kodova koji su nastali prilikom postavljanja izvornog novčanika. S obzirom na veličinu cijelog sustava, svaki korisnik ne može pohraniti sve podatke te je upravo s tom namjerom i smišljen novčanik. Korisnik koji se služi novčanikom kreira zapise, te verificira transakcije i informacije pohranjivanjem javnih i privatnih kriptografskih ključeva. Javni ključ služi kako bi stvorio adresu koja zaprima transakcije od drugog korisnika, dok se privatni ključ koristi kao identifikator kojim korisnik pristupa adresi i resursima dodijeljenim tom novčaniku.

Novčanikom se potvrđuju novi zapisi unutar lanca tako što u sebe pohranjuje samo zaglavlja blokova a ne cijele zapise lanca. Kako nema zapis od cijelog „blockchaina“, on se koristi drugim novčanicima odnosno partnerima koji im mogu omogućiti pristup traženom dijelu „blockchaina“.

2.1.2 Rudarenje (mining)

Rudarenje je funkcija koju obavlja određeni korisnik koji odluči prihvatiti funkciju rudara. Rudar prihvaća nove zapise koji su napravljeni od strane novčanika, od njih radi blokove te ih smješta u lanac. Kako bi se dodao novi spisak u lanac, potrebni su računalni resursi koje rudar pruža kako bi se riješili algoritmi koji se u ovom slučaju zovu „proof of stake“ (dokaz o ulogu). Rješavanjem algoritma u lanac se dodaju novi blokovi te kada se transakcije potvrde odnosno „validiraju“, rudar koji je trošio svoje računalne resurse biva nagrađen udjelom „bitcoina“.

2.1.3 Mrežno usmjeravanje

Funkciju mrežnog usmjeravanja će obavljati svaki od navedenih partnera. Govorimo o decentraliziranom sustavu ravnopravnih partnera pa se zato i postavlja potreba za time da svaki od partnera uspostavlja vezu s ostalima u sustavu. Uz mrežno usmjeravanje, partneri će također biti zaduženi za validaciju novih zapisa u lancu.

2.2 Algoritmi

Svaki sustav unutar „blockchaina“ je utemeljen na nekom algoritmu kojim se transakcije odobravaju i vrše upisi u blokove. Postoje različiti algoritmi ali ćemo spomenuti najučestalije koji se koriste u „blockchain“ tehnologiji.

To su:

- „PoW“ (proof-of-work)
- „PoS“ (proof-of-stake)
- „DPoS“ (Delegirani proof-of-stake)

2.2.1 Proof of work (PoW)

„Proof of work“, koji je također prvi algoritam koji se koristi s ovom tehnologijom, osmislio ga je začetnik „blockchain“ tehnologije, Satoshi Nakamoto. Unutar tog algoritma, rudari rješavaju matematičke zadatke koje kad izvrše bivaju nagrađeni udjelom valute. Nakon završenog izračuna, u lanac se dodaje novi blok te njegove pripadajuće transakcije. S obzirom da rudari svi koriste jedan „blockchain“, ukoliko se pri hakiranju odnosno napadu pokuša postaviti lažni blok, stvara se novi lanac te se odlučuje koji je ispravan, a to je onaj koji je duži. To znači da ukoliko se manje od 51% računalne snage u mreži nalazi u rukama jedne ili par osoba, ta kripto valuta se smatra sigurnom.

Poput svih algoritama, ima svoje prednosti:

- U proizvodnju novih sredstava ulažu se struja i računalna oprema
- Svatko može rudariti

I nedostatke:

- Mreža postaje spora ako je koristi veliki broj korisnika
- Velika potrošnja energije
- Rudarenje je postalo isplativo samo za one s profesionalnom opremom

2.2.2 Proof of stake (PoS)

„Proof of stake“, bazira se na sasvim suprotnoj ideji. Umjesto da se rudarenjem kreiraju novi blokovi, tvorac novog bloka određuje se ovisno o njegovom udjelu na računu. Tako osoba koja ima veću svotu na računu ima i veću vjerojatnost da će postati stvoritelj novog bloka. Kod korištenja ovog algoritma kreator novog bloka biva nagrađen na drugačiji način.

Kada se odabere osoba koje će biti stvoritelj bloka, provizija transakcije koju je korisnik potvrdio odlazi na njegov račun. Sustav je visoke sigurnosti jer ako bi tvorac bloka odlučio potvrditi lažne transakcije, ujedno riskira sav svoj ulog te čitavu vrijednost kripto valute.

Kao i prijašnji algoritam ima svoje prednosti:

- Brza obrada transakcija (nema potrebe za rješavanjem teških matematičkih problema)
- Nema velike potrošnje električne energije
- Nema potrebe za zahtjevnim hardverom

I nedostatke:

- Bogatiji se obogaćuju
- Moguće je kontrolirati i manipulirat sustav ako se udruže velike grupacije

2.2.3 DPoS (delegirani PoS)

Kao i svaki sustav koliko god siguran bio, postoji rizik od iskorištavanja i manipuliranja. Tako je „blokchain“ stručnjak Daniel Larimer primijetio da bi se sustav mogao „prevariti“ tako što bi rudarenje postalo centralizirano preko velikih udruženja (mining pools) te se na taj način manipuliralo valutom. S time na umu, razvio je novi sustav velike brzine (100000 transakcija u sekundi) kojem „Bitcoin“ ne može parirati. Sustav, kako kaže sam naziv, radi na principu delegata: odabire se skup od 20-101 članova te se oni koriste kako bi potvrdili transakcije i za to dobivaju proviziju. Članovi koji će biti delegati biraju se stalno prisutnim glasanjem. Svaki korisnik koji posjeduje dio kripto valute ima pravo na izglasavanje delegata. Razina važnosti glasa ovisi, kao i u prijašnjem slučaju, o količini sredstava koje korisnik posjeduje. Znači da što je korisnik bogatiji veći je značaj njegovog glasa kod odabira delegata. Svaki član delegata ima pravo modificirati odnosno odbiti željene transakcije, te time onemogućuju da budu dodane ne neki blok. Samim time, članovi delegata imaju veliku moć, te kako bi im se ograničila moć, sve akcije koje delegati vrše su javno dostupne. U tom slučaju, ukoliko se delegat neprimjereno ponaša, postoji vrlo visoka mogućnost da biva izbačen iz kruga delegata i time gubi svu svoju moć te ju daje svojoj zamjeni, odnosno sljedećem kandidatu.

Prednosti ovakvog načina rada su:

- Brza validacija i obrada transakcija
- Prilikom nepravilnosti brzo ih je moguće detektirati
- Nema velikog utroška energije
- Sustav je djelomično centraliziran, ali počiva na visokoj razini demokracije među korisnicima

Ali isto tako ima nedostatke:

- Ukoliko se većina članova delegata udruže, mogu manipulirati mrežom
- Manji je broj ljudi koji potvrđuju transakcije u mreži pa je samim time lakše izvršiti napad zauzimanjem 51% udjela mreže.

Kao što vidimo iz priloženog, „blockchain“ iako inovativan ima veliki problem što se tiče manipulacije mreže. Ukoliko želimo brze transakcije, bilo da se bira „Pos“ ili „DPos“, oba

algoritma imaju problem s mogućnošću manipulacije i time što najvišu dobit dobiva onaj koji već na početku najviše posjeduje, dok POW, iako donekle možda sigurniji, ima problem sa sporim transakcijama te je za normalno rudarenje potrebno puno uložiti u naprednu opremu kako bi bilo isplativo.

2.3 Struktura blokova

Kako iz naziva možemo saznati, „blockchain“ (lanac blokova) se sastoji od niza blokova koji su povezani u lanac. Svaki blok je podatkovna struktura koja u sebi sadrži informacije. Svaki blok ima svoje zaglavlje u kojem se nalaze meta podatci te liste informacija odnosno podataka.

VELIČINA	NAZIV	OPIS
4 BAJTA	VELIČINA BLOKA	VELIČINA BLOKA U BAJTOVIMA
80 BAJTOVA	ZAGLAVLJE BLOKA	META-PODACI
1-9 BAJTOVA	BROJAČ ZAPISA	KOLIKO ZAPISA SADRŽI BLOK
VARIJABILNO	ZAPISI	ZAPISI POHRANJENI U BLOKU

Slika 1 Struktura bloka

VELIČINA	NAZIV	OPIS
4 BAJTA	VERZIJA	VERZIJA PROTOKOLA
32 BAJTA	HASH PRETHODNOG BLOKA	REFERENCA NA BLOK KOJI PRETHODI
4 BAJTA	KORIJEN BINARNOG STABLA	HASH KOJI IMA INFORMACIJE O SVIM ZAPISIMA U BLOKU
4 BAJTA	VREMENSKA OZNAKA	VRIJEME KADA JE BLOK NASTAO
4 BAJTA	TEŽINSKA OZNAKA	TEŽINA ALGORITMA ČIJE JE RIJEŠENJE POTREBNO ZA UKLJUČIVANJE BLOKA
4 BAJTA	NONCE	BROJ POMOĆU KOJEG JE RIJEŠEN ALGORITAM

Slika 2 Struktura zaglavlja

U zaglavlju unutar meta podataka nalaze se informacije o samom zaglavlju kao i informacije o povezivanju kojima se povezuju ostali blokovi koji se nalaze u „blockchainu“. Važno je napomenuti da da svaki blok ima svoju „hash“ funkciju. „Hash“ prethodnog bloka je rezultat koji se dobije kada se nad blokom dva puta primjeni „hash“ funkcija SHA-256 (secure hash algorithm, 256 bitova). „Hash“ koji se odvija nad blokom ne ulazi u samu strukturu bloka, nego se računa samo ukoliko je to potrebno i to na obje strane bloka. 4 bajta koja se koriste za vremensku oznaku govore kada je blok dodan u lanac. Korijen binarnog „hash“ stabla u sebi sadrži podatak koji je preuzeo od svih zapisa u bloku.

Strukturu i način rada „blockchaina“ možemo usporediti s knjigom: svaka stranica u knjizi je numerirana i nalazi se na određenom poglavlju, te tako i zaglavlje bloka sadrži tehničke informacije i referencu na prijašnji blok. Tako bilo kakvo narušavanje redoslijeda se može primijetiti te se pomoću referenci može urediti na početno stanje.

2.4 Ethereum

„Ethereum“ je otvorena softverska platforma zasnovana na „blockchain“ tehnologiji koja programerima omogućuje izgradnju i implementaciju decentraliziranih aplikacija te je kao i „Bitcoin“, distribuirana javna „blockchain“ mreža. Razlika koju treba napomenuti je da se „Bitcoin“ i „Ethereum“ značajno razlikuju u namjeni i mogućnostima. „Bitcoin“ nudi jednu posebnu primjenu „blockchain“ tehnologije, elektronički gotovinski sustav koji se vrši „peer -to-peer“, pomoću kojeg se omogućavaju online „Bitcoin“ transakcije. Dok se „Bitcoin“ koristi za praćenje vlasništva nad digitalnom valutom, „Ethereum“ se fokusira na pokretanje programskog koda bilo koje decentralizirane aplikacije.

U bloku „Ethereum“, umjesto da rudare za „bitcoin“, rudari rade kako bi zaradili „Ether“, vrstu kripto tokena koji pokreće mrežu. „Ether“ također koriste programeri za plaćanje naknada za transakcije i usluga na mreži „Ethereum“.

Postoji druga vrsta tokena koja se koristi za plaćanje naknada rudarima za uključivanje transakcija u njihov blok, zove se „*gas*“ (plin, koji se koristi kao jedinica troška), a za svako izvršenje pametnog ugovora potrebno je poslati određenu količinu „*gas-a*“ zajedno s njom kako bi privukli rudare da je stave u blockchain.

Pametni ugovor je računalni kod koji može olakšati razmjenu novca, sadržaja, imovine, dionica ili bilo čega vrijednog. Kad se izvodi na „blockchainu“, pametni ugovor postaje poput samo-instaliranog računalnog programa koji se automatski izvršava kada su ispunjeni određeni uvjeti.

Osnovna inovacija „Ethereuma“, „Ethereum Virtual Machine“ (EVM), Turingov je cjelovit softver koji radi na mreži „Ethereum“. Omogućuje da bilo tko pokrene bilo koji program, bez obzira na programski jezik s dovoljno vremena i memorije.“ Ethereum Virtual Machine“ čini postupak stvaranja „blockchain“ aplikacija mnogo lakšim i učinkovitijim. Umjesto da mora izgraditi potpuno originalni „blockchain“ za svaku novu aplikaciju, „Ethereum“ omogućava razvoj potencijalno tisuće različitih aplikacija sve na jednoj platformi.

„Ethereum“ omogućuje programerima izgradnju i implementaciju decentraliziranih aplikacija ili „Dapp“ koje svojim korisnicima daju određenu svrhu. „Bitcoin“ je, na primjer, „Dapp“ koji svojim korisnicima omogućuje „peer-to-peer“ elektronički novčani sustav koji omogućuje

online „bitcoin“ plaćanje. Budući da se decentralizirane aplikacije sastoje od koda koji radi na „blockchain“ mreži, ne kontrolira ih niti jedan pojedinačni ili središnji entitet.
„Ethereum“ se također može koristiti za izgradnju decentraliziranih autonomnih organizacija (DAO). DAO je potpuno autonomna, decentralizirana organizacija bez vođe ili centralnog autoriteta.
DAO-ovi upravljaju programskim kodom, na kolekciji pametnih ugovora napisanih na bloku „Ethereum“. Kod je osmišljen da zamijeni pravila i strukturu tradicionalne organizacije, eliminirajući potrebu za ljudima i centraliziranom kontrolom. DAO je u vlasništvu svih koji kupuju žetone, ali umjesto svakog tokena koji je jednak udjelima i vlasničkim udjelima, tokeni djeluju kao doprinosi koji ljudima daju glasačko pravo.
„Ethereum“ se koristi i kao platforma za pokretanje drugih kripto valuta. Zbog standarda tokena ERC20 koji je definirala „Ethereum Foundation“, drugi programeri mogu izdati vlastite verzije ovog tokena i prikupljati sredstva uz početnu ponudu kovanica (ICO). U ovoj strategiji prikupljanja sredstava, izdavatelji tokena postavljaju iznos koji žele podići, nude ga u masu i dobivaju „Ether“ u zamjenu. ICO-i su u posljednje dvije godine prikupili milijarde dolara na platformi „Ethereum“, a jedna od najcjenjenijih kripto valuta na svijetu je token ERC20.
„Ethereum“ je nedavno stvorio novi standard pod nazivom ERC721 token za praćenje jedinstvene digitalne imovine. Jedan od najvećih slučajeva uporabe takvih žetona digitalni su predmeti jer infrastruktura omogućuje ljudima da dokažu vlasništvo nad oskudnom digitalnom robom.
Budući da se decentralizirane aplikacije pokreću pomoću „blockchaina“, imaju koristi od svih njegovih svojstava:
Nepromjenjivost - treća strana ne može izvršiti nikakve promjene u podacima.

Otpornost na korupciju i mijenjanje - aplikacije se temelje na mreži formiranoj oko principa konsenzusa, što onemogućuje cenzuru.

Sigurnost - bez središnje točke kvara i osiguranja pomoću kriptografije, aplikacije su dobro zaštićene od hakerskih napada i lažnih aktivnosti.

Nemogućnost pada servera - aplikacije se nikad ne isključuju same i nikad se ne mogu isključiti od strane drugih.
Iako donose brojne prednosti, decentralizirane aplikacije nisu besprijekorne. Budući da pametni kod ugovora pišu ljudi, pametni ugovori su podjednako dobri kao i ljudi koji ih pišu. Greške u kodovima ili previdi mogu dovesti do nenamjernih štetnih radnji. Ako se pogreška u

kodu iskoristi, ne postoji učinkovit način na koji se može zaustaviti napad ili iskorištavanje, osim dobivanja mrežnog konsenzusa i prepisivanja temeljnog koda. To ide suprotno samoj biti „blockchaina“ koji bi trebalo biti nemoguće mijenjati.

3 Centralizirane mjenjačnice

3.1 Što su centralizirane mjenjačnice

„Bitcoin“, prva kripto valuta koja je utemeljena na „blockchain“ tehnologiji, stvorena je kao „peer-to-peer“ sistem plaćanja koji svojim korisnicima omogućuje prijenos vrijednosti bez središnjeg autoriteta ili treće strane. Budući da je mreža distribuiranih i uglavnom anonimnih rudara zadužena za obradu transakcija, korisnici su sigurni da problemi poput cenzure, prijevare i drugih nisu mogući.
Mehanizam automatiziranog osiguranja „bitcoina“ putem rudarenja također nastoji ukloniti kontrolu nad izdavanjem novca od banaka u privatnom vlasništvu. Banke u privatnom vlasništvu posuđuju novac vladama uz kamate, stvarajući gospodarstvo temeljeno na dugu, što je, između ostalog, dovelo i do globalnog financijskog pada 2008. godine - događaja koji su i sami potaknuli stvaranje „bitcoina“.

U tom je kontekstu primarni cilj „Bitcoina“ vratiti kontrolu novca svojim vlasnicima, ali redovito povjeravamo svoj „bitcoin“ trećim stranicama. Za većinu ulagača u digitalnu valutu centralizirana razmjena kripto valuta jedno je od najvažnijih i najpopularnijih načina za sklapanje transakcija.
Centralizirane razmjene kripto valuta internetske su platforme koje se koriste za kupnju i prodaju kripto valuta. To su najčešća sredstva koja investitori koriste za kupnju i prodaju kripto valuta.
Neki investitori smatraju da koncept "centralizirane" razmjene je donekle pogrešan, jer se i same digitalne valute vode kao "decentralizirane".
U terminu "centralizirana razmjena kripto valuta", ideja centralizacije odnosi se na korištenje posrednika ili treće strane za pomoć u provođenju transakcija. Kupci i prodavači vjeruju ovom posredniku da upravljaju imovinom. Ovo je uobičajeno u bankovnom setu gdje klijent vjeruje banci da upravlja odnosno drži korisnikov novac. Razlog tom postavljanju je taj što banke nude sigurnost i nadzor koji pojedinac ne može sam izvršiti. U slučaju centralizirane razmjene kripto valuta primjenjuje se isti princip. Osobe koje vrše transakcije ne vjeruju samo

da će razmjena sigurno obaviti transakcije za njih, već također koriste mrežu korisnika u razmjeni kako bi pronašli trgovinske partnere.

3.2 Karakteristike

U slučaju kripto valuta, koje su često pohranjene u digitalnim novčanicima, pojedinac može izgubiti stotine ili tisuće dolara u digitalnoj valuti jednostavno zaboravljajući ključ u novčaniku. Razmjena neće dopustiti da se to dogodi, jer štiti imovinu umjesto ulagača.
Dosta je često da centralizirana razmjena nudi uparivanje kripto valuta. To bi kupcima omogućilo trgovinu, na primjer, „bitcoinom“ za „Etherum“ tokene. Manje razmjena nudi uparivanje valuta / kripto valuta, što bi omogućilo, recimo, zamjenu „bitcoina“ za USD. Međutim, neke od najvećih svjetskih razmjena kripto valuta nude ove parove valuta / kripto valuta. Dio razloga za to je vjerojatno da oni služe kao izravna pristupna točka na tržište kripto valuta.
Budući da su mnogi ulagači relativno novi na području ulaganja u digitalne valute, vjerojatnije je da će se okrenuti tim vrstama razmjena. Primjeri nekih od takvih razmjena uključuju „Coinbase“, „Robinhood“, „Kraken“ i „Gemini“.
Sve vrijeme stalno se pojavljuju nove centralizirane razmjene kripto valuta. Ipak, neće sve biti uspješne i dosta je često da se mjenjačnice povuku. Uspjeh ili neuspjeh mjenjačnice ovisi o velikom broju čimbenika. Međutim, jedna od ključnih komponenti uspjeha je količina trgovanja.
Općenito govoreći, što su više razine trgovanja, niža je brzina kretanja cijena i tržišne manipulacije koje će se vjerojatno odvijati na toj burzi. Brzina kretanja cijena je presudna činjenica. Zbog vremena koje je potrebno da se transakcije izvrše, cijena određenog tokena ili kovanice može se mijenjati u rasponu između inicijalizacije transakcije i vremena kad je transakcija završena. Što je veći volumen trgovine i što se brže može obraditi transakcija, to je manja vjerojatnost da će ta fluktuacija biti problem.
Drugi ključni element uspješne centralizirane burze je sigurnost. Iako niti jedna razmjena nije potpuno imuna na zlonamjerne aktivnosti poput hakova, neki su sigurniji od drugih.
Način na koji razmjena reagira na događaj poput hakiranja nigdje nije definirana. Neke su burze naporno radile kako bi vratile gubitke kupaca, dok su druge u tom pogledu bile manje uspješne. Mnoge burze su se zatvorile upravo kao rezultat ove vrste napada. Za investitore koji žele ući u svijet kripto valute, centralizirana razmjena je još uvijek najčešći način kojim se to radi. Prilikom odabira burze važno je imati na umu mnoštvo čimbenika koji će utjecati na korisničko iskustvo, uključujući i kojim se parovima trguje (ukoliko se trguje), koliko je

veliki volumen trgovanja i sigurnosnim mjerama koje su burze usvojile kako bi zaštitile svoje kupce.

3.3 Prednosti i nedostatci

Centralizacija ima i pozitivne i negativne strane.

Prvo razgovarajmo o prednostima:

jednostavno korištenje: pojedini korisnici ne trebaju raditi ili ulagati nikakve napore. Sve rješava razmjena/burza.

Mogućnost oporavka: u većini slučajeva možete povratiti sredstva od razmjene ako izgubite zaporku. Ako izgubite zaporku, u osnovi većina centraliziranih razmjena ima sigurnosne postupke koji vam omogućuju oporavak zaporke tako što ćete pokazati kopiju putovnice ili pružiti druge podatke za ovjeru.

Brzina: centralizirane razmjene su brze, a trgovine se dovršavaju gotovo odmah.

Likvidnost: oko 99% svih kripto valuta trguje se na centraliziranim burzama.

Prednosti su uglavnom u korisničkom iskustvu i praktičnosti. Zbog toga se većina neprofesionalnih korisnika ne bi trudila trgovati negdje drugdje nego na centraliziranoj burzi (ali u nekim slučajevima ljudi jednostavno ne mogu prepoznati razliku između centralizirane i decentralizirane razmjene). Međutim, mnogo manji podskup tih razmjena je siguran, pouzdan, i pravilno reguliran (većina ljudi u industriji miješa centralizaciju i regulaciju, ako je razmjena centralizirana, ne znači da je pravilno regulirana).

Nedostatci

Ranjivost: svi podaci pohranjuju se na poslužitelje razmjene koji su ranjivi na hakerske napade kao i bilo koji drugi poslužitelj. Samo u 2018. godini kriptirana imovina vrijedna preko milijardu dolara hakirana je i ukradena iz centraliziranih razmjena.

Povjerenje: u potpuno centraliziranom modelu korisnici moraju vjerovati tvrtki u postupanju s novcem i podacima o bankovnim karticama / računima. Uz tako vrijedne podatke, sigurnost korisnika uvijek je glavna briga.

Privatnost: osobni podaci korisnika pohranjuju se i na poslužitelje (servere) tvrtki.

Problemi s infrastrukturom: oslanjanje na poslužitelje i centraliziranu platformu nužno podrazumijeva veliku mogućnost suočavanja s problemima. Na primjer, poslužitelji mogu ponekad biti srušeni, što kažnjava bilo kojeg trgovca koji je želio napraviti neki potez u određeno vrijeme.

Problemi s količinom: 12. studenoga 2018. tijekom velikog naleta korisnika na trgovinskim platformama kripto valuta mnoge su velike burze doživjele kašnjenja i tehničke poteškoće jer se njihovi poslužitelji nisu mogli nositi s velikim priljevom aktivnosti.

Monopolističko okruženje: Samo se nekoliko decentraliziranih mjenjačnica uspjelo natjecati s centraliziranom razmjenom. To je stvorilo tržište na kojem je pregršt centraliziranih razmjena zauzeo većinski udio na tržištu. To je nekim burzama omogućilo da naplaćuju milijune dolara kako bi na burzama mogli biti navedeni njihovi žetoni (tokeni). Neki to vide kao znak da centralizirane razmjene skupljaju previše moći i učinkovito ograničavaju potencijalni rast i usvajanje kripto valuta.
Nedostatak regulacije: Iako se centralizirane razmjene mogu lako regulirati, u većini slučajeva nisu. Znači da nemaju nikakvu pravnu odgovornost prema svojim kupcima.

4 Decentralizirane mjenjačnice

4.1 Što su decentralizirane mjenjačnice?

Kao što smo prije spomenuli, centralizirane burze su najviše korištene jer su jednostavne za korištenje, jednostavno im je pristupiti i pružaju napredne trgovačke funkcionalnosti poput trgovanja maržama među ostalim.
Ali one također predstavljaju sigurnosni rizik za sredstva koja se koriste. Iako su neke razmjene bolje zaštićene od drugih, hakiranja su vrlo česta kad se radi o industriji kripto valuta, a neke poput zloglasnog „Bitfinex“ haka dovele su do toga da tisuće korisnika izgube svoja sredstva.
Neke su burze jednostavno nesposobne ili su zlonamjerne, pa koriste sustave djelomičnih rezervi koji mogu ili dovesti do dobrovoljnog uklanjanja viška instrumenata („Mt. Gox“-ov hack iz lipnja 2011. u kojem je 8.75 milijuna dolara ukradeno od strane hakera), bankrota (propadanje „mybitcoin“-a) ili novog izvlačenja investitora.
Ipak, korisnici trebaju razmjenjivati svoje kripto valute. Postoje određene stavke i usluge koje ne možemo kupiti s „Bitcoin“-om, a da bi nabavili „bitcoin“ ili druge kripto valute, većina ih mora zamijeniti za nacionalnu valutu. Nadalje, neke kripto valute poput „Ether“ (ETH) ili „Monero“ (XMR) imaju posebne značajke ili alate koje „bitcoin“ ne nudi. Pitanje je kako možemo zamijeniti svoje „bitcoine“ bez da ih predamo uslugama koje nudi treća strana? Odgovor leži u decentraliziranim burzama (ili DEX-ovima).

Decentralizirana burza je tržište razmjene koje se ne oslanja na uslugu treće strane za držanje sredstava od mušterija. Umjesto toga, trgovine se odvijaju izravno između korisnika (peer-to-peer) kroz automatizirani postupak. Takav se sustav može uspostaviti stvaranjem „proxy“ tokena (kripto sredstava koji predstavljaju određenu nacionalnu valutu ili kripto valutu) ili sredstava (koja mogu predstavljati dionice u tvrtki, na primjer) ili putem decentraliziranog založnog sustava s više potpisa, a to su samo neka od mogućih rješenja. Ovaj sustav je u suprotnosti s centraliziranim modelom u kojem korisnici polažu svoja sredstva i mjenjačnica odnosno burza izdaje 'IOU' („i owe you“, odnosno dugujem ti) kojim se može slobodno trgovati na platformi. Kad korisnik zatraži da povuče svoja sredstva, ta se sredstva pretvaraju nazad u kripto valutu koju predstavljaju i šalju vlasniku. Budući da korisnici ne trebaju prenijeti svoju imovinu na razmjenu, decentralizirane razmjene smanjuju rizik krađe hakiranjem. Također, one mogu spriječiti manipulaciju cijenama ili lažni volumen trgovanja kroz pranje trgovanja (wash trade), gdje investitor prodaje i kupuje isti financijski instrument kako bi stvorio lažne aktivnosti te prikazao produkt poželjnijim nego što zapravo jest, te su anonimnije od razmjena koje implementiraju pristup KYC („know your customer“ odnosno znajte svog kupca).

4.2 Principi djelovanja

Četiri osnovne funkcije bilo koje razmjene su depoziti kapitala, knjige narudžbi, podudaranje narudžbi i razmjena imovine. Da bi se stvorila potpuno decentralizirana razmjena (DEX), svaka od ovih funkcija mora biti decentralizirana. U većini razmjena decentralizirana je samo razmjena imovine jer su sredstva kripto valute raspoređene na „blockchainu“ koje nijedna središnja jedinica ne kontrolira. Ostale tri funkcije, a posebno depoziti kapitala, obično su centralizirani. Zbog KYC i AML („anti-money laundering“) propisa, razmjene često traže identitet korisnika kako bi se vršio depozit kapitala, stvarajući centralizirano prikupljanje podataka i pohranu osobnih podataka. K tome, centralizirane razmjene daju korisnicima dozvolu za vršenje valutnih transakcija, umjesto stvaranja ekosustava bez dozvole.

Na arhitektonskoj razini, decentralizacija znači da ne postoji centralno upravljani poslužitelj odnosno server, a blokovi mreža su distribuirani. Trenutno, vjerojatno jedina zaista decentralizirana razmjena je „Blocknet BlockDX", jer ostali pokušaji ne decentraliziraju sve četiri funkcije.

Kako se razmjene vrte oko transakcijskih valuta, postoje dva osnovna modela razmjene: valutno centriran i valutno neutralan. Bilo koji od ovih modela može se centralizirati ili decentralizirati, ovisno o tome kako se rukuje sa sve četiri ključne funkcije razmjene.

Mjenjačnice u valutno centriranim modelom izgrađene su na jedinstvenim blockchain platformama, poput „Ethereuma“. Takva valutno centrirana mjenjačnica ograničena je samo na valute za platforme na kojoj je izgrađena, kao što su sredstva ERC20 i drugi ugovori ako se razmjena napravi pomoću „Ethereuma“. To je način na koji se grade tradicionalne razmjene ili burze.

Noviji je model valutno neutralan, koji je konstruiran kako bi povezivao različite izvorne kripto valute, što bi omogućilo korisnicima da se ne moraju pridržavati bilo kojeg određenog valutnog ekosustava. Ovi sustavi omogućuju korisnicima da trguju kripto valutama bez „bitcoina“ koji stoji u osnovi te razmjene, što djeluje kao neka vrsta dodatnog "posrednika" kroz koji više nisu u potpunosti „peer-to-peer“. Primjeri ovih modela uključuju „Bisq“, „altcoin.io“ i „flyp.me“.
Ovi noviji projekti omogućuju pouzdano usklađivanje i rukovanje knjigama naloga, a ne samo razmjenu imovine, na decentralizirani način, što se vrši korištenjem „blockchaina“. Budući da je burza zajednica korisnika, mora postojati način emitiranja i podudaranja naloga. Jedan od načina nepovjerljive trgovine je kroz "atomske razmjene" za usklađivanje narudžbi, ali same atomske razmjene ne mogu stvoriti pouzdano tržište emitiranjem bilo kome na mreži, kao što se to radi od određenog vršnjaka (peer) do drugog. Atomska razmjena je kada se razmjena obavlja u jednoj odnosno u atomskoj operaciji, umjesto da se obavlja kao dvije odvojene transakcije. To se postiže pomoću pametnih ugovora koji djeluju kao „trustless“ depoziti (depoziti kojima moramo slijepo vjerovati, primjer takvog entiteta bi bila banka) koji se drže jedne valute dok drugi korisnik ne pošalje svoju valutu, ili kada se obje valute zajedno otpuštaju.

Idealan model za decentralizirane razmjene bila bi Decentralizirana autonomna organizacija (DAO), transparentna organizacija s kontrolom dioničara, računalno zastupljena organizacija koja je složenija verzija „DApp“-a. Na taj način bi se osigurala puna decentralizacija svih aspekata razmjene, a korisnici bi imali moć odlučivanja umjesto bilo kojeg središnjeg tijela. Dokaz identiteta postaje ne-trivijalni problem s decentraliziranim razmjenama, a posebno DAO razmjenom. Jedno rješenje može se postići decentraliziranim identitetima (DID), koji identifikatore i imena čine suverenima vlastitom entitetu. Postojeći DID-ovi uključuju „NuID“, „Identity.foundation“ i „Sovrin“.

Mnoge pretpostavljene decentralizirane mjenjačnice koriste rukovanje identitetom koje se smatra da je putem prijava u e-poštu - isto kao i većina web-lokacija (Prijava koristeći Gmail). Međutim, nijedna usluga koja zahtijeva e-poštu ili bilo koja imovina koja se prikazuje na centraliziranim poslužiteljima nije u potpunosti decentralizirana.

Stvaranje kripto-razmjene zahtijeva izgradnju četiri temeljne funkcije o kojima smo ranije raspravljali: depoziti kapitala, knjige naloga, usklađivanje naloga i razmjena imovine. Oni uključuju omogućavanje korisnicima da kontroliraju vlastita sredstva, pokretanje mreže na više blokova, ne otkrivanje korisnikovog identiteta i integraciju u postojeće novčanike. Tada se izrađuje sučelje (frontend) koji odgovara korisničkom unosu, poput klika na gumb "kupi", koji je spojen s „Smart Contract“ funkcionalnosti u pozadini (backend).

Gore spomenuto je način na koji su izgrađeni bilo koji „DEX“ sustavi, iako čak i jedna točka centralizacije u sustav uvodi nove ranjivosti. Osim tehničke izrade decentralizirane mjenjačnice, potreban je model upravljanja, koji može biti do tvorca ili korisnika, kao u DAO-u. Nadalje, razmjena mora postići „mrežni učinak“ kako bi postala skalabilna i održala dovoljno visoku likvidnost za ozbiljnu upotrebu.

„BlockDX“ opisuje njihov sustav narudžbe kao "decentralizirani državni stroj", pri čemu je prvi korak predavanje narudžbe, koja će biti poništena ili prihvaćena ovisno o anketama usluga bloka, marketinškim proizvođačima, ovisno dali je emisija primljena i dali primatelj prihvaća ili odbija narudžbu.

Decentralizirane mjenjačnice koriste pametne ugovore za olakšavanje transakcija, poput upotrebe ugovora kao depozita za „peer-to-peer“ transakcije. Ako su sami ugovori vrlo sigurni, tada razmjena ima koristi od kriptografske sigurnosti osnovnog „blockchaina“. Međutim, to često nije slučaj, a pametni ugovori mogu sadržavati mnogo ranjivosti, uključujući prelijevanja, napade stražnjeg ulaza i još mnogo toga. Nadalje, decentralizirane mjenjačnice bi mogle olakšati brže i jeftinije transakcije u odnosu na centraliziranu razmjenu, jer ne postoji autentifikacija od strane trećeg entiteta. Trenutno je to samo teoretski i to tek treba dokazati razmjenom u velikoj mjeri, jer decentralizirane mjenjačnice nisu postigli "mrežni učinak" dostizanja dovoljno korisnika za kritičnu masu.

4.3 Prednosti i nedostatci decentraliziranih mjenjačnica

Kao i centralizirane mjenjačnice/burze, decentralizirane također imaju svoje prednosti i nedostatke. Prvo ćemo spomenuti prednosti decentraliziranih mjenjačnica.

Najočitija korist od decentralizirane razmjene u usporedbi s centraliziranom je njihova "nepovjerljiva" (trustless“) priroda. To znači da korisnik nije obavezan vjerovati u sigurnost ili poštenje razmjene jer korisnik svoja sredstva drži u svom osobnom novčaniku, a ne stavlja ih na čuvanje trećoj strani.

To daje prednost decentraliziranim razmjenama koja je ista kao i kod svake decentralizirane aplikacije koja se vrti oko filozofije izostave posrednika i vraćanja interakcija na vršnjačke (peer-to-peer) modele bez ovlasti koje nemaju središnjih autoriteta. Konkretnije, decentralizacija stvara otpor prema cenzuri, što u slučaju decentralizirane razmjene znači da nijedno središnje tijelo ili autoritet ne može na silu nametnuti propise ili čak zabraniti valute i/ili samu razmjenu.

Bez središnje obrade funkcija razmjene, vlasti poput poreznih i regulatornih tijela nemaju moć nad decentraliziranim mjenjačnicama. Ako bi se decentralizirane mjenjačnice masovno prihvatile i zamijenile centralizirane razmjene, to bi značilo da bi stotine milijardi dolara izbjegle nadležnost tijela za porez i regulaciju.

Zapravo, to bi značilo da bi korisnici platforme, a ne vlasti koje traže iznajmljivanje, kontrolirale sredstva.

Te vlasti koje traže najam već su uložile ogromne napore kako bi zaustavile „blockchain“ revoluciju i održale svoju kontrolu, poput Indije i Kine koje zabranjuje kripto valute. Ostali pokušaji održavanja kontrole uključuju kripto valute koje upravljaju vlade bez velike transparentnosti, poput kripto valute s Venezuele. Nadalje, tradicionalne mega korporacije stvaraju „blockchain“ ekosustave bazirane na dozvolama, poput IBM-a.

Još jedna prednost decentraliziranog modela je privatnost koju on pruža. Korisnici nisu dužni nikome otkriti svoje osobne podatke, osim ako metoda razmjene uključuje bankovne transfere, u kojem slučaju se identitet otkriva samo osobi koja prodaje ili kupuje odnosno od koje se kupuje ili prodaje. Nadalje, usluge posluživanja (hosting) decentraliziranih razmjena distribuira se po svim uključenim blokovima - što znači da ne postoji rizik od zastoja ili rušenja servera.

Budući da korisnici ne trebaju prenijeti svoju imovinu na razmjenu, decentralizirane razmjene smanjuju rizik krađe hakiranjem razmjene. Decentralizirane razmjene također mogu spriječiti manipulaciju cijenama ili lažni volumen trgovanja kroz pranje trgovanja, gdje investitor prodaje i kupuje 1 te isti financijski instrument kako bi stvorio lažne aktivnosti te prikazao produkt poželjnijim nego što zapravo jest. Također, decentralizirane razmjene više su anonimne od razmjena koje implementiraju pristup „znajte svoje kupce“.

Ovo je posebno važno s obzirom na to da mnoge zemlje ograničavaju trgovanje kripto valutama. Tako su dvije najmnogoljudnije države na zemlji, Kina i Indija, zabranile razmjenu kripto valuta, dok su zemlje kao što su Meksiko, Rusija, Saudijska Arabija i Brazil ograničile kripto valute.

Ostale prednosti decentraliziranih mjenjačnica uključuju pojačanu sigurnost. Masovni sigurnosni napadi, poput otprilike 470 milijuna dolara, koji su ukradeni iz „Mt. Gox“, bili su mogući samo zato što su ciljani masivni centralizirani novčanici, što je predstavljalo točku neuspjeha. U decentraliziranim mjenjačnicama svaki korisnik privatno kontrolira vlastita sredstva tako da nema središnje točke napada.

Naravno, kao i uvijek postoji neka iznimka, kako u svemu tako i u ovom slučaju. Postoji mnogo razloga zašto su centralizirane razmjene popularne do te razine na kojoj se nalaze.

Neke decentralizirane razmjene, poput „Bisqa“, od korisnika zahtijevaju da budu prijavljeni u mrežu (online) kako bi narudžba bila uvrštena u listu, i da bi se razmjena mogla obaviti, zahtijevajući od korisnika da izvršavaju određene radnje poput signalizacije da je uplata primljena.

Značajke trgovanja poput trgovanja maržama, posudbi i zaustavnog gubitka trenutno nisu dostupne na mnogim decentraliziranim mjenjačnicama a jer omogućuju samo osnovnu razmjenu valute za unaprijed predodređenu vrijednost.

Najveći nedostatak trenutnih decentraliziranih mjenjačnica je nedostatak funkcionalnosti u odnosu na centralizirane razmjene. Većina decentraliziranih mjenjačnica podržava samo osnovne tržišne funkcije, a ne nude čak ni značajke poput trgovanja maržama i zaustavljanja gubitaka. Tehnologija jednostavno još nije dohvatila onu razinu ambicije koju posjeduje većina decentraliziranih razmjena, iako decentralizirane mjenjačnice poput „BlockDX“-a planiraju podržati dodatne funkcionalnosti. Konačno, zbog ranije spomenutih KYC i AML (know your customer, anti-money laundering) propisa, decentralizirane razmjene ne

podržavaju pretvorbe valuta jer bi to uvelo točku centralizacije. Umjesto toga, korisnici moraju koristiti depozite u kripto valuti.

Bez decentralizirane razmjene, sposobnost ljudi da ulažu u kripto valute podložna je vladama i upravljačkim vlastima, tako da kripto valuta ne postaje nimalo demokratski više nastrojena od tradicionalnog tržišta imovine. Vlade mogu provoditi kontrolu nad centraliziranim razmjenama, a korisnici su podvrgnuti nadležnim tijelima koja u svakom trenutku mogu pratiti i oporezivati korisnike ili zabranjivati valute. Mnoge razmjene tvrde da su decentralizirane, poput „Bancor-a“, ali su doista hibridne, a njihovi centralizirani aspekti predstavljaju ranjivosti. Tako je s „Bancora“ ukradeno oko 23 milijuna dolara, a „Bancor“ je odgovorio pokušajem zamrzavanja ugrađenim u njihov protokol, što je moguće samo s barem djelomično centraliziranom arhitekturom

4.4 Usporedba decentraliziranih mjenjačnica

Trenutno je decentralizirana razmjena još uvijek daleko od postizanja likvidnosti, skalabilnosti i funkcionalnosti potrebnih za masovno usvajanje. Međutim, trenutni pokušaji izgrađeni za tokene temeljene na „Ethereumu“ uključuju „0x protokol“, „Kyber“ mrežu, „EtherDelta“, „BlockDX“ od strane „Blockneta“ i „Radex“. Jedna jedinstvena platforma utemeljena na DAO-u je „IDEX“. Decentralizirane razmjene u ranom razvoju uključuju „Waves“ platformu, „Binance Chain“ i „OasisDEX“, koji je izradio „MakerDAO“. „Protokol 0x“ i mreža „Kyber“ smatraju se ozbiljnim protivnicima za budućnost decentraliziranih razmjena. Oboje koriste svoje interne tokene (KNC za „Kyber“ i ZRX za „0x protokol“). Najveća razlika između njih dvoje je u načinu na koji se vrši podudaranje:

-0x rješava ovaj problem hibridnom metodom gdje se podudaranje naloga vrši izvan „blockchaina“ s posredničkom stranom, a zatim se koristi „blockchain“ za obavljanje razmjene.

-Bilo tko može biti stvaratelj podudaranja izvan lanca time što može voditi knjigu narudžbi.

-Programibilni pametni ugovori omogućavaju proizvođačima tržišta da postave naknade za upravljanje transakcijom.

-„Kyber„ ovaj problem rješava pomoću pametnih ugovora i rezervi.

-Za razliku od 0x, „Kyber“ ne upotrebljava izvan-lančana povezivanja, a umjesto toga, sve rezervne transakcije upravljaju se pomoću „Smart“ ugovora.

-Rezerve pružaju likvidnost, a jedinstvenu rezervu drži „Kyber“.

-Dodatne rezerve mogu biti javne ili privatne.

-Privatne rezerve su privatni vlasnici „bitcoina“ koji odluče ponašati se kao izvor kripto valute za razmjenu i određuju svoje vlastite tečajeve.

-Javne rezerve mogu primati doprinose od strane javnosti, a javne koristi dijeljenjem u dobiti.

Pomoću „EtherDelta“, usklađivanjem knjiga naloga (jedna od četiri ključne funkcije) upravljaju centralizirani poslužitelji „EtherDelta“. Zbog ove centralizacije, nalozi u knjizi naloga mogu se cenzurirati, što znači da je filozofija otpora cenzure postala nepobitna, ali sigurnosna korist kontrole vlastitih sredstava ostaje. „Projekt 0x“ sličan je „EtherDelta“, s tim što je ključna razlika što 0x pruža višenacionalni lanac, gdje mnoge razmjene mogu surađivati u stvaranju veće narudžbe koristeći prednost zajedničkog fonda likvidnosti. 0x ima iste brige za centralizaciju kao „EtherDelta“, pri čemu centralizirani poslužitelji pojedinačnih razmjena obrađuju usklađivanje naloga.

Platforma „IDEX“ nalazi se u vlastitoj kategoriji, budući da djeluje na vrhu“ Aurora DAO“ (Decentralizirana autonomna organizacija), nadahnuta besplatnim bankarstvom:

Razvili su višekutnu strukturu kroz „DAO“, s „IDXM“, „AURA“ i „Borealnim“ tokenima na kojima se „IDXM“ koristi kao žeton članarine.

„AURA“ je tok za označavanje „Snowglobe“-a koji podržava protokol više razmjena.

Proizvođači tržišta nagrađeni su „AURA“-om dok kupci plaćaju naknade za „*gas*“.

Aspekt decentraliziranog kapitala „IDEX“-a korisnicima pruža besplatno bankarstvo i kredite putem „Boreals“-a.

„Snowglobe“, koji koristi gore navedeni tok „AURA“, je protokol koji stvara sekundarnu mrežu dječjih lanaca koji povezuju razmjene radi poboljšanja likvidnosti.

„IDEX“ nije u potpunosti decentraliziran, jer je sam „IDEX“ jedini autoritet koji može podnijeti potpisane ugovore „Ethereumu“.

To osigurava brzinu i neučinkovitost centraliziranih razmjena, formirajući hibridni model.

„OasisDEX“ je konkurent „IDEX“-u, jer ga je izradio „MakerDAO“ i namijenjen je sličnim razinama decentraliziranih interakcija uz decentralizirano upravljanje. Međutim, „OasisDEX„ je samo u alfa fazi te se na njemu ne primjećuju nikakve nove značajke ili napredak u razvoju.

„Oasis“ nema za cilj imati istu tokensku podršku kao „IDEX“, ali namijenjen je za imovinu u registru „Maker“ (trenutno „MKR“, „DAI“ i „ETH“)

„Radex“ je sličan „IDEX“-u po načinu na koji proizvođači na tržištu zarađuju rabat za likvidnost koju pružaju. Ovo je jedinstven prijedlog vrijednosti koju je „Radex“ pružio dok se „IDEX“ nije pojavio, a sada je „IDEX“ razvijenija i decentralizirana platforma.

Upotreba „Radexa“ zahtijeva korištenje centraliziranog dodatka „Saturn novčanika“ u web-pregledniku.

Rukovanje knjigom narudžbi nije idealno u „Radexu“, jer se ne pohranjuje na decentralizirani način, već se umjesto toga dinamički obnavlja čitanjem događaja koje „Radex“ stvara.

Uskoro će izaći „Binance Chain“, za koji se tvrdi da pruža decentralizirane razmjene. Jednom kada „Binance Chain“ postane aktivan, „Binance Coin (BNB)“ bit će zamijenjen novim „bitcoinom“ na temelju „Binance blockchaina“ u omjeru 1: 1. Budući da su planovi objavljeni u ožujku 2018., nije bilo nikakvih ažuriranja, i bilo je malo vjerojatno da je „Binance Chain“ u potpunosti decentraliziran, jer će depoziti kapitala biti izvršeni u „Binanceu“, a sam „Binance“ neće se pretvoriti u decentralizirani model. Nadalje, kako „Binance“ prakticira zamrzavanje sredstava radi usklađivanja s propisima i sprečavanja krađe, to znači da postoji centralizirana kontrola sredstava.

Koliko znamo, „BlockDX“ je najdecentraliziranija platforma jer su sve četiri funkcije razmjene decentralizirane. Daljnje pogodnosti koje pruža uključuju partnerstvo s 0x koje omogućava interoperabilnost s „Ethereum“ tokenima. Za „peer-to-peer“ trgovinu bez središnjeg entiteta, „Blocknet“ koristi atomske razmjene, o kojima se raspravljalo ranije, u tehnologiji nazvanoj „XChat“. „Blocknet“ također stvara inter-lanac prekrivanja pomoću „XBridge“-a, koji pruža vršnjačku (peer-to-peer) mrežu zasnovanu na „DHT“-u. Važno je da „BlockDX“ dolazi pomoću decentraliziranog „API“ (application programming interface) na koji se može povezati preko „localhost“-a bez dopuštenja, te tako omogućuje istinsko decentralizirano trgovanje.

Razvoj tolikog broja „DEX“ i protokola koji obuhvaćaju decentralizirane mjenjačnice jasno pokazuje da su pioniri kripto sfere shvatili da će, kripto valute zahtijevati decentralizirane „peer-to-peer“ razmjene otporne na cenzuru. Međutim, razmjenu kripto valuta u nacionalne valute poput USD, EUR itd. mnogo je teže decentralizirati jer su sami sustavi poput američkog dolara, centralizirani. I zato se na razmjenama kao što su „LocalBitcoins“ i „Bisq“ vidi mali volumen trgovanja. Zanimljivo je da se i ovaj problem može riješiti postojanjem kripto valuta koje su vezane za valute odnosno parirane s nekom nacionalnom valutom. Klasičan primjer takve kripto valute je „Tether“. Nažalost, „Tether“ je nedavno optužen za tržišne manipulacije jer nisu imali američke rezerve razmjerno stvarnom „Tether“-u (USDT) koji su izdali. Unatoč tome, sve više se pojavljuju neki od valutnih projekata koji osiguravaju prijeko potrebnu likvidnost, korektnost i interakciju potrebnu na tržištu.

4.5 Razlika između centraliziranih i decentraliziranih razmjena/burzi

Centralizirane razmjene mogu se koristiti za vođenje trgovanja od valuta-u-kripto valutu (ili obrnuto). Tako također se mogu koristiti za trgovanje između dvije različite kripto valute. Iako se može činiti da obuhvaća sve potencijalne vrste transakcija, još uvijek postoji tržište za drugu vrstu razmjene kripto valuta.

Centralizirana mjenjačnica radi na principima koji su vrlo slični današnjim bankama:

-Svaka posjeduje svog vlasnika.

-Sigurne su (donekle).

-Princip rada slijedi pravila i propise.

Valja spomenuti i koncept „Proof of Keys“ koji je iznio poznati „bitcoin“ savjetnik, Trace Mayer. Taj koncept predlaže da svaki vlasnik „bitcoina“ koji je pohranio na centraliziranu razmjenu treba prenijeti u svoj novčanik.

Ukoliko to ne naprave, kovanice (coins) odnosno sredstva i imovine koje pohranjuje usluga treće strane, zapravo nisu korisnikove.

S tim na umu, treba znati rizike povezane s centraliziranom razmjenom:

-Mogu se lako izvršiti hakerski napadi, kroz koja bi se sredstva mogla izgubiti.

-Cijela mjenjačnica/burza može nestati preko noći.

Međutim, ako se ne bi koristio „Proof of Keys“ a da bi korisnik postao pravi vlasnik svoje imovine, decentralizirana razmjena kripto valuta dolazi kao druga opcija.

Prije nekoliko godina decentralizirana razmjena kripto valuta bila je u problemima i ljudi su gubili sredstva čak i radeći male pogreške. Danas, decentralizirane razmjene su mnogo napredovale, te iako su još neistražene i njihov potencijal nije do kraja iskorišten, one postaju sve veća konkurencija centraliziranim razmjenama.

Razlog k tome je:

-Poboljšana privatnost zbog nepostojanja zahtjeva za registracijom ili „KYC“ (know your customer) postupka.

-Nije potrebno polaganje ili podizanje novca. Sve transakcije koje se događaju između vršnjaka vrše se programski sigurnim pametnim ugovorima.

-Nema niti jedne točke koja može uzrokovati kvar, kontrolu ili regulacije.

-Možda najvažnije, ne postoji treća strana

Ukratko, decentralizirana razmjena je razmjena koja omogućava korisnicima kontrolu nad svojim kripto fondovima, te ova razmjena ne uključuje miješanje neke treće strane!

5 Uniswap protokol

5.1 Što je uniswap protokol?

„Uniswap“ je protokol temeljen na „Ethereumu“ koji je osmišljen kako bi olakšao automatsku razmjenu digitalnih sredstava između „ETH“ i „ERC20“ tokena.
„Uniswap“ je u potpunosti smješten „na lancu“, a kako bi pojedinci mogu koristiti protokol sve što je potrebno je da imaju instaliran „MetaMask“. „MetaMask“ je aplikacija dizajnirana kao „most“ koji omogućuje da se posjeti distribuirani web u pregledniku. Omogućuje da u pregledniku se pokrene „Ethereum dApps“ bez pokretanja čitavog „Ethereum“ bloka. „MetaMask“ uključuje sigurni trezor identiteta, pruža korisničko sučelje za upravljanje vašim identitetima na različitim web lokacijama i potpisivanje „blockchain“ transakcija. „Uniswap„ protokol nudi sučelje za razmjenu „ERC20“ tokena na „Ethereumu“. Taj protokol omogućuje mnogo bržu i efikasnu razmjenu tako što izbacuje nepotrebne oblike iznuđivanja članarine i posrednika gdje je prioritet fokusiran na stvaranje kompromisa, sigurnost, otpor ka cenzuri te decentralizaciju. „Uniswap“ protokol je otvorenog koda (open source) te se bilježi i funkcionira kao javno dobro. U njemu ne postoji token ili platforma niti se za iste izdaje naknada. Za razliku od ostalih, ono ne nudi nikakve pogodnosti programerima ili ranim investitorima. Popis svih tokena je otvoren, javno dostupan i besplatan, sve funkcije koje koriste pametni ugovori su javne, a sve nadogradnje (plug-in) su omogućene.
Jedna od prednosti korištenja „Uniswap“ protokola za razmjenu digitalnih sredstava je činjenica da je vrlo učinkovit kad je u pitanju plin (gas). Trošak „*gas-a*“ nastao prilikom obavljanja razmjene na „Uniswapu“ vidljivo je jeftiniji od alternativnih decentraliziranih razmjena. Kao što referentna vrijednost za „*gas*“ pokazuje u nastavku: „ETH“ za „ERC20“, „ERC20“ za „ETH“ i „ERC20“ za „ERC20“ zamjene su značajno jeftinije od razmjene poput „Bancor“, „EtherDelta“ itd.

Parametar povezan s potrošnjom „*gas-a*“ za slanje transakcije je „Gas Price“ (cijena plina). Taj se iznos obično označava u gwei-u (10^9 wei) i ne utječe na izvršenje transakcije ili interakciju pametnog ugovora, već na brzinu kojom se transakcija dodaje u blok. Na dole prikazanoj slici imamo prikazanu potrošnju „*gas-a*“ po mjenjačnicama, te vidimo da je „Uniswap“ puno efikasniji po pitanju potrošnje „*gas-a*“ od mjenjačnica.

Exchange	Uniswap	EtherDelta	Bancor	Radar Relay (0x)	IDEX	Airswap
ETH to ERC20	46,000	108,000	440,000	113,000	143,000	90,000
ERC20 to ETH	60,000	93,000	403,000	113,000	143,000	120,000
ERC20 to ERC20	88,000	X	538,000	113,000	X	X

Slika 3 Efikasnost „gas-a“ po burzama

Efikasnost „*gas-a*“ samo je jedna od prednosti „Uniswap“ protokola, a neke od mnogih drugih prednosti uključuju:

-„Uniswap“ je decentraliziran, tako da se za svoj rad ne oslanja na treće strane te je slobodno dostupan svima koji se žele spojiti na protokol.

-Troškovi obavljanja razmjene na „Uniswapu“ relativno su jeftini u usporedbi s drugim digitalnim razmjenama imovine.

-„Uniswap“ omogućava bilo kojem korisniku da stvori ugovor o razmjeni za bilo koji dani „ERC20“ token. Međutim, „Uniswap“ također dolazi sa svojim ograničenjima:

„Uniswap“ se oslanja na arbitražno trgovanje kako bi kontrolirao tečajne cijene tokena na protokolu. To znači da se „Uniswap“ oslanja na postojanje drugih digitalnih razmjena imovine kako bi se tečajevi održali uravnoteženima.

„Uniswap“ je još uvijek jako eksperimentalan, potrebno je više razvoja na protokolu kako bi se vidjelo koliko je učinkovit u utjelovljenju digitalne razmjene imovine.

„Uniswap“ se sastoji od dvije vrste pametnih ugovora:

-Ugovor o razmjeni

-Tvornički ugovor

Ti su ugovori napisani na programskom jeziku „Vyper“ koji se koristi za programiranje pametnih ugovora i glavni su temelj za funkcioniranje „Uniswap“ protokola. Ugovor o razmjeni podržava točno jedan „ERC20“, token a svaki ugovor o razmjeni ima pričuvu „ETH“ i njihov podržani „ERC20“ token. To znači da se razmjene izvršene na određenom ugovoru o razmjeni se temelje na relativnoj opskrbi „ETH“ i „ERC20„ tokena koji se nalaze u ugovoru. Trgovine koje se izvršavaju na ugovoru o razmjeni također omogućavaju izravne „ERC20“ u „ERC20“ razmjene koristeći „ETH“ kao posrednika.

Tvornički se ugovor može koristiti za stvaranje novog ugovora o razmjeni, tako da svaki token „ERC20“ koji još nema ugovor o razmjeni može stvoriti neki korištenjem tvorničkog ugovora. Funkcija 'createExchange ()' omogućuje bilo kojem korisniku na „Ethereumu“ da razmjeni ugovor o razmjeni koristeći tvornički ugovor. Važno je napomenuti da tvornički ugovor služi kao registar ugovora o razmjeni „Uniswapa“, što znači da se tvornički ugovor može koristiti za traženje svih tokena i razmjenu adresa koje su dodane u sustav. Tvornički ugovor ne vrši provjeru znaka kad se pokrene ugovor o razmjeni (osim ograničenja jednog ugovora razmjena po žetonu), stoga bi korisnici trebali komunicirati samo s ugovorima o razmjeni u koje imaju puno povjerenje.

„Uniswap“ se sastoji od niza ugovora o razmjeni „ETH“-„ERC20“. Postoji točno jedan ugovor o razmjeni po „ERC20“ tokenu. Ako token još nema mjenjačnicu/burzu, može ga kreirati svatko tko koristi „Uniswap“ tvornički ugovor. Tvornica služi kao javni registar i koristi se za pretraživanje svih tokena i adresa razmjena dodanih u sustav. Svaka burza sadrži rezerve i „ETH“-a i „ERC20“ tokena koji je s njim uparen odnosno koji mu pripada. Svatko može postati davatelj likvidnosti na razmjeni i doprinijeti njezinim rezervama. Takav pristup je drugačiji od kupovine ili prodaje; on zahtijeva polaganje „ETH“-a i ekvivalentne vrijednosti njemu odgovarajućeg „ERC20“ tokena. Likvidnost se nakuplja (pools) kod svih pružatelja usluga, a interni "pool token" (ERC20) koristi se za praćenje relativnog doprinosa svakog pružatelja usluga. „Pool tokeni“ se kuju odnosno stvaraju onda kad se likvidnost pohrani u sustav i mogu se u bilo kojem trenutku istrošiti odnosno spaliti kako bi se povukao proporcionalan udio rezervi. Ugovori o razmjeni automatski su tvorci tržišta između parova „ETH“-„ERC20“. Trgovci mogu prelaziti s jednog na drugi token u bilo kojem trenu tako što bi dodali u rezerve likvidnosti jednog i povukli iz rezerve drugog. Budući da je „ETH“ zajednički par za sve „ERC20“ razmjene, može se koristiti kao jedan tip posrednika koji omogućava izravne „ERC20“-„ERC20“ razmjene u jednoj transakciji. Korisnici mogu odrediti adresu primatelja ako žele primiti kupljene tokene na drugoj adresi od one koja se koristi za obavljanje transakcije.

5.2 Likvidnost

Dizajn arhitekture „Uniswap“ protokola razlikuje se od modela pronađenog u okviru tradicionalnih razmjena digitalnih dobara. Većina tradicionalnih razmjena održava knjigu narudžbi i koriste je za usklađivanje kupaca i prodavača određene imovine. „Uniswap“ s

druge strane, koristi rezerve likvidnosti za olakšavanje razmjene digitalne imovine u svom protokolu.

Rezerve u ugovorima o zamjeni se osiguravaju pomoću mreža pružatelja likvidnosti. Ovi pružatelji likvidnosti polažu ekvivalentnu vrijednost „ETH“ i „ERC20“ tokena u odgovarajući ugovor o razmjeni tokena „ERC20“. Prvi davatelj likvidnosti koji je likvidnost dodao na ugovor o razmjeni početno će postaviti tečaj između „ETH“ i pridruženog „ERC20“ tokena tečajnog ugovora. Pružatelj likvidnosti to čini tako što polaže ono za što vjeruje da je ekvivalentna vrijednost između „ETH“ i tokena „ERC20“ ugovora o razmjeni. Ako vrijednost postavljena od pružatelja likvidnosti nije u skladu s širim tržištem, tada će arbitražni trgovci vrijednost između „ETH“ i tokena „ERC20“ dovesti do tečaja za koji tržište smatra ispravnim. Svi naknadni davatelji likvidnosti nakon toga deponirati će likvidnost po tečaju u trenutku njihovog depozita.

„Uniswap“ koristi i takozvane „žetone likvidnosti“, koji su sami po sebi „ERC20“ kompatibilni. Ovi se tokeni mogu smatrati reprezentacijom doprinosa pružatelja likvidnosti prema ugovoru o razmjeni. Obrazloženje koje stoji iza limita „Uniswapa“ za razmjenu ugovora po tokenu je poticanje pružatelja likvidnosti da svoje likvidnosti udruže u jednu rezervu. „Uniswap“ će umanjiti znakove likvidnosti kako bi se pratio relativni udio ukupnih rezervi koje je doprinio svaki davatelj likvidnosti. Davatelji likvidnosti mogu upaliti svoje žetone likvidnosti u trenutku po vlastitom izboru, tako da mogu povući svoj proporcionalni udio „ETH“ i „ERC20“ tokena iz ugovora o razmjeni.

Davatelji likvidnosti također mogu odlučiti prodati ili prenijeti svoje žetone likvidnosti između računa bez potrebe za uklanjanjem likvidnosti iz ugovora o razmjeni. Međutim, žetone likvidnosti „Uniswap“ strogo su specifične za ugovor o razmjeni. Ne postoji niti jedan osnovni izvorni digitalni element koji je povezan s protokolom „Uniswap“. Davatelji likvidnosti također mogu deponirati likvidnost u ugovor o razmjeni pozivom na funkciju „addLiquidity ()“. U zamjenu za opskrbu likvidnošću, davatelji likvidnosti dobit će udio naknada za transakcije kada se trgovina izvrši.

„Uniswap“ koristi formulu „konstantnog proizvoda“ za izradu tržišta koja postavlja tečaj utemeljen na relativnoj veličini rezervi „ETH“ i „ERC20“ i iznosu s kojim nadolazeća razmjena pomiče ovaj omjer. Prodaja „ETH“ za „ERC20“ tokene povećava veličinu rezerve „ETH“ i smanjuje veličinu rezerve „ERC20“. Ovo pomiče omjer rezervi, povećavajući cijenu tokena „ERC20“ u odnosu na „ETH“ za sljedeće transakcije. Što je veća razmjena u odnosu na ukupnu veličinu rezervi, to će se više dogoditi „proklizavanje“ cijena, odnosno što je veća razmjena to će cijena na cijeloj burzi više se promijeniti. Sve u svemu to bi značilo da ugovori

o razmjeni koriste otvoreno financijsko tržište kako bi odlučili o veličini relativne vrijednosti para „ETH“ i „ERC20“ te to koriste kao strategiju za stvaranje tržišta.
Mala naknada (0,3%) za davatelja likvidnosti se vadi iz svake razmjene i dodaje se u rezerve. Iako se omjer rezervi „ETH-ERC20“ stalno mijenja, naknade osiguravaju da se ukupna kombinirana veličina rezervi povećava sa svakom trgovinom. To funkcionira kao isplata pružateljima likvidnosti koja se prikuplja kada spaljuju „pool tokene“ kako bi povukli svoj dio ukupnih rezervi. Zajamčene mogućnosti arbitraže zbog oscilacija cijena trebale bi gurnuti stalan protok transakcija kroz sustav i povećati iznos generiranog prihoda od naknada.
Budući da je „Uniswap“ u potpunosti „na lancu“, cijene se mogu mijenjati između momenta kad je transakcija potpisana odnosno obavljena i kad je upisana u blok. Trgovci mogu ograničiti oscilacije cijena određivanjem minimalnog iznosa kupljenog na nalogu za prodaju ili maksimalnog iznosa prodanog na kupovnom nalogu te tako stvoriti nalog koji djeluje kao limitni nalog i koji će se automatski poništiti ako nije ispunjen. Također je moguće postaviti rokove transakcija koji će otkazati narudžbe ako se ne izvrše dovoljno brzo.
Razlog zbog kojeg se samo jedna razmjena po tokenu može registrirati u tvornici je kako bi potaknula pružatelje usluga da likvidnost objedine u jednu rezervu. Međutim, „Uniswap“ ima ugrađenu podršku za „ERC20-u-ERC20“ obrt tako što koristi javne „bazene“ (pool) iz tvornice s jedne strane transakcije i prilagođeni, korisnički „bazen“ s druge strane. Prilagođeni bazeni mogli bi imati upravitelje fondova, koristiti alternativne mehanizme određivanja cijena, ukloniti naknade pružatelja likvidnosti i još mnogo toga. Oni samo trebaju implementirati „Uniswap“ sučelje i prihvatiti ETH kao posredničku imovinu. Prilagođeni „bazeni„ nemaju ista sigurnosna svojstva kao javni. Korisnicima se preporučuje da jedinu interakciju ostvaruju samo s revidiranim pametnim ugovorima otvorenog koda.
Teško je stvoriti decentralizirane pametne ugovore otporne na cenzuru.

5.3 Trgovanje na uniswapu

5.3.1 ETH u ERC20

Jedna vrsta razmjene koja se može obaviti na „Uniswap“ protokolu je razmjena „ETH“ za bilo koji dati „ERC20“ token. Kao što je već spomenuto, tečaj između „ETH“ i tokena „ERC20“ temelji se na relativnoj veličini bazena likvidnosti već spomenute imovine u sklopu ugovora o razmjeni. Tečaj je podupiran formulom „Uniswapa“:
ETH * token pool = invarijant

Ovaj se invarijant održava konstantnim tijekom izvršavanja bilo kakve trgovine na Uniswap protokolu. Nadalje, invarijant će se promijeniti samo kad se likvidnost doda ili ukloni iz ugovora o razmjeni na kojem se obavlja trgovina. Kako bi se olakšalo shvaćanje načina na koji funkcionira razmjena, sada ćemo na primjeru prikazati proces.

Radi primjera reći ćemo da određena osoba, imena Ivan želi pokrenuti trgovinu na način da zamijeni svoj 1 „ETH“ za token „ERC20“, „BAT“ („basic attention token“, token pažnje). Ivan će izvršiti ovu trgovinu pomoću postojećeg ugovora o razmjeni na „Uniswap“ protokolu. Davatelji likvidnosti su deponirali iznos „ETH“ i „BAT“ u ugovor o razmjeni, koji u ovom primjeru iznosi 10 „ETH“ i 500 „BAT“. Osnovna invariantna formula je postavljena na:

„ETH“ bazen * „BAT“ pool = invariant.

„ETH“ bazen = 10

„OMG“ bazen = 500

Invariantno = 10 * 500 = 5.000

Ivan će započeti svoju trgovinu slanjem 1 „ETH“ u bazen „ETH“ u ugovoru o razmjeni, nakon čega se povlači 0,3% naknade davatelja likvidnosti. Preostalih 0.997 „ETH“ dodaje se u „ETH“ bazen. Invariant se zatim dijeli s novom količinom „ETH“ u bazenu likvidnosti za potrebe određivanja nove veličine „BAT“ bazena. Preostali „BAT“ tokeni tada se šalju kupcu, što je u ovom slučaju Ivan.

Ivan šalje: 1 „ETH“

Naknada = 0,003 „ETH“

„ETH“ bazen = 10 + (1 - 0,003) = 10,997

„BAT“ bazen = 5000 / 10.997 = 454.67

Ivan prima: 500 - 454,67 = 45,33 „BAT“

Naknada za pružanje likvidnosti, koja je ranije bila povučena kada je Ivan pokrenuo transakciju, sada se dodaje u fond za likvidnost. To funkcionira kao isplata pružateljima likvidnosti, koja se može prikupiti kada ti davatelji uklone svoj doprinos likvidnosti s tržišta. Budući da se naknada dodaje nakon izračuna cijene, invarijant se postupno povećava sa svakom trgovinom koja se obavlja na ugovoru o razmjeni, čineći akt ulaganja likvidnosti u razmjenski ugovor profitabilan za pružatelje likvidnosti.

„ETH“ bazen = 10,997 + 0,003 = 11

„BAT“ bazen = 454,67

novi invariant = 5,001,37

U toj je trgovini Ivan primio stopu od 45,33 „BAT“ / „ETH“.

1 „ETH“ unutra

45.33 „BAT“ van

Stopa = 45,33 „BAT“ / „ETH“

5.3.2 ERC20 u ERC20

Druga vrsta trgovine koja se može obaviti na „Uniswap“ je razmjena jedne vrste „ERC20“ tokena za drugu vrstu „ERC20“ tokena. Budući da se „ETH“ koristi kao zajednički par za sve „ERC20“ tokene, „Uniswap“ koristi „ETH“ kao posredničku imovinu za izravnu „ERC20“ do „ERC20“ razmjenu. „Uniswap“ omogućava, na primjer, pretvaranje iz „BAT“ u „ETH“ na jednom ugovoru o razmjeni, a potom iz „ETH“ u „OMG“ u drugi ugovor o razmjeni, a sve u okviru jedne pojedinačne transakcije.

Ova formula funkcionira slično uobičajenom tržištu, što više žetona kupite to je viši granični tečaj koji bi morali platiti za svaku dodatnu jedinicu kupljenog tokena.

5.3.3 Trgovanje „uniswapom“ i arbitražno trgovanje

Važno je napomenuti da, iako je „Uniswap“ decentralizirana digitalna razmjena imovine „na lancu“, ne postoji kako bi zamijenio centralizirane razmjene. U slučaju da mehanizam razmjene na „Uniswapu“ se pokvari, mora postojati mehanizam pomoću kojeg se to može ispraviti. Ovaj mehanizam postoji u obliku arbitražnog trgovanja.

Arbitražno trgovanje je strategija koja se najbolje može shvatiti kao trgovac koji iskorištava razlike u cijeni koje postoje između dva tržišta. U slučaju kripto valute, ta razlika u cijenama može se naći u razlikama u cijeni digitalne imovine između 2 mjenjačnice kripto valuta. Ako je trgovac identificirao priliku za arbitražno trgovanje, tada bi kupio digitalnu imovinu u jednoj razmjeni, a zatim je prodao na drugoj mjenjačnici kripto valuta. Trgovina arbitražom presudna je za funkcioniranje „Uniswapa“ jer trgovci mogu iskoristiti alternativne tečajeve koji postoje u drugim burzama kripto valuta kako bi ispravili bilo kakve promjene u cijenama koje se mogu pojaviti na „Uniswapu“.

Efikasnost „*gas-a*“ samo je jedna od prednosti „Uniswap“ protokola, a više prednosti uključuju:

„Uniswap“ je decentraliziran, tako da se za svoj rad ne oslanja na treće strane. Nadalje, „Uniswap“ je slobodno dostupan svima koji se žele spojiti na protokol. Troškovi obavljanja trgovine na „Uniswap“-u relativno su jeftini u usporedbi s drugim digitalnim razmjenama

imovine. „Uniswap“ omogućava bilo kojem korisniku da stvori ugovor o razmjeni za bilo koji dani „ERC20“ token.
Međutim, „Uniswap“ dolazi sa svojim ograničenjima:
„Uniswap“ se oslanja na arbitražno trgovanje kako bi kontrolirao tečajne cijene tokena na protokolu. To znači da se „Uniswap“ oslanja na postojanje drugih digitalnih razmjena imovine kako bi se tečajevi održali uravnoteženima.
„Uniswap“ je još uvijek jako eksperimentalan, potrebno je više razvoja na protokolu kako bi se vidjelo koliko je učinkovit u olakšanju digitalne razmjene imovine.

Zaključak

Kako svijetu kripto valuta treba vremena da bi sazrio i razvio se u istaknuti ekosustav, kripto valute moraju zauzeti glavnu pozornicu! U posljednje vrijeme „coin“ i žetoni su glavni oblik kojim korisnici mogu ulagati u određene investicije, što nam omogućava pristup trgovačkim platformama koje poprimaju sve veći oblik u industriji! Postoji mnogo „startupa“ koji se kreću većinom mjenjačnica.
Decentralizirane odnosno „trustless“ razmjene itekako su potrebne za sigurnu trgovinu digitalnim valutama: centralizirane razmjene su po svojoj naravi vrlo osjetljive na ljudske pogreške, pohlepu i hakerske rizike. Mreža Ethereum je primjer pomoću koje je izgrađeno mnoštvo „DEX“ sustava, s različitim arhitekturama. Međutim, potpuno „trustless“ razmjene u Ethereum mreži gube od strane centraliziranih razmjena po pitanju funkcionalnosti.
Izbor najbolje decentralizirane razmjene ili centralizirane razmjene u potpunosti će ovisiti o korisniku! Ukoliko se koristi decentralizirana razmjena, za zaštitu vlastite imovine uvijek je potrebna viša razina odgovornosti. Kod centralizirane je lakše pristupit sredstvima i obavljati razmjene, ali isto tako imaju veći sigurnosni rizik. Uniswap predstavlja značajan korak u omogućavanju digitalne razmjene imovine u ekosustavu, čineći postupak razmjene imovine znatno učinkovitijim. Uniswap je još uvijek pretežno u razvoju, no bit će zanimljivo vidjeti kako se ovaj novi protokol razvija u budućnosti.
Decentralizacija nam donosi novi svijet „trustless“ okruženja, ali korisnik se mora pouzdati u sebe i sam bit odgovoran za svoje postupke!

Literatura

https://www.bug.hr/tehnologije/sto-je-u-stvari-blockchain-i-kako-radi-3011

https://blockgeeks.com/guides/ethereum/

https://blockgeeks.com/guides/decentralized-exchanges/

https://hackernoon.com/centralized-vs-decentralized-cryptocurrency-exchanges-explained-simply-639411ecb452

https://docs.uniswap.io/

https://www.mycryptopedia.com/what-is-uniswap-a-detailed-beginners-guide/

httpshttps://www.netokracija.com/sto-je-blockchain-132284://www.bug.hr/tehnologije/sto-je-u-stvari-blockchain-i-kako-radi-3011

https://www.brookings.edu/blog/techtank/2015/01/13/the-blockchain-what-it-is-and-why-it-matters/

https://www.ictbusiness.info/kolumne/sto-je-blockchain-koje-su-njegove-prednosti-i-mane

https://hackernoon.com/using-a-decentralized-exchange-in-2019-is-much-easier-than-it-was-two-years-ago-eb936039ea2f

https://www.cryptocompare.com/exchanges/guides/what-is-a-decentralized-exchange/

https://www.investopedia.com/tech/what-are-centralized-cryptocurrency-exchanges/

https://hacken.io/research/education/decentralized-and-centralized-exchanges-advantages-vs-disadvantages-aa9a27da4584/

https://coinsutra.com/decentralized-vs-centralized-crypto-exchange/

https://coincassogroup.com/centralized-vs-decentralized-cryptocurrency-exchanges-comparison/